Some New Non-binary Quantum Codes from One-generator Quasi-cyclic Codes

Tushar Bag, Hai Q Dinh, Daniel Panario

Some New Non-binary Quantum Codes from One-generator Quasi-cyclic Codes *

Tushar Bag[1], Hai Q. Dinh[2] , Daniel Panario[3]

1. Univ Lyon, Inria, ENS Lyon, UCBL, LIP, 69342 Lyon Cedex 07, France
2. Kent State University, Warren, OH 44483, USA
3. School of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada.

December 17, 2024

Abstract

This article studies one-generator and two-generator quasi-cyclic codes over finite fields. We present two versions of necessary and sufficient conditions for the symplectic self-orthogonality of one-generator quasi-cyclic codes, using both matrix and polynomial approaches. We provide two versions of necessary and sufficient conditions for two-generator quasi-cyclic codes for symplectic self-orthogonality and the symplectic dual-containing condition. Additionally, using these necessary and sufficient conditions, we construct new quantum codes with record-breaking parameters that improve upon current records.

Keywords: Quasi-cyclic codes (QCs), quantum error-correcting codes (QECCs).
Mathematics Subject Classifications(2010): 94B05, 94B15, 94B60.

1 Introduction

Quasi-cyclic (QC) codes are a prominent class of linear error-correcting codes. They possess a well-developed algebraic structure that generalizes the concept of cyclic codes. This generalization allows for greater flexibility in code design, enabling the construction of asymptotically good codes that approach the modified Gilbert-Varshamov bound [14, 18]. The study of QC codes has yielded numerous record-breaking linear codes, particularly over small finite fields. Several key contributions have been made to the understanding of QC codes. Research by Conan et al. [9] studied into the structural attributes of quasi-cyclic codes, providing both an enumeration of these codes and a characterization of their duals. Another study by Seguin [24] examined the properties of a specific class of one-generator QC codes. Ling and Solé research deeply into the algebraic structure of QC codes across a series of articles [17, 19, 20, 21]. Lally et al. [16] explored the structure and duals of arbitrary QC codes, with a particular focus on self-dual QC codes with an index of 2. Aydin et al. [4] investigated the structure of 1-generator quasi-twisted codes and constructed new linear codes.

Quantum error-correcting codes (QECCs) are essential for protecting quantum information from decoherence and quantum noise, playing a significant role in both quantum computing and communication. Quantum computers are theorized to solve problems significantly faster than classical computers. However, mitigating errors caused by decoherence and noise remains a critical challenge. Here, QECCs emerge as a powerful tool, safeguarding quantum information in both communication and computation. The concept of QECCs was first proposed in [7, 25, 26]. The Calderbank-Shor-Steane (CSS) structure [8] has served as the foundation for a substantial portion of recent research on QECCs. Construction of non-binary quantum codes techniques is explored in [2, 3, 15].

Symplectic self-orthogonal quasi-cyclic (QC) codes have not only proven themselves to be an excellent family for constructing new linear codes, but they have also become pivotal in constructing numerous

*Email: tushar.bag@ens-lyon.fr (T. Bag) [corresponding author], hdinh@kent.edu (H. Q. Dinh), daniel@math.carleton.ca (D. Panario)

new binary quantum codes. The study of quantum code construction from QC codes began recently after the work of Galindo et al. [10], where the authors studied a specific class of 2-generator QC codes using Euclidean, Hermitian, and symplectic structures of QC codes. Following this, Lv et al. [22, 23] and Guan et al. [12, 13] constructed many record-breaking binary quantum codes utilizing the symplectic structure of QC codes. Additionally, explicit dual generators of QC codes have been studied in [1, 6].

The motivation for this study is to examine the necessary and sufficient conditions for symplectic self-orthogonality and the symplectic dual-containing condition in a simplified form that applies to the general version of quasi-cyclic codes. While some specific forms have been previously studied in the literature, we aim to encompass all these forms, provide a simpler, more general version, and demonstrate that our approach can construct new codes with record-breaking parameters.

This paper is organized as follows. In Section 2, we present the basics of linear codes and quasi-cyclic codes. In Section 3, we study one-generator quasi-cyclic codes and present the symplectic self-orthogonality condition over finite fields. Section 4 focuses on two-generator quasi-cyclic codes, showing both the symplectic self-orthogonality condition and the symplectic dual-containing condition for the general form of two-generator quasi-cyclic codes over finite fields. In Section 5, we construct new quantum codes with record-breaking parameters based on our study. Finally in Section 6, we conclude our work giving further research problems.

2 Preliminaries

Let $\mathbb{F}_q$ be the finite field with $q = p^r$ elements, where p is a prime number and r is a positive integer. A code C is a linear code of length $2n$ over $\mathbb{F}_q$ if C forms a subspace of the vector space $\mathbb{F}_q^{2n}$. The elements of C are called codewords. Suppose $\mathbf{a} = (a_0, a_1, \ldots, a_{2n-1})$ and $\mathbf{b} = (b_0, b_1, \ldots, b_{2n-1})$ are codewords of C. We define the (minimum) Hamming weight of C as $w_H(C) = \min\{w_H(\mathbf{a}) \mid \mathbf{a} \in C, \mathbf{a} \neq 0\}$, where $w_H(\mathbf{a})$ is the number of non-zero components of $\mathbf{a}$. The (minimum) Hamming distance of C is $d_H(C) = \min\{d_H(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}\}$, where $d_H(\mathbf{a}, \mathbf{b}) = |\{i \mid a_i \neq b_i\}|$.

The symplectic inner product of $\mathbf{u} = (\mathbf{u}_1, \mathbf{u}_2) \in \mathbb{F}_q^{2n}$ and $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2) \in \mathbb{F}_q^{2n}$ is defined as

$$\langle \mathbf{u}, \mathbf{v} \rangle_s = \langle \mathbf{u}_1, \mathbf{v}_2 \rangle_e - \langle \mathbf{v}_1, \mathbf{u}_2 \rangle_e,$$

where $\mathbf{u}_1, \mathbf{u}_2, \mathbf{v}_1, \mathbf{v}_2 \in \mathbb{F}_q^n$ and $\langle \cdot, \cdot \rangle_e$ is the standard Euclidean inner product in $\mathbb{F}_q^n$. We observed that this inner product can also be written as

$$\langle \mathbf{u}, \mathbf{v} \rangle_s = \mathbf{u} \Omega \mathbf{v}^t,$$

where

$$\Omega = \begin{pmatrix} O_n & I_n \\ -I_n & O_n \end{pmatrix},$$

where I_n denotes the $n \times n$ identity matrix, and O_n denotes the $n \times n$ zero matrix.

