A Comparison of Distance Bounds for Quasi-Twisted Codes

Martianus Frederic Ezerman, John Mark Lampos, San Ling, Buket Özkaya, and Jareena Tharnnukhroh

***Abstract*—Spectral bounds on the minimum distance of quasi-twisted codes over finite fields are proposed, based on eigenvalues of polynomial matrices and the corresponding eigenspaces. They generalize the Semenov-Trifonov and Zeh-Ling bounds in a way similar to how the Roos and shift bounds extend the BCH and HT bounds for cyclic codes. The eigencodes of a quasi-twisted code in the spectral theory and the outer codes in its concatenated structure are related. A comparison based on this relation verifies that the Jensen bound always outperforms the spectral bound under special conditions, which yields a similar relation between the Lally and the spectral bounds. The performances of the Lally, Jensen and spectral bounds are presented in comparison with each other.**

***Index Terms*—quasi-twisted code, concatenated code, minimum distance bound, polynomial matrices, spectral analysis**

I. Introduction

Cyclic codes have been widely studied, since their algebraic structure provides effective encoding and decoding. Several lower bounds on the minimum distance of cyclic codes had been derived. The first and perhaps the most famous one was obtained by Bose and Chaudhuri ([5]) and by Hocquenghem ([14]), known as the BCH bound. An extension of the BCH bound was formulated by Hartmann and Tzeng in [13], which can be considered as a two-directional BCH bound. The Roos bound ([23]) generalized this idea further by allowing the HT bound to have a certain number of gaps in both directions, which was extended to constacyclic codes in [22]. Another remarkable extension of the HT bound, known as the shift bound, was introduced by van Lint and Wilson in [19]. The shift bound is known to be particularly powerful on many nonbinary codes (*e.g.* see [10]).

Quasi-twisted (QT) codes form an important class of block codes that includes cyclic codes, quasi-cyclic (QC) codes and constacyclic codes as special subclasses. In addition to their rich algebraic structure ([16], [26]), QT codes are also known to be asymptotically good ([8], [9], [30]) and they yield good parameters ([1], [2], [21], [24]).

Even though QC and QT codes are interesting from both theoretical and practical points of view, the study on their minimum distance estimates is not as rich as for cyclic and constacyclic codes. Jensen derived a significant bound in [15], which is valid for many code classes having a concatenated structure, including QT codes ([20]). Lally gave another estimate on the minimum distance of a given QC code, which is obtained by a simpler concatenation [17], depending only on the index and the co-index of the QC code in consideration. More recently, Semenov and Trifonov developed a spectral analysis of QC codes ([25]), based on the work of Lally and Fitzpatrick in [18], and formulated a BCH-like minimum distance bound, together with a comparison with a few other bounds for QC codes. Their approach was generalized by Zeh and Ling in [28], by using the HT bound. They extended the spectral method to QC product codes in [29]. The first spectral analysis of QT codes appeared in [11], where a spectral bound under some restricted conditions was proven and then this bound was only compared with the BCH-like and HT-like versions.

In this work, we investigate the spectral theory for QT codes, by following the steps in [11], [25], that is centered around the eigenvalues of a given QT code. They can be considered as the QT analogues of the zeros of constacyclic codes. We aim at deriving a general spectral bound which holds for a larger choice of eigenvalues than the more constrained version in [11]. For this, we focus on connecting the concatenated structure of QT codes to the key elements of the spectral method. Using this relation, we prove three important results. First, we push the general spectral bound to the largest possible extent and show that it holds for any nonempty subset of eigenvalues. Second, we establish a theoretical link between the spectral and Jensen bounds. We show that deploying all of the eigenvalues causes the Jensen bound to win against the spectral bound, but looking at proper subsets of the eigenvalues may occasionally turn the situation to the opposite, allowing the spectral bound to beat the Jensen bound. At last, we prove a relation between the Lally and spectral bounds, which mimics the result when comparing the spectral bound with the Jensen bound, except that this time the largest possible set of eigenvalues is considered. The numerical comparisons at the end present how all these three bounds behave over a large number of randomly chosen QT codes.

This paper is organized as follows. Section II recalls some

M. F. Ezerman, S. Ling, B. Özkaya, and J. Tharnnukhroh are with the School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, e-mails: {fredezerman, lingsan, buketozkaya}@ntu.edu.sg, jareena001@e.ntu.edu.sg.

J. M. Lampos is with the Institute of Mathematical Sciences and Physics, University of the Philippines, Los Baños, Laguna, Philippines 4031, e-mail: jtlampos@up.edu.ph.

M. F. Ezerman, S. Ling, and B. Özkaya are supported by Nanyang Technological University Research Grant No. 04INS000047C230GRT01.

J. M. Lampos is supported by DOST-ASTHRDP Dissertation Grant and CHED K-12 Transition Program Scholarship for Graduate Studies Abroad.

J. Tharnnukhroh's scholarship is from the Development and Promotion of Science and Technology (DPST) talent project of Thailand.

The fourth section of this paper contains results presented at the 2019 IEEE International Symposium on Information Theory [11].

required background on the algebraic structure of constacyclic and QT codes. Section III studies the spectral method in terms of the concatenated structure of QT codes. Using this unified approach, Section IV modifies the spectral method of Semenov-Trifonov to QT codes. A generalized spectral bound on the minimum distance of QT codes is formulated and proven, where the Roos-like and shift-like bounds for QT codes follow as special cases. In Section V, we first prove that the Jensen bound performs at least as well as the spectral bound under certain assumptions. Then we formulate the Lally bound for QT codes and compare it with the spectral bound in a similar way. Section VI presents explicit examples and constructions over a large set of random QT codes, displaying the performances of these three bounds in terms of sharpness and rank. All computations were carried out in MAGMA [6].

II. Background

A. Constacyclic codes and minimum distance bounds from defining sets

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a prime power. Let m be throughout a positive integer with $\gcd(m,q)=1$. For a fixed $\lambda \in \mathbb{F}_q \backslash \{0\}$, a linear code $C \subseteq \mathbb{F}_q^m$ is called a λ-*constacyclic* code if it is invariant under the λ-constashift of codewords, *i.e.*, $(c_0,\ldots,c_{m-1}) \in C$ implies $(\lambda c_{m-1}, c_0, \ldots, c_{m-2}) \in C$. In particular, if $\lambda = 1$ or $q = 2$, then C is a cyclic code.

Consider the principal ideal $I = \langle x^m - \lambda \rangle$ of $\mathbb{F}_q[x]$ and define the residue class ring $R := \mathbb{F}_q[x]/I$. For an element $\mathbf{a} \in \mathbb{F}_q^m$, we associate an element of R via the following $\mathbb{F}_q$-module isomorphism:

$$\begin{array}{rcl} \phi: \ \mathbb{F}_q^m & \longrightarrow & R \\ \mathbf{a} = (a_0,\ldots,a_{m-1}) & \longmapsto & a(x) := a_0 + \cdots + a_{m-1}x^{m-1}. \end{array} \tag{1}$$

While elements in R are cosets of the form $b(x) + I$ where $b(x) \in \mathbb{F}_q[x]$, we write them with a slight abuse of notation as $b(x)$. Observe that the λ-constashift in $\mathbb{F}_q^m$ corresponds to multiplication by x in R. Therefore, a λ-constacyclic code $C \subseteq \mathbb{F}_q^m$ can be viewed as an ideal of R. Since every ideal in R is principal, there exists a unique monic polynomial $g(x) \in R$ such that $C = \langle g(x) \rangle$, *i.e.*, each codeword $c(x) \in C$ is of the form $c(x) = a(x)g(x)$, for some $a(x) \in R$. The polynomial $g(x)$, which is a divisor of $x^m - \lambda$, is called the *generator polynomial* of C, whereas the *check polynomial* of C, say $h(x) \in R$, satisfies $g(x)h(x) = x^m - \lambda$.

Let $\mathrm{wt}(c)$ denote the number of nonzero coefficients in $c(x) \in C$. Recall that the minimum distance of C is defined as $d(C) := \min\{\mathrm{wt}(c) : 0 \neq c(x) \in C\}$ when C is not the trivial zero code. For any positive integer p, let $\mathbf{0}_p$ denote throughout the all-zero vector of length p. We have $C = \{\mathbf{0}_m\}$ if and only if $g(x) = x^m - \lambda$. In this case, we assume throughout that $d(C) = \infty$.

Let r be the smallest divisor of $q-1$ with $\lambda^r = 1$ and let α be a primitive rm^{th} root of unity such that $\alpha^m = \lambda$. Then, $\xi := \alpha^r$ is a primitive m^{th} root of unity and the roots of $x^m - \lambda$ are of the form $\alpha, \alpha\xi, \ldots, \alpha\xi^{m-1}$. Henceforth, let $\Omega := \{\alpha\xi^k : 0 \le k \le m-1\} = \{\alpha^{1+kr} : 0 \le k \le m-1\}$ be the set of all m^{th} roots of λ and let $\mathbb{F}$ be the smallest extension of $\mathbb{F}_q$ that contains Ω (equivalently, $\mathbb{F} = \mathbb{F}_q(\alpha)$ so that $\mathbb{F}$ is the splitting field of $x^m - \lambda$). Given the λ-constacyclic code $C = \langle g(x) \rangle$, the set of roots of its generator polynomial, say

$$L := \{\alpha\xi^k \ : \ g(\alpha\xi^k) = 0\} \subseteq \Omega,$$

is called the *zero set* of C. The power set $\mathcal{P}(L)$ of L is called the *defining set* of C. Clearly, $L = \emptyset$ if and only if $C = \langle 1 \rangle = \mathbb{F}_q^m$. Note that $\alpha\xi^k \in L$ implies $\alpha^q\xi^{qk} \in L$, for each k, where $\alpha^q\xi^{qk} = \alpha\xi^{k'}$ with $k' = \frac{q-1}{r} + qk \mod m$. A nonempty subset $E \subseteq \Omega$ is said to be *consecutive* if there exist integers e, n and δ with $e \ge 0, \delta \ge 2, n > 0$ and $\gcd(m,n) = 1$ such that

$$E := \{\alpha\xi^{e+zn} \ : \ 0 \le z \le \delta - 2\} \subseteq \Omega. \tag{2}$$

Let $\mathcal{P}(\Omega)$ denote the power set of Ω. Observe that any $P \in \mathcal{P}(\Omega)$ is the zero set of some λ-constacyclic code $D_P \subseteq \mathbb{F}^m$ since $x^m - \lambda$ splits into linear factors over $\mathbb{F}$. Let C be a nontrivial λ-constacyclic code of length m over some subfield of $\mathbb{F}$ with zero set $L \subseteq \Omega$. Then, for any $P \subseteq L$, C is contained in D_P and therefore we have $d(C) \ge d(D_P)$. Throughout, we define a *defining set bound* to be a member of a chosen family $\mathcal{B}(C) := \{(P, d_P)\} \subseteq \mathcal{P}(\Omega) \times (\mathbb{N} \cup \{\infty\})$ such that, for any $(P, d_P) \in \mathcal{B}(C)$, $P \subseteq L$ implies $d(C) \ge d(D_P) \ge d_P$ (a more detailed formulation given for the cyclic codes can be found in [7]). We set

$$\begin{aligned} \mathcal{B}_1(C) := \{(P, d(D_P)) : \\ D_P \subseteq \mathbb{F}^m \text{ has zero set } P, \text{ for all } P \subseteq L\}. \end{aligned}$$

In particular, following the notation given above in the case when $P = L = \Omega$, we have $D_\Omega = \{\mathbf{0}_m\}$ over $\mathbb{F}$ with $d(D_\Omega) = \infty$ and consequently, we include (Ω, ∞) in every collection $\mathcal{B}(C)$ as a convention when $L = \Omega$.

If we choose

$$\mathcal{B}_2(C) := \{(E, |E|+1) : E \subseteq L \text{ is consecutive}\},$$

then we obtain the BCH bound, where E is of the form given in (2). Similarly, we formulate the HT bound as

$$\begin{aligned} \mathcal{B}_3(C) := \{(D, \delta + s) : \\ D = \{\alpha\xi^{e+zn_1+yn_2} : 0 \le z \le \delta - 2, 0 \le y \le s\} \subseteq L\}, \end{aligned}$$

for integers $e \ge 0$, $\delta \ge 2$ and positive integers s, n_1 and n_2 such that $\gcd(m, n_1) = 1$ and $\gcd(m, n_2) < \delta$. Note that any union of defining set bounds is again a defining set bound.

We are now ready to present the Roos bound on the minimum distance of a given λ-constacyclic code (see [23, Theorem 2] for the original version by C. Roos for cyclic codes). For the proof of the result below, we refer to [22, Theorem 6].

Theorem 1 (Roos bound)**.** *Let N and M be two nonempty subsets of Ω. If there exists a consecutive set M' containing M such that $|M'| \le |M| + d_N - 2$, then we have $d_{MN} \ge |M| + d_N - 1$ where $MN := \dfrac{1}{\alpha} \bigcup_{\varepsilon \in M} \varepsilon N$.*

If N is consecutive like in (2), then we obtain the following.

Corollary 1. *[22, Corollary 1],[23, Corollary 1] Let N, M and M' be as in Theorem 1, with N consecutive. Then $|M'| < |M| + |N|$ implies $d_{MN} \geq |M| + |N|$.*

Remark 1. In particular, the case $M = \{\alpha\}$ yields the BCH bound for the associated constacyclic code (see [22, Corollary 2]). The original BCH bound for cyclic codes can be found in [5] and [14]. By taking $M' = M$, we obtain the HT bound (see [22, Corollary 3]) and the HT bound for cyclic codes is given in [13, Theorem 2].

Another improvement to the HT bound for cyclic codes was provided by van Lint and Wilson in [19], which is known as the shift bound. We proceed by formulating the shift bound for constacyclic codes. To do this, we need the notion of an *independent set*, which can be constructed over any field in a recursive way, as given below.

Let S be a subset of some field $\mathbb{K}$ of any characteristic. One inductively defines a family of finite subsets of $\mathbb{K}$, called independent with respect to S, as follows.

1) $\emptyset$ is independent with respect to S.
2) If $A \subseteq S$ is independent with respect to S, then $A \cup \{b\}$ is independent with respect to S, for any $b \in \mathbb{K} \setminus S$.
3) If A is independent with respect to S and c is any nonzero element in $\mathbb{K}$ such that $cA \subseteq S$, then cA is independent with respect to S.

The recursive construction starts with the smallest independent set, say $A_0 = \emptyset$. Then $A_1 = \emptyset \cup \{b_0\} = \{b_0\}$, for some $b_0 \in \mathbb{K} \setminus S$. One can continue with $A_2 = c_1 A_1 \cup \{b_1\}$ provided that $c_1 A_1 \subseteq S$ for some $c_1 \in \mathbb{K} \setminus \{0\}$ and $b_1 \in \mathbb{K} \setminus S$. This ensures that A_2 is again independent with respect to S. The process stops at the t^{th} step when there is no constant $c \in \mathbb{K} \setminus \{0\}$ such that $cA_t \subseteq S$. Observe that $|A_0| = 0$ and $|A_{i+1}| = |A_i| + 1$ for all $i \in \{0, \ldots, t-1\}$.

