symmetry

IMPACT FACTOR 2.940

CITESCORE 4.3

Article

Lower Bounds for Quasi-Cyclic Codes and New Binary Quantum Codes

Yiting Liu, Chaofeng Guan, Chao Du and Zhi Ma

MDPI

https://doi.org/10.3390/sym15030643

symmetry

MDPI

Article

Lower Bounds for Quasi-Cyclic Codes and New Binary Quantum Codes

Yiting Liu [1,2], Chaofeng Guan [2,3], Chao Du [1,2] and Zhi Ma [1,2,*]

[1] The State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China
[2] Henan Key Laboratory of Network Cryptography Technology, Zhengzhou 450001, China
[3] Fundamentals Department, Air Force Engineering University, Xi'an 710051, China
* Correspondence: ma_zhi@163.com

Abstract: This paper considers three kinds of quasi-cyclic codes of index two with one generator or two generators and their applications in quantum code construction. In accordance with the algebraic structure of linear codes, we determine the lower bounds of the symplectic weights of these quasi-cyclic codes. Quasi-cyclic codes with the dual-containing property enable the construction of quantum codes. Defining the coefficient symmetric polynomials of the generator polynomials gives a concise condition for the dual-containing of the quasi-cyclic codes. The lower bound results can significantly reduce the scope of the search for a larger minimum distance of quasi-cyclic codes. With these algebraic results and computer supports, we obtain classical quasi-cyclic codes with better parameters and some new quantum codes under the symplectic construction. In particular, two examples of the new quantum codes $[[63, 42, 6]]_2$, $[[51, 35, 5]]_2$ improve the corresponding codes in Grassl's code table.

Keywords: quasi-cyclic codes; symplectic distance; quantum codes

Citation: Liu, Y.; Guan, C.; Du, C.; Ma, Z. Lower Bounds for Quasi-Cyclic Codes and New Binary Quantum Codes. *Symmetry* **2023**, *15*, 643. https://doi.org/10.3390/sym15030643

Academic Editor: Jerzy Kowalski-Glikman

Received: 2 February 2023
Revised: 20 February 2023
Accepted: 1 March 2023
Published: 3 March 2023

1. Introduction

In recent decades, quantum error-correcting has developed rapidly in the area of quantum computation and quantum information. Quantum codes were introduced to protect quantum information from decoherence and quantum noise. Quantum error correction codes (QECCs) lie at the lowest level of the fault-tolerant quantum computing model and their error correction capability has a significant impact on the quantum computing model. Therefore, the search for quantum error correction codes with good parameters has been a research goal of scholars. QECCs were first proposed by Shor and Steane [1,2]. Calderbank et al. in [3] proposed a method to construct binary quantum error-correcting codes via classical error-correcting codes over $GF(4)$. Later, the QECCs construction scheme was further extended to the non-binary case [4,5], which greatly expands the family of quantum codes. There are three mainstream QECC construction methods, Euclidean, Hermitian, and symplectic construction which respect Euclidean, Hermitian, and symplectic inner products, respectively. Many optimal classical cyclic, constacyclic, repeated-root cyclic, skew-cyclic code, quasi-cyclic (QC), generalized QC codes, simplex codes etc. with good dual-containing properties have been given in recent years, and corresponding QECCs [6–17] with good parameters are constructed based on them.

QC codes are a native generalization of cyclic codes with a rich algebraic structure and they are widely studied over finite fields [18–20] and finite rings [13,21]. A wider range of quantum code parameters is available in QC codes [22–24]. Many QC codes have improved the earlier known minimum distances since Kasami et al. [25] showed that QC codes satisfy the modified Gilbert–Varshamov (GV) bound. Since the algebraic structure of one-generator QC codes has been proposed, a large number of one-generator quasi-cyclic codes with good parameters have appeared [26–29]. With further research, Chen et al. [23] gave the algebraic structure of two-generator and three-generator QC

codes from simplex codes. Hagiwara et al. [16,30] studied constructions of QECCs by QC Low-Density Parity Check (LDPC) codes focusing on long code length and probabilistic construction. Sangwisut et al. [31] proposed the algebraic structure of Hermitian self-dual QC codes. Aydin et al. [32] constructed 62 new binary codes using a comprehensive search strategy with QC codes. Later, Galindo et al. [15] deduced the algebraic structure of the dual form for a family of two-generator QC codes with index two, which opened up a new way to construct quantum codes by QC codes under different construction. Ezerman et al. [33] obtained quantum codes with strictly improved parameters by quantum Construction X on quasi-cyclic codes with large Hermitian hulls.

We construct new quantum codes by searching for the QC codes under the symplectic dual-containing relation over three different types of QC codes with the help of the lower bounds. The constructions of the quantum codes all require the classical codes that have self-orthogonality (or dual-containing) property. In order to give the conditions for the self-orthogonality (dual-containing), Galindo et al. [15] deform the generator polynomial in the article to make it a coefficient-symmetric form of the original polynomial which is useful in inner product calculations. In this paper, we also use this transformation of polynomials and we rename them as symmetric polynomials. Using the good symmetry of these polynomials and the form of the generator polynomials, it is easy to give dual-containing conditions for QC codes under different structures. Then, in this paper, we calculate the lower bounds on the symplectic distance of three kinds of QC codes with known structures. These lower bounds can somewhat reduce our difficulty in obtaining better quantum codes. Akre, Aydin et al. [34] pointed out that obtaining codes with better parameters is challenging. The minimum distance of a linear code is difficult to compute and the problem is NP-hard [35]. Furthermore, the code space of a fixed code length increases rapidly with the number of dimensions. Therefore it is impossible to search for good codes by exhaustive computer searching. Scholars try to find codes with a special algebraic structure that has better parameters. This paper then reduces the difficulty of finding good codes in terms of reducing the search space by giving a lower bound on the symplectic distance. We provide some examples of QC codes with good parameters and some stabilizer quantum codes. The parameters of the obtained new codes are competitive with the code table [36].

2. Preliminaries

In this section, we recall some basic concepts of QC codes and some connections between QC codes and quantum codes under symplectic construction that are necessary for the development of this work.

Let F_q be the finite field of q elements where q is a prime power and $R = \frac{F_q[x]}{x^n-1}$ be a ring of q-ary polynomials module $x^n - 1$. A classical linear $[n, k, d]$ code C over F_q is a k-dimensional subspace of F_q^n with $d = \min\{wt(\vec{c}) : \vec{c} \in C \setminus \{\mathbf{0}\}\}$ where $wt(\vec{c})$ denotes the Hamming weight of a codeword $\vec{c}$. The cyclic shift τ on F_q^n is the shift

$$\tau(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, \ldots, c_{n-2}).$$

A linear space $C \subset F_q^n$ is said to be a cyclic code if $C = \tau(C)$. Given a polynomial $g(x) \in R$ and $[g(x)]$ denotes the residue class of $g(x)$ in R. Then a cyclic code can be identified with an idea of R via the mapping:

$$[c(x)] = [c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}],$$

and $\tau(c)$ corresponding to the class $[xc(x)]$. A linear code $C \subset F_q^{nl}$ is called a QC code of index l if it is invariant under a shift of codewords by l units. Let $\vec{c}$ be a codeword of C: $\vec{c} = (c_{0,0}, c_{0,1}, \ldots, c_{0,n-1}, c_{1,0}, \ldots, c_{1,n-1}, c_{l-1,0}, c_{l-1,n-1})$. Then define a map $\psi : F_q^{ln} \to R^l$:

$$\phi(\vec{c}) = ([c_0(x)], [c_1(x)], \ldots, [c_{l-1}(x)]),$$

where $c_j(x) = c_{j,0} + c_{j,1}x + \ldots + c_{j,n-1}x^{n-1} \in R$. Each $c_j(x)$ corresponds to a codeword of cyclic code generated by $[c_j(x)] \in R$. Therefore, a QC code can be identified with an R-submodule of R^l. A QC code generated by two elements in R^2,

$$([g_1(x)], [g_2(x)]),\ ([f_1(x)], [f_2(x)]),$$

can be regarded as the R-module:

$$\{[a_1(x)g_1(x)], [a_1(x)g_2(x)] + [a_2(x)f_1(x)], [a_2(x)f_2(x)] \mid a_i(x) \in F_q[x]\}$$