The symplectic dual code $C^{\perp_s}$ of C is defined as $C^{\perp_s} = \{\mathbf{u} \in \mathbb{F}_p^{2n} \mid \langle \mathbf{u}, \mathbf{v} \rangle_s = 0, \text{ for all } \mathbf{v} \in C\}$. A linear code C is called symplectic self-orthogonal if $C \subseteq C^{\perp_s}$, and symplectic dual-containing if $C^{\perp_s} \subseteq C$. Let $\mathbf{c} = (\mathbf{x}, \mathbf{y}) \in \mathbb{F}_q^{2n}$, where $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$. We define the (minimum) symplectic weight of C as $w_S(C) = \min\{w_S(\mathbf{c}) \mid \mathbf{c} \in C, \mathbf{c} \neq 0\}$, where $w_S(\mathbf{c}) = w_S(\mathbf{x}, \mathbf{y}) = |\{i \mid (x_i, y_i) \neq (0, 0)\}|$.

Suppose C is a linear code of length n over $\mathbb{F}_q$. Then C is a cyclic code if for any codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$, we have $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. Let us denote by $R = \mathbb{F}_q[x]/\langle x^n - 1 \rangle$. We can identify a codeword $(c_0, c_1, \ldots, c_{n-1}) \in C$ by a polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in R$. It is easy to show that C is a cyclic code of length n over $\mathbb{F}_q$ if it forms an ideal of R.

Definition 2.1. *Suppose C is a linear code of length ln over $\mathbb{F}_q$. Any codeword $\mathfrak{c} = (c_{0,0}, c_{0,1}, \ldots, c_{0,l-1}, c_{1,0}, \ldots, c_{1,l-1}, \ldots, c_{n-1,0}, \ldots, c_{n-1,l-1}) \in C$ can be written as*

$$\mathfrak{c} = \begin{pmatrix} c_{0,0} & c_{0,1} & \cdots & c_{0,l-1} \\ c_{1,0} & c_{1,1} & \cdots & c_{1,l-1} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n-1,0} & c_{n-1,1} & \cdots & c_{n-1,l-1} \end{pmatrix}.$$

In this case, C is a quasi-cyclic (QC) code of index l if for any $\mathfrak{c} \in C$, we get

$$\begin{pmatrix} c_{n-1,0} & c_{n-1,1} & \cdots & c_{n-1,l-1} \\ c_{0,0} & c_{0,1} & \cdots & c_{0,l-1} \\ \vdots & \vdots & \vdots & \vdots \\ c_{n-2,0} & c_{n-2,1} & \cdots & c_{n-2,l-1} \end{pmatrix} \in C.$$

3 One-generator QC codes

A QC code of length $2n$ and index 2 can be represented as $C = (C_1, C_2)$, where each C_j is a cyclic code of length n. Suppose C_j is generated by a polynomial $c_j(x)$ such that $c_j(x) \mid x^n - 1$ for $j = 1, 2$. Then, a one-generator QC code with index 2 can be interpreted as a 2-tuple of polynomials $(c_1(x), c_2(x))$.

Any one-generator QC code of length $2n$ and index 2 can be written as

$$C = \{r(x)\big(c_1(x), c_2(x)\big) \mid r(x) \in R\} = \{\big(r(x)c_1(x), r(x)c_2(x)\big) \mid r(x) \in R\}.$$

Theorem 3.1. *Let C be a one-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$. Then a generator of C is of the form $(r_1(x)g_1(x), r_2(x)g_2(x))$, where $g_i(x)h_i(x) = x^n - 1$ and $\gcd\big(r_i(x), h_i(x)\big) = 1$ for $i = 1, 2$.*

Proof. Let C be a one-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$, generated by $(c_1(x), c_2(x))$. Any element of C can be written in the form $\big(s(x)c_1(x), s(x)c_2(x)\big)$ for some polynomial $s(x) \in R$.

For $i = 1, 2$, we define a map $\Psi_i : C \longrightarrow R$ by

$$\Psi_i\big(s(x)c_1(x), s(x)c_2(x)\big) = s(x)c_i(x).$$

It is easy to show that, this map Ψ_i is a module homomorphism. Since $\Psi_i(C)$ is the image of C under a module homomorphism, it forms an ideal of R.

In the ring $R = \mathbb{F}_q[x]/\langle x^n - 1\rangle$, every ideal is a cyclic code of length n over $\mathbb{F}_q$. Because R is a principal ideal domain, any ideal $\Psi_i(C)$ is generated by a single polynomial $g_i(x)$ such that $g_i(x) \mid x^n - 1$. Therefore, we can write $\Psi_i(C) = (g_i(x))$.

Thus, the code C can be expressed as

$$C = \big(r_1(x)g_1(x), r_2(x)g_2(x)\big),$$

where $g_i(x)h_i(x) = x^n - 1$ and $\gcd(r_i(x), h_i(x)) = 1$ for $i = 1, 2$. This completes the proof. □

Definition 3.2. *Let C be a one-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$. Then the monic polynomial $h(x)$ of minimum degree such that*

$$h(x)\big(r_1(x)g_1(x), r_2(x)g_2(x)\big) = (0, 0)$$

is the parity-check polynomial of C.

Theorem 3.3. *Let $C = \big(r_1(x)g_1(x), r_2(x)g_2(x)\big)$ be a one-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$, where $g_i(x)h_i(x) = x^n - 1$ and $\gcd(r_i(x), h_i(x)) = 1$ for $i = 1, 2$. Then $\dim(C) = \deg(h(x))$.*

Proof. We define a module homomorphism $\Phi : R \to C$ by

$$\Phi(a(x)) = a(x)\big(r_1(x)g_1(x), r_2(x)g_2(x)\big).$$

Let $h(x) = \operatorname{lcm}(h_1(x), h_2(x))$ be the parity-check polynomial of C. We note that $\operatorname{Ker}(\Phi) = (h(x))$. Since the map Φ is surjective, we get $R/(h(x)) \cong C$, which implies that the $\dim(C) = \deg(h(x))$. □

Remark 3.4. An important fact about Theorem 3.3, is that, without the conditions $\gcd(r_i(x), h_i(x)) = 1$ for $i = 1, 2$, we cannot assert that $\dim(C) = \deg(h(x))$. We illustrate this with the following example.□

Example 3.5. We consider $R = \mathbb{F}_3[x]/\langle x^{10} - 1\rangle$, and

$$x^{10} - 1 = (x + 1)(x + 2)(x^4 + x^3 + x^2 + x + 1)(x^4 + 2x^3 + x^2 + 2x + 1) \in \mathbb{F}_3[x].$$

We take

$$g_1(x) = (x+2)(x^4+2x^3+x^2+2x+1), \quad g_2(x) = (x^4+x^3+x^2+x+1)(x^4+2x^3+x^2+2x+1),$$

$$r_1(x) = 2x^4+2x^3+2x^2+2x+2, \quad \text{and} \quad r_2(x) = 2x^5+2x^4+x^3+x^2+2x.$$

We have that $g_i(x) \mid x^n-1$, and $r_i(x) \in R$, for $i = 1, 2$. Also, as $g_i(x)h_i(x) = x^n-1$ for $i = 1, 2$, we get

$$h_1(x) = x^5+2x^4+2x^3+2x^2+2x+1, \quad \text{and} \quad h_2(x) = x^2+2.$$

From the above we get,

$$\gcd(r_1(x), h_1(x)) = x^4+x^3+x^2+x+1, \quad \text{and} \quad \gcd(r_2(x), h_2(x)) = 1.$$

Then $h(x) = \text{lcm}(h_1(x), h_2(x)) = x^6+x^5+2x+2$, implying $\deg(h(x)) = 6$.

