mathematics

MDPI

Article

Lower Bound on the Minimum Distance of Single-Generator Quasi-Twisted Codes

Adel Alahmadi [1,*], Patrick Solé [2] and Ramy Taki Eldin [3,4]

[1] Math Department, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[2] I2M, (Aix Marseille Univ., CNRS, Centrale Marseille), 13009 Marseilles, France; sole@enst.fr
[3] Faculty of Engineering, Ain Shams University, Cairo 11517, Egypt; ramy.farouk@eng.asu.edu.eg
[4] Egypt University of Informatics, Knowledge City, New Administrative Capital, Cairo, Egypt
* Correspondence: analahmadi@kau.edu.sa

Abstract: We recall a classic lower bound on the minimum Hamming distance of constacyclic codes over finite fields, analogous to the well-known BCH bound for cyclic codes. This BCH-like bound serves as a foundation for proposing some minimum-distance lower bounds for single-generator quasi-twisted (QT) codes. Associating each QT code with a constacyclic code over an extension field, we obtain the first bound. This is the QT analogue to a result in the literature for quasi-cyclic codes. We point out some weaknesses in this bound and propose a novel bound that takes into account the Chinese remainder theorem approach to QT codes as well as the BCH bound of constacyclic codes. This proposed bound, in contrast to previous bounds in the literature, does not presuppose a specific form of code generator and does not require calculations in any extension field. We illustrate that our bound meets the one in the literature when the code generator adheres to the specific form assumed in that study. Various numerical examples enable us to compare and discuss these bounds.

Keywords: quasi-twisted codes; constacyclic codes; quasi-cyclic codes; BCH bound

MSC: 94B15; 94B65

check for updates

Citation: Alahmadi, A.; Solé, P.; Taki Eldin, R. Lower Bound on the Minimum Distance of Single-Generator Quasi-Twisted Codes. *Mathematics* **2023**, *11*, 2539. https://doi.org/10.3390/math11112539

Academic Editors: Sergey Bezzateev, Jiyou Li and Marjan Mernik

Received: 25 March 2023
Revised: 21 April 2023
Accepted: 23 May 2023
Published: 31 May 2023

1. Introduction

Due to their simple algebraic structures, cyclic codes over finite fields constitute one of the classes of linear codes that have attracted considerable attention in the literature. This has inspired researchers to explore more general classes of linear codes that have a similar structure. Generalizing the shift constant of cyclic codes introduces the class of constacyclic codes [1], and generalizing the shift index of cyclic codes introduces the class of quasi-cyclic (QC) codes [2]. Eventually, the class of quasi-twisted (QT) codes appeared to generalize QC and constacyclic codes. A λ-QT code of index ℓ is a linear code that is invariant under the λ-constacyclic shift of ℓ coordinates. In particular, a one-QT code is QC, while a λ-QT code of index $\ell = 1$ is λ-constacyclic.

Having a code with the largest minimum distance is beneficial for real-world communication systems, as the code's error-correction capability is proportional to its minimum distance. Databases such as [3] list codes with the best-known parameters. However, as pointed out by ref. [4], determining the minimum distance of a linear code is an NP-hard problem. As such, researchers have focused on providing lower and upper bounds to the minimum distance as an alternative. The Hartmann–Tzeng bound and the Bose–Chaudhuri–Hocquenghem (BCH) bound are two of the well-known lower bounds for cyclic codes. The BCH bound for cyclic codes was extended to constacyclic codes in [5,6]. Furthermore, Lally [7] studied a lower bound on the minimum distance of QC codes. Specifically, a cyclic code over some extension field was built, and its minimum distance was employed to determine a lower bound on the minimum distance of the given QC code. Therefore, to compute this bound, it is necessary to perform calculations in an extension field of the field over which the QC code is defined. Lower bounds for single-generator QT codes are presented in [5,8], where the code generator has a specific pattern. These bounds can also be calculated by employing the BCH bound for constacyclic codes.

This paper begins with a proof of the BCH bound for constacyclic codes. We prove this bound for completeness, as all subsequent bounds depend on it. Our study focuses on the lower bounds on the minimum distance of single-generator QT codes. We establish an analogous bound to Lally's result [7] for the QT code. Specifically, we associate a constacyclic code over an extension field to each QT code, and then we employ the BCH bound of constacyclic codes to determine a minimum-distance lower bound for the QT code. For general single-generator QT codes, some weaknesses, however, are notable for this bound. We propose an alternative lower bound to tackle this weakness. To this end, we implicitly utilize the Chinese remainder theorem (CRT) to decompose the QT code into a direct sum of minimal QT subcodes. The proposed bound employs this decomposition in conjunction with the BCH bound for constacyclic codes. We outline two advantages for the proposed bound: firstly, it does not presuppose any specific form for the code generator; secondly, all calculations are carried over the same field of the code alphabet, not an extension field.

We compare our proposed lower bound with those presented in [5,7,8] by analyzing several examples with various parameters. Although the lower bound proposed in [5] assumes a specific form for the code generator, we do not assume any specific form in our bound. We show that when the code generator has the designed form in [5], the two bounds coincide. This shows that the proposed bound generalizes that in [5]. Theorem III.2 in [8] presents another lower bound on the minimum distance of any single-generator QT code; however, we contradict this bound with Example 6 below.

The remainder of this paper is divided into the following sections: In Section 2, the algebraic structures of constacyclic and QT codes are reviewed. Section 3 presents the lower bound of single-generator QT codes, which mimics the work in [7] on QC codes. Section 4 provides the proposed bound in detail. Section 5 then examines the proposed bound on several numerical examples. Finally, the paper is concluded in Section 6.

2. Algebraic Structures of QT Codes

A **cyclic** code of length m over a finite field $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^m$ that is invariant under the **shift** transformation

$$(c_0, c_1, \ldots, c_{m-1}) \mapsto (c_{m-1}, c_0, c_1, \ldots, c_{m-2}).$$

Cyclic codes form a subclass of constacyclic codes. For a nonzero $\lambda \in \mathbb{F}_q$, a λ-**constacyclic** code over $\mathbb{F}_q$ of length m is a linear subspace of $\mathbb{F}_q^m$ that is invariant under the **constacyclic shift**

$$(c_0, c_1, \ldots, c_{m-1}) \mapsto (\lambda c_{m-1}, c_0, c_1, \ldots, c_{m-2}).$$

The polynomial representation to the codewords of constacyclic codes endows them with the algebraic structure of an ideal of a ring. Let $\mathcal{R} = \mathbb{F}_q[x]/\langle x^m - \lambda\rangle$ be the ring of all polynomials over $\mathbb{F}_q$ of degrees less than m, where the addition and multiplication are defined as modulo $x^m - \lambda$. The codeword $(c_0, c_1, \ldots, c_{m-1})$ of a λ-constacyclic code $\mathcal{C}$ is mapped to the polynomial $c_0 + c_1 x + \cdots + c_{m-1}x^{m-1}$ in $\mathcal{R}$. Hence, $\mathcal{C}$ is regarded as an ideal of $\mathcal{R}$. Conversely, any ideal of $\mathcal{R}$ corresponds to a constacyclic code. Throughout this paper, we refer to the λ-constacyclic code $\mathcal{C}$ over $\mathbb{F}_q$ of length m as an ideal of $\mathcal{R}$. We call λ the shift constant of $\mathcal{C}$. It follows that a cyclic code is constacyclic with a shift constant equal to unity.

By increasing the number of coordinates that must be shifted for the code to be invariant under this shifting, cyclic codes can be generalized to **quasi-cyclic** (QC) codes. A QC code over $\mathbb{F}_q$ of length n is a linear subspace of $\mathbb{F}_q^n$ that is invariant under the cyclic shift by ℓ coordinates. The length of a QC code is divisible by ℓ, that is, $n = m\ell$, where ℓ is the **index**, and m is the **co-index**. A typical QC codeword can be subdivided as

$$(c_{0,1}, c_{0,2}, \ldots, c_{0,\ell}, c_{1,1}, c_{1,2}, \ldots, c_{1,\ell}, \ldots, c_{m-1,1}, c_{m-1,2}, \ldots, c_{m-1,\ell}),$$

and represented as a polynomial vector $(c_1(x), c_2(x), \ldots, c_\ell(x))$, where $c_j(x) = \sum\limits_{i=0}^{m-1} c_{i,j}x^i$ for $1 \leq j \leq \ell$. In the polynomial representation, a QC code is an $\mathbb{F}_q[x]$ submodule of $\oplus_{j=1}^{\ell}\mathbb{F}_q[x]/\langle x^m - 1\rangle$. In turn, each $\mathbb{F}_q[x]$ submodule of $\oplus_{j=1}^{\ell}\mathbb{F}_q[x]/\langle x^m - 1\rangle$ corresponds to a QC code over the $\mathbb{F}_q$ of index ℓ and co-index m. It follows that a cyclic code is a QC of index $\ell = 1$.