Each polynomial of the generator of QC code corresponds to a generator of a cyclic code, which determines a circulant matrix, so the generator matrix of a 2-QC code with index 2 has the following form:

$$G = \begin{pmatrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \end{pmatrix}.$$

In this paper, we only deal with one-generator and two-generator QC codes (1-QC and 2-QC for simplicity). For a linear space $C \subset F_q^n$, $C^\perp$ denotes its Euclidean dual under:

$$C^\perp = \{\vec{x} \in F_q^n \mid \langle \vec{x}, \vec{y} \rangle = 0,\ for\ all\ \vec{y} \in C\}.$$

If $C \subset C^\perp$, the code $C^\perp$ is a Euclidean dual-containing code. The symplectic weight of vector $\vec{u} \in F_q^{2n}$ is $w_s(\vec{u}) = \#\{i \mid (u_i, u_{i+n}) \neq (0,0),\ 0 \leq i \leq n-1\}$. The minimum symplectic weight of code C is $d_s(C) = \min\{w_s(\vec{u}) \mid \vec{u} \in C)\}$. The symplectic inner product of two vectors $\vec{u}, \vec{v} \in F_q^{2n}$ is defined as $\langle \vec{u}, \vec{v} \rangle_s = \sum_{i=0}^{n-1} (u_i v_{n+i} - u_{n+i} v_i)$. So the symplectic dual code of C is denoted as:

$$C^{\perp_s} = \{\vec{x} \in F_q^{2n} \mid \langle \vec{x}, \vec{y} \rangle_s = 0,\ for\ all\ \vec{y} \in C\}.$$

If $C \subset C^{\perp_s}$, the code C is symplectic self-orthogonal code and $C^{\perp_s}$ is a symplectic dual-containing code. If $C^{\perp_s} = C$, the code C is a symplectic self-dual code.

Lemma 2.4 in [37] gives a relationship between symplectic and Hamming weights of vector $(\vec{u}, \vec{v}) \in F_q^{2n}$:

Lemma 1. *Let $\vec{u}, \vec{v}$ be two vectors in F_q^{2n}, then we have*

$$q w_s(\vec{u}, \vec{v}) = w_H(\vec{u}) + w_H(\vec{v}) + \sum_{\beta \in F_q \setminus \{0\}} w_H(\beta \vec{u} + \vec{v}),$$

where w_H denotes the Hamming weight, the number of non-zero terms of vector $\vec{v}$.

Let $g(x) = g_0 + g_1 x + \ldots + g_{n-1}x^{n-1} \in R$ and define $\bar{g}(x) = x^n g(\frac{1}{x}) = g_0 + g_{n-1}x + \ldots + g_1 x^{n-1}$ of which the coefficients of polynomials are symmetrically exchanged (except for constant terms). When $g(x) \mid x^n - 1$, there exists a $h(x) = \frac{x^n-1}{g(x)}$; define $g^\perp(x) = \frac{1}{h(0)} x^{deg(h(x))} h(\frac{1}{x})$. The coefficient weight of $g(x)$, denoted by $cw(g(x)))$, is defined to be the smallest distance among non-zero terms of $g(x)$ which is a non-negative integer given by:

$$cw(g(x)) = \begin{cases} 0, & \text{if g(x) is a monomial,} \\ \min\{|\ i-j\ ||\ a_i, a_j \neq 0,\ i \neq j\}, & \text{otherwise.} \end{cases} \quad (1)$$

Then we have the following lemma [38].

Lemma 2. *If the degree of $g(x)$ is less than $cw(f(x))$, the following equation holds:*

$$w_H(f(x)g(x)) = w_H(f(x)) \cdot w_H(g(x)). \quad (2)$$

A q-ary quantum code $\mathcal{Q}$ of length n, distance d and dimension k is a q^k-dimensional subspace of a q^n-dimensional Hilbert space $(\mathbb{C}^q)^{\otimes n}$. Usually, $\mathcal{Q}$ can be designed to correct up to $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors caused by Pauli operators X, Y, Z. Symplectic construction is a powerful method for constructing QECCs which establishes a correlation between symplectic self-orthogonal or dual-containing codes and QECCs. Here we give this CRSS [3] construction:

Lemma 3 ([3,5]). *Let $C \subset F_q^{2n}$ be a symplectic self-orthogonal $[2n, n-k]$ linear code, where C is a symplectic self-orthogonal code such that $C \subset C^{\perp_s}$ and $d(C^{\perp_s} \setminus C) = d$, then there exists a stabilizer QECC with parameter $[[n,k,d]]_q$.*

3. Results

In this section, we focus on three proposed QC structures [39–41]. By analyzing the form of their generator elements, we give corresponding lower bounds over the symplectic distance. According to the symplectic construction scheme of QECCs that the symplectic distance of QC codes with a dual-containing relationship is the minimum distance of a quantum code. Thus we are able to search for quantum codes with larger minimal distances with the help of lower bounds and computer supports. These codes have larger code distances than codes of the same code length and dimension compared with the online code table [36].

The following table gives the specific forms and generator elements of the three kinds of QC codes and their symplectic dual codes.

In the first part, we will discuss the use of a class of one-generator QC codes with index 2 (case 1 in Table 1) to find the symplectic dual code to construct QECCs. We also calculate a lower bound of the distance of the symplectic dual code, then construct QECCs with good parameters based on the given lower bound.

Table 1. The specific forms of the three types of proposed QC codes and their symplectic dual codes.

Quasi-Cyclic Code Construction	Generator	Conditions [1]	Symplectic Dual Code
$(G_1 \quad G_2)$ [39]	$([g(x)], \quad [g(x)f(x)])$	$g^{\perp_e}(x) \mid g(x)$	$\begin{pmatrix} [1], & [\bar{f}(x)] \\ [0], & [g^{\perp}(x)] \end{pmatrix}$
$\begin{pmatrix} G_1 & G_1 \\ G_2 & G_{h2} \end{pmatrix}$ [40]	$\begin{pmatrix} [f(x)], & [f(x)] \\ [g(x)], & [g(x)h(x)] \end{pmatrix}$	$g^{\perp_e}(x) \mid f(x), \quad \bar{f}(x) = f(x)$	$\begin{pmatrix} [f^{\perp}(x)], & [\bar{h}(x)f^{\perp}(x)] \\ [g^{\perp}(x)], & [g^{\perp}(x)] \end{pmatrix}$
$\begin{pmatrix} G_{h1} & G_1 \\ G_2 & G_{h2} \end{pmatrix}$ [41]	$\begin{pmatrix} [h(x)g(x)], & [g(x)] \\ [f(x)], & [f(x)h(x)] \end{pmatrix}$	$f(x) \mid g^{\perp_e}(x), \quad \bar{h}(x) = h(x)$	$\begin{pmatrix} [g^{\perp}(x)], & [\bar{h}(x)g^{\perp}(x)] \\ [\bar{h}(x)f^{\perp}(x)], & [f^{\perp}(x)] \end{pmatrix}$

[1] The conditions for the QC codes to be dual-containing or symplectic self-dual.