On the other hand, using MAGMA computations, we find that the dimension of the QC code generated by $(r_1(x)g_1(x), r_2(x)g_2(x))$ is 2. □

Corollary 3.6. *[4] Let $C = (r_1(x)g(x), r_2(x)g(x))$ be a one-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$. Then $\dim(C) = n - \deg(g(x))$. Moreover, $d'(C) \geq 2d_H$, where d' is the minimum Hamming distance of C and d_H is the minimum Hamming distance of C_i for $i = 1, 2$.* □

Theorem 3.7. *[27] Let C be a linear code of length $2n$ over $\mathbb{F}_q$ with generator matrix G. Suppose G is an $m \times 2n$ matrix. Then C is a symplectic self-orthogonal code if and only if $G\Omega G^t = O_m$, where O_m is the $m \times m$ zero matrix and G^t denotes the transpose of G.*

Proof. Suppose C is a symplectic self-orthogonal code and $c = uG \in C$ an arbitrary codeword for some vector $u \in \mathbb{F}_q^m$. Then

$$\langle c, c\rangle_s = c\Omega c^t = (uG)\Omega(uG)^t = u(G\Omega G^t)u^t.$$

Therefore, $\langle c, c\rangle_s = 0$ if and only if $G\Omega G^t = O_m$. □

We recall a generator of a one-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$ as $C = (r_1(x)g_1(x), r_2(x)g_2(x))$, and we denote $a(x) = r_1(x)g_1(x)$ and $b(x) = r_2(x)g_2(x)$. We note that $a(x), b(x) \in R$. Then a generator matrix of C can be expressed as $G = (A \mid B)$, where A and B are $n \times n$ circulant matrices generated by $a_1(x)$ and $b_1(x)$, respectively. Here, $\mid$ denotes the horizontal concatenation of the two circulant matrices A and B. Then we have the following result.

Theorem 3.8. *Let C be a one-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$, whose generator matrix is $G = (A \mid B)$. Then $C \subseteq C^{\perp_s}$ if and only if $AB^t = BA^t$, where A^t and B^t represent the transposes of A and B, respectively.*

Proof. By Theorem 3.7, $C \subseteq C^{\perp_s}$ if and only if $G\Omega G^t$ is a zero matrix. For this one-generator QC code, the generator matrix G is of the form $G = (A \mid B)$. Thus, we have

$$G\Omega G^t = \begin{pmatrix} A & B \end{pmatrix} \begin{pmatrix} O_n & I_n \\ -I_n & O_n \end{pmatrix} \begin{pmatrix} A & B \end{pmatrix}^t = \begin{pmatrix} -B & A \end{pmatrix} \begin{pmatrix} A^t \\ B^t \end{pmatrix} = -BA^t + AB^t.$$

Therefore, $AB^t - BA^t = O_n$, implies $AB^t = BA^t$. Hence, $C \subseteq C^{\perp_s}$ if and only if $AB^t = BA^t$. □

We can also present Theorem 3.8 in terms of polynomials. To do so, we need to discuss the transpose of a polynomial, and its relation with the generator matrix described as follows.

Let $t(x) = t_0 + t_1x + t_2x + \cdots + t_{n-2}x^{n-2} + t_{n-1}x^{n-1} \in \mathbb{F}_q[x]/\langle x^n-1\rangle$. We define the transpose polynomial $\overline{t}(x)$ of $t(x)$ as

$$\overline{t}(x) = x^n t(x^{-1}) = t_0 + t_{n-1}x + t_{n-2}x^2 + \cdots + t_2x^{n-2} + t_1x^{n-1}.$$

We present the following result on the symplectic self-orthogonality of a one-generator quasi-cyclic code in terms of the generator polynomials.

Theorem 3.9. *Let C be a one-generator QC code of length $2n$ and index 2 generated by $(a(x), b(x))$. Then $C \subseteq C^{\perp_s}$ if and only if $a(x)\overline{b}(x) - b(x)\overline{a}(x) \equiv 0 \mod (x^n-1)$.*

Proof. By Theorem 3.8, the condition $C \subseteq C^{\perp_s}$ holds if and only if $AB^t = BA^t$. We aim to express this condition using polynomials.

If the circulant matrix A is generated by the polynomial $a(x)$, then its transpose A^t is generated by the transpose polynomial $\overline{a}(x)$. Similarly, the transpose B^t of the circulant matrix B, generated by the polynomial $b(x)$, is represented by the transpose polynomial $\overline{b}(x)$.

Additionally, considering that the circulant matrix A is generated by $a(x)$ and B^t is generated by $\overline{b}(x)$, the product matrix AB^t corresponds to the circulant matrix generated by $a(x)\overline{b}(x) \mod (x^n - 1)$. Similarly, BA^t corresponds to the circulant matrix generated by $b(x)\overline{a}(x) \mod (x^n - 1)$.

Therefore, $AB^t = BA^t$ if and only if $a(x)\overline{b}(x) - b(x)\overline{a}(x) \equiv 0 \mod (x^n - 1)$. □

Here, we present a detailed example explaining all the concepts discussed above.

Example 3.10. We consider $R = \mathbb{F}_3[x]/\langle x^{11} - 1\rangle$, and

$$x^{11} - 1 = (x + 2)(x^5 + 2x^3 + x^2 + 2x + 2)(x^5 + x^4 + 2x^3 + x^2 + 2) \in \mathbb{F}_3[x].$$

We take

$$g_1(x) = (x + 2)(x^5 + x^4 + 2x^3 + x^2 + 2), \quad \text{and} \quad g_2(x) = x^5 + x^4 + 2x^3 + x^2 + 2.$$

Then

$$h_1(x) = (x^5 + 2x^3 + x^2 + 2x + 2), \quad \text{and} \quad h_2(x) = (x + 2)(x^5 + 2x^3 + x^2 + 2x + 2).$$