Theorem 2 (Shift bound)**.** *[19, Theorem 11] Let $0 \neq f(x) \in \mathbb{K}[x]$ and $S = \{\theta \in \mathbb{K} \ : \ f(\theta) = 0\}$. Then* $\mathrm{wt}(f) \geq |A|$, for every subset A of $\mathbb{K}$ that is independent with respect to S.

The shift bound for a given λ-constacyclic code follows by considering the weights of its codewords $c(x) \in C$ and the independent sets with respect to subsets of its zero set L. Observe that, in this case, the universe of the independent sets is Ω, not the extension field $\mathbb{F}$, because all of the possible roots of the codewords are contained in Ω. Moreover, we choose b from $\Omega \setminus P$ in Condition (2) above, where $P \subseteq L$, and c in Condition (3) is of the form $\xi^k \in \mathbb{F} \setminus \{0\}$, for some $0 \leq k \leq m-1$.

Corollary 2. *The BCH and the HT bounds for a given λ-constacyclic code C can be obtained from the shift bound as follows:*

i. The set $B_\delta := \{\alpha\xi^{e+zn} : 0 \leq z \leq \delta - 1\}$ is independent with respect to the consecutive set E in (2) and $d(C_E) \geq |B_\delta| = \delta$.

ii. Let $D = \{\alpha\xi^{e+zn_1+yn_2} : 0 \leq z \leq \delta - 2, 0 \leq y \leq s\}$, for integers $e \geq 0$, $\delta \geq 2$ and positive integers s, n_1 and n_2 such that $\gcd(m, n_1) = 1$ and $\gcd(m, n_2) < \delta$. Then, for any fixed $\zeta \in \{0, \ldots, \delta - 2\}$, the set

$$A_\zeta := \{\alpha\xi^{e+zn_1} : 0 \leq z \leq \delta - 2\} \cup \{\alpha\xi^{e+\zeta n_1 + yn_2} : 0 \leq y \leq s+1\}$$

is independent with respect to D and $d(C_D) \geq \delta + s$.

Proof. i. We construct a sequence $B_0, B_1, \ldots, B_\delta \subseteq \Omega$ of independent sets with respect to E as follows.

$$\begin{aligned}
B_0 &= \emptyset, \\
B_1 &= B_0 \cup \{\alpha\xi^{e+(\delta-1)n}\} = \{\alpha\xi^{e+(\delta-1)n}\}, \\
B_2 &= \xi^{-n} B_1 \cup \{\alpha\xi^{e+(\delta-1)n}\} \\
&= \{\alpha\xi^{e+(\delta-2)n}, \alpha\xi^{e+(\delta-1)n}\}, \\
&\vdots \\
B_\delta &= \xi^{-n} B_{\delta-1} \cup \{\alpha\xi^{e+(\delta-1)n}\} \\
&= \{\alpha\xi^{e}, \alpha\xi^{e+n}, \ldots, \alpha\xi^{e+(\delta-1)n}\}.
\end{aligned}$$

Since there is no element $\xi^k \in \mathbb{F} \setminus \{0\}$ such that $\xi^k B_\delta \subseteq E$, for all $k \in \{0, \ldots, m-1\}$, the process stops. By Theorem 2, $|B_\delta| = \delta$ implies $d(C_E) \geq \delta$.

ii. Let $a := \alpha\xi^{e+(\delta-1)n_1+sn_2}$ and $b_\zeta := \alpha\xi^{e+\zeta n_1+(s+1)n_2}$, for some fixed $\zeta \in \{0, \ldots, \delta-2\}$. Note that $a, b_\zeta \in \Omega \setminus D$ and consider the following sequence of independent sets with respect to D.

$$\begin{aligned}
A_0 &= \emptyset, \\
A_1 &= A_0 \cup \{a\} = \{\alpha\xi^{e+(\delta-1)n_1+sn_2}\}, \\
A_2 &= \xi^{-n_1} A_1 \cup \{a\} \\
&= \{\alpha\xi^{e+(\delta-2)n_1+sn_2}, \alpha\xi^{e+(\delta-1)n_1+sn_2}\}, \\
&\vdots \\
A_{\delta-1} &= \xi^{-n_1} A_{\delta-2} \cup \{a\} \\
&= \{\alpha\xi^{e+n_1+sn_2}, \alpha\xi^{e+2n_1+sn_2}, \ldots, \\
&\qquad \alpha\xi^{e+(\delta-1)n_1+sn_2}\}, \\
A_\delta &= \xi^{-n_1} A_{\delta-1} \cup \{b_\zeta\} \\
&= \{\alpha\xi^{e+sn_2}, \alpha\xi^{e+n_1+sn_2}, \ldots, \\
&\qquad \alpha\xi^{e+(\delta-2)n_1+sn_2}, \alpha\xi^{e+\zeta n_1+(s+1)n_2}\}, \\
A_{\delta+1} &= \xi^{-n_2} A_\delta \cup \{b_\zeta\} \\
&= \{\alpha\xi^{e+(s-1)n_2}, \ldots, \alpha\xi^{e+(\delta-2)n_1+(s-1)n_2}, \\
&\qquad \alpha\xi^{e+\zeta n_1+sn_2}, \alpha\xi^{e+\zeta n_1+(s+1)n_2}\}, \\
&\vdots \\
A_{\delta+s} &= \xi^{-n_2} A_{\delta+s-1} \cup \{b_\zeta\} = A_\zeta.
\end{aligned}$$

We have no $\xi^k \in \mathbb{F} \setminus \{0\}$ such that $\xi^k A_z \subseteq D$, for all $k \in \{0, \ldots, m-1\}$. Thus, we obtain $d(C) \geq |A_\zeta| = \delta + s$. □

Remark 2. Let C be a nontrivial λ-constacyclic code of length m over some subfield of $\mathbb{F}$ with zero set $L \subseteq \Omega$. Then, the Roos bound corresponds to the choice

$$\mathcal{B}_4(C) := \{(MN, |M|+d_N-1) : \text{there exists a consecutive set } M' \subseteq \Omega \text{ such that } M' \supseteq M \text{ with } |M'| \leq |M|+d_N-2\},$$

for any $\emptyset \neq MN \subseteq L$ with $MN = \frac{1}{\alpha}\bigcup_{\varepsilon\in M}\varepsilon N$. On the other hand, if we pick

$$\mathcal{B}_5(C) := \{(T_A, |A|) : A \subseteq \Omega \text{ is independent with respect to } L,\ T_A = A \cap L\},$$

then we obtain the shift bound.

B. Quasi-twisted codes and their concatenated structure

We assume the notation above and let ℓ be a positive integer. A linear code $C \subseteq \mathbb{F}_q^{m\ell}$ is called a λ-quasi-twisted (λ-QT) code of index ℓ and co-index m if it is invariant under the λ-constashift of codewords by ℓ positions and ℓ is the least positive integer with this property. In particular, if $\ell = 1$, then C is a λ-constacyclic code, and if $\lambda = 1$ or $q = 2$, then C is a QC code of index ℓ. If we view a codeword $\mathbf{c} \in C$ as an $m \times \ell$ array

$$\mathbf{c} = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix}, \tag{3}$$

then being invariant under λ-constashift by ℓ positions in $\mathbb{F}_q^{m\ell}$ corresponds to being closed under row λ-constashift in $\mathbb{F}_q^{m\times\ell}$.

If T_λ denotes the λ-constashift operator on $\mathbb{F}_q^{m\ell}$, we denote its action on $\mathbf{v} \in \mathbb{F}_q^{m\ell}$ by $T_\lambda\cdot\mathbf{v}$. Then $\mathbb{F}_q^{m\ell}$ has an $\mathbb{F}_q[x]$-module structure given by the multiplication

$$\begin{array}{rcl} \mathbb{F}_q[x] \times \mathbb{F}_q^{m\ell} & \longrightarrow & \mathbb{F}_q^{m\ell} \\ (a(x), \mathbf{v}) & \longmapsto & a(T_\lambda^\ell)\cdot\mathbf{v}. \end{array}$$

Note that, for $a(x) = x^m - \lambda$, we have $a(T_\lambda^\ell)\cdot\mathbf{v} = (T_\lambda^{m\ell})\cdot\mathbf{v} - \lambda\mathbf{v} = 0$. Hence, a multiplication by elements of R is induced on $\mathbb{F}_q^{m\ell}$ and it can be viewed as an R-module. Therefore, a λ-QT code $C \subseteq \mathbb{F}_q^{m\ell}$ of index ℓ is an R-submodule of $\mathbb{F}_q^{m\ell}$.

For an element $\mathbf{c} \in \mathbb{F}_q^{m\times\ell} \simeq \mathbb{F}_q^{m\ell}$, which is represented as in (3), we associate an element of R^ℓ (cf. (1))

$$\mathbf{c}(x) := (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) \in R^\ell, \tag{4}$$

where, for each $0 \le j \le \ell - 1$,

$$c_j(x) := c_{0,j} + c_{1,j}x + c_{2,j}x^2 + \cdots + c_{m-1,j}x^{m-1} \in R. \tag{5}$$

The isomorphism ϕ in (1) extends naturally to

$$\begin{array}{rcl} \Phi : \mathbb{F}_q^{m\ell} & \longrightarrow & R^\ell \\ \mathbf{c} = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \longmapsto & \mathbf{c}(x) \\ & & \| \\ & & (c_0(x), \ldots, c_{\ell-1}(x)) \\ \downarrow \quad\quad \downarrow & & \\ c_0(x) \quad \ldots \quad c_{\ell-1}(x) & & \end{array} \tag{6}$$

Observe that the row λ-constashift invariance in $\mathbb{F}_q^{m\times\ell}$ corresponds to being closed under componentwise multiplication by x in R^ℓ. Therefore, the map Φ above yields an R-module isomorphism and any λ-QT code $C \subseteq \mathbb{F}_q^{m\ell} \simeq \mathbb{F}_q^{m\times\ell}$ of index ℓ can be viewed as an R-submodule of R^ℓ.

We now describe the decomposition of a λ-QT code over $\mathbb{F}_q$ into shorter codes over (field) extensions of $\mathbb{F}_q$. We refer the reader to [16] for the respective proofs of the following assertions and for the treatment that includes the general repeated-root case (*i.e.*, when $\gcd(m, q) \ge 1$). We assume that $x^m - \lambda$ factors into irreducible polynomials in $\mathbb{F}_q[x]$ as

$$x^m - \lambda = f_1(x)f_2(x)\cdots f_s(x). \tag{7}$$

Since m is relatively prime to q, there are no repeating factors in (7). By the Chinese Remainder Theorem (CRT), we have the following ring isomorphism

$$R \cong \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle f_i(x)\rangle. \tag{8}$$

For each $i \in \{1, 2, \ldots, s\}$, let u_i be the smallest nonnegative integer such that $f_i(\alpha\xi^{u_i}) = 0$. The $\mathbb{F}_q$-conjugacy class (or the q-cyclotomic class) containing $\alpha\xi^{u_i}$ in Ω is defined as

$$\begin{aligned} \left[\alpha\xi^{u_i}\right] &= \left\{\alpha\xi^{u_i}, \alpha^q\xi^{qu_i}, \alpha^{q^2}\xi^{q^2u_i}, \ldots, \alpha^{q^{e_i-1}}\xi^{q^{e_i-1}u_i}\right\} \\ &\subseteq \Omega, \end{aligned} \tag{9}$$

where $e_i = \deg(f_i)$ and therefore $\left[\alpha\xi^{u_i}\right]$ contains all roots of the irreducible polynomial f_i, for each i. Note that Ω is a disjoint union of such $\mathbb{F}_q$-conjugacy classes.

Since the $f_i(x)$'s are irreducible, the direct summands in (8) can be viewed as field extensions of $\mathbb{F}_q$, obtained by adjoining the element $\alpha\xi^{u_i}$. If we set $\mathbb{E}_i := \mathbb{F}_q(\alpha\xi^{u_i}) \cong \mathbb{F}_q[x]/\langle f_i(x)\rangle$, for each $1 \le i \le s$, then $\mathbb{E}_i$ is an intermediate field between $\mathbb{F}$ and $\mathbb{F}_q$ such that $\left[\mathbb{E}_i : \mathbb{F}_q\right] = e_i$ and we have (cf. (8))

$$\begin{array}{rcl} R & \simeq & \mathbb{E}_1 \oplus \cdots \oplus \mathbb{E}_s \\ a(x) & \mapsto & \left(a(\alpha\xi^{u_1}), \ldots, a(\alpha\xi^{u_s})\right). \end{array} \tag{10}$$

This implies that

$$\begin{array}{rcl} R^\ell & \simeq & \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell \\ \mathbf{a}(x) & \mapsto & \left(\mathbf{a}(\alpha\xi^{u_1}), \ldots, \mathbf{a}(\alpha\xi^{u_s})\right), \end{array} \tag{11}$$

where $\mathbf{a}(\delta)$ denotes the componentwise evaluation at $\delta \in \mathbb{F}$, for any $\mathbf{a}(x) = \big(a_0(x), \ldots, a_{\ell-1}(x)\big) \in R^\ell$. Hence, a λ-QT code $C \subseteq R^\ell$ can be viewed as an $(\mathbb{E}_1 \oplus \cdots \oplus \mathbb{E}_s)$-submodule of $\mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell$ and it decomposes as

$$C \simeq C_1 \oplus \cdots \oplus C_s, \tag{12}$$

where C_i is a linear code in $\mathbb{E}_i^\ell$, for each i. These linear codes over various extensions of $\mathbb{F}_q$ are called the *constituents* of C (see [16, §7] for explicit examples).

Let $C \subseteq R^\ell$ be generated as an R-module by

$$\left\{\big(a_{1,0}(x), \ldots, a_{1,\ell-1}(x)\big), \ldots, \big(a_{r,0}(x), \ldots, a_{r,\ell-1}(x)\big)\right\}.$$

Then, for $1 \le i \le s$, we have

$$C_i = \mathrm{Span}_{\mathbb{E}_i}\left\{\big(a_{b,0}(\alpha\xi^{u_i}), \ldots, a_{b,\ell-1}(\alpha\xi^{u_i})\big) : 1 \le b \le r\right\}. \tag{13}$$

Note that each field $\mathbb{E}_i$ is isomorphic to a minimal λ-constacyclic code of length m over $\mathbb{F}_q$; namely, the λ-constacyclic code in $\mathbb{F}_q^m$ with the irreducible check polynomial $f_i(x)$. If we denote by θ_i the generating primitive idempotent (see [20, Theorem 1]) for the minimal λ-constacyclic code

$\langle\theta_i\rangle$ in consideration, then the isomorphism is given by the maps

$$\begin{array}{rcl@{\qquad}rcl} \varphi_i : \langle\theta_i\rangle & \longrightarrow & \mathbb{E}_i & \psi_i : \mathbb{E}_i & \longrightarrow & \langle\theta_i\rangle \\ a(x) & \longmapsto & a(\alpha\xi^{u_i}) & \delta & \longmapsto & \sum_{k=0}^{m-1} a_k x^k, \end{array} \tag{14}$$

where

$$a_k = \frac{1}{m}\mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}(\delta\alpha^{-k}\xi^{-ku_i}).$$

Observe that, for each $i \in \{1,\ldots,s\}$, the maps φ_i and ψ_i are inverses of each other, regardless of the choice of the representative in the $\mathbb{F}_q$-conjugacy class $[\alpha\xi^{u_i}]$, since $\mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}(\epsilon^q) = \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}(\epsilon)$, for any $\epsilon \in \mathbb{E}_i$.

