Spectral bounds for quasi-twisted codes

Ezerman, Martianus Frederic; Ling, San; Özkaya, Buket; Tharnnukhroh, Jareena

2019

Ezerman, M. F., Ling, S., Özkaya, B., & Tharnnukhroh, J. (2019). Spectral bounds for quasi-twisted codes. Proeeding of the 2019 IEEE International Symposium on Information Theory (ISIT), 1922-1926. IEEE. doi:10.1109/ISIT.2019.8849734

https://hdl.handle.net/10356/138705

https://doi.org/10.1109/ISIT.2019.8849734

Spectral Bounds for Quasi-Twisted Codes

Martianus Frederic Ezerman, San Ling, Buket Özkaya, and Jareena Tharnnukhroh

***Abstract*—New lower bounds on the minimum distance of quasi-twisted codes over finite fields are proposed. They are based on spectral analysis and eigenvalues of polynomial matrices. They generalize the Semenov-Trifonov and Zeh-Ling bounds in a manner similar to how the Roos and shift bounds extend the BCH and HT bounds for cyclic codes.**

***Index Terms*—Quasi-twisted code, Roos bound, shift bound, eigenvalues, polynomial matrices, spectral analysis.**

I. Introduction

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 ([10]), QT codes are also asymptotically good ([5], [6]) and they yield good parameters ([1], [2]).

Several bounds on the minimum distance of cyclic codes had been derived. The first and perhaps the most famous one was the BCH bound, given by Bose and Chaudhuri ([3]), and by Hocquenghem ([9]). An extension of the bound was formulated by Hartmann and Tzeng in [8]. One can consider the HT bound as a two-directional BCH bound. The Roos bound in [14] generalized this idea further by allowing the HT bound to have a certain number of gaps in both directions. The Roos bound was extended to constacyclic codes in [13]. Another remarkable extension of the HT bound, known as the shift bound, was introduced by van Lint and Wilson in [12]. This bound is known to be particularly powerful on many non-binary codes ([7]).

Despite being interesting from both theoretical and practical points of view, studies on the minimum distance estimates for QC and QT codes are not as rich as for cyclic and constacyclic codes. Semenov and Trifonov developed a spectral analysis of QC codes ([15]), based on the work done by Lally and Fitzpatrick in [11], and formulated a BCH-like bound, together with a comparison with a few other bounds for QC codes. Their approach is generalized by Zeh and Ling, by using the HT bound, in [16].

This paper is organized as follows. Section II recalls necessary background material and adapts the spectral method of Semenov-Trifonov to QT codes. We formulate and prove a generalized spectral bound on the minimum distance in Section III, where the Roos and shift bounds for QT codes are derived as special cases. Section IV supplies numerical examples showing how the proposed bound performs in comparison with the Semenov-Trifonov (ST) and Zeh-Ling (ZL) bounds.

The authors are with the School of Physical and Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, Singapore 637371, e-mails: {fredezerman, lingsan, buketozkaya, jareena001}@ntu.edu.sg.

M. F. Ezerman, S. Ling, and B. Özkaya are supported by Nanyang Technological University Research Grant M4080456.

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

II. Background

A. Constacyclic codes and minimum distance bounds from their 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 some nonzero element $\lambda \in \mathbb{F}_q$, 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 $R := \mathbb{F}_q[x]/I$. To a vector $\vec{a} \in \mathbb{F}_q^m$, we associate an element of R via the isomorphism:

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

Note that the λ-constashift in $\mathbb{F}_q^m$ amounts to multiplication by x in R. Hence, a λ-constacyclic code $C \subseteq \mathbb{F}_q^m$ can be viewed as an ideal of R. Since R is a principal ideal ring, 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.

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 $\vec{0}_p$ denote throughout the all-zero vector of length p. A λ-constacyclic code $C = \{\vec{0}_m\}$ if and only if $g(x) = x^m - \lambda$.