We also consider

$$r_1(x) = 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2, \quad \text{and}$$

$$r_2(x) = 2x^7 + 2x^6 + 2x^5 + x^4 + x^3 + 2x^2 + x \in R.$$

Then $C = (r_1(x)g_1(x), r_2(x)g_2(x))$ is a one-generator QC code of length 22 over $\mathbb{F}_3$. We can check that $\gcd(r_i(x), h_i(x)) = 1$ for $i = 1, 2$. Then $\dim(C) = \deg(h(x)) = 6$, where

$$h(x) = \operatorname{lcm}(h_1(x), h_2(x)) = x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 1.$$

As per Theorem 3.8, we take $a(x) = r_1(x)g_1(x) \in R$, and $b(x) = r_2(x)g_2(x) \in R$. Then A is generated by $a(x)$, B is generated by $b(x)$, A^t is generated by $\overline{a}(x)$ and B^t is generated by $\overline{b}(x)$, where

$$a(x) = x^9 + x^5 + x^4 + x^3 + x + 1,$$

$$\overline{a}(x) = x^{10} + x^8 + x^7 + x^6 + x^2 + 1,$$

$$b(x) = 2x^{10} + 2x^8 + 2x^7 + x^6 + x^5 + x^2 + x + 1,$$

$$\overline{b}(x) = x^{10} + x^9 + x^6 + x^5 + 2x^4 + 2x^3 + 2x + 1.$$

It is easy to check that $AB^t = BA^t$, also $a(x)\overline{b}(x) - b(x)\overline{a}(x) \equiv 0 \mod (x^n - 1)$. Thus, $C \subseteq C^{\perp_s}$. □

Remark 3.11. A key property of the transpose polynomial is that if C is an $[n, \dim(C)]$ code with generator matrix $G \in \mathbb{F}_q^{n\times n}$, where G is the circulant matrix generated by $g(x)$, then the code C^t is also an $[n, \dim(C)]$ code with generator matrix $G^t \in \mathbb{F}_q^{n\times n}$, which is generated by $\overline{g}(x)$, the transpose polynomial of $g(x)$. This holds because $\dim(C) = \operatorname{rank}(G) = \operatorname{rank}(G^t) = \dim(C^t)$. It's important to note that the circulant generator matrix is not required to have full rank. □

In the following result, we present a theorem that allows us to determine the dimension of a one-generator QC code without the gcd conditions as in Theorem 3.3.

Theorem 3.12. *Let C be a one-generator QC code of length $2n$ and index 2 generated by $(a(x), b(x))$, where $a(x), b(x) \in R$. Then $\dim(C) = n - \deg(f(x))$, where $f(x) = \gcd\big(a(x), b(x), x^n - 1\big)$.*

Proof. Suppose $\gcd\big(a(x), b(x), x^n - 1\big) = f(x)$. Then the polynomial $f(x)$ divides both $a(x)$ and $b(x)$, as well as $x^n - 1$. Thus, $f(x)$ defines a cyclic code of length n over $\mathbb{F}_q$, whose dimension is $n - \deg(f(x))$.

The one-generator QC code C generated by $(a(x), b(x))$ can be expressed in terms of polynomials as

$$C = \{a(x)p(x) + b(x)q(x) \mid p(x), q(x) \in R\}.$$

We show that $\{a(x)p(x) + b(x)q(x) \mid p(x), q(x) \in R\}$ is exactly the principal ideal generated by $f(x)$.

As both $a(x)$ and $b(x)$ are multiples of $f(x)$, any linear combination of $a(x)$ and $b(x)$ will also be a multiple of $f(x)$. This implies that $(f(x))$, the ideal generated by $f(x)$, is contained in the ideal generated by $a(x)$ and $b(x)$, denoted as $(a(x), b(x))$. Thus, $(f(x)) \subseteq (a(x), b(x))$.

For the other side, we take $d(x) \in (a(x), b(x))$, then

$$d(x) = a(x)u(x) + b(x)v(x) = f(x)\big(u'(x) + v'(x)\big) \quad \text{implies} \quad d(x) \in (f(x)),$$

where $a(x) = f(x)u'(x)$ and $b(x) = f(x)v'(x)$, for some $u(x), v(x), u'(x), v'(x) \in R$. Therefore, $(a(x), b(x)) \subseteq (f(x))$.

Thus, $(a(x), b(x)) = (f(x))$, and the dimension of C is given by the dimension of the cyclic code generated by $f(x)$, which is $n - \deg(f(x))$. Hence, $\dim(C) = n - \deg(f(x))$. □

Remark 3.13. There are no non-trivial dual-containing one-generator quasi-cyclic codes. This is because the dimension of a one-generator QC code of length $2n$ and index 2 is given by $\dim(C) = n - \deg(f(x))$. Consequently, the dimension of the dual code is $n + \deg(f(x))$. For a code to be dual-containing, the dimension of the dual code must be less than or equal to the dimension of the original code, hence $n - \deg(f(x)) \geq n + \deg(f(x))$, which implies $\deg(f(x)) \leq 0$. □

4 Two-generators QC codes

In this section, we present two-generator QC codes, along with the necessary and sufficient conditions for self-orthogonality and the dual-containing property.

In the earlier section, we discussed one-generator QC codes of the form $(a_1(x), b_1(x))$, where $a_1(x) = r_1(x)g_1(x), b_1(x) = r_2(x)g_2(x)$ such that $g_i(x) \mid x^n - 1$ and $r_i(x) \in R$ for $i = 1, 2$. Similarly, we now introduce two-generator QC codes, where the generators are of the form $(a_1(x), b_1(x))$ and $(a_2(x), b_2(x))$. These generators are defined as follows:

$$a_1(x) = t_1(x)g_1(x), \quad b_1(x) = t_2(x)g_2(x), \quad a_2(x) = t_3(x)g_3(x), \quad b_2(x) = t_4(x)g_4(x), \tag{1}$$

where $a_i(x), b_i(x) \in R$, $g_j(x) \mid x^n - 1$ and $t_j(x) \in R$ for $j = 1, 2, 3, 4$.

In this two-generator case, handling four factors $g_i(x)$ of $x^n - 1$ and four other polynomials $t_i(x) \in R$ can be quite involved. Therefore, some special forms have been considered for study. For example, in [10], [23], and [12] consecutively, the generators are considered as follows:

$$\begin{pmatrix} f(x) & h(x)f(x) \\ 0 & g(x) \end{pmatrix}, \quad \begin{pmatrix} g_1(x) & g_1(x) \\ g_2(x) & u(x)g_2(x) \end{pmatrix}, \quad \text{and} \quad \begin{pmatrix} v(x)g_1(x) & g_1(x) \\ g_2(x) & v(x)g_2(x) \end{pmatrix}.$$

In this work, we aim to present a self-orthogonality and dual-containing condition that applies to any two-generator QC codes and can be viewed as a continuation of the one-generator case study. To achieve this, we consider the generator matrix corresponding to the generator $(a_1(x), b_1(x))$ as $G_1 = (A_1 \mid B_1)$ and for $(a_2(x), b_2(x))$ as $G_2 = (A_2 \mid B_2)$, where A_i are circulant matrices generated by the polynomial $a_i(x)$ for $i = 1, 2$, and B_i are circulant matrices generated by the polynomial $b_i(x)$ for $i = 1, 2$. A generator matrix of the two-generator QC code is then constructed as follows:

$$G = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix} = \begin{pmatrix} A_1 & B_1 \\ A_2 & B_2 \end{pmatrix}. \tag{2}$$

Next we give the dimension formula for a two-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$.