Constacyclic codes are not a subclass of QC codes. Therefore, it is convenient to introduce the class of **quasi-twisted** (QT) codes, which generalizes both constacyclic and QC codes. For a nonzero $\lambda \in \mathbb{F}_q$, a λ-QT code $\mathcal{Q}$ over $\mathbb{F}_q$ of length $m\ell$, index ℓ, and co-index m is a linear subspace of $\mathbb{F}_q^{m\ell}$ that is invariant under the λ-constacyclic shift by ℓ coordinates. Again, we refer to λ as the shift constant of $\mathcal{Q}$. QT codes, as with QC codes, have a polynomial representation, which turns them into $\mathbb{F}_q[x]$-submodules of $\mathcal{R}^\ell$, where $\mathcal{R} = \mathbb{F}_q[x]/\langle x^m - \lambda\rangle$. Throughout this paper, we regard QT codes as submodules of $\mathcal{R}^\ell$. It follows that a constacyclic code is a QT of index $\ell = 1$, but a QC code is 1-QT. A QT code is said to be a single generator if there exists $\mathbf{g} = (g_1(x), g_2(x), \ldots, g_\ell(x)) \in \mathcal{R}^\ell$ such that $\mathcal{Q} = \mathbb{F}_q[x]\mathbf{g}$. For each $1 \leq j \leq \ell$, $g_j(x)$ is an element of $\mathcal{R}$. Nevertheless, in the sequel, we may mean that $g_j(x)$ is the equivalent polynomial of degree less than m in the polynomial ring $\mathbb{F}_q[x]$. This happens throughout the paper, and the reader should be able to identify to which polynomial we are referring, whether it belongs to $\mathcal{R}$ or $\mathbb{F}_q[x]$. For instance, to determine the greatest common divisor of some polynomials, denoted gcd, or the roots of a polynomial, it is beneficial to think of these polynomials as elements of the principal ideal domain $\mathbb{F}_q[x]$.

We conclude this section by summarizing some of the results in [7]. Suppose $\mathcal{Q}$ is a single-generator QC code over $\mathbf{F}_q$ of length $m\ell$ generated by $\mathbf{g} = (g_1(x), g_2(x), \ldots, g_\ell(x))$. In [7], $\mathcal{Q}$ is associated with a cyclic code $\mathcal{C}$ over $\mathbb{F}_{q^\ell}$ of length m as follows: Fix an element $\alpha \in \mathbb{F}_{q^\ell}$ of degree ℓ over $\mathbb{F}_q$. By viewing $g_j(x)$ as a polynomial in $\mathbb{F}_q[x]$, define $f(x) = \sum_{j=1}^{\ell} g_j(x)\alpha^{j-1}$, which is now considered an element of $\mathfrak{R} = \mathbb{F}_{q^\ell}[x]/\langle x^m - 1\rangle$. The ideal generated by $f(x)$ in $\mathfrak{R}$ is the cyclic code $\mathcal{C}$ associated with $\mathcal{Q}$. We can write $\mathcal{C} = \mathbb{F}_{q^\ell}[x]f(x)$; therefore, $\mathcal{C}$ is an $\mathbb{F}_{q^\ell}[x]$ submodule of $\mathfrak{R}$. On the other hand, $\mathfrak{R}$ can be thought of as an $\mathbb{F}_q[x]$ module. The codewords of $\mathcal{Q}$ are in one-to-one correspondence with the elements of the $\mathbb{F}_q[x]$ submodule of $\mathfrak{R}$ generated by $f(x)$. This correspondence given by $a(x)\mathbf{g} \mapsto a(x)f(x)$. It is shown in [7] that the dimension of $\mathcal{Q}$ as an $\mathbb{F}_q$-vector space is

$$k = m - \deg\Big(\gcd_{1\leq j\leq \ell}\{g_j(x)\}\Big).$$

Furthermore, a lower bound on the minimum Hamming distance $d(\mathcal{Q})$ of $\mathcal{Q}$ is given by

$$d(\mathcal{Q}) \geq d(\mathcal{C})d(\mathcal{B}),$$

where $\mathcal{B}$ is the linear code over $\mathbb{F}_q$ of length ℓ generated by the vector equivalent of the coefficients of $f(x)$ with respect to the $\mathbb{F}_q$ basis $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\right\}$ of $\mathbb{F}_{q^\ell}$. In the next section, we generalize this result from QC codes to QT codes.

3. Constacyclic and QT Codes Bound

The objective of this section is to provide the expected generalization of the result in [7] for single-generator QT codes. It seems reasonable that the equivalent bound of QT codes would require a BCH bound for constacyclic codes, because the bound of QC codes requires a BCH bound for cyclic codes. In fact, the BCH bound for constacyclic codes is essential to all lower bounds that we present in this paper as well as for use in our generalization of [7]. As a result, we begin this section with a simple proof of this BCH bound for the convenience of the reader.

Let $\mathcal{C}$ be a λ-constacyclic code over $\mathbb{F}_q$ of length m, which is regarded as an ideal in the quotient ring $\mathcal{R} = \mathbb{F}_q[x]/\langle x^m - \lambda\rangle$. Because $\mathcal{R}$ is a principal ideal ring, there is a generator polynomial $g(x) \in \mathcal{R}$, such that $\mathcal{C} = \mathbb{F}_q[x]g(x) = \langle g(x)\rangle$. Instead of introducing some notations to differentiate between polynomials in $\mathbb{F}_q[x]$ and their images in $\mathcal{R}$, we leave it up to the reader to determine our meaning. Hence, the generator polynomial of $\mathcal{C}$ as an element of $\mathbb{F}_q[x]$, which we also denote by $g(x)$, is defined as the unique monic codeword of $\mathcal{C}$ of a minimum degree. It is noted that $g(x)$ divides $x^m - \lambda$. Suppose that $\mathcal{C}_1$ and $\mathcal{C}_2$ are λ-constacyclic codes with generator polynomials $g_1(x)$ and $g_2(x)$, respectively. Accordingly, $\mathcal{C}_1 + \mathcal{C}_2$ is a λ-constacyclic code with the generator polynomial $\gcd\{g_1(x), g_2(x)\}$, which is the greatest common divisor of $g_1(x)$ and $g_2(x)$ in $\mathbb{F}_q[x]$. In general, let $\{\mathcal{C}_t\}$, $t \in \mathcal{I}$, be a collection of λ-constacyclic codes indexed by a set $\mathcal{I}$, and let $g_t(x)$ be the generator polynomial of $\mathcal{C}_t$ for each $t \in \mathcal{I}$. Then, $\gcd_{t\in\mathcal{I}}\{g_t(x)\}$ is the generator polynomial of $\sum_{t\in\mathcal{I}} \mathcal{C}_t$.

Lemma 1. *Let $\{g_t(x)\}$ be a collection of elements of $\mathcal{R}$ indexed by a set $\mathcal{I}$. Then, $\langle g(x)\rangle \subseteq \mathcal{R}$ is the smallest λ-constacyclic code that contains $\{g_t(x)\}_{t\in\mathcal{I}}$, where*

$$g(x) = \gcd_{t\in\mathcal{I}}\{g_t(x)\}.$$

Proof. Let $\mathcal{C} \subseteq \mathcal{R}$ be any λ-constacyclic code that contains $\{g_t(x)\}_{t\in\mathcal{I}}$. Then $\langle g_t(x)\rangle \subseteq \mathcal{C}$ for each $t \in \mathcal{I}$. Consequently, $\langle g(x)\rangle = \sum_{t\in\mathcal{I}}\langle g_t(x)\rangle \subseteq \mathcal{C}$. On the other hand, $\langle g(x)\rangle$ is a λ-constacyclic code. As a result, it is the smallest code that contains $\{g_t(x)\}_{t\in\mathcal{I}}$. □