If $\mathfrak{C}_i$ is a linear code in $\mathbb{E}_i^\ell$, for each i, then we denote its concatenation with $\langle\theta_i\rangle$ by $\langle\theta_i\rangle\square\mathfrak{C}_i$ and the concatenation is carried out by the map ψ_i. Here, $\langle\theta_i\rangle$ and $\mathfrak{C}_i$ are called the inner and outer codes of the concatenation, respectively.

Theorem 3. *[20, Theorem 2]*

i. Let C be an R-submodule of R^ℓ (i.e., a q-ary λ-QT code). Then, for some subset $\mathcal{I}$ of $\{1,\ldots,s\}$, there exist linear codes $\mathfrak{C}_i \subseteq \mathbb{E}_i^\ell$ such that

$$C = \bigoplus_{i\in\mathcal{I}} \langle\theta_i\rangle\square\mathfrak{C}_i.$$

ii. Conversely, let $\mathfrak{C}_i$ be a linear code over $\mathbb{E}_i$ of length ℓ, for each $i \in \mathcal{I} \subseteq \{1,\ldots,s\}$. Then,

$$C = \bigoplus_{i\in\mathcal{I}} \langle\theta_i\rangle\square\mathfrak{C}_i$$

is a q-ary λ-QT code of length $m\ell$ and index ℓ.

Moreover, each constituent C_i in (12) is equal to the outer code $\mathfrak{C}_i$ in the concatenated structure, for each i (see [20, Theorem 3]).

By (14) and Theorem 3, an arbitrary codeword $\mathbf{c} \in C$ can be written as an $m \times \ell$ array in the form (see [20])

$$\mathbf{c} = \frac{1}{m}\begin{pmatrix} \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}\left(\kappa_{i,t}\alpha^{-0}\xi^{-0u_i}\right)\right)_{0\le t\le \ell-1} \\ \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}\left(\kappa_{i,t}\alpha^{-1}\xi^{-u_i}\right)\right)_{0\le t\le \ell-1} \\ \vdots \\ \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}\left(\kappa_{i,t}\alpha^{-(m-1)}\xi^{-(m-1)u_i}\right)\right)_{0\le t\le \ell-1} \end{pmatrix}, \tag{15}$$

where $\kappa_i = (\kappa_{i,0},\ldots,\kappa_{i,\ell-1}) \in C_i$, for all i. Since $mC = C$, every codeword in C can still be written in the form of (15) with the constant $\frac{1}{m}$ removed.

Note that the trace representation in (15) involves traces down to $\mathbb{F}_q$ from various extensions. Recall that $\mathbb{F}$ is the splitting field of $x^m - \lambda$ and each $\mathbb{E}_i$ is an intermediate field extension between $\mathbb{F}$ and $\mathbb{F}_q$, for $1 \le i \le s$. The next lemma enables us to rewrite the traces in (15) from $\mathbb{F}$ to $\mathbb{F}_q$, instead of treating them over different extensions.

Lemma 4. *[12, Lemma 4.1] Let $\mathbb{F}_q \subset \mathbb{K} \subset \mathbb{L}$ be field extensions. If $b \in \mathbb{L}$ is an element with $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(b) = 1$, then we have $\mathrm{Tr}_{\mathbb{L}/\mathbb{F}_q}(b\mu) = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}_q}(\mu)$, for any $\mu \in \mathbb{K}$.*

Using Lemma 4, we can rewrite (15), without the constant $\frac{1}{m}$, as (cf. (4.3) in [12])

$$\mathbf{c} = \begin{pmatrix} \left(\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}\left(\sum_{i=1}^{s} b_i\kappa_{i,t}\alpha^{-0}\xi^{-0u_i}\right)\right)_{0\le t\le \ell-1} \\ \left(\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}\left(\sum_{i=1}^{s} b_i\kappa_{i,t}\alpha^{-1}\xi^{-u_i}\right)\right)_{0\le t\le \ell-1} \\ \vdots \\ \left(\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}\left(\sum_{i=1}^{s} b_i\kappa_{i,t}\alpha^{-(m-1)}\xi^{-(m-1)u_i}\right)\right)_{0\le t\le \ell-1} \end{pmatrix}, \tag{16}$$

where $b_1,\ldots,b_s \in \mathbb{F}$ are such that $\mathrm{Tr}_{\mathbb{F}/\mathbb{E}_i}(b_i) = 1$, for each $i \in \{1,\ldots,s\}$. Such b_i's exist since the trace map is onto.

Jensen derived a minimum distance bound in [15, Theorem 4], which is valid for all concatenated codes (*i.e.*, the inner and outer codes can be any linear code). Therefore, it applies to QT codes as well. We formulate the Jensen bound for QT codes as follows.

Theorem 5. *Let $C \subseteq R^\ell$ be a λ-QT code with the concatenated structure $C = \bigoplus_{i\in\mathcal{I}}\langle\theta_i\rangle\square C_i$, for some $\mathcal{I} \subseteq \{1,\ldots,s\}$. Assume that $C_{i_1},\ldots,C_{i_t}$ are the nonzero outer codes (constituents) of C, for $\{i_1,\ldots,i_t\} \subseteq \mathcal{I}$, such that $d(C_{i_1}) \le d(C_{i_2}) \le \cdots \le d(C_{i_t})$. Then we have*

$$d(C) \ge \min_{1\le r\le t}\left\{d(C_{i_r})d(\langle\theta_{i_1}\rangle \oplus \cdots \oplus \langle\theta_{i_r}\rangle)\right\}. \tag{17}$$

C. Spectral theory for quasi-twisted codes

Lally and Fitzpatrick proved in [18] that every QC code has a polynomial generating set in the form of a reduced Gröbner basis. We provide an easy adaptation of their findings for QT codes.

Consider the ring homomorphism:

$$\begin{array}{rcl} \Psi : \mathbb{F}_q[x]^\ell & \longrightarrow & R^\ell \\ (\widetilde{f}_0(x),\ldots,\widetilde{f}_{\ell-1}(x)) & \longmapsto & (f_0(x),\ldots,f_{\ell-1}(x)), \end{array} \tag{18}$$

which projects elements in $\mathbb{F}_q[x]^\ell$ onto R^ℓ in the obvious way. Given a λ-QT code $C \subseteq R^\ell$, it follows that the preimage $\widetilde{C}$ of C in $\mathbb{F}_q[x]^\ell$ is an $\mathbb{F}_q[x]$-submodule containing $\widetilde{K} = \{(x^m-\lambda)\mathbf{e}_j : 0 \le j \le \ell-1\}$, where each $\mathbf{e}_j$ denotes the standard basis vector of length ℓ with 1 at the j^{th} coordinate and 0 elsewhere. The tilde will represent throughout structures over $\mathbb{F}_q[x]$.

Since $\widetilde{C}$ is a submodule of the finitely generated free module $\mathbb{F}_q[x]^\ell$ over the principal ideal domain $\mathbb{F}_q[x]$ and contains $\widetilde{K}$, it has a generating set of the form

$$\{\mathbf{u}_1,\ldots,\mathbf{u}_p,(x^m-\lambda)\mathbf{e}_0,\ldots,(x^m-\lambda)\mathbf{e}_{\ell-1}\},$$

where p is a nonnegative integer and when $p > 0$, $\mathbf{u}_b = (u_{b,0}(x),\ldots,u_{b,\ell-1}(x)) \in \mathbb{F}_q[x]^\ell$, for each $b \in \{1,\ldots,p\}$. Hence, the rows of

$$\mathcal{G} = \begin{pmatrix} u_{1,0}(x) & \dots & u_{1,\ell-1}(x) \\ \vdots & & \vdots \\ u_{p,0}(x) & \dots & u_{p,\ell-1}(x) \\ x^m - \lambda & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & x^m - \lambda \end{pmatrix}$$

generate $\widetilde{C}$. By using elementary row operations, we triangularise $\mathcal{G}$ so that another equivalent generating set is obtained from the rows of an upper-triangular $\ell \times \ell$ matrix over $\mathbb{F}_q[x]$ as:

$$\widetilde{G}(x) = \begin{pmatrix} g_{0,0}(x) & g_{0,1}(x) & \dots & g_{0,\ell-1}(x) \\ 0 & g_{1,1}(x) & \dots & g_{1,\ell-1}(x) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g_{\ell-1,\ell-1}(x) \end{pmatrix}, \quad (19)$$

where $\widetilde{G}(x)$ satisfies the following conditions (see [18, Theorem 2.1]):

1) $g_{i,j}(x) = 0$, for all $0 \le j < i \le \ell - 1$.
2) $\deg(g_{i,j}(x)) < \deg(g_{j,j}(x))$, for all $i < j$.
3) $g_{j,j}(x) \mid (x^m - \lambda)$, for all $0 \le j \le \ell - 1$.
4) If $g_{j,j}(x) = (x^m - \lambda)$, then $g_{i,j}(x) = 0$, for all $i \ne j$.

Note that the rows of $\widetilde{G}(x)$ are nonzero and each nonzero element of $\widetilde{C}$ can be expressed in the form

$$(0, \dots, 0, c_j(x), \dots, c_{\ell-1}(x)), \text{ where } j \ge 0,\ c_j(x) \ne 0 \text{ and } g_{j,j}(x) \mid c_j(x).$$

This implies that the rows of $\widetilde{G}(x)$ form a Gröbner basis of $\widetilde{C}$ with respect to the position-over-term (POT) order in $\mathbb{F}_q[x]$, where the standard basis vectors $\{\mathbf{e}_0, \dots, \mathbf{e}_{\ell-1}\}$ and the monomials x^n are ordered naturally in each component. Moreover, the second condition above implies that the rows of $\widetilde{G}(x)$ provide a reduced Gröbner basis for $\widetilde{C}$, which is uniquely defined, up to multiplication by constants, with monic diagonal elements.

Let $G(x)$ be the matrix with the rows of $\widetilde{G}(x)$ under the image of the homomorphism Ψ in (18). Clearly, the rows of $G(x) := \widetilde{G}(x) \mod I$ is an R-generating set for C. When C is the trivial zero code of length $m\ell$, we have $p = 0$, which gives $G(x) = \mathbf{0}_\ell$. Otherwise, we say that C is an r-generator λ-QT code, generated as an R-submodule, if $G(x)$ has r (nonzero) rows. The $\mathbb{F}_q$-dimension of C is given by (see [18, Corollary 2.4] for the proof)

$$m\ell - \sum_{j=0}^{\ell-1} \deg(g_{j,j}(x)) = \sum_{j=0}^{\ell-1} [m - \deg(g_{j,j}(x))]. \quad (20)$$

In [25], Semenov and Trifonov used the polynomial matrix $\widetilde{G}(x)$ in (19) to develop a spectral theory for QC codes, which gives rise to a BCH-like minimum distance bound. Their bound was improved by Zeh and Ling in [28] by using the HT bound ([13]), which generalizes the BCH bound for cyclic codes. We now translate their results from QC to QT codes.

Given a λ-QT code $C \subseteq R^\ell$, let the associated $\ell \times \ell$ upper-triangular matrix $\widetilde{G}(x)$ be as in (19) with entries in $\mathbb{F}_q[x]$. The *determinant* of $\widetilde{G}(x)$ is defined as

$$\det(\widetilde{G}(x)) := \prod_{j=0}^{\ell-1} g_{j,j}(x)$$

and an *eigenvalue* β of C is a root of $\det(\widetilde{G}(x))$. Note that all eigenvalues are elements of Ω (*i.e.*, $\beta = \alpha\xi^k$, for some $k \in \{0, \dots, m-1\}$), since $g_{j,j}(x) \mid (x^m - \lambda)$, for each $0 \le j \le \ell - 1$. The *algebraic multiplicity* of β is the largest integer a such that $(x - \beta)^a \mid \det(\widetilde{G}(x))$. The *geometric multiplicity* of β is defined as the dimension of the null space of $\widetilde{G}(\beta)$, where this null space is called the *eigenspace* of β and it is denoted by $\mathcal{V}_\beta$. In other words, we have

$$\mathcal{V}_\beta := \{\mathbf{v} \in \mathbb{F}^\ell : \widetilde{G}(\beta)\mathbf{v}^\top = \mathbf{0}_\ell^\top\},$$

where $\mathbb{F}$ is the splitting field of $x^m - \lambda$ as before. Semenov and Trifonov showed in [25] that, for a given QC code and the associated $\widetilde{G}(x) \in \mathbb{F}_q[x]^{\ell \times \ell}$, the algebraic multiplicity a of an eigenvalue β is equal to its geometric multiplicity $\dim_{\mathbb{F}}(\mathcal{V}_\beta)$. We state the QT analogue of this result below, which can be shown in the same way and therefore the proof is omitted.

Lemma 6. *[25, Lemma 1] The algebraic multiplicity of any eigenvalue of a λ-QT code C is equal to its geometric multiplicity.*

Throughout, we let $\overline{\Omega} \subseteq \Omega$ denote the set of all eigenvalues of C. Notice that $\overline{\Omega} = \emptyset$ if and only if the diagonal elements $g_{j,j}(x)$ in $\widetilde{G}(x)$ are constant polynomials and C is the trivial full space code. From this point on, we exclude the full space code and we assume that $|\overline{\Omega}| = t > 0$. Choose an arbitrary eigenvalue $\beta_i \in \overline{\Omega}$ with multiplicity n_i, for some $i \in \{1, \dots, t\}$. Let $\{\mathbf{v}_{i,0}, \dots, \mathbf{v}_{i,n_i-1}\}$ be a basis for the corresponding eigenspace $\mathcal{V}_i$. Consider the matrix

$$V_i := \begin{pmatrix} \mathbf{v}_{i,0} \\ \vdots \\ \mathbf{v}_{i,n_i-1} \end{pmatrix} = \begin{pmatrix} v_{i,0,0} & \dots & v_{i,0,\ell-1} \\ \vdots & \vdots & \vdots \\ v_{i,n_i-1,0} & \dots & v_{i,n_i-1,\ell-1} \end{pmatrix}, \quad (21)$$

having the basis elements as its rows. We let

$$H_i := (1, \beta_i, \dots, \beta_i^{m-1}) \otimes V_i$$

and define

$$H := \begin{pmatrix} H_1 \\ \vdots \\ H_t \end{pmatrix} = \begin{pmatrix} V_1 & \beta_1 V_1 & \dots & \beta_1^{m-1} V_1 \\ \vdots & \vdots & & \vdots \\ V_t & \beta_t V_t & \dots & \beta_t^{m-1} V_t \end{pmatrix}. \quad (22)$$

Observe that H has $n := \sum_{i=1}^t n_i$ rows. By Lemma 6, we have $n = \sum_{j=0}^{\ell-1} \deg(g_{j,j}(x))$. To prove the following lemma, it remains to show that all these n rows are linearly independent, which was already shown in [25, Lemma 2].