Theorem 4.1. *Let C be a two-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$, with generator matrix G of the form (2) given by*

$$G = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}.$$

Then, $\dim(C) = \text{rank}(G) = \text{rank}(G_1) + \text{rank}(G_2) - \dim(\textit{row space}(G_1) \cap \textit{row space}(G_2))$.

Remark 4.2. The result of Theorem 4.1 can also be expressed as

$$\dim(C) = \dim(C_1) + \dim(C_2) - \dim(C_1 \cap C_2),$$

where we can think C_i as one-generator QC codes generated by G_i, for $i = 1, 2$. We observed that

$$\dim(C_i) = \deg(f_i(x)), \text{ where } f_i(x) = \gcd\left(a_i(x), b_i(x), x^n - 1\right), \text{ for } i = 1, 2.$$

So far, we have been unable to establish the degree correspondence of $\dim(C_1 \cap C_2)$ using the polynomials considered in this study. Addressing this issue likely demands further investigation and a more detailed exploration of the polynomials, which we plan to undertake in a future project concentrating on the explicit dual construction of two-generator QC codes. □

4.1 Self-orthogonal QC codes

Theorem 4.3. *Let C be a two-generator QC code of length $2n$ and index 2 generated by $(a_1(x), b_1(x))$ and $(a_2(x), b_2(x))$, where $a_i(x), b_i(x) \in R$ and are of the form (1) for $i = 1, 2$. A generator matrix of this QC code C is of the form (2). Then $C \subseteq C^{\perp_s}$ if and only if the following conditions hold:*

$$A_1 B_1^t = B_1 A_1^t, \quad A_2 B_2^t = B_2 A_2^t, \quad \textit{and} \quad A_1 B_2^t = B_1 A_2^t,$$

where A_i^t and B_i^t denote the transposes of A_i and B_i, respectively, for $i = 1, 2$.

Proof. By Theorem 3.7, C is a symplectic self-orthogonal code, if and only if $G\Omega G^t$ is a zero matrix. Here C is a two-generator QC code of length $2n$ over $\mathbb{F}_q$, whose generator matrix is G is of the form (1). Then

$$\begin{aligned} G\Omega G^t &= \begin{pmatrix} A_1 & B_1 \\ A_2 & B_2 \end{pmatrix} \begin{pmatrix} O_n & I_n \\ -I_n & O_n \end{pmatrix} \begin{pmatrix} A_1^t & A_2^t \\ B_1^t & B_2^t \end{pmatrix} \\ &= \begin{pmatrix} -B_1 & A_1 \\ -B_2 & A_2 \end{pmatrix} \begin{pmatrix} A_1^t & A_2^t \\ B_1^t & B_2^t \end{pmatrix} \\ &= \begin{pmatrix} -B_1 A_1^t + A_1 B_1^t & -B_1 A_2^t + A_1 B_2^t \\ -B_2 A_1^t + A_2 B_1^t & -B_2 A_2^t + A_2 B_2^t \end{pmatrix}. \end{aligned}$$

Therefore,

$$G\Omega G^t = \begin{pmatrix} -B_1 A_1^t + A_1 B_1^t & -B_1 A_2^t + A_1 B_2^t \\ -B_2 A_1^t + A_2 B_1^t & -B_2 A_2^t + A_2 B_2^t \end{pmatrix} = \begin{pmatrix} O_n & O_n \\ O_n & O_n \end{pmatrix}.$$

By noting that $-B_1 A_2^t + A_1 B_2^t = (-B_2 A_1^t + A_2 B_1^t)^t$, and comparing both sides, we obtain the result. □

Remark 4.4. Using ideas from Theorem 3.8, we can consider the conditions $A_1 B_1^t = B_1 A_1^t$ and $A_2 B_2^t = B_2 A_2^t$ as the symplectic self-orthogonality conditions for the two constituent one-generator QC codes $(a_1(x), b_1(x))$ and $(a_2(x), b_2(x))$, respectively. Additionally, the condition $A_1 B_2^t = B_1 A_2^t$ imposes self-orthogonality between the two constituent one-generator QC codes $(a_1(x), b_1(x))$ and $(a_2(x), b_2(x))$, which together generate the two-generator QC code. □

Similar to the one-generator case, we also present an alternative criterion for the symplectic self-orthogonality condition in terms of the generator polynomials for the two-generator QC codes.

Theorem 4.5. *Let C be a two-generator QC code of length $2n$ and index 2 generated by $(a_1(x), b_1(x))$ and $(a_2(x), b_2(x))$, where $a_i(x), b_i(x) \in R$ and are of the form (1) for $i = 1, 2$. Then $C \subseteq C^{\perp_s}$ if and only if $a_1(x)\overline{b}_1(x) - b_1(x)\overline{a}_1(x) \equiv 0 \mod (x^n - 1)$, $a_2(x)\overline{b}_2(x) - b_2(x)\overline{a}_2(x) \equiv 0 \mod (x^n - 1)$ and $a_1(x)\overline{b}_2(x) - b_1(x)\overline{a}_2(x) \equiv 0 \mod (x^n - 1)$.*

Proof. This proof follows a similar line of arguments as the proof of Theorem 3.9. □

4.2 Dual-containing QC codes

We have examined the symplectic self-orthogonality condition $C \subseteq C^{\perp_s}$ for two-generator QC codes. Similarly, we can derive a necessary and sufficient condition for the symplectic dual-containing property $C^{\perp_s} \subseteq C$. Before proceeding, we need the following result.

Theorem 4.6. *Let C be a linear code of length $2n$ over $\mathbb{F}_q$ with a parity-check matrix H. Suppose H is an $m \times 2n$ matrix. Then C is a symplectic dual-containing code if and only if $H\Omega H^t = O_m$, where O_m is the $m \times m$ zero matrix and H^t denotes the transpose of H.*

Proof. Let us assume C is a symplectic dual-containing code, which means $C_s^\perp \subseteq C$. This gives us:

$$\begin{aligned} C_s^\perp \subseteq C &\iff \forall x \in C_s^\perp, \quad x \in C \\ &\iff \forall x \in C_s^\perp, \quad H\Omega x^t = 0 \\ &\iff \text{for all rows } r \text{ of } H, \quad H\Omega r^t = 0 \\ &\iff H\Omega H^t = 0. \end{aligned}$$

□

To determine the dual-containing property of two-generator QC codes, we need to construct a parity-check matrix. Our objective is to start with a generator matrix G of a two-generator QC code of length $2n$ and index 2 in the form (2). We consider circulant matrices P_i generated by the polynomial $p_i(x)$ for $i = 1, 2$, and circulant matrices Q_i generated by the polynomial $q_i(x)$ for $i = 1, 2$ to form a parity-check matrix H of the form:

$$H = \begin{pmatrix} P_1 & Q_1 \\ P_2 & Q_2 \end{pmatrix}, \tag{3}$$

such that $G\Omega H^T = O_{2n}$, where O_{2n} denotes the $2n \times 2n$ zero matrix.