Recall that the BCH bound on the minimum distance of a cyclic code of length m necessitates the determination of the mth roots of unity in some extension field of $\mathbb{F}_q$. Similarly, finding the m zeros of $x^m - \lambda$ in an extension field $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$ is required to determine the BCH bound on the minimum distance of a λ-constacyclic code of length m. Specifically, assume m and q are coprime, the multiplicative order of λ is r, and the multiplicative order of q modulo mr is e. Then, the splitting field of $x^m - \lambda$ is $\mathbb{F}_{q^e}$. The m zeros of $x^m - \lambda$ are precisely $\{\beta\gamma^i | 0 \le i \le m-1\}$, where β and γ are the mth roots of λ and unity, respectively, in $\mathbb{F}_{q^e}$. In other words, if ζ is a primitive element of $\mathbb{F}_{q^e}$ and $\lambda = \zeta^{(q^e-1)l/r}$ for some integer l, then the zeros of $x^m - \lambda$ are

$$\left\{\zeta^{\frac{q^e-1}{m}\left(\frac{l}{r}+i\right)} \middle| 0 \le i \le m-1\right\}.$$

Definition 1. *Suppose m and q are coprime. Let $g(x)$ denote the generator polynomial of a λ-constacyclic code over $\mathbb{F}_q$ of length m. Furthermore, let β and γ be the mth roots of λ and unity, respectively, in $\mathbb{F}_{q^e}$. Define $\eta(g(x)) = \delta$, where δ is the largest positive integer such that*

$$g\left(\beta\gamma^b\right) = g\left(\beta\gamma^{b+1}\right) = g\left(\beta\gamma^{b+2}\right) = \cdots = g\left(\beta\gamma^{b+\delta-2}\right) = 0$$

for some integer $0 \le b \le m-1$. If $g\left(\beta\gamma^b\right) \neq 0$ for all $0 \le b \le m-1$, define $\eta(g(x)) = 1$.

It is important to select the integer b of Definition 1 with care in order to maximize the number of consecutive mth roots of λ that are zeros of $g(x)$, as this can lead to a better lower bound on the minimum distance; this is shown in the following theorem. The following theorem presents a BCH-like bound for constacyclic codes. The proof, utilizing elementary linear algebra techniques, can be found in [6].

Theorem 1. *Suppose m and q are coprime. Let $\mathcal{C}$ be a λ-constacyclic code over $\mathbb{F}_q$ of length m with generator polynomial $g(x)$. Then, the minimum distance $d(\mathcal{C})$ of $\mathcal{C}$ is at least $\eta(g(x))$.*

We are now ready to imitate Lally's work [7] in order to give a lower bound for QT codes. Let $\mathcal{Q}$ be a single-generator λ-QT code over $\mathbb{F}_q$ of length $m\ell$ and index ℓ. Suppose that $\mathcal{Q} = \mathbb{F}_q[x]\mathbf{g}$, where $\mathbf{g} = (g_1(x), g_2(x), \ldots, g_\ell(x)) \in \mathcal{R}^\ell$ is a generator of $\mathcal{Q}$. Fix an element α of degree ℓ over $\mathbb{F}_q$; hence, $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}\right\}$ is a basis of $\mathbb{F}_{q^\ell}$ as a vector space over $\mathbb{F}_q$. Define $f(x) = \sum_{j=1}^{\ell} g_j(x)\alpha^{j-1}$ as an element of $\mathfrak{R} = \mathbb{F}_{q^\ell}[x]/\langle x^m - \lambda\rangle$. This polynomial generates an ideal of $\mathfrak{R}$ that is a λ-constacyclic code over $\mathbb{F}_{q^\ell}$ of length m, which we denote by $\widetilde{\mathcal{C}}$. Each codeword $\mathbf{c} = (c_1(x), c_2(x), \ldots, c_\ell(x)) \in \mathcal{Q}$ is linked with the codeword $\sum_{j=1}^{\ell} c_j(x)\alpha^{j-1} \in \widetilde{\mathcal{C}}$. A lower bound on the minimum distance of $\widetilde{\mathcal{C}}$ can be found with Theorem 1, which may be utilized to establish a lower bound on the minimum distance of $\mathcal{Q}$ (cf. Theorem 3 in [7]). The result is precisely as follows:

Theorem 2. *Let $\mathcal{Q}$ be a λ-QT code over $\mathbb{F}_q$ of index ℓ and co-index m, generated by $\mathbf{g} = (g_1(x), g_2(x), \ldots, g_\ell(x)) \in \mathcal{R}^\ell$. Let $f(x) = \sum_{j=1}^{\ell} g_j(x)\alpha^{j-1} = f_0 + f_1 x + \cdots + f_{m-1}x^{m-1} \in \mathfrak{R}$; and let $\widetilde{\mathcal{C}}$ denote the λ-constacyclic code over $\mathbb{F}_{q^\ell}$ of length m generated by $f(x)$. Let $\mathcal{B}$ be the linear code over $\mathbb{F}_q$ of length ℓ generated by the vectors equivalent to the coefficients $f_0, f_1, \ldots, f_{m-1} \in \mathbb{F}_{q^\ell}$ with respect to the basis $\left\{1, \alpha, \ldots, \alpha^{\ell-1}\right\}$ of $\mathbb{F}_{q^\ell}$. Then,*

$$d(\mathcal{Q}) \geq d(\widetilde{\mathcal{C}})d(\mathcal{B}).$$

Proof. Assume that $\mathbf{c} = (c_1(x), c_2(x), \ldots, c_\ell(x)) \in \mathcal{Q}$ is an arbitrary nonzero codeword, where $c_j(x) = \sum_{i=0}^{m-1} c_{i,j}x^i$ and $c_{i,j} \in \mathbb{F}_q$. Then, $\sum_{j=1}^{\ell} c_j(x)\alpha^{j-1} \in \widetilde{\mathcal{C}}$. This can be rearranged as $\sum_{j=1}^{\ell} c_j(x)\alpha^{j-1} = \sum_{j=1}^{\ell}\sum_{i=0}^{m-1} c_{i,j}x^i\alpha^{j-1} = \sum_{i=0}^{m-1}\left(\sum_{j=1}^{\ell} c_{i,j}\alpha^{j-1}\right)x^i = \sum_{i=0}^{m-1} c_i(\alpha)x^i$, where $c_i(\alpha) = \sum_{j=1}^{\ell} c_{i,j}\alpha^{j-1}$. Because the latter is a codeword of $\widetilde{\mathcal{C}}$, the number of nonzero $c_i(\alpha)$ for $0 \leq i \leq m-1$ is at least $d(\widetilde{\mathcal{C}})$. There is also a polynomial $a(x) \in \mathbb{F}_q[x]$, such that $\sum_{i=0}^{m-1} c_i(\alpha)x^i = \sum_{j=1}^{\ell} c_j(x)\alpha^{j-1} = \sum_{j=1}^{\ell} a(x)g_j(x)\alpha^{j-1} = a(x)f(x) = a(x)\big(f_0 + f_1x + \cdots + f_{m-1}x^{m-1}\big)$. This means that each $c_i(\alpha)$ is an $\mathbb{F}_q$-linear combination of $f_0, f_1, \ldots, f_{m-1}$. Therefore, $(c_{i,1}, c_{i,2}, \ldots, c_{i,\ell}) \in \mathcal{B}$ for every $0 \leq i \leq m-1$. The result follows, because for every nonzero $c_i(\alpha)$, we have $\mathrm{wt}(c_i(\alpha)) \geq d(\mathcal{B})$. □

The dimension of the QT code described in Theorem 2 can be determined using the following theorem, the proof of which is nearly identical to that of Theorem 2 in [7].