Theorem 1. *Consider the QC code Q with generator matrix G:*

$$G = \begin{pmatrix} [1], & [\bar{f}(x)] \\ [0], & [g^{\perp}(x)] \end{pmatrix},$$

where we assume that $g(x) \mid x^n - 1$ and $f(x)$ satisfies that $\gcd(\bar{f}(x) - \beta, x^n - 1) = 1$ for all non-zero $\beta \in F_q$. Then, a lower bound on the symplectic weight of Q is the following value

$$d_{low1} = \min\{d([g^{\perp}(x)]),\ d([\frac{x^n-1}{\gcd(x^n-1, \bar{f}(x))}]),\ d([\bar{f}(x)]),$$
$$d([\frac{g^{\perp}(x)}{\gcd(g^{\perp}(x), \bar{f}(x))}]),\ 1 + d([\gcd(\bar{f}(x), g^{\perp}(x))])/q\},$$

Proof. The symplectic weight of any codeword of Q can be represented as:

$$w_s = w_s([a(x)], [a(x)\bar{f}(x) + b(x)g^{\perp}(x)]),$$

where $a(x)$ and $b(x)$ are arbitrary polynomials in R.

(1) If $a(x) = 0$ then $w_s = w_H([b(x)g^{\perp}(x)]) \geq d([g^{\perp}(x)])$.
(2) If $a(x) \neq 0$ and $b(x) = 0$, then the weight is represented as $w_s = w_s([a(x)], [a(x)\bar{f}(x)])$.

(i) If $a(x)\bar{f}(x) = 0 \mod (x^n - 1)$, then $\frac{x^n-1}{\gcd(x^n-1,\bar{f}(x))} \mid \frac{a(x)\bar{f}(x)}{\gcd(x^n-1,\bar{f}(x))}$. Since $\gcd(\frac{x^n-1}{\gcd(x^n-1,\bar{f}(x))}, \frac{\bar{f}(x)}{\gcd(x^n-1,\bar{f}(x))}) = 1$, we have $\frac{x^n-1}{\gcd(x^n-1,\bar{f}(x))} \mid a(x)$. Therefore, the cyclic code generated by $[a(x)]$ belongs to $[\frac{x^n-1}{\gcd(x^n-1,\bar{f}(x))}]$. So the lower bound of symplectic weight is $w_s \geq d([a(x)]) \geq d([\frac{x^n-1}{\gcd(x^n-1,\bar{f}(x))}])$.

(ii) When $a(x)\bar{f}(x) \neq 0 \mod (x^n - 1)$, according to Lemma 1, we have

$$w_s = \frac{1}{q}(w_H([a(x)]) + w_H([a(x)\bar{f}(x)]) + \sum_{\beta \in F_q \setminus \{0\}} w_H([a(x)(\bar{f}(x) + \beta)])).$$

If $deg(\bar{f}(x)) < cw(a(x))$ then $w_H([a(x)\bar{f}(x)]) = w_H([a(x)])w_H([\bar{f}(x)])$. So the symplectic weight has the following lower bound:

$$w_s = \frac{1}{q}(w_H([a(x)]) + w_H([a(x)])w_H([\bar{f}(x)]) + (q-1)w_H([a(x)]) \sum_{\beta \in F_q \setminus \{0\}} w_H([\bar{f}(x) + \beta])).$$

the lower bound is given by $w_s \geq d([\bar{f}(x)])$ as there exists at most one $\beta \in F_q^*$ such that $\bar{f}(x) + \beta$ has no constant term.

Else, when $deg(f(x)) \geq cw(a(x))$, then

$$w_s \geq d([a(x)])/q + d([a(x)\bar{f}(x)]) \geq 1 + d([\bar{f}(x)]).$$

(3) If $a(x) \neq 0$, $b(x) \neq 0$, and $a(x)\bar{f}(x) + b(x)g^{\perp}(x) = 0 \mod (x^n - 1)$ then we can deduce $g^{\perp}(x) \mid a(x)\bar{f}(x)$. Then we can gain $\frac{g^{\perp}(x)}{\gcd(g^{\perp}(x),\bar{f}(x))} \mid \frac{a(x)\bar{f}(x)}{\gcd(g^{\perp}(x),\bar{f}(x))}$, as $\gcd(\frac{g^{\perp}(x)}{\gcd(g^{\perp}(x),\bar{f}(x))}) = 1$, $\frac{\bar{f}(x)}{\gcd(g^{\perp}(x),\bar{f}(x)))}$ we obtain $\frac{g^{\perp}(x)}{\gcd(g^{\perp}(x),\bar{f}(x))} \mid a(x)$. Finally, we have $w_s = w_H([a(x)]) \geq d([\frac{g^{\perp}(x)}{\gcd(g^{\perp}(x),\bar{f}(x))}])$.

(4) If $a(x) \neq 0$, $b(x) \neq 0$, and $a(x)\bar{f}(x) + b(x)g^{\perp}(x) \neq 0$, then the symplectic weight is

$$\begin{aligned} w_s = \frac{1}{q}&(w_H([a(x)]) + w_H([a(x)\bar{f}(x) + b(x)g^{\perp}(x)]) \\ &+ \sum_{\beta \in F_q \setminus \{0\}} w_H([a(x)(\bar{f}(x) + \beta) + b(x)g^{\perp}(x)])). \end{aligned} \tag{3}$$

If some summand of the summation in Equation (3) is zero then $[a(x)(\bar{f}(x) + \beta)] = -[b(x)g^{\perp}(x)]$ for some $\beta \in F_q^*$.This means $g^{\perp}(x) \mid a(x)$, as $(\bar{f}(x) + \beta)$ is a unit modulo $x^n - 1$. So

$$w_s \geq w_H([a(x)] \geq d([g^{\perp}(x)]).$$

Otherwise (all summands in Equation (3) are nonzero),

$$\begin{aligned} w_s &\geq \frac{1}{q}(d([a(x)]) + d([\gcd(\bar{f}(x), g^{\perp}(x))]) + (q-1)) \\ &\geq 1 + d([\gcd(\bar{f}(x), g^{\perp}(x))])/q \end{aligned}$$

which concludes the proof. □

Then we can give the QECC constructed by QC code of type 1, and the expression of the code parameters.

Lemma 4. *With the above notation, assume that the polynomial $f(x)$ satisfies that $\gcd(\bar{f}(x) - \beta, x^n - 1) = 1$ for all non-zero $\beta \in F_q$ and $g^{\perp_e}(x) \mid g(x)$. Then the type 1 QC code $C = [2n, n -$*

$deg(g(x))]$ is symplectic self-orthogonal and the QECC with parameters $[[n, deg(g(x)), \geq d_{low1}]]$ can be constructed.

When it comes to QC codes with two generators, the analysis becomes a little more complex. However, when we have analyzed all cases, we can simplify the lower bound expression by combining the lower bound values that have the inclusion relationship. Furthermore, under the condition given in Table 1, the QC codes of types 2 and 3 are dual-containing codes. So the distance of the QECC constructed by symplectic construction can be low bounded by the lower bound of the original QC codes' distance.