By solving $G\Omega H^T = O_{2n}$, we derive the following equations:

$$\begin{aligned} A_1 \cdot Q_1^T &= B_1 \cdot P_1^T \\ A_1 \cdot Q_2^T &= B_1 \cdot P_2^T \\ A_2 \cdot Q_1^T &= B_2 \cdot P_1^T \\ A_2 \cdot Q_2^T &= B_2 \cdot P_2^T. \end{aligned}$$

The generator matrix G in the form (2) and the parity-check matrix H in the form (3) may not always have full rank. Consequently, H does not always generate the dual QC code of C. The condition $G\Omega H^T = O_{2n}$ indicates that if a two-generator QC code C is generated by the matrix G in the form (2), and another two-generator QC code C' is generated by the matrix H in the form (3), then all codewords of C are orthogonal to those of C'. However, C' is not always equal to $C_s^\perp$, the symplectic dual of C. If the matrix H satisfies $\text{rank}(G) + \text{rank}(H) = 2n$, i.e., $\dim(C_s^\perp) + \dim(C') = 2n$, we can assert that H is the parity-check matrix of C that generates $C_s^\perp$.

Example 4.7. We consider $R = \mathbb{F}_3[x]/\langle x^{15} - 1\rangle$, and

$$x^{15} - 1 = (x+2)^3(x^4 + x^3 + x^2 + x + 1)^3 \in \mathbb{F}_3[x].$$

We take

$$g_1(x) = (x+2)(x^4 + x^3 + x^2 + x + 1), \quad g_2(x) = (x+2)^3(x^4 + x^3 + x^2 + x + 1),$$

$$g_3(x) = (x^4 + x^3 + x^2 + x + 1)^2, \text{ and } g_4(x) = (x^4 + x^3 + x^2 + x + 1)$$

such that $g_i(x) \mid x^n - 1$ for $i = 1, 2, 3, 4$. We also take $t_i(x) \in R$ for $i = 1, 2, 3, 4$ such that

$$\begin{aligned} t_1(x) &= 2x^{12} + 2x^{11} + 2x^{10} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2, \\ t_2(x) &= 2x^{11} + 2x^{10} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2, \\ t_3(x) &= 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2, \\ t_4(x) &= 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2. \end{aligned}$$

Then C is a two-generator QC code of length 30 and index 2 generated by $(a_1(x), b_1(x))$ and $(a_2(x), b_2(x))$, where $a_i(x) \equiv t_i(x)g_i(x) \mod (x^n - 1)$ for $i = 1, 2$ and $b_j(x) \equiv t_j(x)g_j(x) \mod (x^n - 1)$ for $j = 3, 4$. Then the generator matrix G is of the form (2).

We consider $p_i(x) \equiv g_i^{\perp}(x)\bar{t}_i(x) \mod (x^n - 1)$ for $i = 1, 2$ and $q_j(x) \equiv g_j^{\perp}(x)\bar{t}_j(x) \mod (x^n - 1)$ for $j = 3, 4$. Then the parity-check matrix H is of the form (3). We can check that $G\Omega H^T = O_{2n}$ and $\text{rank}(G) + \text{rank}(H) = 2n$. Thus H generates the symplectic dual of the QC code C. □

Assuming we have a parity-check matrix for two-generator QC codes of length $2n$ and index 2 that generate $C_s^{\perp}$, we derive the necessary and sufficient condition for dual-containing two-generator QC codes of length $2n$ and index 2 over $\mathbb{F}_q$, expressed in terms of matrices.

Theorem 4.8. *Let C be a two-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$. A parity-check matrix of this QC code C is of the form (3). Then $C^{\perp_s} \subseteq C$ if and only if the following conditions hold:*

$$P_1Q_1^t = Q_1P_1^t, \quad P_2Q_2^t = Q_2P_2^t, \quad \text{and} \quad P_1Q_2^t = Q_1P_2^t,$$

where P_i^t and Q_i^t denote the transposes of P_i and Q_i, respectively, for $i = 1, 2$.

Proof. The proof follows a similar approach to the proof of Theorem 4.3. □

A necessary and sufficient condition for two-generator QC codes of length $2n$ and index 2 over $\mathbb{F}_q$ that contain their dual can be expressed in terms of polynomials as follows.

Theorem 4.9. *Let C be a two-generator QC code of length $2n$ and index 2 over $\mathbb{F}_q$. A parity-check matrix of this QC code C is of the form (3). Then $C^{\perp_s} \subseteq C$ if and only if $p_1(x)\overline{q}_1(x) - q_1(x)\overline{p}_1(x) \equiv 0 \mod (x^n - 1), p_2(x)\overline{q}_2(x) - q_2(x)\overline{p}_2(x) \equiv 0 \mod (x^n - 1)$, and $p_1(x)\overline{q}_2(x) - p_2(x)\overline{q}_1(x) \equiv 0 \mod (x^n - 1)$, where $\overline{p}(x)$ denotes the transpose polynomial of $p(x)$.*

Proof. This proof follows a similar line of arguments as the proof of Theorem 3.9. □

Example 4.10. Continuing from Example 4.7, we can demonstrate that the two-generator QC code C described in Example 4.7 meets both the necessary and sufficient conditions for the dual-containing property as stated in Theorem 4.8 and Theorem 4.9. Consequently, this code is a dual-containing QC code of length $2n$ and index 2 over $\mathbb{F}_3$. □

Remark 4.11. The duals of single-generator QC codes have been addressed in [1, 6]. However, duals of two-generator quasi-cyclic codes pose significantly greater complexity, primarily due to the management of the eight polynomials in the generator matrix G. This study aims to identify symplectic self-orthogonal and symplectic dual-containing codes without explicitly deriving the generators of the dual code. While minimum distance bounds for specific types of two-generator quasi-cyclic codes have been discussed in [10, 23], establishing these bounds for general two-generator QC codes remains an open challenge. □

5 QECCs from QC codes

Most of the quantum codes that have been studied in the literature are primarily based on the well-known CSS structure [8]. The study of quantum codes has also developed through the use of Hermitian and symplectic structures over $\mathbb{F}_q$, where q is a prime power, as explored in [3, 15]. We recall the symplectic self-orthogonal result from [15] and present a similar result corresponding to the dual-containing property.