Theorem 3. *Suppose $\mathcal{Q}$ is a λ-QT code over $\mathbb{F}_q$ of index ℓ and co-index m generated by $\mathbf{g} = (g_1(x), g_2(x), \ldots, g_\ell(x))$. The dimension of $\mathcal{Q}$ as an $\mathbb{F}_q$-vector space is*

$$k = m - \deg(\gcd\{x^m - \lambda, g_1(x), g_2(x), \ldots, g_\ell(x)\}).$$

Example 1. *Consider the single-generator* 2*-QT code $\mathcal{Q}$ over $\mathbb{F}_3$ of index $\ell = 4$, co-index $m = 7$, and generator*

$$\mathbf{g} = \left(x^4 + x^3 + 2x^2 + 1, x^4 + 2x^3 + 2x^2 + 2x + 1, x^3 + 2x, x^4 + 2x^3 + 2x^2 + 2x + 1\right).$$

In $\mathbb{F}_3[x]$, $\gcd\{x^7 - 2, g_1(x), \ldots, g_4(x)\} = x - 2$. Theorem 3 states that the dimension of $\mathcal{Q}$ is 6*. Let α denote a zero of the primitive polynomial $x^4 + 2x^3 + 2 \in \mathbb{F}_3[x]$. The* 2*-constacyclic code $\widetilde{\mathcal{C}}$ described in Theorem 2 is generated by $f(x) = \sum_{j=1}^{4} g_j(x)\alpha^{j-1} = (\alpha^3 + \alpha + 1)x^4 + (2\alpha^3 + \alpha^2 + 2\alpha + 1)x^3 + (2\alpha^3 + 2\alpha + 2)x^2 + (2\alpha^3 + 2\alpha^2 + 2\alpha)x + \alpha^3 + \alpha + 1$. We employ Theorem 1 to determine a lower bound to $d(\widetilde{\mathcal{C}})$. In fact, the splitting field of $x^7 - 2$ is $\mathbb{F}_{3^{12}}$. If ζ is a zero of the primitive polynomial $x^{12} + x^6 + x^5 + x^4 + x^2 + 1 \in \mathbb{F}_3[x]$, then $\alpha = \zeta^{\frac{3^{12}-1}{3^4-1}}$. We set $\beta = \zeta^{\frac{3^{12}-1}{14}}$ and $\gamma = \zeta^{\frac{3^{12}-1}{7}}$, which are the* 7*th root of* 2 *and unity, respectively. Observe that $\{\beta\gamma, \beta\gamma^2, \beta\gamma^3, \beta\gamma^6\}$ are the zeros of $f(x)$. By Definition 1, $\eta(f(x)) = 4$. It follows from*

Theorem 1 that $d(\widetilde{\mathcal{C}}) \geq 4$. The generator matrix of the code $\mathcal{B}$ over $\mathbb{F}_3$ of length $\ell = 4$ described in Theorem 2 is

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 2 & 1 & 2 & 1 \\ 2 & 0 & 2 & 2 \\ 2 & 2 & 2 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

We find that $d(\mathcal{B}) = 2$; hence, $d(\mathcal{Q}) \geq 8$. The exact minimum distance of $\mathcal{Q}$ is found to be $d(\mathcal{Q}) = 13$.

In Example 1, the polynomial $f(x)$ has a degree of 4, and all of its zeros are zeros of $x^m - \lambda$. Thus, $f(x)$ divides $x^m - \lambda$. In this situation, we observe that Theorem 2 yields an acceptable bound. However, when $f(x)$ does not divide $x^m - \lambda$, we observe that the lower bound provided by Theorem 2 is a weak bound in most cases. We show this with the following example, which employs a randomly generated QT code.

Example 2. *We examine a single-generator ω-QT code $\mathcal{Q}$ over $\mathbb{F}_4$ of index $\ell = 6$, co-index $m = 5$, where ω is a zero of $x^2 + x + 1 \in \mathbb{F}_2[x]$. We randomly construct $\mathbf{g}$ which is described by the starting values $g_0 = 0, g_1 = 1, g_2 = \omega, g_3 = \omega^2$ and the linear recurrence relation $g_i = g_{i-1} + \omega g_{i-2} + \omega g_{i-3} + \omega g_{i-4}$ for $i = 4, 5, \ldots, 29$. This results in*

$$\mathbf{g} = \Big(0,1,\omega,\omega^2,\omega,\omega,\omega^2,\omega,\omega^2,\omega,1,0,0,1,\omega^2,1,\omega,\omega^2,\omega^2,\omega^2,0,1,1,\omega,\omega,1,\omega^2,1,1,0\Big)$$

whose polynomial representation is as follows

$$\mathbf{g} = \Big(\omega x(x^3 + \omega x^2 + x + \omega^2), \omega(x^4 + \omega x^3 + x^2 + \omega x + 1), \omega^2(x^2 + x + \omega)(x^2 + \omega^2 x + 1),$$
$$\omega^2(x+1)(x+\omega^2)(x^2 + \omega^2 x + \omega^2), \omega x(x+1)(x+\omega)^2, (x+\omega^2)(x^2 + \omega x + \omega)\Big).$$

Let α denote a zero of $x^6 + x^5 + \omega x^4 + \omega^2 x^3 + x^2 + x + \omega \in \mathbb{F}_4[x]$. The ω-constacyclic code $\widetilde{\mathcal{C}}$ described in Theorem 2 is generated by $f(x) = \sum_{j=1}^{\ell} g_j(x)\alpha^{j-1} = (\omega\alpha^4 + \omega^2\alpha^3 + \omega^2\alpha^2 + \omega\alpha + \omega)x^4 + (\alpha^5 + \omega\alpha^4 + \omega^2\alpha^3 + \alpha^2 + \omega^2\alpha + \omega^2)x^3 + (\alpha^5 + \alpha^4 + \omega^2\alpha^3 + \omega\alpha + \omega)x^2 + (\omega^2\alpha^5 + \alpha^4 + \omega\alpha^3 + \omega^2\alpha + 1)x + \alpha^5 + \alpha^3 + \alpha^2 + \omega\alpha$. It is only necessary to observe that $f(x)$ is coprime to $x^5 - \omega$. Then, $\widetilde{\mathcal{C}} = \mathbb{F}_{4^6}^5$; hence, $d(\widetilde{\mathcal{C}}) = 1$. The generator matrix of code $\mathcal{B}$ over $\mathbb{F}_4$ of length $\ell = 6$ described in Theorem 2 is

$$\begin{pmatrix} 0 & \omega & \omega^2 & \omega^2 & \omega & \omega \\ 1 & \omega & \omega^2 & 1 & \omega^2 & \omega^2 \\ 1 & 1 & \omega^2 & 0 & \omega & \omega \\ \omega^2 & 1 & \omega & 0 & \omega^2 & 1 \\ 1 & 0 & 1 & 1 & \omega & 0 \end{pmatrix}.$$

We find that $d(\mathcal{B}) = 2$; hence, $d(\mathcal{Q}) \geq 2$. The exact minimum distance of $\mathcal{Q}$ is found to be $d(\mathcal{Q}) = 17$.

Example 2 explores one of the weaknesses of Theorem 2. The other disadvantages of using Theorem 2 are that it requires calculations over an extension field as well as determining the exact minimum distance of $\mathcal{B}$, which is generally NP-hard. In response to these weaknesses, we propose a novel lower bound on the minimum distance of single-generator QT codes in the next section.

4. Novel Bound to QT Codes

We expect the lower bound given in Theorem 2 to be far from the exact minimum distance for a general single-generator QT code. This is demonstrated in Example 2, especially when the polynomial $f(x)$, as an element of $\mathbb{F}_{q^\ell}[x]$, is coprime to $x^m - \lambda$. In effect, this results in $d(\widetilde{\mathcal{C}}) = 1$ and, hence, $d(\mathcal{Q}) \geq d(\mathcal{B})$. In this section, we deal with this problem by establishing a completely new lower bound for single-generator QT codes. We apply the CRT to decompose any single-generator QT code before employing Theorem 1 at each polynomial coordinate. Throughout this section, $\mathcal{Q}$ denotes a single-generator QT code over $\mathbb{F}_q$ of index ℓ and co-index m, where m and q are coprime. Suppose

$$\mathbf{g} = (g_1(x), g_2(x), \ldots, g_\ell(x)) \in \mathcal{R}^\ell$$

is a generator of $\mathcal{Q}$, where $\mathcal{R} = \mathbb{F}_q[x]/\langle x^m - \lambda\rangle$. Then, $\mathcal{Q} = \langle \mathbf{g}\rangle$, which is the cyclic $\mathbb{F}_q[x]$ submodule of $\mathcal{R}^\ell$ generated by $\mathbf{g}$. Because m and q are coprime, $x^m - \lambda = \prod_{t=1}^{s} p_t(x)$, where $p_1(x), p_2(x), \ldots, p_s(x)$ are distinct irreducible polynomials in $\mathbb{F}_q[x]$. Now, we define $\mathcal{Q}_t = \langle \mathbf{g}_t\rangle$ for each $1 \leq t \leq s$, where

$$\mathbf{g}_t = \left(\frac{x^m - \lambda}{p_t(x)}\right)\mathbf{g} = \left(\frac{x^m - \lambda}{p_t(x)}\right)(g_1(x), g_2(x), \ldots, g_\ell(x)) \in \mathcal{R}^\ell. \tag{1}$$

Clearly, $\mathcal{Q}_t$ is a single-generator QT code annihilated by $p_t(x)$. Then, $\mathcal{Q}_t$ is a minimal QT subcode of $\mathcal{Q}$ because $\mathbf{g}_t \in \mathcal{Q}$. To exclude constituents $\mathcal{Q}_t$, which are not involved in the construction of $\mathcal{Q}$, we define the set $X = \{1 \leq t \leq s \mid \mathbf{g}_t \neq \mathbf{0}\}$, or, equivalently, using (1), we have the following alternative definition:

$$X = \{1 \leq t \leq s \mid p_t(x) \nmid \mathrm{Ent}_j(\mathbf{g}) \text{ for at least one } 1 \leq j \leq \ell\}. \tag{2}$$

The following result shows that $\mathcal{Q}$ can be decomposed to the direct sum of the minimal QT subcodes $\mathcal{Q}_t$ through employing the CRT implicitly.