Theorem 2. *Consider the QC code Q with generator matrix G:*

$$G = \begin{pmatrix} G_1 & G_1 \\ G_2 & G_{f2} \end{pmatrix} = \begin{pmatrix} [f(x)], & [f(x)] \\ [g(x)], & [g(x)h(x)] \end{pmatrix},$$

where we assume that $h(x)$ satisfies that $\gcd(h(x) - \beta, x^n - 1) = 1$ for all non-zero $\beta \in F_q$. Then, a lower bound on the symplectic weight of Q is the following value

$$\begin{aligned} d_{low2}(Q) = \min\{&d([f(x)]),\ d([\frac{x^n - 1}{\gcd(x^n - 1, h(x))}]),\ \frac{1}{q}d([h(x)g(x)]) + d([g(x)]), \\ &d([g(x)(h(x) - 1)]),\ \frac{1}{q}d([\gcd(f(x), g(x)h(x))]) + d([gcd(f(x), g(x))])\}. \end{aligned} \tag{4}$$

Proof. The idea of the proof is similar to that of Theorem 1, and the detailed proof procedure is given in Appendix A. □

Lemma 5. *With the above notation, assume that the polynomial $h(x)$ satisfies that $\gcd(h(x) - \beta, x^n - 1) = 1$ for all non-zero $\beta \in F_q$ and $g^{\perp_e}(x) \mid f(x)$, $\bar{h}(x) = h(x)$. Then the type 2 QC code $C = [2n, 2n - deg(g(x)) - deg(f(x))]$ is symplectic dual-containing linear code, and the QECC with parameters $[[n, n - deg(g(x)) - deg(f(x)), \geq d_{low2}]]_q$ can be constructed.*

As the generator form of the code in case 3 is identical to its symplectic dual code, we give the form of a lower bound on the symplectic distance of the original structure which can also apply to the symplectic dual code.

Theorem 3. *Consider the QC code Q with generator matrix G :*

$$G = \begin{pmatrix} G_{h1} & G_1 \\ G_2 & G_{h2} \end{pmatrix} = \begin{pmatrix} [h(x)g(x)], & [g(x)] \\ [f(x)], & [f(x)h(x)] \end{pmatrix},$$

where we assume that $g(x) \mid x^n - 1$, $f(x) \mid x^n - 1$ and $h(x)$ satisfies that $\gcd(h(x) - \beta, x^n - 1) = 1$ for all non-zero $\beta \in F_q$. Then, a lower bound on the symplectic weight of Q is the following value

$$\begin{aligned} d_{low3}(Q) = \min\{&d([\frac{x^n - 1}{\gcd(h(x), x^n - 1)}]),\ \frac{1}{q}d([f(x)h(x)]) + d([f(x)]),\ \frac{1}{q}d([g(x)h(x)]) + d([g(x)]), \\ &d([f(x)])d(h[x]),\ d(\gcd(g(x)h(x), \mathrm{lcm}(f(x), g(x)))), \\ &d([\mathrm{lcm}(f(x), \frac{g(x)}{\gcd(g(x), h(x))})]), d([\mathrm{lcm}(g(x), \frac{f(x)}{\gcd(f(x), h(x))})]), \\ &\frac{1}{q}(d([g(x)]) + d([\gcd(f(x), h(x)g(x))]) + (q-1)d([\gcd(g(x), f(x))])), \\ &\frac{1}{q}(d([f(x)]) + d([\gcd(g(x), h(x)f(x))]) + (q-1)d([\gcd(g(x), f(x))])), \\ &\frac{1}{q}(d([\gcd(g(x)h(x), f(x))]) + d([\gcd(g(x), f(x)h(x))]) + (q-1)d([\gcd(g(x), f(x))]))\}. \end{aligned}$$

Proof. The idea of the proof is similar to that of Theorem 1, and the detailed proof procedure is given in Appendix A. □

The paper [41] gives the parameters of QECC constructed by symplectic dual code QC and the condition for a QC to be a symplectic self-orthogonal code in type 3. Based on the symplectic self-orthogonal condition, and the lower bound on the symplectic distance given in this paper, combined with Lemma 3, we give QECCs with good parameters in the next section.

Lemma 6. *With the above notation, assume that the polynomial* $h(x)$ *satisfies that* $\gcd(h(x) - \beta, x^n - 1) = 1$ *for all non-zero* $\beta \in F_q$ *and* $f(x) \mid g^{\perp_e}(x)$, $\bar{h}(x) = h(x)$, $\gcd(g(x), f(x)) = 1$. *Then the type 3 QC code* $C = [2n, 2n - deg(g(x)) - deg(f(x))]$ *is symplectic dual-containing linear code and the quantum code with parameters* $[[n, n - deg(g(x)) - deg(f(x)), \geq d_{low3}]]_q$ *can be constructed.*

4. New QC Codes and QECCs

Similar to classical error-correcting theory, one of the core tasks of quantum error-correcting theory is to construct QECCs with good parameters. For a QECC with parameters $[[n, k, d]]_q$, when the code length n and dimension k are fixed, it is desirable to obtain a QECC with a larger minimum distance d. Similarly, when the minimum distance d is fixed, it is desirable to make the code rate k/n as large as possible. Some bounds are proposed to measure the merit of the parameters of QECCs, such as quantum Hamming bound [42,43], quantum Singleton bound [44,45], and quantum GV-bound [46,47]. Quantum codes that can achieve Singleton bound are called quantum MDS code. However, Huber and Grassl [48] in 2020 proved that there are no quantum MDS codes with length larger than $(q^2 + d - 2)$ over F_q. The QECCs that satisfy the GV-bound exist, so constructing QECCs beyond the GV-bound is a major research problem for scholars.

Lemma 7. *([45] Quantum GV bound)*

Suppose $n > k_{GV} \geq 2$, $n = k_{GV} \pmod 2$ *and* $d \geq 2$, *then there exist quantum codes with parameters* $[[n, k_{GV}, d]]_q$ *satisfying:*

$$\frac{q^{n-k_{GV}+2}-1}{q^2-1} \geq \sum_{i=1}^{d-1} (q^2-1)^{i-1} \binom{n}{i}.$$

Once the dimension k of a QECC is greater than k_{GV}, we consider that this quantum code is good. The work in this paper improves the lower bounds that can help to exclude bad results and reduce the computation power of finding new QC codes and QECCs with good parameters. To a certain extent, the search scope is trimmed to be the first to filter out the poor parameter cases, which helps to strengthen the overall grasp of the relationship between QECCs and classical codes. Based on the new distance lower bounds we gave, we give some QECCs that are nearly optimal using the algebra system Magma [49].

We provide some examples of good stabilizer QECCs coming from symplectic construction. Then, for the construction of type 1, we can have the following examples based on CRSS construction:

Example 1. *Let* $q = 2$ *and* $n = 63$. *We can obtain a symplectic dual-containing QC code* C *of length 126. The generator* $([g(x)], [g(x)f(x)])$ *of* C *is specified as:* $g(x) = x^{48} + x^{47} + x^{43} + x^{42} + x^{40} + x^{39} + x^{37} + x^{35} + x^{30} + x^{29} + x^{28} + x^{27} + x^{23} + x^{22} + x^{20} + x^{14} + x^{13} + x^{12} + x^{11} + x^8 + x^7 + x^6 + x^4 + 1$ *and* $f(x) = x^6 + x^5 + x^3 + x^2 + 1$. *The definition set of each polynomial does not intersect and, according to the lower bound given in Theorem 1, we can drive a new binary* $[[63, 48, 4]]_2$ *stabilizer quantum code.*

In addition, according to Grassl's code table [36], a code with parameters $[[63, 48, 4]]_2$ *is the best known binary linear code with length 63 and dimension 48.*

Example 2. *In the same code length as in Example 1, let* $g(x) = x^{42} + x^{41} + x^{39} + x^{38} + x^{37} + x^{32} + x^{31} + x^{30} + x^{29} + x^{24} + x^{19} + x^{17} + x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^3 + x^2 + x + 1$, *and* $f(x) = x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^7 + x^5 + 1$. *the cyclic code*

generated by $g(x)$ has parameter $[63, 21, 16]_2$. As $g^{\perp_e}(x) \mid g(x)$, the QC code of structure 1 is symplectic self-orthogonal.