Lemma 7. *The rank of the matrix H in (22) is equal to $m\ell - \dim_{\mathbb{F}_q}(C)$.*

We observe that $H\mathbf{c}^\top = \mathbf{0}_n^\top$, for any codeword $\mathbf{c} \in C$. Together with Lemma 7, we easily obtain the following result (see [25, Theorem 1] for the QC analogue of the result).

Proposition 8. *The $n \times m\ell$ matrix H in (22) is a parity-check matrix for C.*

Remark 3. The eigenvalues are the QT analogues of the zeros of constacyclic codes. Recall that a constacyclic code has an empty zero set if and only if it is equal to the full space. Similarly, $\overline{\Omega} = \emptyset$ if and only if $C = \mathbb{F}_q^{m\ell}$. In this case, the construction of the parity-check matrix H in (22) is impossible, hence, we have assumed $\overline{\Omega} \neq \emptyset$. The other extreme case is when the zero set of a given constacyclic code is Ω, which implies that we have the trivial zero code. However, we emphasize that a λ-QT code with $\overline{\Omega} = \Omega$ is not necessarily the zero code. By using Lemma 7 above, one can easily deduce that a given λ-QT code C is the zero code $\{\mathbf{0}_{m\ell}\}$ if and only if $\overline{\Omega} = \Omega$, each $\mathcal{V}_i = \mathbb{F}^\ell$ (equivalently, each $V_i = I_\ell$, where I_ℓ denotes the $\ell \times \ell$ identity matrix), and $n = m\ell$ so that we obtain $H = I_{m\ell}$. On the other hand, $\overline{\Omega} = \Omega$ whenever $(x^m - \lambda) \mid \det(\widetilde{G}(x))$ but C is nontrivial unless each m^{th} root of λ in Ω has multiplicity ℓ, which happens only if $\widetilde{G}(x) = (x^m - \lambda)I_\ell$.

Definition 1. We define the *eigencode* corresponding to an eigenspace $\mathcal{V} \subseteq \mathbb{F}^\ell$ by

$$\mathbb{C}(\mathcal{V}) = \mathbb{C} := \left\{ \mathbf{u} \in \mathbb{F}_q^\ell \ : \ \sum_{j=0}^{\ell-1} v_j u_j = 0, \forall \mathbf{v} \in \mathcal{V} \right\}.$$

In case we have $\mathbb{C} = \{\mathbf{0}_\ell\}$, then it is assumed that $d(\mathbb{C}) = \infty$.

Semenov and Trifonov proved a BCH-like minimum distance bound for a given QC code (see [25, Theorem 2]), which is expressed in terms of the size of a consecutive subset of eigenvalues in $\overline{\Omega}$ and the minimum distance of the common eigencode related to this consecutive subset. Zeh and Ling generalized their approach and derived an HT-like bound in [28, Theorem 1] without using the parity-check matrix in their proof. The eigencode, however, is still needed. In [11], a general spectral bound is proven for any QT code with a nonempty set of eigenvalues that is different from Ω. The QT analogues of Semenov-Trifonov and Zeh-Ling bounds were proven in terms of the Roos-like and shift-like bounds as a corollary. The observations in the next section are crucial for extending this bound to the general case of any nonempty set of eigenvalues.

III. Eigencodes and Constituents

Recall the factorization into irreducibles $x^m - \lambda = f_1(x) \cdots f_s(x)$ given in (7). If we fix a root $\alpha\xi^{u_i}$ of $f_i(x)$, for each $i \in \{1, \ldots, s\}$, then we know that Ω is the disjoint union of the $\mathbb{F}_q$-conjugacy classes $\left[\alpha\xi^{u_i}\right]$, each of the form as in (9) and of size $e_i = \deg(f_i)$. By Theorem 3, any λ-QT code C, viewed as an R-submodule of R^ℓ, decomposes as

$$C = \bigoplus_{i=1}^{s} \langle \theta_i \rangle \square C_i, \tag{23}$$

where each inner code $\langle \theta_i \rangle$ is a minimal λ-constacyclic code of length m satisfying $\langle \theta_i \rangle \cong \mathbb{E}_i \cong \mathbb{F}_q[x]/\langle f_i(x) \rangle$ (see (14)) and each outer code (constituent) C_i is a linear code in $\mathbb{E}_i^\ell$, for $i \in \{1, \ldots, s\}$. By using (11) and (13), we can write each constituent C_i explicitly as

$$C_i = \left\{ \mathbf{c}(\alpha\xi^{u_i}) : \mathbf{c}(x) \in C \right\}. \tag{24}$$

On the other hand, any codeword $\mathbf{c}(x) \in C$ is of the form $\mathbf{c}(x) = \mathbf{a}(x)\widetilde{G}(x) \mod I$, for some $\mathbf{a}(x) \in \mathbb{F}_q[x]^\ell$. Hence, the $\mathbb{E}_i$-span of the rows of $\widetilde{G}(\alpha\xi^{u_i})$ is the constituent C_i, for each i. If all the diagonal elements in $\widetilde{G}(\alpha\xi^{u_i})$ are nonzero (*i.e.*, $\widetilde{G}(\alpha\xi^{u_i})$ has full rank ℓ), then $C_i = \mathbb{E}_i^\ell$ and $\alpha\xi^{u_i}$ is *not* an eigenvalue of C. Otherwise, $\alpha\xi^{u_i}$ is an eigenvalue of C and the corresponding nonzero eigenspace $\mathcal{V}_i$ is described as $\mathcal{V}_i = \{\mathbf{v} \in \mathbb{F}^\ell : \widetilde{G}(\alpha\xi^{u_i})\mathbf{v}^\top = \mathbf{0}_\ell^\top\}$. Now let $\overline{C}_i$ denote the $\mathbb{F}$-span of the rows of $\widetilde{G}(\alpha\xi^{u_i})$, for each i, which immediately implies $\mathcal{V}_i = \overline{C}_i^\perp$. Clearly, each constituent C_i is the $\mathbb{E}_i$-subcode of $\overline{C}_i$, for all i. Note that the $\mathbb{F}$-span of the rows of $\widetilde{G}(\alpha^q\xi^{qu_i})$ is

$$\begin{aligned} \overline{C}_i^q &= \{(d_0^q, \ldots, d_{\ell-1}^q) : (d_0, \ldots, d_{\ell-1}) \in \overline{C}_i\} \\ &\supseteq C_i^q = \{\mathbf{c}(\alpha^q\xi^{qu_i}) : \mathbf{c}(x) \in C\}, \end{aligned}$$

for any $i \in \{1, \ldots, s\}$. Since each entry of $\widetilde{G}(\alpha^q\xi^{qu_i})$ is the q^{th} power of the corresponding entry in $\widetilde{G}(\alpha\xi^{u_i})$, for each i, the dual of $\overline{C}_i^q$ consists of elements $\mathbf{v}^q = (v_0^q, \ldots, v_{\ell-1}^q)$, where $\mathbf{v} \in \mathcal{V}_i$, which implies the following.

Lemma 9. *If $\alpha\xi^{u_i}$ is an eigenvalue of C, for some $i \in \{1, \ldots, s\}$, then all elements in its $\mathbb{F}_q$-conjugacy class $\left[\alpha\xi^{u_i}\right]$ are also eigenvalues with respective eigenspaces $[\mathcal{V}_i] := \left\{\mathcal{V}_i, \mathcal{V}_i^q, \ldots, \mathcal{V}_i^{q^{e_i-1}}\right\}$.*

Recall that, for each $1 \leq i \leq s$, the eigencode $\mathbb{C}_i$ corresponding to the eigenspace $\mathcal{V}_i$ is given as (cf. Definition 1)

$$\mathbb{C}_i = \left\{ \mathbf{u} \in \mathbb{F}_q^\ell \ : \ \sum_{j=0}^{\ell-1} v_j u_j = 0, \forall \mathbf{v} \in \mathcal{V}_i \right\}.$$

The fact that $\mathcal{V}_i = \overline{C}_i^\perp$ implies $\mathbb{C}_i = \overline{C}_i\big|_{\mathbb{F}_q}$. Obviously, $\overline{C}_i\big|_{\mathbb{F}_q} = \overline{C}_i^q\big|_{\mathbb{F}_q} = \cdots = \overline{C}_i^{q^{e_i-1}}\big|_{\mathbb{F}_q}$ and, therefore, $\mathbb{C}_i$ is the common eigencode of all the eigenspaces in $[\mathcal{V}_i]$.

Lemma 10. *For each $1 \leq i \leq s$, the eigencode $\mathbb{C}_i$ corresponding to the eigenspaces in $[\mathcal{V}_i]$ is the $\mathbb{F}_q$-subcode of $\overline{C}_i$.*

Now we reorder the constituents. Let $C_1 = \cdots = C_r = \{\mathbf{0}_\ell\}$ be the zero constituents. Let $C_{r+1} = \cdots = C_t$ be the full space constituents, where $\widetilde{G}(\alpha\xi^{u_i})$ has full rank ℓ, for $r+1 \leq i \leq t$. Note that $\widetilde{G}(\alpha\xi^{u_i})$ having full rank ℓ is equivalent to $\alpha\xi^{u_i}$ not being an eigenvalue and, therefore, $\left[\alpha\xi^{u_i}\right] \notin \overline{\Omega}$, for $r+1 \leq i \leq t$. Finally, let $C_{t+1}, \ldots, C_s$ be the nontrivial constituents, *i.e.*, they are neither the full space codes nor the zero codes. We have the disjoint unions

$$\Omega = \bigcup_{i=1}^{s} \left[\alpha\xi^{u_i}\right] \quad \text{and} \quad \Omega \setminus \overline{\Omega} = \bigcup_{i=r+1}^{t} \left[\alpha\xi^{u_i}\right]. \tag{25}$$

Let Γ denote the set of indices

$$\Gamma := \{1, \ldots, r, t+1, \ldots, s\} = \{1, \ldots, s\} \backslash \{r+1, \ldots, t\} \tag{26}$$

such that $\overline{\Omega} = \bigcup_{i\in\Gamma} \left[\alpha\xi^{u_i}\right]$, by (25). The common eigenspace $\mathcal{V}_{\overline{\Omega}}$ satisfies

$$\mathcal{V}_{\overline{\Omega}} = \bigcap_{\beta\in\overline{\Omega}} \mathcal{V}_\beta = \bigcap_{i\in\Gamma} \bigcap_{j=0}^{e_i-1} \mathcal{V}_i^{q^j}$$

and the associated eigencode is

$$\begin{aligned} \mathbb{C}_{\overline{\Omega}} = (\mathcal{V}_{\overline{\Omega}})^\perp\Big|_{\mathbb{F}_q} &= \left(\sum_{i\in\Gamma}\sum_{j=0}^{e_i-1} (\mathcal{V}_i^{q^j})^\perp\right)\Big|_{\mathbb{F}_q} \qquad (27)\\ &= \left(\sum_{i\in\Gamma}\sum_{j=0}^{e_i-1} \overline{C}_i^{q^j}\right)\Big|_{\mathbb{F}_q}. \end{aligned}$$

A linear code $\mathcal{C}$ of length n over a field $\mathbb{K} \supseteq \mathbb{F}_q$ is called *Galois closed* if $\mathcal{C} = \mathcal{C}^q$, where

$$\mathcal{C}^q := \left\{(c_0^q, c_1^q, \ldots, c_{n-1}^q) \,:\, (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}\right\}.$$

With this definition, it is easy to observe that $(\mathcal{V}_{\overline{\Omega}})^\perp$ is Galois closed. Theorem 12.17 in [4] says $d(\mathcal{C}) = d(\mathcal{C}|_{\mathbb{F}_q})$ if $\mathcal{C}$ is Galois closed. Therefore, we conclude that $d((\mathcal{V}_{\overline{\Omega}})^\perp) = d(\mathbb{C}_{\overline{\Omega}})$. Note that each constituent code C_i, for $i \in \Gamma$, is the subfield subcode of a summand $\overline{C}_i$ in $(\mathcal{V}_{\overline{\Omega}})^\perp$ and it is a well-known fact that $d(A) \geq d(A+B)$, for any pair of linear codes A and B. Hence, we obtain the following.

Lemma 11. *Let C be a λ-QT code with a nonempty eigenvalue set $\overline{\Omega} \subseteq \Omega$ which decomposes as in (23). Then*

$$d(C_i) \geq d(\overline{C}_i) \geq d\left((\mathcal{V}_{\overline{\Omega}})^\perp\right) = d\left((\mathcal{V}_{\overline{\Omega}})^\perp\big|_{\mathbb{F}_q}\right) = d(\mathbb{C}_{\overline{\Omega}}),$$

for each $i \in \Gamma$.

Equation (27) will play a key role in the next two sections. It is part of the proof of the general spectral bound in Section IV. Together with Lemma 11, the equation allows us to compare the Jensen and spectral bounds in Section V, where an analogous relation between the Lally and spectral bounds follows as a result of similar observations.

IV. Spectral bound for quasi-twisted codes

The general spectral bound proven in [11, Theorem 11] was shown for QT codes with nonempty eigenvalue set $\overline{\Omega} \subsetneq \Omega$. In fact, the bound remains valid when $\overline{\Omega} = \Omega$. To show this we need the following Lemma.

Lemma 12. *Let C be a λ-QT code of length $m\ell$ and index ℓ over $\mathbb{F}_q$ with $\overline{\Omega} = \Omega$. Then $C = \{\mathbf{0}_{m\ell}\}$ if and only if $\mathbb{C}_\Omega = \{\mathbf{0}_\ell\}$.*

Proof. Let B be the q-ary linear code of length ℓ that is generated by the rows of the codewords in C, which are represented as the $m \times \ell$ arrays in (3) or, equivalently, as in (16). That is, the codewords of B are generated by the elements

$$\left(\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}\left(\sum_{i=1}^{s} b_i\kappa_{i,t}\,\alpha^{-k}\,\xi^{-ku_i}\right)\right)_{0\leq t\leq \ell-1},$$

where $k \in \{0, \ldots, m-1\}$, $b_i \in \mathbb{F}$ such that $\mathrm{Tr}_{\mathbb{F}/\mathbb{E}_i}(b_i) = 1$, and each $\kappa_i = (\kappa_{i,0}, \ldots, \kappa_{i,\ell-1})$ is a codeword in the constituent C_i, for all i.