Lemma 2. *With the above notation,* $\mathcal{Q} = \oplus_{t\in X}\mathcal{Q}_t$.

Proof. Because $\mathcal{Q}_t \subseteq \mathcal{Q}$ for every $t \in X$, $\sum_{t\in X}\mathcal{Q}_t \subseteq \mathcal{Q}$. Because $\gcd_{1\leq t\leq s}\left\{\frac{x^m-\lambda}{p_t(x)}\right\} = 1$ in $\mathbb{F}_q[x]$, there are polynomials $a_t(x) \in \mathbb{F}_q[x]$ such that $\sum_{1\leq t\leq s} a_t(x)\left(\frac{x^m-\lambda}{p_t(x)}\right) = 1$. Consequently,

$$\mathbf{g} = \sum_{1\leq t\leq s} a_t(x)\left(\frac{x^m - \lambda}{p_t(x)}\right)\mathbf{g} = \sum_{1\leq t\leq s} a_t(x)\mathbf{g}_t = \sum_{t\in X} a_t(x)\mathbf{g}_t \in \sum_{t\in X}\mathcal{Q}_t.$$

Accordingly, $\mathcal{Q} \subseteq \sum_{t\in X}\mathcal{Q}_t$; therefore, $\mathcal{Q} = \sum_{t\in X}\mathcal{Q}_t$. Now suppose that $\sum_{t\in X} b_t(x)\mathbf{g}_t = \mathbf{0}$, then

$$\mathbf{0} = \sum_{t\in X} b_t(x)\left(\frac{x^m - \lambda}{p_t(x)}\right)\mathbf{g} = \left(\sum_{t\in X} b_t(x)\frac{x^m - \lambda}{p_t(x)}\right)\mathbf{g}.$$

Then, $\sum_{t\in X} b_t(x)\frac{x^m-\lambda}{p_t(x)}$ annihilates $\mathcal{Q}$. However, $\mathcal{Q}$ is annihilated by $\prod_{t\in X} p_t(x)$; then, $\prod_{t\in X} p_t(x) | \sum_{t\in X} b_t(x)\frac{x^m-\lambda}{p_t(x)}$. For every arbitrary $\tau \in X$, $p_\tau(x) | \sum_{t\in X} b_t(x)\frac{x^m-\lambda}{p_t(x)} = b_\tau(x)\frac{x^m-\lambda}{p_\tau(x)} + \sum_{t\in X, t\neq\tau} b_t(x)\frac{x^m-\lambda}{p_t(x)}$. Because $p_\tau(x) | \sum_{t\in X, t\neq\tau} b_t(x)\frac{x^m-\lambda}{p_t(x)}$, we infer that $p_\tau(x) | b_\tau(x)\frac{x^m-\lambda}{p_\tau(x)}$, so $p_\tau(x) | b_\tau(x)$. Therefore, $b_\tau(x)\mathbf{g}_\tau = \mathbf{0}$ for every $\tau \in X$, and we conclude that $\mathcal{Q} = \oplus_{t\in X}\mathcal{Q}_t$. □

Recall that the power set of X is the set of all subsets of X. We denote the power set of X after excluding the empty set by $\mathcal{P}(X)$. That is, $\mathcal{P}(X)$ is the set of all nonempty subsets of X. We now prove that every nonzero codeword of $\mathcal{Q}$ corresponds to a unique element of $\mathcal{P}(X)$.

Lemma 3. *For each nonzero* $\mathbf{c}(x) \in \mathcal{Q}$*, there exist a unique* $\mathcal{I} \in \mathcal{P}(X)$ *and nonzero polynomials* $a_t(x) \in \mathbb{F}_q[x]$ *(for* $t \in \mathcal{I}$*) such that* $\mathbf{c}(x) = \sum_{t\in\mathcal{I}} a_t(x)\mathbf{g}_t$*.*

Proof. From Lemma 2, $\mathbf{c}(x) \in \mathcal{Q} = \sum_{t\in X} \mathcal{Q}_t = \sum_{t\in X}\langle \mathbf{g}_t\rangle$. Thus, we have $\mathbf{c}(x) = \sum_{t\in X} a_t(x)\mathbf{g}_t$ for some $a_t(x) \in \mathbb{F}_q[x]$. The result is achieved by defining

$$\mathcal{I} = \{t \in X \mid a_t(x) \neq 0\}.$$

□

The following definition attempts to avoid the zero coordinates for each $\mathcal{I} \in \mathcal{P}(X)$. This is achieved by defining the set

$$\mathcal{J}(\mathcal{I}) = \{1 \leq j \leq \ell \mid \mathrm{Ent}_j(\mathbf{g}_t) \neq 0 \text{ for at least one } t \in \mathcal{I}\},$$

where $\mathrm{Ent}_j(\mathbf{g}_t) \in \mathcal{R}$ denotes the jth entry of $\mathbf{g}_t$, or, equivalently, using (1), we have the following alternative definition:

Definition 2. *For each* $\mathcal{I} \in \mathcal{P}(X)$*, define*

$$\mathcal{J}(\mathcal{I}) = \{1 \leq j \leq \ell \mid p_t(x) \nmid \mathrm{Ent}_j(\mathbf{g}) \text{ for at least one } t \in \mathcal{I}\}.$$

In other words, if $\mathcal{I}$ is the associated element in $\mathcal{P}(X)$ with the codeword $\mathbf{c}(x) \in \mathcal{Q}$, as shown by Lemma 3, then $\mathcal{J}(\mathcal{I})$ keeps a record of the nonzero coordinates of $\mathbf{c}(x)$. The following result gives a lower bound on the weight $\mathrm{wt}(\mathbf{c}(x))$ of any codeword $\mathbf{c}(x)$.

Lemma 4. *Assume* $\mathbf{c}(x)$ *is a nonzero codeword of* $\mathcal{Q}$*, and let* $\mathbf{c}(x) = \sum_{t\in\mathcal{I}} a_t(x)\mathbf{g}_t$*, where* $\mathcal{I} \in \mathcal{P}(X)$ *and* $0 \neq a_t(x) \in \mathbb{F}_q[x]$ *for each* $t \in \mathcal{I}$*. Then,*

$$\mathrm{wt}(\mathbf{c}(x)) \geq \sum_{j\in\mathcal{J}(\mathcal{I})} \eta\left(\mathrm{gcd}_{t\in\mathcal{I}}\{\mathrm{Ent}_j(\mathbf{g}_t)\}\right).$$

Proof.

$$\mathrm{wt}(\mathbf{c}(x)) = \sum_{j=1}^{\ell} \mathrm{wt}(\mathrm{Ent}_j(\mathbf{c}(x))) = \sum_{j\in\mathcal{J}(\mathcal{I})} \mathrm{wt}(\mathrm{Ent}_j(\mathbf{c}(x))) = \sum_{j\in\mathcal{J}(\mathcal{I})} \mathrm{wt}\left(\sum_{t\in\mathcal{I}} a_t(x)\mathrm{Ent}_j(\mathbf{g}_t)\right) \tag{3}$$

Now, for each $j \in \mathcal{J}(\mathcal{I})$, let $\mathcal{C}_j$ be the smallest λ-constacyclic code over $\mathbb{F}_q$ of length m that contains $\{\mathrm{Ent}_j(\mathbf{g}_t)\}_{t\in\mathcal{I}}$. From Lemma 1, $\mathrm{gcd}_{t\in\mathcal{I}}\{\mathrm{Ent}_j(\mathbf{g}_t)\}$ generates $\mathcal{C}_j$. We then deduce from Theorem 1 that $d(\mathcal{C}_j) \geq \eta\left(\mathrm{gcd}_{t\in\mathcal{I}}\{\mathrm{Ent}_j(\mathbf{g}_t)\}\right)$. Therefore, $\mathrm{wt}\left(\sum_{t\in\mathcal{I}} a_t(x)\mathrm{Ent}_j(\mathbf{g}_t)\right) \geq \eta\left(\mathrm{gcd}_{t\in\mathcal{I}}\{\mathrm{Ent}_j(\mathbf{g}_t)\}\right)$ because $\sum_{t\in\mathcal{I}} a_t(x)\mathrm{Ent}_j(\mathbf{g}_t) \in \mathcal{C}_j$. The result follows from (3). □