The minimum symplectic weight of the symplectic dual quantum code is 6. Therefore, we obtain a binary quantum code with parameter $[[63, 42, 6]]_2$, which is superior to the best-known $[[63, 42, 5]]_2$ binary quantum code that appeared in [36]. Although the lower bound of the symplectic distance is not tight in this example, it reduces the computational cost required to obtain this good code.

For the construction of type 2, we can give an example that improves the record in Edel's table [50] and breaks the GV bound.

Example 3. *Let $q = 3$ and $n = 23$. Utilizing the cyclotomic cosets as defining sets of the generator polynomial, we have $g(x) = x^{11} + x^{10} + x^9 + 2x^8 + 2x^7 + x^5 + x^3 + 2$, $f(x) = x^{11} + x^{10} + x^9 + 2x^8 + 2x^7 + x^5 + x^3 + 2$, and $h(x) = 2x^{22} + x^{21} + 2x^{20} + 2x^{19} + 2x^{17} + x^{14} + 2x^{13} + 2x^{10} + x^9 + 2x^6 + 2x^4 + 2x^3 + x^2 + 2x$. Based on the polynomial given above, the QC code C_2 generated in type 2 is symplectic dual-containing code and we construct a QECC of length 23, dimension 1, accordingly. The value of our lower bound is 8 and the QEEC given by our construction is also 8. Although the dimension of this code is 1, our parameter also breaks the GV bound. The best-known QECC of the same length and dimension in Edel's code table is $[[23, 1, 5]]_3$, so our result improves the minimum distance in the code table.*

The following is an example constructed from type 3.

Example 4. *Let $q = 2$ and $n = 51$. The generator polynomials are in the following forms: $g(x) = x^8 + x^5 + x^4 + x^3 + 1$, $f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x + 1$, and $h(x) = x^{48} + x^{45} + x^{44} + x^{42} + x^{41} + x^{10} + x^9 + x^7 + x^6 + x^3$. The QC code generated by the above polynomials is symplectic dual-containing and has a minimum distance 5. The best distance for quantum codes of the same code length and dimension known from Grassl's code table is 4, so our result $[[51, 35, 5]]_2$ improves the code table.*

From this section, classical and quantum codes with better parameters are given for different types of proposed QC code structures. These examples reflect the significance of our work.

5. Conclusions

This paper investigates three classes of 1-QC and 2-QC codes, and determines the parameters of the QECCs constructed on them. We mainly focus on the minimum distance of the QECCs. As the calculation of the minimum distance of linear codes is NP-hard, we reduce the difficulty of searching for the optimal QECCs by calculating a lower bound of the symplectic distance of the QC codes. The lower bound is given to add constraints to the search for QECCs with good parameters, enabling early exclusion of bad results that occur during construction. In summary, our work can reduce computational power consumption and help to search for QECCs with good parameters. Finally, some examples of record-breaking or competitive binary QECCs are derived from the symplectic construction.

In the future, the structure of the 1-QC codes can be further investigated to calculate a general form of a lower bound on the symplectic distance under arbitrary indexes, which are useful for searching optimal codes. As mentioned in the introduction, QC codes are closely related to many LDPC codes and Turbo codes [51]. However, the characteristics of the QC codes used in the construction of LDPC are different from those utilized in this paper. Here we look for the relationship between the generator elements and the minimum code distance from the perspective of the QC code generator polynomial. The construction of quantum LDPC is carried out with the help of knowledge of matrix theory and graph theory in [16,30]. How to implement the construction concretely is an open and interesting question.

Author Contributions: Conceptualization, Y.L.; Methodology, C.G.; Writing—original draft, Y.L.; Writing—review & editing, Y.L.; Supervision, C.D. and Z.M.; Funding acquisition, Z.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work is contributed by the National Natural Science Foundation of China (Grants No.61972413,62002385) and the National Key R&D Program of China (No.2021YFB3100100).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of Open Access Journals
QC	Quasi-cyclic code
QECC	Quantum error correcting code

Appendix A

The proof for Theorem 2.

Proof. Consider the symplectic weight

$$w_s = w_s([a(x)f(x) + b(x)g(x)], [a(x)f(x) + b(x)g(x)h(x)]).$$

(1) If $a(x) = 0,\ b(x) \neq 0$ and $b(x)g(x)h(x) = 0$ which means $(x^n - 1) \mid b(x)g(x)h(x)$ then $w_s = w_H([b(x)g(x)])$. The cyclic code generated by $([b(x)g(x)])$ belongs to the cyclic code generated by $([\frac{x^n-1}{\gcd(h(x),x^n-1)}])$, so $w_s \geq d([\frac{x^n-1}{\gcd(h(x),x^n-1)}])$.

(2) If $a(x) = 0,\ b(x) \neq 0,\ b(x)g(x)h(x) \neq 0$, the $w_s = w_s([b(x)g(x)], [b(x)g(x)h(x)])$. According to the relation between symplectic and Hamming weights of vectors from Lemma 1 we have:

$$w_s = \frac{1}{q}(w_H([b(x)g(x)]) + w_H[(b(x)h(x)g(x)]) + \sum_{\beta \in F_q \setminus \{0\}} w_H([b(x)g(x)(\beta + h(x))])).$$

If $\deg(h(x)) < cw(b(x)g(x))$, we have:

$$\begin{aligned} w_s &= \frac{1}{q}(w_H(b(x)g(x)) + w_H(b(x)h(x)g(x)) + \sum_{\beta \in F_q \setminus \{0\}} w_H([b(x)g(x)])w_H([h(x) + \beta])) \\ &\geq \frac{1}{q}(d([g(x)]) + qd([b(x)g(x)]) - (q-1)) \\ &\geq \frac{1}{q}(d([g(x)])) + d([g(x)])d([h(x)]) - \frac{q-1}{q} \\ &\geq \frac{1}{q}(d([g(x)])) + d([g(x)])d([h(x)]). \end{aligned}$$

Else, the symplectic weight can be represented as:

$$\begin{aligned} w_s &\geq \frac{1}{q}(d([g(x)]) + d([h(x)g(x)]) + (q-1)d([g(x)])) \\ &\geq d([g(x)]) + d([h(x)g(x)])/q. \end{aligned} \tag{A1}$$

(3) Suppose $a(x) \neq 0,\ b(x) = 0$,
we have $w_s = w_s([a(x)f(x)], [a(x)f(x)]) = w_H([a(x)f(x)]) \geq d([f(x)])$.