Consider a linear code C. To construct a quantum code from C, it is necessary to satisfy the condition $C \subseteq C^{\perp_s}$ or $C^{\perp_s} \subseteq C$. The primary motivation of this paper is to establish necessary and sufficient conditions for efficiently constructing such linear codes, ensuring they possess the symplectic self-orthogonal or symplectic dual-containing property. Based on these two properties, we derive the corresponding results that we use to construct quantum codes from our study.

Theorem 5.1. *([2]) Let C be a linear code of length $2n$ over $\mathbb{F}_q$ with parameters $[2n, k]$. If $C \subseteq C^{\perp_s}$, then there exists a quantum error-correcting code Q with parameters $[[n, n - k, d_s]]$ over $\mathbb{F}_q$, where $d_s = \min\{w_s(c) \mid c \in (C^{\perp_s} \setminus C)\}$.*

We can also state the above result in terms of the dual-containing property.

Theorem 5.2. *Let C be a linear code of length $2n$ over $\mathbb{F}_q$ with parameters $[2n, k]$. If $C^{\perp_s} \subseteq C$, then there exists a quantum error-correcting code Q with parameters $[[n, k-n, d_s]]$ over $\mathbb{F}_q$, where $d_s = \min\{w_s(c) \mid c \in (C \setminus C^{\perp_s})\}$.*

Proof. Let C be a linear code of length $2n$ over $\mathbb{F}_q$ with parameters $[2n, k]$, such that $C \subseteq C^{\perp_s}$. Consider $D = C^{\perp_s}$, which is a linear code of length $2n$ over $\mathbb{F}_q$ with parameters $[2n, 2n-k]$. Since $D = C^{\perp_s}$, it follows that $D^{\perp_s} = C$. Therefore, $C^{\perp_s} \subseteq C$ implies $D \subseteq D^{\perp_s}$.

By Theorem 5.2, there exists a quantum error-correcting code Q with parameters $[[n, n-(2n-k), d_s]]$, which simplifies to $[[n, k-n, d_s]]$, where $d_s = \min\{w_s(c) \mid c \in (C \setminus C^{\perp_s})\}$. □

For ease of computation, we primarily consider one-generator quasi-cyclic codes C of the form $(r_1(x)g(x), r_2(x)g(x))$, where $g(x) \mid x^n - 1$ and $r_1(x), r_2(x) \in R$. We observe that a quantum code generated from a symplectic self-orthogonal quasi-cyclic code C of this form has a degree given by $n - k = n - (n - \deg(g(x))) = \deg(g(x))$. The advantage of this form is that it allows us to fix the degree of the quantum code to match the dimension of the parameter code we want to improve. All computations are done using MAGMA [5].

Example 5.3. We consider $q = 5$ and $n = 11$. Then $R = \mathbb{F}_5[x]/\langle x^{11} - 1\rangle$. We take two polynomials $r_1(x), r_2(x) \in R$, where

$$r_1(x) = 4x^8 + 4x^7 + 4x^6 + 4x^5 + 4x^4 + 4x^3 + 4x^2 + 4x + 4,$$

$$r_2(x) = 4x^6 + 2x^5 + 4x^4 + 2x^3 + 4x^2, \quad g(x) = 1.$$

Next, we consider two circulant matrices of size 11, A and B, generated by $r_1(x)$ and $r_2(x)$ over $\mathbb{F}_5$. This C is a QC code of length 22 of index 2 whose generator matrix is $G = (A \mid B)$, where $\mid$ represents the horizontal concatenation of the two circulant matrices A and B. We note that $AB^t = BA^t$, which implies C is a symplectic self-orthogonal code with parameters $[22, 11, 8]$ over $\mathbb{F}_5$. Therefore, by Theorem 5.1, we obtain a QECC with parameters $[[11, 0, 6]]$, which are record-breaking parameters. The previous record was $[[11, 0, 5]]$. This newly constructed code has been already updated to the quantum code table [11]. □

Example 5.4. We consider $q = 3$ and $n = 13$. Then $R = \mathbb{F}_3[x]/\langle x^{13} - 1\rangle$. We take $g(x) \mid x^{13} - 1$ and $r_1(x), r_2(x) \in R$, where

$$g(x) = 2x^6 + x^5 + 2x^4 + x^3 + x^2 + x + 2,$$

$$r_1(x) = 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1,$$

$$r_2(x) = 2x^6 + 2x^5 + 2x^4 + x^3 + 2x^2 + 2x + 2.$$

Next, we consider two circulant matrices of size 13, A and B, generated by $g(x)r_1(x)$ and $g(x)r_2(x)$ over $\mathbb{F}_3$. Then C is a QC code of length 26 with index 2 whose generator matrix is $G = (A \mid B)$, where $\mid$ represents the horizontal concatenation of the two circulant matrices A and B. We note that $AB^t = BA^t$, which implies C is a symplectic self-orthogonal code with parameters $[26, 7, 12]$ over $\mathbb{F}_3$. By Theorem 5.1, we obtain a QECC with parameters $[[13, 6, 4]]$, which are record-breaking parameters. The previous record was $[[13, 6, 3]]$. This newly constructed code is also already updated to the online quantum code table [11]. □

Example 5.5. We consider $q = 3$ and $n = 23$. Then $R = \mathbb{F}_3[x]/\langle x^{23} - 1\rangle$. We take $g(x) \mid x^{23} - 1$ and $r_1(x), r_2(x) \in R$, where

$$g(x) = x^{12} + 2x^{11} + 2x^9 + x^8 + 2x^7 + x^6 + x^5 + x^3 + 1,$$

$$r_1(x) = 2x^{11} + 2x^{10} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 2,$$

$$r_2(x) = 2x^{10} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + x^3 + 2x^2 + 1.$$

Next, we consider two circulant matrices of size 23, A and B, generated by $g(x)r_1(x)$ and $g(x)r_2(x)$ over $\mathbb{F}_3$. Then C is a QC code of length 46 with index 2 whose generator matrix is $G = (A \mid B)$, where $\mid$ represents the horizontal concatenation of the two circulant matrices A and B. We note that $AB^t = BA^t$, which implies C is a symplectic self-orthogonal code with parameters $[46, 11, 21]$ over $\mathbb{F}_3$. By Theorem 5.1, we obtain a QECC with parameters $[[23, 12, 5]]$, which are record-breaking parameters. The previous record was $[[23, 12, 4]]$. This newly constructed code already appears updated in the online quantum code table [11]. □

Example 5.6. We consider $q = 3$ and $n = 16$. Then $R = \mathbb{F}_3[x]/\langle x^{16} - 1\rangle$. We take $g(x) \mid x^{16} - 1$ and $r_1(x), r_2(x) \in R$, where

$$g(x) = 2x^6 + x^4 + 1,$$
$$r_1(x) = 2x^9 + 2x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + 2x^3 + 2x^2 + 2x + 1,$$
$$r_2(x) = 2x^9 + 2x^8 + x^7 + 2x^6 + x^5 + x^4 + 2x^3 + x.$$