Lemma 3 asserts that each codeword of $\mathcal{Q}$ corresponds to an element $\mathcal{I} \in \mathcal{P}(X)$. However, Lemma 4 provides a lower bound for each codeword from its corresponding $\mathcal{I}$. Hence, taking into account all elements of $\mathcal{P}(X)$ ensures that no codeword is missed. Therefore, a lower bound on $d(\mathcal{Q})$ is stated as follows:

Theorem 4. *Let* $\mathcal{Q} = \mathbb{F}_q[x]\mathbf{g}$ *be a single-generator QT code over* $\mathbb{F}_q$ *of index* ℓ *and co-index* m*, where* m *and* q *are coprime. With the notation introduced above,*

$$d(\mathcal{Q}) \geq \min_{\mathcal{I}\in\mathcal{P}(X)} \left\{ \sum_{j\in\mathcal{J}(\mathcal{I})} \eta\left(\frac{x^m - \lambda}{\prod_{\tau} p_\tau(x)}\right) \right\}, \tag{4}$$

where τ *runs over* $\{t \in \mathcal{I} \mid p_t(x) \nmid \mathrm{Ent}_j(\mathbf{g})\}$*.*

Proof. The following lower bound on $d(\mathcal{Q})$ is now immediately available from the previous discussion:

$$d(\mathcal{Q}) \geq \min_{\mathcal{I} \in \mathcal{P}(X)} \left\{ \sum_{j \in \mathcal{J}(\mathcal{I})} \eta\left(\mathrm{gcd}_{t \in \mathcal{I}}\{\mathrm{Ent}_j(\mathbf{g}_t)\}\right) \right\}.$$

Therefore, (4) follows from (1) by observing that

$$\mathrm{gcd}_{t \in \mathcal{I}}\{\mathrm{Ent}_j(\mathbf{g}_t)\} = \frac{x^m - \lambda}{\prod_\tau p_\tau(x)}.$$

This is because $p_t(x) \nmid \mathrm{gcd}_{t \in \mathcal{I}}\{\mathrm{Ent}_j(\mathbf{g}_t)\}$ if and only if $p_t(x) \nmid \mathrm{Ent}_j(\mathbf{g})$. □

Although Theorem 4 is applied to several numerical examples in Section 5, we conclude this section by applying it to Example 1. Recall that Theorem 2 provides a lower bound of 8 on the minimum distance of the code presented in Example 1. Indeed, as mentioned at the beginning of this section, Theorem 2 provides an acceptable lower bound when $f(x)$ divides $x^m - \lambda$, which is the case in Example 1. However, to establish a fair comparison between Theorems 2 and 4, they must be examined on a randomly generated code, which is performed in the next section.

Example 3. *We proceed with the QT code $\mathcal{Q}$ considered in Example 1. Recall that*

$$\mathbf{g} = \left((x+1)(x^3+2x+1), (x+1)^2(x^2+1), x(x+1)(x+2), (x+1)^2(x^2+1)\right)$$

generates $\mathcal{Q}$. The irreducible factors of $x^7 - 2$ in $\mathbb{F}_3[x]$ are $p_1(x) = x+1$ and $p_2(x) = x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 1$. Equation (2) implies that $X = \{2\}$; hence, $\mathcal{P}(X) = \{\{2\}\}$. By Definition 2, $\mathcal{J}(X) = \{1,2,3,4\}$. By Theorem 4, we find

$$d(\mathcal{Q}) \geq \sum_{j=1}^{4} \eta\left(\frac{x^7-2}{p_2(x)}\right) = \sum_{j=1}^{4} \eta(x+1) = 8,$$

where $\eta(x+1) = 2$ by Definition 1.

In Examples 1 and 3, recall that the polynomial $f(x)$ defined in Theorem 2 divides $x^m - \lambda$. Although these examples show that Theorems 2 and 4 give the same lower bound, Theorem 4 has the advantage in that it does not require any calculations over any extension fields nor does it require calculating the minimum distance of another linear code: $\mathcal{B}$. On the other hand, a disadvantage of the lower bound of Theorem 4 appears when $x^m - \lambda$ decomposes to many irreducible factors. In fact, the size of $\mathcal{P}(X)$ exponentially increases with the size of X.

5. Numerical Examples

We have four goals in this section: We first compare the proposed bound to the one provided in Theorem 2. Indeed, as demonstrated by Example 2, the latter bound has some weaknesses. Therefore, we inspect the bound of Theorem 4 on the code of Example 2. Second, we investigate the lower bound suggested in Theorem 4 for codes with different indices. Third, we consider the lower bound introduced in Theorem 3.2 of [5]. In fact, this bound does not apply to all single-generator QT codes: it only suits a specific form for the code generator. We consider this specific form and prove that Theorem 4 and Theorem 3.2 in [5] are equivalent under the assumption of this form. Therefore, we may argue that the proposed bound generalizes that in Theorem 3.2 in [5] since it does not require any specific form for the code generator. Lastly, we present a counterexample to the lower bound provided in Theorem III.2 in [8].

We begin with the following example to examine Theorem 4 on a nonbinary QT code. Remember that the QT code introduced in Example 2 shows a flaw in the lower bound given by Theorem 2. Specifically, Theorem 2 gives a lower bound of 2 to a QT of minimum distance 17. We need to determine what lower bound Theorem 4 can achieve for the same code.

Example 4. *Let $\mathcal{Q}$ be the QT code of Example 2 generated by the randomly chosen codeword*

$$\begin{aligned}\mathbf{g} = \Big(&\omega x(x^3+\omega x^2+x+\omega^2), \omega(x^4+\omega x^3+x^2+\omega x+1), \omega^2(x^2+x+\omega)(x^2+\omega^2 x+1),\\ &\omega^2(x+1)(x+\omega^2)(x^2+\omega^2 x+\omega^2), \omega x(x+1)(x+\omega)^2, (x+\omega^2)(x^2+\omega x+\omega)\Big).\end{aligned} \tag{5}$$

Because $m=5$ and $\lambda=\omega$, $p_1(x)=x+\omega^2$, $p_2(x)=x^2+x+\omega$, $p_3(x)=x^2+\omega x+\omega$. Let ζ be a zero of the primitive polynomial $x^2+x+\omega \in \mathbb{F}_4[x]$. Then, $\omega=\zeta^5$, while $\gamma=\zeta^3$ and $\beta=\zeta$ are the primitive 5th *root of unity and ω, respectively. The zero of $(x+\omega^2)$ is $\{\beta\gamma^3\}$, the zeros of $(x^2+x+\omega)$ are $\{\beta\gamma^0,\beta\gamma^1\}$, and the zeros of $(x^2+\omega x+\omega)$ are $\{\beta\gamma^2,\beta\gamma^4\}$.*

From Theorem 3, the dimension of $\mathcal{Q}$ is $k=5$. Equation (2) implies that $X=\{1,2,3\}$.

1. *For $\mathcal{I}=\{1\}$, by Definition 2, $\mathcal{J}(\mathcal{I})=\{1,2,3,5\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})}\eta\left(\frac{x^5-\omega}{p_1(x)}\right) = 4\eta\left((x^2+x+\omega)(x^2+\omega x+\omega)\right)=16$.*
2. *For $\mathcal{I}=\{2\}$, by Definition 2, $\mathcal{J}(\mathcal{I})=\{1,2,4,5,6\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})}\eta\left(\frac{x^5-\omega}{p_2(x)}\right) = 5\eta\left((x+\omega^2)(x^2+\omega x+\omega)\right)=20$.*
3. *For $\mathcal{I}=\{3\}$, by Definition 2, $\mathcal{J}(\mathcal{I})=\{1,2,3,4,5\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})}\eta\left(\frac{x^5-\omega}{p_3(x)}\right) = 5\eta\left((x+\omega^2)(x^2+x+\omega)\right)=20$.*
4. *For $\mathcal{I}=\{1,2\}$, by Definition 2, $\mathcal{J}(\mathcal{I})=\{1,2,3,4,5,6\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})}\eta\left(\frac{x^5-\omega}{\prod_\tau p_\tau(x)}\right) = 3+3+4+4+3+4=21$.*
5. *For $\mathcal{I}=\{2,3\}$, by Definition 2, $\mathcal{J}(\mathcal{I})=\{1,2,3,4,5,6\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})}\eta\left(\frac{x^5-\omega}{\prod_\tau p_\tau(x)}\right) = 2+2+4+2+2+4=16$.*
6. *For $\mathcal{I}=\{1,3\}$, by Definition 2, $\mathcal{J}(\mathcal{I})=\{1,2,3,4,5\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})}\eta\left(\frac{x^5-\omega}{\prod_\tau p_\tau(x)}\right) = 3+3+3+4+3=16$.*
7. *For $\mathcal{I}=\{1,2,3\}$, by Definition 2, $\mathcal{J}(\mathcal{I})=\{1,2,3,4,5,6\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})}\eta\left(\frac{x^5-\omega}{\prod_\tau p_\tau(x)}\right) = 1+1+3+2+1+4=12$.*

Therefore, $d(\mathcal{Q})\geq 12$, where the minimum distance of $\mathcal{Q}$ is found to be $d(\mathcal{Q})=17$.