(4) Suppose $a(x) \neq 0,\ b(x) \neq 0,\ b(x)g(x)h(x) = 0$, we can deduce that $\frac{x^n-1}{\gcd(x^n-1,h(x))} \mid b(x)g(x)$. The symplectic distance is $w_s = w_s([a(x)f(x) + b(x)g(x)], [a(x)f(x)])$.

$$w_s = \frac{1}{q}(w_H([a(x)f(x) + b(x)g(x)]) + w_H([a(x)f(x)]) + \sum_{\beta \in F_q \setminus \{0\}} w_H([(\beta+1)a(x)f(x) + \beta b(x)g(x)])). \tag{A2}$$

(i) If $x^n - 1 \mid a(x)f(x) + b(x)g(x)$, we have

$$w_s = \frac{1}{q}(w_H([-b(x)g(x)]) + \sum_{\beta \in F_q \setminus \{0\}} w_H([-b(x)g(x)])) = w_H([b(x)g(x)]) \geq d([\frac{x^n-1}{\gcd(x^n-1,h(x))}]).$$

(ii) If there exists a $\beta_0 \in F_q^*$ satisfying $x^n - 1 \mid (\beta_0+1)a(x)f(x) + \beta_0 b(x)g(x)$, then

$$w_s = \frac{1}{q}(w_H([b(x)g(x)]) + w_H([-\beta_0 b(x)g(x)]) + \sum_{\beta \in F_q \setminus \{0\}} w_H([(\beta-\beta_0)b(x)g(x)])) \geq w_H([b(x)g(x)]) \geq d([\frac{x^n-1}{\gcd(x^n-1,h(x))}]).$$

Else, if all summands in Equation (A2) are nonzero:

$$\begin{aligned} w_s &= \frac{1}{q}(w_H([a(x)f(x) + b(x)g(x)]) + w_H([a(x)f(x)]) \\ &\quad + \sum_{\beta \in F_q \setminus \{0,q-1\}} w_H([(\beta+1)a(x)f(x) + \beta b(x)g(x)]) + w_H([(q-1)b(x)g(x)])) \\ &\geq \frac{1}{q}(d([gcd(g(x),f(x))]) + d([f(x)]) + (q-2)d([gcd(f(x),g(x))]) + d([\frac{x^n-1}{\gcd(x^n-1,h(x))}])) \\ &= \frac{1}{q}((q-1)d([gcd(g(x),f(x))]) + d([f(x)]) + d([\frac{x^n-1}{\gcd(x^n-1,h(x))}])) \end{aligned}$$

(5) Suppose now that $a(x) \neq 0, b(x) \neq 0,\ b(x)g(x)h(x) \neq 0$,

$$w_s = \frac{1}{q}(w_H([a(x)f(x) + b(x)g(x)]) + w_H([a(x)f(x) + b(x)g(x)h(x)]) + \sum_{\beta \in F_q \setminus \{0\}} w_H([(\beta+1)a(x)f(x) + b(x)g(x)(\beta + h(x))])). \tag{A3}$$

In case the first summand in Equation (A3) is zero, we get

$$w_s = w_H([(h(x)-1)b(x)g(x)]) \geq d([g(x)(h(x)-1)]).$$

In case the second summand in Equation (A3) is zero, we get

$$w_s = \frac{1}{q}(w_H([a(x)f(x) + b(x)g(x)]) + \sum_{\beta \in F_q \setminus \{0\}} w_H([\beta(a(x)f(x) + b(x)g(x))])) \geq d([g(x)(h(x)-1))]).$$

If some summand of the summation in Equation (A3) is zero, then $(\beta_0+1)a(x)f(x) = -(h(x)+\beta_0)b(x)g(x)$ for a $\beta_0 \in F_q^*$. So we have $\mathrm{lcm}(f(x),g(x)) \mid b(x)g(x)$ as $h(x)+\beta$ is a unit. So

$$\begin{aligned} w_s &= \frac{1}{q}(w_H([a(x)f(x)+b(x)g(x)]) + w_H([a(x)f(x)+b(x)g(x)h(x)]) \\ &\quad + \sum_{\beta\in F_q\setminus\{0\}} w_H([(\beta+1)a(x)f(x)+b(x)g(x)(\beta+h(x))])) \\ &\geq \frac{1}{q}(w_H([(h(x)-1)b(x)g(x)]) + w_H([\beta_0(h(x)-1)b(x)g(x)]) \\ &\quad + \sum_{\beta\in F_q\setminus\{0\}} w_H([(\beta_0-\beta)(h(x)-1)b(x)g(x)])) \\ &\geq w_H([b(x)g(x)]) \ \geq d([\mathrm{lcm}(f(x),g(x))]). \end{aligned}$$

Otherwise,

$$\begin{aligned} w_s &= \frac{1}{q}(w_H([a(x)f(x)+b(x)g(x)]) + w_H([a(x)f(x)+b(x)g(x)h(x)]) \\ &\quad + \sum_{\beta\in F_q\setminus\{0\}} w_H([(\beta+1)a(x)f(x)+b(x)g(x)(\beta+h(x))]) + w_H([b(x)g(x)(q-1+h(x))])) \\ &\geq \frac{1}{q}(d([\gcd(f(x),g(x))]) + d([\gcd(f(x),g(x)h(x))]) + (q-2)d([\gcd(f(x),g(x))]) + d([g(x)])) \\ &\geq \frac{1}{q}((q-1)d([\gcd(f(x),g(x))]) + d([\gcd(f(x),g(x)h(x))]) + d([g(x)])) \\ &\geq \frac{1}{q}d([\gcd(f(x),g(x)h(x))]) + d([\gcd(f(x),g(x))]). \end{aligned}$$

Then we conclude the proof. □

The detailed proof for Theorem 3 is as following.

Proof. To obtain the lower bound of the symplectic weight of the QC code Q, we need to consider the codewords in the following form

$$w_s = w_s([a(x)h(x)g(x)+b(x)f(x)], [a(x)g(x)+b(x)f(x)h(x)]).$$

(1) If $a(x) = 0$, $b(x) \neq 0$ and $b(x)f(x)h(x) = 0$ which means $(x^n-1) \mid b(x)f(x)h(x)$ then $w_s = w_H([b(x)f(x)])$. The cyclic code generated by $[b(x)f(x)]$ belongs to the cyclic code generated by $[\frac{x^n-1}{\gcd(h(x),x^n-1)}]$, so $w_s \geq d([\frac{x^n-1}{\gcd(h(x),x^n-1)}])$.

(2) If $a(x) = 0$, $b(x) \neq 0$ and $b(x)f(x)h(x) \neq 0$, we have

$$w_s = w_s([b(x)f(x)], [b(x)f(x)h(x)])$$

If $deg(h(x)) < cw(b(x)f(x))$, then $w_H([b(x)f(x)h(x)]) = w_H([h(x)])w_H([b(x)f(x)])$. So the symplectic weight can be expressed as:

$$\begin{aligned} w_s &\geq \frac{1}{q}(w_H([b(x)f(x)]) + w_H([b(x)f(x)h(x)]) + \sum_{\beta\in F_q\setminus\{0\}} w_H(b(x)f(x)(\beta+h(x)))) \\ &\geq \frac{1}{q}(d([f(x)]) + d([f(x)])d([h(x)]) + (q-1)d([f(x)]) - d([f(x)])) \\ &= d([f(x)])d([h(x)]). \end{aligned}$$

Else,

$$\begin{aligned} w_s &\geq \frac{1}{q}(d([f(x)]) + d([f(x)h(x)]) + (q-1)d([f(x)])) \\ &= \frac{1}{q}d([f(x)h(x)]) + d([f(x)]). \end{aligned}$$

(3) If $a(x) \neq 0$, $b(x) = 0$ and $a(x)h(x)g(x) = 0$, similar to case (1) we have $w_s \geq d([\frac{x^n-1}{\gcd(h(x),x^n-1)}])$.