Next, we consider two circulant matrices of size 16, A and B, generated by $g(x)r_1(x)$ and $g(x)r_2(x)$ over $\mathbb{F}_3$. Then C is a QC code of length 32 with index 2 whose generator matrix is $G = [A \mid B]$, where $\mid$ represents the horizontal concatenation of the two circulant matrices A and B. We note that $AB^t = BA^t$, which implies C is a symplectic self-orthogonal code with parameters $[32, 10, 12]$ over $\mathbb{F}_3$. By Theorem 5.1, we obtain a QECC with parameters $[[16, 6, 5]]$, which are record-breaking parameters. The previous record was $[[16, 6, 4]]$. This newly constructed code is in online the quantum code table [11]. □

Example 5.7. By [7, Theorem 6], if a quantum code with parameters $[[n, k, d]]$ exists then a quantum code with parameters $[[n + 1, k, d]]$ also exists, when $k > 0$. Therefore, from the above-constructed quantum code parameters $[[16, 6, 5]]$, we get a quantum code with parameters $[[17, 6, 5]]$ which is also new and breaks the previous record which is $[[17, 6, 4]]$. This newly constructed code is in the online quantum code table [11]. □

6 Conclusion and Future work

In this work, we study one-generator and two-generator quasi-cyclic (QC) codes over $\mathbb{F}_q$, where q is a prime power. We present a necessary and sufficient condition for symplectic self-orthogonal one-generator quasi-cyclic codes. Based on this condition, we have constructed new quantum codes that set new records. Extending our study to two-generator QC codes over finite fields, we present necessary and sufficient conditions for both symplectic self-orthogonality and symplectic dual-containing properties. For each factor $g(x)$ of $x^n - 1$, we choose two polynomials $r_1(x)$ and $r_2(x)$ to construct a quantum code from the one-generator QC codes. We know that skew polynomial rings are not unique factorization domains; hence, any skew polynomial can have multiple factorizations over our standard commutative polynomial ring $\mathbb{F}_q[x]$. This multiplicity increases the potential to find more factors and, consequently, more possibilities to construct codes. It will be interesting to study one-generator skew quasi-cyclic codes and apply our necessary and sufficient conditions to explore new record-breaking quantum codes.

Acknowledgement

T. Bag's work is funded by the European Research Council (ERC Grant AlgoQIP, Agreement No. 851716). T. Bag also acknowledges support from a government grant administered by the Agence Nationale de la Recherche under the Plan France 2030, reference ANR-22-PETQ-0006. T. Bag is grateful to Prof. Markus Grassl for numerous discussions on quantum codes. D. Panario was funded by the Natural Sciences and Engineering Research Council of Canada (NSERC), reference number RPGIN-2018-05328.

References

[1] K. Abdukhalikov, T. Bag and D. Panario, One-generator quasi-cyclic codes and their dual codes, Discrete Math. 346(6), 113369, (2023).

[2] S. A. Aly, A. Klappenecker and P. K. Sarvepalli, On quantum and classical BCH codes, IEEE Trans. Inf. Theory 53(3), 1183–1188, (2007).

[3] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, IEEE Trans. Inf. Theory 47, 3065–3072, (2001).

[4] N. Aydin, I. Siap and D. K. Ray-Chaudhuri, The structure of 1-generator quasi-twisted codes and new linear codes, Des. Codes Cryptogr. 24, 313–326, (2001).

[5] W. Bosma, J. Cannon, C. Fieker and A. Steel (eds.), Handbook of magma functions, Edition 2.19, 5488 pages, (2013).

[6] S. Benjwal, M. Bhaintwal, On the duals of quasi-cyclic codes and their application to quantum codes, Quantum Inf. Process 23, 113, (2024).

[7] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, Phys. Rev. A 54(2), 1098–1105, (1996).

[8] A. R. Calderbank, E. M. Rains, P. M. Shor and N. J. A. Sloane, Quantum error-correction via codes over GF(4), IEEE Trans. Inf. Theory 44, 1369–1387, (1998).

[9] J. Conan and G. Seguin, Structural properties and enumeration of quasi cyclic codes, AAECC 4, 25–39, (1993).

[10] C. Galindo, F. Hernando and R. Matsumoto, Quasi-cyclic constructions of quantum codes, Finite Fields their Appl. 52, 261–280, (2018).

[11] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, Online available at http://www.codetables.de, Accessed on 2024-06-08.

[12] C. Guan, R. Li and L. Lu, New binary quantum codes constructed from quasi-cyclic codes, Int. J. Theor. Phys 61, 172, (2022).

[13] C. Guan, R. Li, J. Lv and Z. Ma, Symplectic self-orthogonal quasi-cyclic codes, ArXiv:2212.14225.

[14] T. Kasami, A Gilbert-Varshamov bound for quasi-cyclic codes of rate $\frac{1}{2}$, IEEE Trans. Inf. Theory 20, 679, (2018).

[15] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, Nonbinary stabilizer codes over finite fields, IEEE Trans. Inf. Theory 52, 4892—4914, (2006).

[16] K. Lally and P. Fitzpatrick, Algebraic structure of quasicyclic codes, Discrete Appl. Math. 11, 157–175, (2001).

[17] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, IEEE Trans. Inf. Theory 47(7), 2751–2760, (2001).

[18] S. Ling and P. Solé, Good self-dual quasi-cyclic codes exist, IEEE Trans. Inf. Theory 49(4), 1052–1053, (2003).

[19] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes II: chain rings, Des. Codes Cryptogr. 30, 113–130, (2003).

[20] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes III: generator theory, IEEE Trans. Inf. Theory 51(5), 2692–2700, (2005).

[21] S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes IV: repeated roots, Des. Codes Cryptogr. 38, 337–361, (2006).

[22] J. Lv, R Li and J. Wang, New binary quantum codes derived from one-generator quasi-cyclic codes, IEEE Access 7, 85782–85785, (2019).

[23] J. Lv, R. Li and J. Wang, An explicit construction of quantum stabilizer codes from quasi-cyclic codes, IEEE Commun. Lett. 24(5), 1067–1071, (2020).

[24] G. E. Seguin, A class of 1-generator quasi-cyclic codes, IEEE Trans. Inf. Theory 50, 1745–1753, (2004).

[25] A. M. Steane, Simple quantum error-correcting codes, Phys. Rev. A 54, 4741–4751, (1996).

[26] P. W. Shor, Scheme for reducing decoherence in quantum memory, Phys. Rev. A 52, 2493–2496, (1995).

[27] H. Xu and W. Du, On some binary symplectic self-orthogonal codes, AAECC 33, 321–337, (2022).