We now examine Theorem 4 on several binary QC codes of the same length with varied indices and co-indices.

Example 5. *We randomly generate the binary codeword*

$$\begin{aligned}\mathbf{g} = (&1,1,0,1,0,0,1,0,0,0,0,1,1,0,0,0,1,1,1,1,1,0,1,1,1,0,1,1,0,1,1,1,1,\\ &1,1,1,1,0,1,0,0,0,1,1,0)\end{aligned}$$

of length 45. *This codeword is interpreted as a generator of several QC codes $\mathcal{Q}$ of length* 45 *and different indices. We determine the lower bound on $d(\mathcal{Q})$ provided by Theorem 4 for different ℓ values.*

1. *Let $\ell=15$. Then, $m=3$, $p_1(x)=x+1$, and $p_2(x)=x^2+x+1$. The zeros of (x^2+x+1) are $\{\zeta,\zeta^2\}$, and the zero of $(x+1)$ is $\{\zeta^0\}$. In polynomial representation,*

$$\begin{aligned}\mathbf{g} = \Big(&x+1,1,1,x^2,1,x(x+1),x^2+x+1,x(x+1),x^2+1,x^2+1,\\ &x^2+x+1,x^2+x+1,x^2+1,0,x+1\Big).\end{aligned}$$

From Theorem 3, the dimension of $\mathcal{Q}$ is $k=3$. Equation (2) implies that $X=\{1,2\}$.

(a) *For $\mathcal{I}=\{1\}$, $\sum_{j\in\mathcal{J}(\mathcal{I})}\eta(x^2+x+1)=7\times 3=21$.*

(b) *For* $\mathcal{I} = \{2\}$, $\sum_{j \in \mathcal{J}(\mathcal{I})} \eta(x+1) = 11 \times 2 = 22$.

(c) *For* $\mathcal{I} = X$, $\sum_{j \in \mathcal{J}(\mathcal{I})} \eta\left(\frac{x^3-1}{\prod_\tau p_\tau(x)}\right) = 2+1+1+1+1+2+3+2+2+2+3+3+2+2 = 27$.

Therefore, $d(\mathcal{Q}) \geq 21$. *In fact, we find* $d(\mathcal{Q}) = 21$.

2. *Let* $\ell = 9$. *Then* $m = 5$, $p_1(x) = x+1$, *and* $p_2(x) = x^4+x^3+x^2+x+1$. *Let* ζ *be a zero of the primitive polynomial* $x^4+x+1 \in \mathbb{F}_2[x]$. *Then,* $\gamma = \zeta^3$ *is the primitive 5th root of unity. The zeros of* $(x^4+x^3+x^2+x+1)$ *are* $\{\gamma, \gamma^2, \gamma^3, \gamma^4\}$, *and the zero of* $(x+1)$ *is* $\{\gamma^0\}$. *In polynomial representation,*

$$\mathbf{g} = \Big(x^3+x+1, x, x(x+1), x(x+1)^3, (x+1)(x^3+x+1), x(x^3+x+1), \\ x^4+x^3+x^2+x+1, x^3+x+1, (x+1)x^2\Big).$$

From Theorem 3, the dimension of $\mathcal{Q}$ *is* $k = 5$. *Equation (2) implies that* $X = \{1, 2\}$.

(a) *For* $\mathcal{I} = \{1\}$, $\sum_{j \in \mathcal{J}(\mathcal{I})} \eta\left(x^4+x^3+x^2+x+1\right) = 5 \times 5 = 25$.

(b) *For* $\mathcal{I} = \{2\}$, $\sum_{j \in \mathcal{J}(\mathcal{I})} \eta(x+1) = 8 \times 2 = 16$.

(c) *For* $\mathcal{I} = X$, $\sum_{j \in \mathcal{J}(\mathcal{I})} \eta\left(\frac{x^5-1}{\prod_\tau p_\tau(x)}\right) = \eta(1) + \eta(1) + \eta(x+1) + \eta(x+1) + \eta(x+1) + \eta(1) + \eta\left(x^4+x^3+x^2+x+1\right) + \eta(1) + \eta(x+1) = 1+1+2+2+2+1+5+1+2 = 17$.

Therefore, $d(\mathcal{Q}) \geq 16$. *In fact, we find* $d(\mathcal{Q}) = 19$.

3. *Let* $\ell = 5$. *Then,* $m = 9$, $p_1(x) = x+1$, $p_2(x) = x^2+x+1$, *and* $p_3(x) = x^6+x^3+1$. *Let* ζ *be a zero of the primitive polynomial* $x^6+x^4+x^3+x+1 \in \mathbb{F}_2[x]$. *Then,* $\gamma = \zeta^7$ *is the primitive 9th root of unity. The zeros of* $\left(x^6+x^3+1\right)$ *are* $\{\gamma, \gamma^2, \gamma^4, \gamma^5, \gamma^7, \gamma^8\}$, *the zeros of* $\left(x^2+x+1\right)$ *are* $\{\gamma^3, \gamma^6\}$, *and the zero of* $(x+1)$ *is* $\{\gamma^0\}$. *In polynomial representation,*

$$\mathbf{g} = \Big((x+1)^3(x^3+x^2+1), x^2(x+1)^2(x^4+x^3+x^2+x+1), \\ x^8+x^6+x^5+x^4+x^2+x+1, (x+1)(x^7+x^5+x^3+x+1), (x+1)(x^6+x+1)\Big).$$

From Theorem 3, the dimension of $\mathcal{Q}$ *is* $k = 9$. *Equation (2) implies that* $X = \{1, 2, 3\}$. *For* $\mathcal{I} = \{1\}$ *or* $\mathcal{I} = X$, *the right side of (4) has the smallest value. Therefore,* $d(\mathcal{Q}) \geq \eta\left((x^2+x+1)(x^6+x^3+1)\right) = 9$. *We found* $d(\mathcal{Q}) = 9$.

4. *Let* $\ell = 3$. *Then* $m = 15$, $p_1(x) = x+1$, $p_2(x) = x^2+x+1$, $p_3(x) = x^4+x+1$, $p_4(x) = x^4+x^3+1$, *and* $p_5(x) = x^4+x^3+x^2+x+1$. *Let* ζ *be a zero of the primitive polynomial* $x^4+x+1 \in \mathbb{F}_2[x]$. *The zeros of* $\left(x^4+x+1\right)$ *are* $\{\zeta, \zeta^2, \zeta^4, \zeta^8\}$, *the zeros of* $\left(x^4+x^3+1\right)$ *are* $\{\zeta^7, \zeta^{11}, \zeta^{13}, \zeta^{14}\}$, *the zeros of* $\left(x^4+x^3+x^2+x+1\right)$ *are* $\{\zeta^3, \zeta^6, \zeta^9, \zeta^{12}\}$, *the zeros of* $\left(x^2+x+1\right)$ *are* $\{\zeta^5, \zeta^{10}\}$, *and the zero of* $(x+1)$ *is* $\{\zeta^0\}$. *In polynomial representation,*

$$\mathbf{g} = \Big((x+1)(x^5+x^3+x^2+x+1)(x^6+x^4+x^3+x+1), \\ x(x^2+x+1)^4(x^5+x^3+x^2+x+1), (x+1)^2(x^3+x+1)(x^8+x^7+x^5+x^3+1)\Big).$$

From Theorem 3, the dimension of $\mathcal{Q}$ *is* $k = 15$. *Equation (2) implies that* $X = \{1, 2, 3, 4, 5\}$. *For* $\mathcal{I} = X$, *the right side of (4) has the smallest value. Therefore,* $d(\mathcal{Q}) \geq \eta(x+1) + \eta\left(x^2+x+1\right) + \eta(x+1) = 2+2+2 = 6$. *We found* $d(\mathcal{Q}) = 10$.