(4) If $a(x) \neq 0$, $b(x) = 0$ and $a(x)h(x)g(x) \neq 0$, the symplectic weight is represented as

$$\begin{aligned} w_s &= w_s([a(x)h(x)g(x)], [a(x)g(x)]) \\ &= w_s([a(x)g(x)], [a(x)h(x)g(x)]) \\ &\geq \frac{1}{q}d([g(x)h(x)]) + d([g(x)]). \end{aligned}$$

(5) Suppose now that $a(x) \neq 0, b(x) \neq 0$, $b(x)h(x)f(x) \neq 0$ $a(x)h(x)g(x) = 0$, then the symplectic weight is

$$\begin{aligned} w_s &= w_s([b(x)f(x)], [a(x)g(x) + b(x)f(x)h(x)]) \\ &= \frac{1}{q}(w_H([b(x)f(x)]) + w_H([a(x)g(x) + b(x)h(x)f(x)]) \\ &+ \sum_{\beta \in F_q \setminus \{0\}} w_H([(\beta + h(x))b(x)f(x) + a(x)g(x)])). \end{aligned} \tag{A4}$$

In case the second summand in Equation (A4) is zero, we get

$$w_s = w_H([b(x)f(x)])$$

and $[b(x)f(x)]$ belongs to the cyclic code generated by $[\frac{g(x)}{\gcd(g(x),h(x))}]$. So

$$w_s \geq d\Big([\mathrm{lcm}(f(x), \tfrac{g(x)}{\gcd(g(x),h(x))})]\Big).$$

If some summand of the summation in Equation (A4) is zero, then $[(\beta + h(x))b(x)f(x)] = -[a(x)g(x)]$ for some $\beta \in F_q^*$. This means that $\mathrm{lcm}(f(x), g(x)) \mid b(x)f(x)$ as $h(x) + \beta$ is a unit. So

$$w_s \geq w_H([b(x)f(x)]) \geq d(\mathrm{lcm}(f(x), g(x))).$$

Otherwise (all summands in Equation (A4) are nonzero)

$$w_s \geq \tfrac{1}{q}(d([f(x)]) + d([\gcd(g(x), h(x)f(x))]) + (q-1)d([\gcd(g(x), f(x))])).$$

(6) Suppose now that $a(x) \neq 0, b(x) \neq 0$, $b(x)h(x)f(x) = 0$ and $a(x)h(x)g(x) \neq 0$, then the lower bound of symplectic weight is similar to (5).

(7) Suppose now that $a(x) \neq 0, b(x) \neq 0$, $b(x)h(x)f(x) \neq 0$ and $a(x)h(x)g(x) \neq 0$, then the symplectic weight is

$$\begin{aligned} w_s &= w_s([a(x)g(x)h(x) + b(x)f(x)], [a(x)g(x) + b(x)f(x)h(x)]) \\ &= \frac{1}{q}(w_H([a(x)g(x)h(x) + b(x)f(x)]) + w_H([a(x)g(x) + b(x)h(x)f(x)]) \\ &+ \sum_{\beta \in F_q \setminus \{0\}} w_H([(\beta + h(x))b(x)f(x) + (\beta h(x) + 1)a(x)g(x)])). \end{aligned} \tag{A5}$$

In case the second summand in Equation (A5) is zero, then we can deduce $x^n - 1 \mid a(x)g(x) + b(x)f(x)h(x) \mid a(x)g(x)h(x) + b(x)f(x)h^2(x)$ and $\mathrm{lcm}(f(x), \frac{g(x)}{\gcd(g(x),h(x))}) \mid b(x)f(x)$. So

$$\begin{aligned} w_s &= w_H([a(x)g(x)h(x) + b(x)f(x)]) \\ &= w_H(b(x)f(x)(h^2(x) - 1)) \\ &\geq d([\mathrm{lcm}(f(x), \frac{g(x)}{\gcd(g(x), h(x))})]). \end{aligned}$$

The calculation process is the same if the first summand is zero: $w_s \geq d([\mathrm{lcm}(g(x), \frac{f(x)}{\gcd(f(x),h(x))})])$. If some summand of the summation in Equation (A5) is zero, then $[(\beta_0 + h(x))b(x)f(x)] = -[(\beta_0 h(x) + 1)a(x)g(x)]$ for some $\beta_0 \in F_q^*$. This means that $\mathrm{lcm}(f(x), g(x)) \mid b(x)f(x)$ as $h(x) + \beta$ is a unit. So

$$w_s \geq \frac{1}{q}(2d([\gcd(g(x)h(x), \mathrm{lcm}(f(x), g(x)))]) + (q-2)d([\gcd(g(x)h(x), \mathrm{lcm}(f(x), g(x)))])) \quad \text{(A6)}$$

$$\geq d(\gcd(g(x)h(x), \mathrm{lcm}(f(x), g(x)))) \quad \text{(A7)}$$

Otherwise (all summands in Equation (A5) are nonzero)

$$w_s \geq \frac{1}{q}(d([\gcd(g(x)h(x), f(x))]) + d([\gcd(g(x), f(x)h(x))]) + (q-1)d([\gcd(g(x), f(x))]))$$

which concludes the proof. □

References

1. Shor, P.W. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A* **1995**, *52*, R2493–R2496. [CrossRef]
2. Steane, A.M. Error correcting codes in quantum theory. *Phys. Rev. Lett.* **1996**, *77*, 793–797. [CrossRef] [PubMed]
3. Calderbank, A.R.; Rains, E.M.; Shor, P.W.; Sloane, N.J.A. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory* **1997**, *44*, 1369–1387. [CrossRef]
4. Rains, E. Nonbinary quantum codes. *IEEE Trans. Inf. Theory* **1999**, *45*, 1827–1832. [CrossRef]
5. Ketkar, A.; Klappenecker, A.; Kumar, S.; Sarvepalli, P. Nonbinary stabilizer codes over finite fields. *IEEE Trans. Inf. Theory* **2006**, *52*, 4892–4914. [CrossRef]
6. Nguyen, D.M.; Kim, S. New constructions of quantum stabilizer codes based on difference sets. *Symmetry* **2018**, *10*, 655. [CrossRef]
7. Pereira, F.R.F.; Mancini, S. Entanglement-assisted quantum codes from cyclic codes. *Entropy* **2022**, *25*, 37. [CrossRef]
8. Xing, L.; Li, Z. Some New Quantum BCH Codes over Finite Fields. *Entropy* **2021**, *23*, 712. [CrossRef] [PubMed]
9. Li, Z.; Xing, L. Universal framework for quantum error-correcting codes. *Entropy* **2021**, *23*, 937. [CrossRef] [PubMed]
10. Dinh, H.Q.; Le, H.T.; Nguyen, B.T.; Maneejuk, P. Some classes of new quantum MDS and synchronizable codes constructed from repeated-root cyclic codes of length $6p^s$. *IEEE Access* **2021**, *9*, 138543–138552. [CrossRef]
11. Shi, M.J.; Alahmadi, A.; Sole, P. Skew cyclic codes. In *Codes and Rings*; Academic Press: Cambridge, MA, USA, 2017; pp. 211–226.
12. Hsieh, M.H.; Brun, T.A.; Devetak, I. Quantum quasi-cyclic low-density parity-check codes. *arXiv* **2008**, arXiv:0803.0100.
13. Islam, H.; Prakash, O. Construction of LCD and new quantum codes from cyclic codes over a finite non-chain ring. *Cryptogr. Commun.* **2022**, *14*, 59–73. [CrossRef]
14. Kai, X.; Zhu, S.; Li, P. Constacyclic codes and some new quantum MDS codes. *IEEE Trans. Inf. Theory* **2014**, *60*, 2080–2086. [CrossRef]
15. Galindo, C.; Hernando, F.; Matsumoto, R. Quasi-cyclic constructions of quantum codes. *Finite Fields Their Appl.* **2018**, *52*, 261–280. [CrossRef]
16. Hagiwara, M.; Imai, H. Quantum quasi-cyclic LDPC codes. In Proceedings of the 2007 IEEE International Symposium on Information Theory, Nice, France, 24–29 June 2007; pp. 806–810.
17. Qian, J.; Ma, W.; Wang, X. Quantum error-correcting codes from quasi-cyclic codes. *Int. J. Quantum Inf.* **2008**, *6*, 1263–1269. [CrossRef]