Since we have assumed that the λ-QT code C has the eigenvalue set $\overline{\Omega} = \Omega$, we cannot have full space constituents. In order to have a constituent code that has full rank, there must be at least one m^{th} root of λ which is not a root of any diagonal element in the upper-triangular matrix $\widetilde{G}(x)$ that corresponds to C. Together with the notation provided in (26), we rewrite the generators of B as

$$\left(\mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}\left(\sum_{i\in\Gamma} b_i\kappa_{i,t}\,\alpha^{-k}\,\xi^{-ku_i}\right)\right)_{0\leq t\leq \ell-1}. \qquad (28)$$

On the other hand, recall that $\mathbb{C}_{\overline{\Omega}} = (\mathcal{V}_{\overline{\Omega}})^\perp|_{\mathbb{F}_q}$, where $(\mathcal{V}_{\overline{\Omega}})^\perp$ is Galois closed. Theorem 12.17 in [4] tells us that, if a linear code $\mathcal{C}$ over a field $\mathbb{K} \supseteq \mathbb{F}_q$ is Galois closed, then $\mathcal{C}|_{\mathbb{F}_q} = \mathrm{Tr}_{\mathbb{K}/\mathbb{F}_q}(\mathcal{C})$. Using this property, we rewrite (27) as

$$\begin{aligned} \mathbb{C}_\Omega = \mathbb{C}_{\overline{\Omega}} = (\mathcal{V}_{\overline{\Omega}})^\perp\Big|_{\mathbb{F}_q} &= \left(\sum_{i\in\Gamma}\sum_{j=0}^{e_i-1} (\mathcal{V}_i^{q^j})^\perp\right)\Big|_{\mathbb{F}_q}\\ &= \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}\left(\sum_{i\in\Gamma}\sum_{j=0}^{e_i-1} (\mathcal{V}_i^{q^j})^\perp\right)\\ &= \mathrm{Tr}_{\mathbb{F}/\mathbb{F}_q}\left(\sum_{i\in\Gamma}\sum_{j=0}^{e_i-1} \overline{C}_i^{q^j}\right). \qquad (29) \end{aligned}$$

It is clear that if $C = \{\mathbf{0}_{m\ell}\}$, then $\mathcal{V}_\Omega = \mathbb{F}^\ell$ and therefore $\mathbb{C}_\Omega = \{\mathbf{0}_\ell\}$. For the converse, note that, for each $i \in \Gamma$, we have $b_i\kappa_i \in \overline{C}_i$ since $\kappa_i \in C_i$ and $b_i \in \mathbb{F}$. Using (28) and (29), one can easily see that B is a subcode of $\mathbb{C}_\Omega$. Hence, if $\mathbb{C}_\Omega = \{\mathbf{0}_\ell\}$, then $B = \{\mathbf{0}_\ell\}$, which immediately implies $C = \{\mathbf{0}_{m\ell}\}$. □

Now we are ready to state and prove a general spectral bound for a given λ-QT code.

Theorem 13. *Let $C \subseteq R^\ell$ be a λ-QT code of index ℓ with nonempty eigenvalue set $\overline{\Omega} \subseteq \Omega$, let $D_{\overline{\Omega}}$ be the λ-constacyclic code of length m over $\mathbb{F}$ with zero set $\overline{\Omega}$ and let $\mathcal{B}(D_{\overline{\Omega}}) \subseteq \mathcal{P}(\Omega) \times (\mathbb{N} \cup \{\infty\})$ be an arbitrary family of defining set bounds for $D_{\overline{\Omega}}$. For any nonempty $P \subseteq \overline{\Omega}$ such that $(P, d_P) \in \mathcal{B}(D_{\overline{\Omega}})$, we define $\mathcal{V}_P := \bigcap_{\beta\in P} \mathcal{V}_\beta$ as the common eigenspace of the eigenvalues in P and let $\mathbb{C}_P = (\mathcal{V}_P)^\perp\big|_{\mathbb{F}_q}$ denote the corresponding eigencode. Then,*

$$d(C) \geq \min\left\{d_P, d(\mathbb{C}_P)\right\}.$$

Proof. Given the λ-QT code C with nonempty eigenvalue set $\overline{\Omega} \subseteq \Omega$, we first consider the case when $P = \overline{\Omega} = \Omega$ and $d_\Omega = d(D_\Omega)$, where the λ-constacyclic code $D_\Omega \subseteq \mathbb{F}^m$ has Ω as its zero set. Recall that we always have $d_\Omega = \infty$ in this case since $D_\Omega = \{\mathbf{0}_m\}$. Moreover, by Lemma 12, C is the zero code if and only if $\mathbb{C}_\Omega = \{\mathbf{0}_\ell\}$ if and only if $d(\mathbb{C}_\Omega) = \infty$. Hence, we have shown that both d_Ω and $d(\mathbb{C}_\Omega)$ become ∞ if and only if $C = \{\mathbf{0}_{m\ell}\}$. If C is not the zero code, then the rows of any codeword $\mathbf{c} \in C$, represented as in (3), lie in $\mathbb{C}_\Omega$, as shown in the proof of Lemma 12. This immediately implies that $\mathrm{wt}(\mathbf{c}) \geq d(\mathbb{C}_\Omega)$, for any nonzero $\mathbf{c} \in C$, and we get $d(C) \geq \min\{d_\Omega, d(\mathbb{C}_\Omega)\} = d(\mathbb{C}_\Omega)$.

Thus, it remains to prove that $d(C) \geq \min\{d_P, d(\mathbb{C}_P)\}$, for any fixed $\emptyset \neq P \subseteq \overline{\Omega} \subseteq \Omega$ such that $(P, d_P) \in \mathcal{B}(D_{\overline{\Omega}})$ and d_P is finite. To do this, we assume that $P = \{\alpha\xi^{u_1}, \alpha\xi^{u_2}, \ldots, \alpha\xi^{u_r}\} \subseteq \overline{\Omega}$, where $0 < r < m$. We define

$$\widetilde{H}_P := \begin{pmatrix} 1 & \alpha\xi^{u_1} & (\alpha\xi^{u_1})^2 & \ldots & (\alpha\xi^{u_1})^{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha\xi^{u_r} & (\alpha\xi^{u_r})^2 & \ldots & (\alpha\xi^{u_r})^{m-1} \end{pmatrix}. \quad (30)$$

Recall that P is the zero set of some $D_P \subseteq \mathbb{F}^m$, which contains $D_{\overline{\Omega}}$ as a subcode, and $\widetilde{H}_P$ is a parity-check matrix of this D_P. Note that $d(D_{\overline{\Omega}}) \geq d(D_P) \geq d_P$, by definition.

In the rest of the proof we focus on the quantity $\min\{d_P, d(\mathbb{C}_P)\}$. We have assumed $P \neq \emptyset$ to ensure that $\widetilde{H}_P$ is well-defined. For any nonzero λ-QT code C, we have $d(C) \geq 1$. In particular, when $\mathcal{V}_P = \{\mathbf{0}_\ell\}$, which implies $\mathbb{C}_P = \mathbb{F}_q^\ell$ and $d(\mathbb{C}_P) = 1$, we have $d(C) \geq 1 = \min\{d_P, d(\mathbb{C}_P)\}$ since $d_P \geq 1$.

Now assume that $\mathcal{V}_P \neq \{\mathbf{0}_\ell\}$ and let V_P be the matrix, say of size $t \times \ell$, whose rows form a basis for the common eigenspace $\mathcal{V}_P$ (cf. (21)). If we set $\widehat{H}_P := \widetilde{H}_P \otimes V_P$, then $\widehat{H}_P\, \mathbf{c}^\top = \mathbf{0}_{rt}^\top$, for all $\mathbf{c} \in C$. In other words, $\widehat{H}_P$ is a submatrix of some matrix H of the form in (22).

Recall that d_P is assumed to be finite. If $d_P = 1$, then $\min\{d_P, d(\mathbb{C}_P)\} = 1$, so $d(C) \geq 1 = \min\{d_P, d(\mathbb{C}_P)\}$ as above.

When $d_P \geq 2$, we have $\min\{d_P, d(\mathbb{C}_P)\} = 1$ if and only if $d(\mathbb{C}_P) = 1$, in which case we have $d(C) \geq \min\{d_P, d(\mathbb{C}_P)\} = 1$ automatically.

We now let $d_P \geq 2$ and $d(\mathbb{C}_P) \geq 2$ (hence, $\widehat{H}_P$ is well-defined). We assume the existence of a codeword $\mathbf{c} \in C$ of weight ω such that $0 < \omega < \min\{d_P, d(\mathbb{C}_P)\}$. For each $0 \leq k \leq m-1$, let $\mathbf{c}_k = (c_{k,0}, \ldots, c_{k,\ell-1})$ be the k^{th} row of the codeword $\mathbf{c}$ given as in (3) and we consider the column vector $\mathbf{s}_k := V_P\, \mathbf{c}_k^\top$. Since $d(\mathbb{C}_P) > \omega$ and $\mathrm{wt}(\mathbf{c}_k) \leq \omega$, we have $\mathbf{c}_k \notin \mathbb{C}_P$ and therefore $\mathbf{s}_k = V_P\, \mathbf{c}_k^\top \neq \mathbf{0}_t^\top$, for all $\mathbf{c}_k \neq \mathbf{0}_\ell$, $k \in \{0, \ldots, m-1\}$. Hence, $0 < |\{\mathbf{s}_k : \mathbf{s}_k \neq \mathbf{0}_t^\top\}| \leq \omega < \min\{d_P, d(\mathbb{C}_P)\}$. Let $S := [\mathbf{s}_0\ \mathbf{s}_1 \cdots \mathbf{s}_{m-1}]$. Then $\widetilde{H}_P\, S^\top = \mathbf{0}_{r\times t}^\top$, which implies that the rows of the matrix S lie in the right kernel of $\widetilde{H}_P$. In other words, any row of S lies in $D_P \subseteq \mathbb{F}^m$ and there is at least one nonzero row in S, so by definition of d_P, the weight of this nonzero row of S must be at least d_P. But this is a contradiction since any row of S has weight at most $\omega < d_P$. □

We emphasize that Theorem 13 allows us to use *any* defining set bound derived for constacyclic codes. The following special cases are immediate after the preparation in Section II (cf. Theorems 1 and 2, and Remark 2). The proof is omitted since it is identical to that of [11, Corollary 12].

Corollary 3. *Let $C \subseteq R^\ell$ be a λ-QT code of index ℓ with $\overline{\Omega} \subseteq \Omega$ as its nonempty set of eigenvalues.*

i. Let N and M be two nonempty subsets of Ω such that $MN \subseteq \overline{\Omega}$, where $MN := \frac{1}{\alpha}\bigcup_{\varepsilon\in M} \varepsilon N$. If there exists a consecutive set $M' \supseteq M$ with $|M'| \leq |M| + d_N - 2$, then $d(C) \geq \min(|M| + d_N - 1, d(\mathbb{C}_{MN}))$.

ii. For every $A \subseteq \Omega$ that is independent with respect to $\overline{\Omega}$, we have $d(C) \geq \min(|A|, d(\mathbb{C}_{T_A}))$, where $T_A := A \cap \overline{\Omega}$.

Remark 4. By using Remark 1 and Corollary 2, we can obtain the QT analogues of the BCH-like bound given in [25, Theorem 2] and the HT-like bound in [28, Theorem 1].

Let the λ-QT code C with nonempty eigenvalue set $\overline{\Omega} \subseteq \Omega$ and the associated λ-constacyclic code $D_{\overline{\Omega}} \subseteq \mathbb{F}^m$ with the selected collection of defining set bounds $\mathcal{B}(D_{\overline{\Omega}})$ be given as in Theorem 13. From this point on, we denote the estimate of the spectral bound by

$$d_{Spec}(\mathcal{B}(D_{\overline{\Omega}}); P, d_P) := \min\{d_P, d(\mathbb{C}_P)\},$$

where $\emptyset \neq P \subseteq \overline{\Omega}$ such that $(P, d_P) \in \mathcal{B}(D_{\overline{\Omega}})$, and we set

$$d_{Spec}(\mathcal{B}(D_{\overline{\Omega}})) := \max_{\substack{(P,d_P)\in\mathcal{B}(D_{\overline{\Omega}}) \\ \emptyset\neq P\subseteq\overline{\Omega}}} \left\{d_{Spec}(\mathcal{B}(D_{\overline{\Omega}}); P, d_P)\right\}.$$

Observe that $d_{Spec}(\mathcal{B}(D_{\overline{\Omega}}))$ and $d_{Spec}(\mathcal{B}(D_{\overline{\Omega}}); P, d_P)$, for any $\emptyset \neq P \subseteq \overline{\Omega} \subseteq \Omega$ with $(P, d_P) \in \mathcal{B}(D_{\overline{\Omega}})$, are well-defined for any nontrivial λ-QT code C. Namely, $d_{Spec}(\mathcal{B}(D_{\overline{\Omega}})) = \infty$ if and only if C is the zero code, which is the only case when $\overline{\Omega} = \Omega$ and $d_{Spec}(\mathcal{B}(D_\Omega); \Omega, d_\Omega) = \infty$, by Lemma 12.

V. Comparison results

In [25, Section IV], Semenov and Trifonov gave a comparison of their BCH-like spectral bound with the Lally bound in [17], the Barbier-Chabot-Quintin bound in [3], and the Tanner bound in [27], all for QC codes. Here, we consider the performance of the generalized spectral bound given in Theorem 13 against the Jensen bound in Theorem 5. A similar performance comparison against the Lally bound for QT codes will be provided right after.

A. Jensen against Spectral

Given C with the concatenated structure as in (23), recall the ordering of the constituents in Section III, where $C_1 = \cdots = C_r = \{\mathbf{0}_\ell\}$ are the zero constituents, $C_{r+1} = \cdots = C_t$ are the full space constituents, and $C_{t+1}, \ldots, C_s$ are the nontrivial constituents. Without loss of generality, we assume that $1 \leq d(C_{t+1}) \leq \cdots \leq d(C_s)$.