Theorem 3.2 in [5] introduces a lower bound on the minimum distance of a single-generator QT code $\mathcal{Q}$, where the code generator is assumed to be of the form

$$\mathbf{g} = (f_1(x)g(x), f_2(x)g(x), \ldots, f_\ell(x)g(x)). \tag{6}$$

$g(x)$ divides $x^m - \lambda$, and $f_j(x)$ is coprime to $(x^m - \lambda)/g(x)$ for $1 \leq j \leq \ell$, as elements of $\mathbb{F}_q[x]$. It was shown that $d(\mathcal{Q}) \geq \ell\eta(g(x))$ under this particular form (6) of $\mathbf{g}$. In fact, this lower bound is limited to single-generator QT codes with this generator form. For instance, it does not apply to the code in Example 4. Specifically, (5) forces us to choose $g(x) = 1$, so $f_3(x)$ is not coprime to $\left(x^5 - \omega\right)$. This reinforces our proposed bound, which has the advantage of being applicable to any single-generator QT code because Theorem 4 makes no assumptions about the code generator. Furthermore, we prove in Corollary 1 below that Theorem 4 generalizes Theorem 3.2 in [5]. To this end, assuming the code has generator (6), we show that the lower bound of Theorem 4 is reduced to that of Theorem 3.2 in [5].

Corollary 1. *Let $\mathcal{Q}$ be a QT code over $\mathbb{F}_q$ of index ℓ and co-index m, where m and q are coprime. Assume $\mathcal{Q} = \mathbb{F}_q[x]\mathbf{g}$ with*

$$\mathbf{g} = (f_1(x)g(x), f_2(x)g(x), \ldots, f_\ell(x)g(x)),$$

where $g(x)$ divides $x^m - \lambda$, and $f_j(x)$ is coprime to $(x^m - \lambda)/g(x)$ for $1 \le j \le \ell$. Then

$$d(\mathcal{Q}) \ge \ell\eta(g(x)).$$

Proof. Suppose that $x^m - \lambda = \prod_{t=1}^{s} p_t(x)$ and, without loss of generality, that $g(x) = \prod_{t=r+1}^{s} p_t(x)$ for some $1 \le r \le s$. Then, $\mathbf{g}_t \ne \mathbf{0}$ for $1 \le t \le r$ and $\mathbf{g}_t = \mathbf{0}$ for $r+1 \le t \le s$. Hence, $X = \{1, 2, \ldots, r\}$. The condition on $f_j(x)$ implies that for every $\mathcal{I} \in \mathcal{P}(X)$, $\mathcal{J}(\mathcal{I}) = \{1, 2, \ldots, \ell\}$. Consequently, the value of the right side of (4) is the smallest when $\mathcal{I} = X$. From Theorem 4, we find

$$d(\mathcal{Q}) \ge \sum_{j=1}^{\ell} \eta\left(\mathrm{gcd}_{1\le t\le r}\left\{\frac{x^m - \lambda}{p_t(x)} f_j(x)g(x)\right\}\right) = \sum_{j=1}^{\ell} \eta(g(x)) = \ell\eta(g(x)).$$

□

We conclude this section by contradicting Theorem III.2 in [8], which provides a lower bound on the minimum distance of any single-generator QT code. Specifically, Theorem III.2 in [8] states that $d(\mathcal{Q}) \ge \ell\eta\left(\mathrm{gcd}_{1\le j\le \ell}\{g_j(x)\}\right)$ for any single-generator QT code with generator $\mathbf{g} = (g_1(x), g_2(x), \ldots, g_\ell(x))$. This theorem is contradicted by the following example.

Example 6. *Let $\mathcal{Q}$ be the binary QC code of index $\ell = 2$ and co-index $m = 7$ generated by*

$$\mathbf{g} = \left((x+1)(x^3+x^2+1), (x^3+x+1)(x^3+x^2+1)\right).$$

From Theorem III.2 in [8], $d(\mathcal{Q}) \ge 2\eta\left(x^3+x^2+1\right) = 6$. However, the codeword $(x+1)\mathbf{g} = \left(x^5+x^4+x^3+1, 0\right) \in \mathcal{Q}$ has a weight of 4, which contradicts the lower bound. On the other hand, Theorem 4 demonstrates that $d(\mathcal{Q}) \ge 4$. This can be shown as follows: We have $p_1(x) = x+1$, $p_2(x) = x^3+x+1$, and $p_3(x) = x^3+x^2+1$. Equation (2) implies that $X = \{1, 2\}$.

1. *For $\mathcal{I} = \{1\}$, $\mathcal{J}(\mathcal{I}) = \{2\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})} \eta\left(\frac{x^7-1}{p_1(x)}\right) = \eta\left((x^3+x+1)(x^3+x^2+1)\right) = 7$.*
2. *For $\mathcal{I} = \{2\}$, $\mathcal{J}(\mathcal{I}) = \{1\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})} \eta\left(\frac{x^7-1}{p_2(x)}\right) = \eta\left((x+1)(x^3+x^2+1)\right) = 4$.*
3. *For $\mathcal{I} = \{1, 2\}$, $\mathcal{J}(\mathcal{I}) = \{1, 2\}$ and $\sum_{j\in\mathcal{J}(\mathcal{I})} \eta\left(\frac{x^7-1}{\prod_\tau p_\tau(x)}\right) = 4 + 7 = 11$.*

Therefore, $d(\mathcal{Q}) \ge 4$; hence, $d(\mathcal{Q}) = 4$.

6. Conclusions

We proposed two different lower bounds on the minimum distance of single-generator QT codes. Imitating the work in [7] on QC codes, the first lower bound was established by associating a constacyclic code over $\mathbb{F}_{q^\ell}$ of length m to each QT code over $\mathbb{F}_q$ of index ℓ and co-index m. We noted the weakness of this lower bound for general single-generator QT codes. To address this, we introduced a novel bound, which implicitly relies on the decomposition of single-generator QT codes using the CRT to avoid computations over extension fields. We then examined the effectiveness of the proposed bound for codes over various finite fields and various indices. Additionally, we offered a counterexample to one of the bounds of single-generator QT codes addressed in [8].

In future work, we will attempt to generalize Theorem 4 to establish a lower bound on the minimum distance of multigenerator QT codes.

Author Contributions: Conceptualization, A.A.; Formal analysis, R.T.E.; Investigation, P.S. All authors have read and agreed to the published version of the manuscript.

Funding: This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia, under grant No. KEP-Msc-28-130-40.

Data Availability Statement: Not applicable.

Acknowledgments: The authors, therefore, acknowledge with thanks the technical and financial support from the DSR.

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

References

1. Chen, B.; Fan, Y.; Lin, L.; Liu, H. Constacyclic codes over finite fields. *Finite Fields Their Appl.* **2012**, *18*, 1217–1231. [CrossRef]
2. Lally, K.; Fitzpatrick, P. Algebraic structure of quasicyclic codes. *Discret. Appl. Math.* **2001**, *111*, 157–175. [CrossRef]
3. Grassl, M. Bounds on the Minimum Distance of Linear Codes and Quantum Codes. 2007. Available online: http://www.codetables.de (accessed on 25 March 2023).
4. Vardy, A. The intractability of computing the minimum distance of a code. *IEEE Trans. Inf. Theory* **1997**, *43*, 1757–1766. [CrossRef]
5. Aydin, N.; Siap, I.; Ray-Chaudhuri, D.K. The structure of 1-generator quasi-twisted codes and new linear codes. *Des. Codes Cryptogr.* **2001**, *24*, 313–326. [CrossRef]
6. Krishn, A.; Sarwate, D.V. Pseudocyclic maximum-distance-separable codes. *IEEE Trans. Inf. Theory* **1990**, *36*, 880–884. [CrossRef]
7. Lally, K. Quasicyclic codes of index ℓ over $\mathbb{F}_q$ viewed as $\mathbb{F}_q[x]$-submodules of $\mathbb{F}_{q^\ell}[x]/\langle x^m - 1\rangle$. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*; Fossorier, M., Hoeholdt, T., Poli, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2003; pp. 244–253.
8. Aydin, N.; Guidotti, T.; Liu, P. New linear codes as quasi-twisted codes from long constacyclic codes. In *2020 Algebraic and Combinatorial Coding Theory (ACCT)*; IEEE: Piscataway, NJ, USA 2020.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.