18. Lally, K.; Fitzpatrick, P. Algebraic structure of quasi-cyclic codes. *Discret. Appl. Math.* **2001**, *111*, 157–175. [CrossRef]
19. Conan, J.M.; Séguin, G.E. Structural properties and enumeration of quasi-cyclic codes. *Appl. Algebra Eng. Commun. Comput.* **2005**, *4*, 25–39. [CrossRef]
20. Ling, S.; Solé, P. On the algebraic structure of quasi-cyclic codes I: Finite fields. *IEEE Trans. Inf. Theory* **2001**, *47*, 2751–2760. [CrossRef]
21. Aydin, N.; Ray-Chaudhuri, D.K. Quasi-cyclic codes over Z_4 and some new binary codes. *IEEE Trans. Inf. Theory* **2002**, *48*, 2065–2069. [CrossRef]
22. Conan, J.M.; Séguin, G.E. Algebraic properties of quasi-cyclic codes and their duals. In Proceedings of the 1991 IEEE International Symposium on Information Theory, Budapest, Hungary, 24–28 June 1991; p. 14.
23. Chen, E.Z. New quasi-cyclic codes from simplex codes. *IEEE Trans. Inf. Theory* **2007**, *53*, 1193–1196. [CrossRef]
24. Chen, E.Z.; Aydin, N. New quasi-twisted codes over $F_1$1—Minimum distance bounds and a new database. *J. Inf. Optim. Sci.* **2015**, *36*, 129–157. [CrossRef]
25. Kasami, T. A Gilbert-Varshamov bound for quasi-cycle codes of rate 1/2. *IEEE Trans. Inf. Theory* **1974**, *20*, 679. [CrossRef]
26. Siap, I.; Aydin, N.; Ray-Chaudhuri, D. New ternary quasi-cyclic codes with better minimum distances. *IEEE Trans. Inf. Theory* **2000**, *46*, 1554–1558. [CrossRef]
27. Daskalov, R.; Hristov, P. New binary one-generator quasi-cyclic codes. *IEEE Trans. Inf. Theory* **2003**, *49*, 3001–3005. [CrossRef]
28. Seguin, G. A class of 1-generator quasi-cyclic codes. *IEEE Trans. Inf. Theory* **2004**, *50*, 1745–1753. [CrossRef]
29. Ling, S.; Niederreiter, H.; Solé, P. On the algebraic structure of quasi-cyclic codes IV: Repeated roots. *Des. Codes Cryptogr.* **2006**, *38*, 337–361. [CrossRef]
30. Hagiwara, M.; Kasai, K.; Imai, H.; Sakaniwa, K. Spatially coupled quasi-cyclic quantum LDPC codes. In Proceedings of the 2011 IEEE International Symposium on Information Theory, St. Petersburg, Russia, 31 July–5 August 2011; pp. 638–642.
31. Sangwisut, E.; Jitman, S.; Udomkavanich, P. Constacyclic and quasi-twisted Hermitian self-dual codes over finite fields. *Adv. Math. Commun.* **2017**, *11*, 595–613. [CrossRef]
32. Aydin, N.; Connolly, N.; Murphree, J. New binary linear codes from quasi-cyclic codes and an augmentation algorithm. *Appl. Algebra Eng. Commun. Comput.* **2017**, *28*, 339–350. [CrossRef]
33. Ezerman, M.F.; Ling, S.; Özkaya, B.; Solé, P. Good stabilizer codes from quasi-cyclic codes over F_4 and F_9. In Proceedings of the 2019 IEEE International Symposium on Information Theory (ISIT), Paris, France, 7–12 July 2019; pp. 2898–2902.
34. Akre, D.; Aydin, N.; Harrington, M.J.; Pandey, S.R. New Binary and Ternary Quasi-Cyclic Codes with Good Properties. In Proceedings of the 2022 Virtual Joint Mathematics Meetings (JMM 2022), Virtual, 6–9 April 2022.
35. Vardy, A. The intractability of computing the minimum distance of a code. *IEEE Trans. Inf. Theory* **1997**, *43*, 1757–1766. [CrossRef]
36. Grassl, M. Bounds on the Minimum Distance of Linear Codes and Quantum Codes. 2007. Available online: http://www.codetables.de (accessed on 1 March 2023).
37. Ling, S.; Luo, J.; Xing, C. Generalization of Steane's enlargement construction of quantum codes and applications. *IEEE Trans. Inf. Theory* **2010**, *56*, 4080–4084. [CrossRef]
38. Luo, L.; Ma, Z. Non-binary quantum synchronizable codes from repeated-root cyclic codes. *IEEE Trans. Inf. Theory* **2018**, *64*, 1461–1470. [CrossRef]
39. Jingjie, L.; Ruihu, L.; Junli, W. New binary quantum codes derived from one-generator quasi-cyclic codes. *IEEE Access* **2019**, *7*, 85782–85785.
40. Jingjie, L.; Ruihu, L.; Junli, W. An explicit construction of quantum stabilizer codes from quasi-cyclic codes. *IEEE Commun. Lett.* **2020**, *24*, 1067–1071.
41. Guan, C.; Li, R.; Lu, L.; Yao, Y. New binary quantum codes constructed from quasi-cyclic codes. *Int. J. Theor. Phys.* **2022**, *61*, 172. [CrossRef]
42. Gottesman, D. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A* **1996**, *54*, 1862. [CrossRef]
43. Li, Z.; Xing, L. On a problem concerning the quantum Hamming bound for impure quantum codes. *IEEE Trans. Inf. Theory* **2010**, *56*, 4731–4734. [CrossRef]
44. Knill, E.; Laflamme, R. Theory of quantum error-correcting codes. *Phys. Rev. A* **1997**, *55*, 900–911. [CrossRef]
45. Grassl, M.; Huber, F.; Winter, A. Entropic proofs of Singleton bounds for quantum error-correcting codes. *IEEE Trans. Inf. Theory* **2022**, *68*, 3942–3950. [CrossRef]
46. Feng, K.; Ma, Z. A finite Gilbert-Varshamov bound for pure stabilizer quantum codes. *IEEE Trans. Inf. Theory* **2004**, *50*, 3323–3325. [CrossRef]
47. Ouyang, Y. Concatenated quantum codes can attain the quantum Gilbert–Varshamov bound. *IEEE Trans. Inf. Theory* **2014**, *60*, 3117–3122. [CrossRef]
48. Huber, F.; Grassl, M. Quantum codes of maximal distance and highly entangled subspaces. *Quantum* **2020**, *4*, 284. [CrossRef]
49. Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system I: The user language. *J. Symb. Comput.* **1997**, *24*, 235–265. [CrossRef]

50. Edel, Y. Some Good Quantum Twisted Codes. 2007. Available online: https://www.mathi.uni-heidelberg.de (accessed on 1 March 2023).
51. Tanner, R.M. Toward an algebraic theory for turbo codes. In Proceedings of the 2nd International Symposium on Turbo Codes, Brest, France, 4–7 September 2000.