With this grouping of the constituents, we obtain the following ordering of their distances

$$1 = d(C_{r+1}) = \cdots = d(C_t) \leq d(C_{t+1}) \leq \cdots \leq d(C_s),$$

which allows us to rewrite the Jensen bound (given in (17)) in an organized way as

$$d(C) \geq \min_{r+1\leq i\leq s} \left\{d(C_i) d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_i\rangle)\right\}. \quad (31)$$

In other words, the Jensen bound is the minimum of the following distances

$$\begin{aligned} &d(C_{r+1})\, d(\langle\theta_{r+1}\rangle), \\ &\qquad\vdots \\ &d(C_t)\, d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_t\rangle), \\ &d(C_{t+1})\, d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_t\rangle \oplus \langle\theta_{t+1}\rangle), \\ &\qquad\vdots \\ &d(C_s)\, d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_t\rangle \oplus \cdots \oplus \langle\theta_s\rangle). \end{aligned}$$

Since $d(C_{r+1}) = \cdots = d(C_t) = 1$ and $d(\langle\theta_{r+1}\rangle) \geq d(\langle\theta_{r+1}\rangle \oplus \langle\theta_{r+2}\rangle) \geq \cdots \geq d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_t\rangle)$, we can shorten the above list as

$$\begin{array}{c} d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_t\rangle), \\ d(C_{t+1})\, d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_t\rangle \oplus \langle\theta_{t+1}\rangle), \\ \vdots \\ d(C_s)\, d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_t\rangle \oplus \cdots \oplus \langle\theta_s\rangle). \end{array} \tag{32}$$

Now we look into the spectral bound in Theorem 13 in the particular case when $P = \overline{\Omega}$. The related λ-constacyclic code over $\mathbb{F}_q$ with zero set $\overline{\Omega}$, say $C_{\overline{\Omega}}$, has check polynomial $f(x) = f_{r+1}(x)\cdots f_t(x)$ and by using CRT we get

$$C_{\overline{\Omega}} = \left\langle \frac{x^m - \lambda}{f(x)} \right\rangle \cong \bigoplus_{i=r+1}^{t} \mathbb{F}_q[x]/\langle f_i(x)\rangle = \langle\theta_{r+1}\rangle \oplus \ldots \oplus \langle\theta_t\rangle. \tag{33}$$

Hence, $C_{\overline{\Omega}} = \langle\theta_{r+1}\rangle \oplus \ldots \oplus \langle\theta_t\rangle$ is the λ-constacyclic code over $\mathbb{F}_q$ with the largest possible set $P = \overline{\Omega}$ associated to all eigenvalues. Now we fix $d_{\overline{\Omega}} = d(D_{\overline{\Omega}})$, where $D_{\overline{\Omega}}$ is the λ-constacyclic code over $\mathbb{F}$ with zero set $\overline{\Omega}$. Using (27) and (33), we get

$$\begin{aligned} d(C) &\geq \min\{d_{\overline{\Omega}}, d(\mathbb{C}_{\overline{\Omega}})\} \\ &= \min\left\{ d_{\overline{\Omega}}, d\left(\left(\sum_{i\in\Gamma} \sum_{j=0}^{e_i-1} \overline{C}_i^{q^j} \right)\Big|_{\mathbb{F}_q} \right) \right\}. \end{aligned} \tag{34}$$

Comparing (34) with (32) leads to the following cases.

Case 1: When $d_{\overline{\Omega}} \leq d(\mathbb{C}_{\overline{\Omega}})$. In this case, the fixed spectral bound (34) yields $d(C) \geq d_{\overline{\Omega}}$. Note that $d(C_{\overline{\Omega}})$ is also a member of the list (32), as the topmost element. For an easier representation, let

$$A_i := d(\langle\theta_{r+1}\rangle \oplus \cdots \oplus \langle\theta_i\rangle), \text{ for } t+1 \leq i \leq s,$$

so that the collection (32) becomes

$$d(C_{\overline{\Omega}}), d(C_{t+1})A_{t+1}, \ldots, d(C_s)A_s. \tag{35}$$

By definition of $d_{\overline{\Omega}}$, we have $d_{\overline{\Omega}} \leq d(C_{\overline{\Omega}})$. Using Lemma 11, we get $d(C_i) \geq d(\overline{C}_i) \geq d(\mathbb{C}_{\overline{\Omega}}) \geq d_{\overline{\Omega}}$, for $t+1 \leq i \leq s$. Hence, the estimate of the Jensen bound is greater than or equal to the estimate of the fixed spectral bound in this case.

Case 2: When $d(\mathbb{C}_{\overline{\Omega}}) \leq d_{\overline{\Omega}}$. In this case, the fixed spectral bound (34) yields $d(C) \geq d(\mathbb{C}_{\overline{\Omega}})$. Since Lemma 11 tells us $d(C_i) \geq d(\overline{C}_i) \geq d(\mathbb{C}_{\overline{\Omega}})$, for any $i \in \Gamma$, we also have $d(C_i)A_i \geq d(\mathbb{C}_{\overline{\Omega}})$, for all $t+1 \leq i \leq s$. Therefore, the Jensen bound is at least as good as the fixed spectral bound in this case as well.

We have shown the following.

Proposition 14. *Let $C \subseteq R^\ell$ be a λ-QT code with a nonempty eigenvalue set $\overline{\Omega} \subseteq \Omega$ and let $D_{\overline{\Omega}}$ be the λ-constacyclic code over $\mathbb{F}$ with zero set $\overline{\Omega}$. Let d_J denote the estimate on $d(C)$ of the Jensen bound. Then, $d(C) \geq d_J \geq \min\{d(D_{\overline{\Omega}}), d(\mathbb{C}_{\overline{\Omega}})\}$.*

However, for some choices of $\mathcal{B}(D_{\overline{\Omega}})$, if we consider the associated $d_{Spec}(\mathcal{B}(D_{\overline{\Omega}}))$ that maximizes $\min\{d_P, d(\mathbb{C}_P)\}$ over all choices of $(P, d_P) \in \mathcal{B}(D_{\overline{\Omega}})$ with $\emptyset \neq P \subseteq \overline{\Omega}$, then Proposition 14 above does not hold with $\min\{d(D_{\overline{\Omega}}), d(\mathbb{C}_{\overline{\Omega}})\}$ replaced by $d_{Spec}(\mathcal{B}(D_{\overline{\Omega}}))$, as presented in the next example. First, we fix some further notation. Let

$$\begin{aligned} \mathcal{B}_1(D_{\overline{\Omega}}) := \{(P, d(D_P)) : \emptyset \neq P \subseteq \overline{\Omega}, \\ D_P \subseteq \mathbb{F}^m \text{ has zero set } P\}, \end{aligned}$$

and let $\mathcal{B}_2(D_{\overline{\Omega}}), \mathcal{B}_3(D_{\overline{\Omega}}), \mathcal{B}_4(D_{\overline{\Omega}})$ denote the BCH, HT and Roos bounds for $D_{\overline{\Omega}}$, respectively, as done in Section II-A. Note that $\mathcal{B}_2(D_{\overline{\Omega}}) \subseteq \mathcal{B}_3(D_{\overline{\Omega}}) \subseteq \mathcal{B}_4(D_{\overline{\Omega}})$. We also consider their union denoted by

$$\begin{aligned} \mathcal{B}_u(D_{\overline{\Omega}}) &:= \mathcal{B}_1(D_{\overline{\Omega}}) \cup \mathcal{B}_2(D_{\overline{\Omega}}) \cup \mathcal{B}_3(D_{\overline{\Omega}}) \cup \mathcal{B}_4(D_{\overline{\Omega}}) \\ &= \mathcal{B}_1(D_{\overline{\Omega}}) \cup \mathcal{B}_4(D_{\overline{\Omega}}) \end{aligned} \tag{36}$$

as an additional choice.

Example 1. Let $\mathbb{F}_3(\alpha) := \mathbb{F}_{3^6}$ be the splitting field of x^7+1. We consider the $[14, 7, 4]_3$ 2-QT code with $(m, \ell, r) = (7, 2, 1)$, generated by $2x^5 + x^3 + x^2 + 2$ and $x^5 + x^3 + x^2$. The corresponding upper-triangular matrix $\widetilde{G}(x)$ is

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

where $\det(\widetilde{G}(x)) = x^7 + 1$ and, therefore, $\overline{\Omega} = \Omega = \{\alpha^{52}, \alpha^{156}, \alpha^{260}, 2, \alpha^{468}, \alpha^{572}, \alpha^{676}\}$. Over $\mathbb{F}_3$, the scalar generator matrix is of the form

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

There are exactly two choices of $P \subseteq \overline{\Omega}$ for which $d_{Spec}(\mathcal{B}_1(D_{\overline{\Omega}}); P, d_P)$ yields $d_{Spec}(\mathcal{B}_1(D_{\overline{\Omega}}))$, namely

$$P = \{\alpha^{52}, \alpha^{468}, \alpha^{572}\} \text{ and } P = \{\alpha^{156}, \alpha^{260}, \alpha^{676}\},$$

that give $d_P = d(D_P) = 4$ and $d(\mathbb{C}_P) = \infty$, where D_P is the 2-constacyclic code of length 7 with zero set P over $\mathbb{F}_{3^6}$. However, the BCH-like, the HT-like, and the Roos-like bounds for QT codes, namely $d_{Spec}(\mathcal{B}_2(D_{\overline{\Omega}}))$, $d_{Spec}(\mathcal{B}_3(D_{\overline{\Omega}}))$ and $d_{Spec}(\mathcal{B}_4(D_{\overline{\Omega}}))$, are not sharp, for any nonempty $P \subseteq \overline{\Omega}$, where they all yield $d_P = |P| + 1 = 3$ and $d(\mathbb{C}_P) = \infty$, for $P = \{\alpha^{52}, \alpha^{468}\}$, as their best estimate. Hence, we have $d_{Spec}(\mathcal{B}_u(D_{\overline{\Omega}})) = d_{Spec}(\mathcal{B}_1(D_{\overline{\Omega}})) = 4$, whereas $d_J = 2$.

Remark 5. Taking a sufficiently large P as well as considering different choices of defining set bounds is crucial when using the spectral bound. For instance, for any fixed choice of defining set bound $\mathcal{B}(D_{\overline{\Omega}})$, if we consider the behaviour of $d_{Spec}(\mathcal{B}(D_{\overline{\Omega}}); P, d_P)$ over the nonempty subsets $P \subseteq \overline{\Omega}$ with $(P, d_P) \in \mathcal{B}(D_{\overline{\Omega}})$, then d_P might be nondecreasing as P approaches $\overline{\Omega}$, whereas $d(\mathbb{C}_P)$ is nonincreasing, which follows from (27) since we might add more to the sum. Hence, the optimized value $d_{Spec}(\mathcal{B}(D_{\overline{\Omega}}))$ might not be obtained by involving all eigenvalues, unlike the case of constacyclic codes, as any nonconstant d_P grows proportionately to the size of P.

Example 2. Let us consider the same $[14, 7, 4]_3$ 2-QT code in Example 1 above with eigenvalues

$$\overline{\Omega} = \Omega = \{\alpha^{52}, \alpha^{156}, \alpha^{260}, 2, \alpha^{468}, \alpha^{572}, \alpha^{676}\}.$$

It is obvious that any subset of $\overline{\Omega}$ with 1 or 2 elements is consecutive. We first take $P = \{\alpha^{52}\}$ and use the BCH-like bound, where we obtain $d_P = 2$ and $d(\mathbb{C}_P) = \infty$, and hence $d_{Spec}(\mathcal{B}_2(D_{\overline{\Omega}}); P, d_P) = 2$ in this case. If we add one more element and consider $P = \{2, \alpha^{52}\}$, then we get $d_P = 3$ but $d(\mathbb{C}_P) = 1$, which makes $d_{Spec}(\mathcal{B}_2(D_{\overline{\Omega}}); P, d_P) = 1$. If we replace 2 by α^{468} and take $P = \{\alpha^{52}, \alpha^{468}\}$ instead, then we obtain $d_{Spec}(\mathcal{B}_2(D_{\overline{\Omega}}); P, d_P) = d_{Spec}(\mathcal{B}_2(D_{\overline{\Omega}})) = 3$, as indicated in Example 1 above.

B. Lally against Spectral

Lally derived a lower bound on the minimum distance of a given QC code in [17]. Her findings can be adapted to QT codes easily and the same minimum distance bound can be extended to the QT codes in an analogous way.

Let C be a λ-QT code of length $m\ell$ and index ℓ over $\mathbb{F}_q$. Let $\{1, \gamma, \ldots, \gamma^{\ell-1}\}$ be some fixed choice of basis of $\mathbb{F}_{q^\ell}$ as a vector space over $\mathbb{F}_q$. We view the codewords of C as $m \times \ell$ arrays as in (3) and consider the following map:

$$\begin{array}{ccccc} \tau: & \mathbb{F}_q^{m\ell} & \longrightarrow & \mathbb{F}_{q^\ell}^{m} \\ \mathbf{c} = \begin{pmatrix} c_{0,0} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \longmapsto & \begin{pmatrix} c_0 \\ \vdots \\ c_{m-1} \end{pmatrix}, \end{array}$$

where $c_i = c_{i,0} + c_{i,1}\,\gamma + \cdots + c_{i,\ell-1}\,\gamma^{\ell-1} \in \mathbb{F}_{q^\ell}$, for all $0 \le i \le m-1$.

Clearly, $\tau(\mathbf{c})$ lies in some λ-constacyclic code, for any $\mathbf{c} \in C$. We now define the smallest such constacyclic code as $\widehat{C}$, which contains all of $\tau(C)$. First, we equivalently extend the map τ above to the polynomial description of codewords as (cf. (1))

$$\begin{array}{rcl} \tau: \mathbb{F}_q[x]^\ell & \longrightarrow & \mathbb{F}_{q^\ell}[x] \\ \mathbf{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x)) & \longmapsto & c(x) = \displaystyle\sum_{j=0}^{\ell-1} c_j(x)\,\gamma^j. \end{array} \tag{37}$$

If C has generating set $\{\mathbf{f}_1, \ldots, \mathbf{f}_r\}$, where

$$\mathbf{f}_k := (f_0^{(k)}(x), \ldots, f_{\ell-1}^{(k)}(x)) \in \mathbb{F}_q[x]^\ell,$$

for each $k \in \{1, \ldots, r\}$, then

$$\widehat{C} = \langle \gcd(f_1(x), \ldots, f_r(x), x^m - \lambda) \rangle$$

such that $f_k = \tau(\mathbf{f}_k) \in \mathbb{F}_{q^\ell}[x]$, for all k [17].

Next, we consider the q-ary linear code of length ℓ that is generated by the rows of the codewords in C, which are represented as $m \times \ell$ arrays as in (3). Recall that this code was denoted by B in the proof of Lemma 12. Namely, B is the linear block code of length ℓ over $\mathbb{F}_q$, generated by $\{\mathbf{f}_{k,i} : k \in \{1, \ldots, r\},\ i \in \{0, \ldots, m-1\}\} \subseteq \mathbb{F}_q^\ell$, where each $\mathbf{f}_{k,i} := (f_{i,0}^{(k)}, \ldots, f_{i,\ell-1}^{(k)}) \in \mathbb{F}_q^\ell$ is the vector of the i^{th} coefficients of the polynomials

$$f_j^{(k)}(x) = f_{0,j}^{(k)} + f_{1,j}^{(k)} x + \cdots + f_{m-1,j}^{(k)} x^{m-1},$$

for all $k \in \{1, \ldots, r\}$ and $j \in \{0, \ldots, \ell-1\}$.

Since the image of any codeword $\mathbf{c}(x) \in C$ under the map τ is an element of the λ-constacyclic code $\widehat{C}$ over $\mathbb{F}_{q^\ell}$, there are at least $d(\widehat{C})$ nonzero rows in each nonzero codeword of C. For any $i \in \{0, \ldots, m-1\}$, the i^{th} row $\mathbf{c}_i = (c_{i,0}, \ldots, c_{i,\ell-1})$ of any $\mathbf{c} \in C$ can be viewed as a codeword in B, therefore, a nonzero $\mathbf{c}_i$ has weight at least $d(B)$. Hence, we have shown the following.

Theorem 15. *(cf. [17, Theorem 5]) Let C be an r-generator λ-QT code of length $m\ell$ and index ℓ over $\mathbb{F}_q$ with generating set $\{\mathbf{f}_1, \ldots, \mathbf{f}_r\} \subseteq \mathbb{F}_q[x]^\ell$. Let the λ-constacyclic code $\widehat{C} \subseteq \mathbb{F}_{q^\ell}^m$ and the linear code $B \subseteq \mathbb{F}_q^\ell$ be defined as above. Then, we have*

$$d(C) \ge d(\widehat{C})\, d(B).$$

We now prove that an analogue of Proposition 14 holds between the Lally and spectral bounds, which is an immediate result of Lemma 12.

Corollary 4. *Let $C \subseteq R^\ell$ be a nontrivial λ-QT code with the eigenvalue set $\overline{\Omega} = \Omega$ and let d_L denote the estimate on $d(C)$ of the Lally bound. Then, $d(C) \ge d_L \ge d(\mathbb{C}_\Omega)$. In particular, $d_L \ge \min\{d_\Omega, d(\mathbb{C}_\Omega)\}$, for any $d_\Omega \ge 1$.*

Proof. By Lemma 12, we already know that B is a subcode of $\mathbb{C}_\Omega$ and therefore we have $d(B) \ge d(\mathbb{C}_\Omega)$. Hence, $d_L = d(\widehat{C})d(B) \ge d(\mathbb{C}_\Omega) \ge \min\{d_\Omega, d(\mathbb{C}_\Omega)\}$. □

However, Corollary 4 does not apply to the case when $d_{Spec}(\mathcal{B}(D_\Omega))$ is considered, instead of some fixed choice for $\min\{d_\Omega, d(\mathbb{C}_\Omega)\}$, as highlighted by the codes in the next two examples.

Example 3. Let $\mathbb{F}_3(\alpha) := \mathbb{F}_{81}$ be the splitting field of $x^{10}+1$. Consider the $[20, 10, 4]_3$ 2-QT code with $(m, \ell, r) = (10, 2, 1)$, generated by $2x^8+2x^7+x^2+x+1$ and $2x^6+2x^5+x^4+x+2$. The associated upper-triangular matrix $\widetilde{G}(x)$ is

$$\begin{pmatrix} 1 & 2x^9 + 2x^7 + 2x^6 + x^5 + 2x^3 + x^2 + 1 \\ 0 & x^{10} + 1 \end{pmatrix},$$

where $\det(\widetilde{G}(x)) = x^{10} + 1$, which implies $\overline{\Omega} = \Omega$. Over $\mathbb{F}_3$, the scalar generator matrix is

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

There are two choices of P, namely

$$P = \{\alpha^{52}, \alpha^{60}, \alpha^{68}\} \text{ and } P = \{\alpha^{20}, \alpha^{44}, \alpha^{76}\},$$

TABLE I: The outcomes on the performance comparison of the bounds. We list the number of instances, with double counting allowed, when a specified bound reached the actual minimum distance, *i.e.*, it was sharp, and when it was greater than or equal to the other two bounds, *i.e.*, it was best-performing.

	QC for $q=2$			QC for $q=3$			QT for $q=3,\lambda=2$		
bound	d_L	d_{Spec}	d_J	d_L	d_{Spec}	d_J	d_L	d_{Spec}	d_J
sharp	16 563	27 438	31 368	14 704	31 711	33 799	4 037	9 257	9 780
best-performing	20 821	61 012	92 506	19 359	83 284	143 010	5 041	35 363	65 275
# nontrivial C	93 467			143 602			65 589		

TABLE II: The outcomes on the comparison of the bounds in strictly decreasing patterns. The label of being sharp applies only to the bound with the largest value among the three.

	QC for $q=2$				QC for $q=3$				QT for $q=3,\lambda=2$			
decreasing order	JSL	JLS	SJL	LJS	JSL	JLS	SJL	LJS	JSL	JLS	SJL	LJS
count	17 976	77	398	11	21 622	25	102	1	22 475	3	165	1
sharp	3 203	69	94	4	965	9	24	0	1 030	0	26	0
# nontrivial C	56 243				53 004				52 915			

that yield $d_{Spec}(\mathcal{B}_1(D_{\overline{\Omega}});P,d_P) = d_{Spec}(\mathcal{B}_1(D_{\overline{\Omega}}))$ with $d_P = d(D_P) = 4$ and $d(\mathbb{C}_P) = \infty$, where D_P is the 2-constacyclic code of length 10 with zero set P over $\mathbb{F}_{81}$. Using the first choice of P, which is consecutive, the BCH-like –and therefore the HT-like and the Roos-like– bounds for QT codes are also sharp, giving $d_P = 4$ and $d(\mathbb{C}_P) = \infty$. Hence, we obtain $d_{Spec}(\mathcal{B}_u(D_{\overline{\Omega}})) = 4 = d_{Spec}(\mathcal{B}_i(D_{\overline{\Omega}}))$, for any $1 \le i \le 4$. Using the second choice of P, which appears in $\mathcal{B}_3(D_{\overline{\Omega}})$ and $\mathcal{B}_4(D_{\overline{\Omega}})$ but not in $\mathcal{B}_2(D_{\overline{\Omega}})$, the HT-like and the Roos-like bounds for QT codes are sharp with $d_P = 4$ and $d(\mathbb{C}_P) = \infty$. Therefore, we have $d_{Spec}(\mathcal{B}_u(D_{\overline{\Omega}})) = 4 = d_{Spec}(\mathcal{B}_i(D_{\overline{\Omega}}))$, for $i \in \{1,3,4\}$, whereas $d_L = 1$ and $d_J = 2$.

Example 4. Let $\mathbb{F}_3(\alpha) := \mathbb{F}_9$ be the splitting field of x^8+2. Consider the $[16,7,5]_3$ QC code with $(m,\ell,r) = (8,2,1)$, generated by $x^7+x^6+x^5+x^4+2x^3+2$ and $x^7+x^5+2x^4+2x^3+x$. The associated upper-triangular matrix $\widetilde{G}(x)$ is

$$\begin{pmatrix} x+1 & x^6+x^5+2x^4+2x^3+2x^2+2x \\ 0 & x^8+2 \end{pmatrix},$$

where $\det(\widetilde{G}(x)) = (x+1)(x^8+2)$ and therefore $\overline{\Omega} = \Omega = \mathbb{F}_9 \setminus \{0\}$.

Over $\mathbb{F}_3$, the scalar generator matrix is of the form

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

There are again two choices of P, namely

$$P = \{\alpha^2, \alpha^3, 2, \alpha^5\} \text{ and } P = \{\alpha, 2, \alpha^6, \alpha^7\},$$

that yield $d_{Spec}(\mathcal{B}_1(D_{\overline{\Omega}});P,d_P) = d_{Spec}(\mathcal{B}_1(D_{\overline{\Omega}}))$ with $d_P = d(D_P) = 5$ and $d(\mathbb{C}_P) = \infty$, where D_P is the cyclic code of length 8 with zero set P over $\mathbb{F}_9$. Using the first choice of P, which is clearly consecutive, the BCH-like, the HT-like and the Roos-like bounds for QC codes are also sharp with $d_P = 5$ and $d(\mathbb{C}_P) = \infty$. Hence, we get $d_{Spec}(\mathcal{B}_u(D_{\overline{\Omega}})) = 5 = d_{Spec}(\mathcal{B}_i(D_{\overline{\Omega}}))$, for $1 \le i \le 4$. The second choice of P is not consecutive but it appears in $\mathcal{B}_3(D_{\overline{\Omega}})$ and $\mathcal{B}_4(D_{\overline{\Omega}})$, making the HT-like and the Roos-like bounds again sharp with $d_P = 5$ and $d(\mathbb{C}_P) = \infty$. Therefore, we obtain $d_{Spec}(\mathcal{B}_u(D_{\overline{\Omega}})) = 5 = d_{Spec}(\mathcal{B}_i(D_{\overline{\Omega}}))$, for $i \in \{1,3,4\}$, whereas $d_L = 2$ and $d_J = 4$.

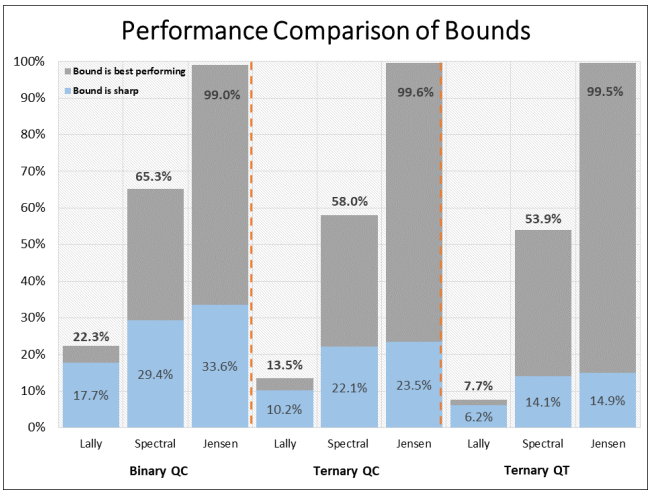
VI. Numerical Comparisons

To compare the performance of the bounds we carried out two procedures. The first one looks into the overall performance of the bounds. The second one investigates their strict ranking.

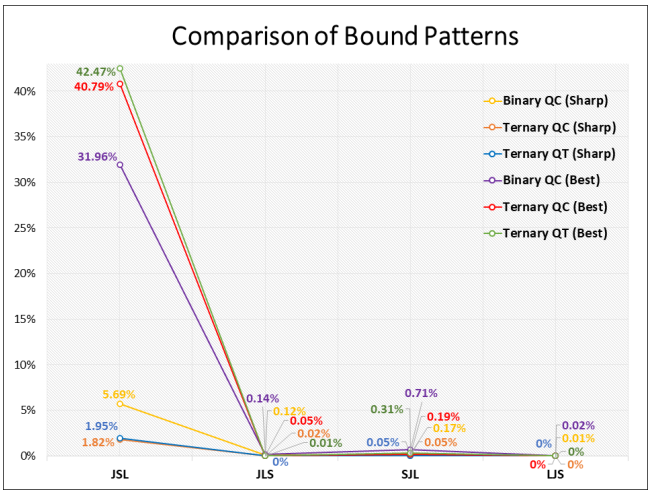
For $q = 2$, we construct 1000 random codes on each input tuple (m,ℓ,r), with $m \in \{3,5,7,9,11\}$, $2 \le \ell \le 6$, and $1 \le r \le \ell$. Once (m,ℓ,r) is fixed, an array $\mathcal{A}$ of generator polynomials is randomly built. The number of polynomials in this array is $r\ell$. The corresponding binary r-generator QC code C is generated by using the `QuasiCyclicCode` function in MAGMA with input $(m\ell,\mathcal{A},r)$. If C was nontrivial, then its minimum distance $d(C)$ and the values given by the three bounds d_L, d_{Spec}, and d_J were determined, where $d_{Spec} := d_{Spec}(\mathcal{B}_u(D_{\overline{\Omega}}))$ (see (36)). We recorded the respective numbers of occasions when each bound was either sharp or was best-performing among the three. Double counting was allowed in cases where two or more bounds were simultaneously sharp. Similarly, double counting was also allowed for coinciding estimates with the best-performing bounds.

An identical routine was carried out for $q = 3$. To keep $\gcd(m,q) = 1$, we used $m \in \{4,5,7,8\}$, with $2 \le \ell \le 6$ and $1 \le r \le \ell$. When $\lambda = 1$, we constructed 2000 random codes on each input tuple (m,ℓ,r). Changing λ to 2, we completed 1000 random constructions on each input tuple. In the strictly QT setup, the `QuasiTwistedCyclicCode` function in MAGMA generated the ternary 2-QT code C on input $(m\ell,\mathcal{A},2)$, built from the randomly generated polynomials in the corresponding array $\mathcal{A}$ of length $r\ell$. The outcomes of the first procedure can be found in Table I with the visualization given in Plot (a) of Figure 1.

Fig. 1: Visualization, in percentage, of the outcomes listed in Tables I and II.



(a) Overall performance.



(b) Performance by patterns.

In the second procedure we recorded the number of random constructions in which the bounds ranked in strictly decreasing order. We label the 6 possible patterns in abbreviated form. The pattern JSL stands for $d_J > d_{Spec} > d_L$. The other patterns are analogously interpreted. Two patterns, namely SLJ and LSJ, for $d_{Spec} > d_L > d_J$ and $d_L > d_{Spec} > d_J$, respectively, never occurred in our constructions. For $q = 2$, we ran 1000 random codes on each input (m, ℓ, r), with $m \in \{3, 5, 7\}$, $2 \le \ell \le 6$ and $1 \le r \le \ell$. For $q = 3, \lambda = 1$ and $q = 3, \lambda = 2$, we used $m \in \{4, 5, 7, 8\}$. The exact counts are presented in Table II and interpreted visually in Plot (b) of Figure 1.

Our random constructions reveal that the Jensen bound has the best overall performances by a wide percentage margin. The situation where $d_J \ge d_{Spec} \ge d_L$ is typical. Consider, for example, the $[8, 2, 6]_3$ 2-QT code with $(m, \ell, r) = (4, 2, 1)$, generated by $2x^3 + 2x + 1$ and $2x^2 + x + 1$. The code is optimal in terms of minimum distance with $d(C) = d_J = 6 > d_{Spec} = 4 > d_L = 3$. It has a generator matrix

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

While it is almost always safe to bet on the Jensen bound, there are occasions where d_L, similarly d_{Spec}, outperforms the other two bounds.

Example 5. We start with an example where $d_L > d_J > d_{Spec}$ and the code is optimal since it reaches the best-possible minimum distance. The $[21, 6, 8]_2$ QC code with $(m, \ell, r) = (7, 3, 1)$, generator polynomials $x^4 + x^3 + x + 1$, $x^4 + 1$, and $x^3 + x$, and generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix},$$

has $d_L = 8 > d_J = 6 > d_{Spec} = 4$.

Here is an example where $d_{Spec} > d_J > d_L$. In the $[21, 7, 6]_2$ QC code with $(m, \ell, r) = (7, 3, 1)$, generated by $x^6 + x^5 + x^4 + x^2 + 1$, $x^6 + x^5 + x^2$, and $x^6 + x^5 + x^4 + 1$, none of the bounds is sharp, since $d(C) = 6 > d_{Spec} = 5 > d_J = 3 > d_L = 1$. The code has a generator matrix

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

Figure 2 illustrates the situation more comprehensively. We average, over a large number of distinct nontrivial codes, the respective ratios of distance estimates d_J, d_{Spec}, d_L over the actual minimum distance d for fixed code rate k/n. For $q = 2$, based on 4 937 distinct nontrivial QC codes, Figure 2 (a) presents the *average ratios*

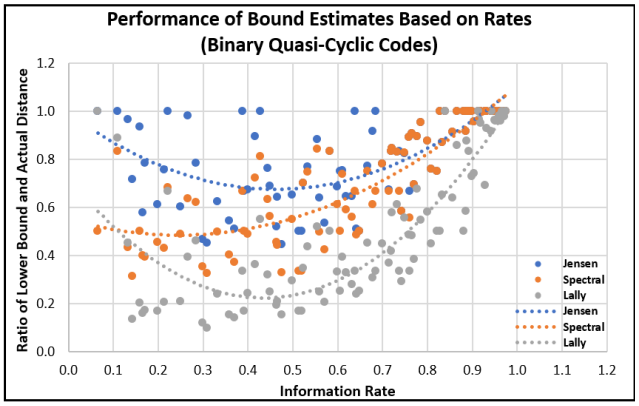
$$\frac{d_J}{d}, \quad \frac{d_{Spec}}{d}, \quad \frac{d_L}{d}$$

on the vertical axis for the indicated code rates along the horizontal axis. The dotted lines are the quadratic curve fitting lines for the respective distance estimates. Limiting the analysis to a specific length, say $n = 42$ as in Figure 2 (b), reveals similar patterns of behaviour. This is the main reason behind our choice of using the rate as reference without fixing the length n. The respective plots in Figure 2 (c) and (d) show the patterns based on 37 063 distinct nontrivial ternary QC codes and 28 853 distinct nontrivial ternary QT codes with $\lambda = 2$. The average values in Figure 2 must of course be interpreted alongside the frequencies shown in Figure 1.

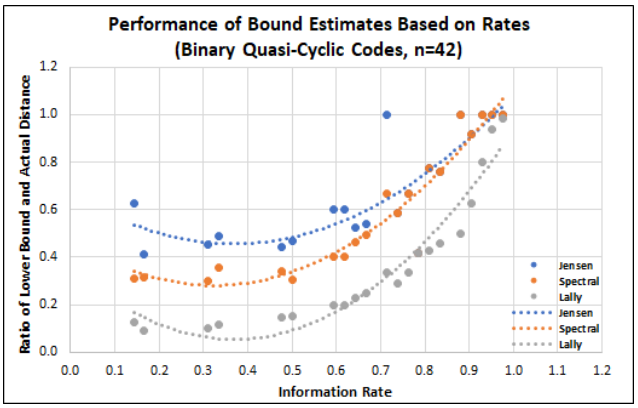
VII. Conclusion

We conclude the paper by restating the key insights that we have gained from comparing distance bounds for quasi-twisted codes.

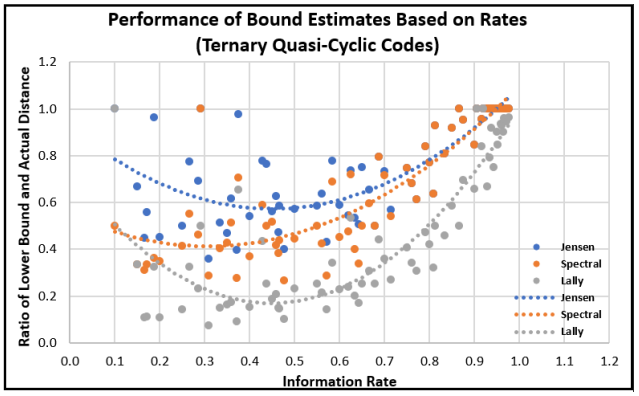
Fig. 2: Patterns showing the ratios of the distance bound estimates given by $\frac{d_J}{d}$, $\frac{d_{Spec}}{d}$, $\frac{d_L}{d}$ in terms of the rate of the codes. The dotted lines are their respective quadratic curve fitting lines.



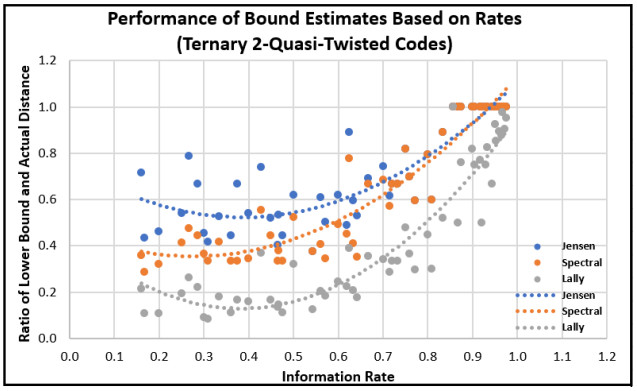
(a) Binary QC



(b) Binary QC of fixed length 42



(c) Ternary QC



(d) Ternary QT with $\lambda = 2$

The general spectral bound, presented as Theorem 13, is encompassing, counting the BCH-like, the HT-like, the Roos-like, and the shift bounds as special cases. It is also intriguingly simple to analyze. Once we have identified a nonempty set of eigenvalues of a given λ-QT code, we can define two parameters based on any chosen nonempty subset of this set. The first parameter is the minimum distance of the eigencode, which corresponds to the common eigenspace of the eigenvalues in the chosen subset. The second parameter is a minimum distance bound for any λ-constacyclic code whose zero set contains the chosen subset. The general spectral bound is computed based on these two derived parameters, each of which is simpler to work on than the original QT code.

In terms of performance, we have seen by numerical comparisons that the bound to beat is overwhelmingly the Jensen bound. Despite its relatively poor performance against the Jensen bound, the general spectral bound may provide a better estimate for QT codes with high dimension. The two parameters of the spectral bound are bounded above by the index and the co-index of the given QT code, whose length is the product of these two. On the other hand, a QT code with a high dimension clearly has many nonzero constituents, which affects the direct sums and the size of the list (32) in the Jensen bound. Hence, its performance starts to decay as the dimension increases whereas the spectral bound gets better, which can be observed in Figure 2. Therefore, it is a good idea to check the estimates of both bounds if the dimension of the given QT code is sufficiently large. The majority of the occasions where the Jensen bound still performs better than the general spectral bound occurs when the QT code with high rate has many full space constituents. In that case, the size of (32) gets smaller with longer direct sums. On the other hand, as indicated in Section III, full space constituents yield a smaller number of eigenvalues. Hence, the general spectral bound might be a better choice than the Jensen bound for QT codes of high dimension, unless they have a high number of full space constituents.

In addition to providing QT analogues of the minimum distance bounds given for constacyclic codes, the general spectral bound offers another major theoretical value. It reveals properties that allow for a direct structural comparison with both the Jensen and the Lally bounds. They serve as links, previously unavailable in the literature, that explicitly connect the three bounds. The poor performance of the Lally bound might be improved by extending its single-layer concatenated structure to a more general setup with some multi-layer concatenation, like in the Jensen bound.

REFERENCES

[1] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaib and P. Solé, "On self-dual double negacirculant codes", *Discrete Appl. Math.*, vol. 222, pp.

205–212, 2017.

[2] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaib and P. Solé, "On complementary-dual multinegacirculant codes", *Cryptogr. Commun.*, vol. 12, pp. 101–113, 2020.

[3] M. Barbier, C. Chabot and G. Quintin, "On quasi-cyclic codes as a generalization of cyclic codes", *Finite Fields Appl.*, vol. 18, pp. 904–919, 2012.

[4] J. Bierbrauer, "Introduction to Coding Theory", *Chapman and Hall/CRC Press*, 2016.

[5] R. C. Bose and D. K. R. Chaudhuri, "On a class of error correcting binary group code", *Inf. Control*, vol. 3, no. 1, pp. 68–79, 1960.

[6] W. Bosma, J. Cannon and C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.*, vol. 24, pp. 235–265, 1997.

[7] J. J. Bernal , M. Guerreiro, and J. J. Simón, "From ds-bounds for cyclic codes to true minimum distance for Abelian codes", *IEEE Trans. Inform. Theory*, vol. 65, no. 3, pp. 1752–1763, 2019.

[8] V. Chepyzhov, "A Gilbert-Vashamov bound for quasi-twisted codes of rate $1/n$", *Proc. of the Joint Swedish-Russian Int. Workshop on Inf. Theory*, Mölle, Sweden, pp. 214–218, 1993.

[9] R. Daskalov and P. Hristov, "New quasi-twisted degenerate ternary linear codes", *IEEE Trans. Inform. Theory*, vol. 49, no. 9, pp. 2259–2263, 2003.

[10] M. van Eupen and J. van Lint, "On the minimum distance of ternary cyclic codes", *IEEE Trans. Inform. Theory*, vol. 39, no. 2, pp. 409–422, 1993.

[11] M. F. Ezerman, S. Ling, B. Özkaya and J. Tharnnukhroh, "Spectral bounds for quasi-twisted codes", *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 1922–1926.

[12] C. Güneri and F. Özbudak, "A bound on the minimum distance of quasi-cyclic codes", *SIAM J. Discrete Math.*, vol. 26, no. 4, pp. 1781–1796, 2012.

[13] C. Hartmann and K. Tzeng, "Generalizations of the BCH bound", *Inf. Control*, vol. 20. no. 5, pp. 489–498, 1972.

[14] A. Hocquenghem, "Codes correcteurs d'Erreurs", *Chiffres (Paris)*, vol. 2, pp. 147–156, 1959.

[15] J. M. Jensen, "The concatenated structure of cyclic and abelian codes", *IEEE Trans. Inform. Theory*, vol. 31, no. 6, pp. 788–793, 1985.

[16] Y. Jia, "On quasi-twisted codes over finite fields", *Finite Fields Appl.*, vol. 18, pp. 237–257, 2012.

[17] K. Lally, "Quasicyclic codes of index ℓ over $\mathbb{F}_q$ viewed as $\mathbb{F}_q[x]$-submodules of $\mathbb{F}_{q^\ell}[x]/\langle x^m-1\rangle$", *Proc. Conf. Appl. Algebra, Algebraic Algorithms and Error-Correcting Codes*, pp. 244–253, Springer, 2003.

[18] K. Lally and P. Fitzpatrick, "Algebraic structure of quasi-cyclic codes", *Discrete Appl. Math.*, vol. 111, no. 1–2, pp. 157–175, 2001.

[19] J. van Lint and R. Wilson, "On the minimum distance of cyclic codes", *IEEE Trans. Inform. Theory*, vol. 32, no. 11, pp. 23–40, 1986.

[20] J. Lv and J. Gao, "A minimum distance bound for 2-dimension λ-quasi-twisted codes over finite fields", *Finite Fields Appl.*, vol. 51, pp. 146–167, 2018.

[21] L. Qian, M. Shi, P. Solé, "On self-dual and LCD quasi-twisted codes of index two over a special chain ring", *Crypt. and Comm., Disc. Struc., Bool. Func. and Seq.*, vol. 11, pp. 717–734, 2019.

[22] D. Radkova and A. J. van Zanten, "Constacyclic codes as invariant subspaces", *Linear Alg. Appl.*, vol. 430, no. 23, pp. 855–864, 2009.

[23] C. Roos, "A new lower bound for the minimum distance of a cyclic code", *IEEE Trans. Inform. Theory*, vol. 29, no. 3, pp. 330–332, 1983.

[24] M. Shi, L. Qian, P. Solé, "On self-dual negacirculant codes of index two and four", *Des. Codes Crypto.*, vol. 11, pp. 2485–2494, 2018.

[25] P. Semenov and P. Trifonov, "Spectral method for quasi-cyclic code analysis", *IEEE Comm. Letters*, vol. 16, no. 11, pp. 1840–1843, 2012.

[26] M. Shi and Y. Zhang, "Quasi-twisted codes with constacyclic constituent codes", *Finite Fields Appl.*, vol. 39, pp. 159–178, 2016.

[27] R. M. Tanner, "A transform theory for a class of group-invariant codes", *IEEE Trans. Inform. Theory*, vol. 34, no. 4, pp. 725–775, 1988.

[28] A. Zeh and S. Ling, "Decoding of quasi-cyclic codes up to a new lower bound on the minimum distance", *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2014, pp. 2584–2588.

[29] A. Zeh and S. Ling, "Spectral analysis of quasi-cyclic product codes", *IEEE Trans. Inform. Theory*, vol. 62, no. 10, pp. 5359–5374, 2016.

[30] R. Wu and M. Shi, "A modified Gilbert-Varshamov bound for self-dual quasi-twisted codes of index four", *Finite Fields Appl.*, vol. 62, pp. 101627, 2020.

Martianus Frederic Ezerman grew up in East Java Indonesia. He received the B.A. degree in philosophy and the B.Sc. degree in mathematics in 2005 and the M.Sc. degree in mathematics in 2007, all from Ateneo de Manila University, Philippines. In 2011 he obtained the Ph.D. degree in mathematics from Nanyang Technological University (NTU), Singapore. After research fellowships at Laboratoire d'Information Quantique, Université Libre de Bruxelles, Belgium and at the Centre for Quantum Technologies (CQT), National University of Singapore, he returned in March 2014 to NTU where he is currently a Senior Research Fellow.

He is interested in coding theory, cryptography, signal sensing, and quantum information processing.

John Mark Lampos received the B.Sc. degree in mathematics in 2006 and the M.Sc. degree in mathematics in 2011, all from University of the Philippines – Los Baños (UPLB). He is currently an Assistant Professor in UPLB and pursuing his Ph.D. in Mathematics from the University of the Philippines – Diliman.

His fields of interest include coding theory, cryptography, and mathematics education.

San Ling received the B.A. degree in mathematics from the University of Cambridge and the Ph.D. degree in mathematics from the University of California, Berkeley. He is currently President's Chair in Mathematical Sciences, at the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, which he joined in April 2005. Prior to that, he was with the Department of Mathematics, National University of Singapore.

His research fields include arithmetic of modular curves and application of number theory to combinatorial designs, coding theory, cryptography and sequences.

Buket Özkaya received her B.S. degree in Mathematics from Boğaziçi University, Istanbul in 2006. She finished her M.S. in Mathematics at Georg-August-Universität Göttingen, Germany in 2009. She pursued her PhD studies at Sabancı University, Istanbul, under the supervision of Cem Güneri and received her degree in 2014. She had postdoctoral postitions at Middle East Technical University, Ankara (2014-2015), Télécom ParisTech, France (2015-2016) and Sabancı University (2016-2017). Currently she is working as a Research Fellow at Nanyang Technological University, Singapore.

She is interested in algebraic coding theory and its applications.

Jareena Tharnnukhroh received the B.Sc and M. Sc. degrees in mathematics from Silpakorn University, Thailand, in 2012 and 2015, respectively. She is currently a Ph.D. candidate at the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore.

Her research interests include algebraic methods in coding theory.