The roots of $x^m - \lambda$ are of the form $\alpha, \alpha\xi, \ldots, \alpha\xi^{m-1}$, where α is a fixed m^{th} root of λ and ξ is a fixed primitive m^{th} root of unity. Henceforth, let $\Omega := \{\alpha\xi^k : 0 \leq k \leq m-1\}$ 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, $\mathbb{F}$ is the splitting field of $x^m - \lambda$). Given the λ-constacyclic code $C = \langle g(x) \rangle$, the set $L := \{\alpha\xi^k : g(\alpha\xi^k) = 0\} \subseteq \Omega$ of roots of its generator polynomial is called the *defining set* of C. Note that $\alpha\xi^k \in L$ implies $\alpha\xi^{qk} \in L$, for each k. A nonempty subset $E \subseteq \Omega$ is said to be *consecutive* if there exist integers e, n and δ with $e \geq 0, \delta \geq 2, n > 0$ and $\gcd(m, n) = 1$ such that

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

We now describe the Roos bound for constacyclic codes (see [14, Theorem 2] for the original Roos bound for cyclic codes). For $P \subseteq \Omega$, let C_P denote any λ-constacyclic code of length m over $\mathbb{F}_q$, whose defining set contains P. Let d_P denote the minimum distance of C_P.

Theorem 1. *[13, Theorem 6] (Roos bound) Let N and M be two nonempty subsets of Ω. If there exists a consecutive set M' containing M such that $|M'| \leq |M| + d_N - 2$, then we have $d_{MN} \geq |M| + d_N - 1$, where $MN := \frac{1}{\alpha} \bigcup_{\varepsilon \in M} \varepsilon N$.*

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

Corollary 2. *[13, Corollary 1], [14, 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 3. In particular, the case $M = \{\alpha\}$ yields the BCH bound for the associated constacyclic code (see [13, Corollary 2] and the original BCH bound for cyclic codes in [3] and [9]). Taking $M' = M$ yields the HT bound (see [13, Corollary 3] and the HT bound for cyclic codes in [8, Theorem 2]).

Another improvement to the HT bound for cyclic codes was given by van Lint and Wilson in [12], which is known as the shift bound. We now formulate 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.

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 all $b \in \mathbb{K} \setminus S$.
3) If A is independent with respect to S and $c \in \mathbb{K}^*$, then cA is independent with respect to S.

Recall that the *weight* of a polynomial $f(x) \in \mathbb{K}[x]$, denoted by $\mathrm{wt}(f)$, is the number of nonzero coefficients in $f(x)$.

Theorem 4. *[12, Theorem 11] (Shift bound) Let $0 \neq f(x) \in \mathbb{K}[x]$ and let $S := \{\theta \in \mathbb{K} \mid f(\theta) = 0\}$. Then $wt(f) \geq |A|$, for every subset A of $\mathbb{K}$ that is independent with respect to S.*

The minimum distance 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 defining set L. Observe that, in this case, the universe of the independent sets is Ω, not $\mathbb{F}$, 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 $\xi^k \in \mathbb{F}^*$, for some $0 \leq k \leq m-1$.

Remark 5. In particular, $A = \{\alpha\xi^{e+zn} \ : \ 0 \leq z \leq \delta - 1\}$ is independent with respect to the consecutive set E in (2), which gives the BCH bound for C_E. Let $D := \{\alpha\xi^{e+zn_1+yn_2} : 0 \leq z \leq \delta - 2, 0 \leq y \leq s\}$, for integers $b \geq 0$, $\delta \geq 2$ 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 $z \in \{0, \ldots, \delta-2\}$, $A_z := \{\alpha\xi^{e+zn_1} : 0 \leq z \leq \delta - 2\} \cup \{\alpha\xi^{e+zn_1+yn_2} : 0 \leq y \leq s+1\}$ is independent with respect to D and we get the HT bound for C_D.

B. Spectral theory of quasi-twisted codes

A linear code $C \subseteq \mathbb{F}_q^{m\ell}$ is called λ-*quasi-twisted* (λ-QT) of index ℓ if it is invariant under the λ-constashift of codewords by ℓ positions with ℓ being the smallest positive integer with this property. In particular, if $\ell = 1$, then C is λ-constacyclic. If $\lambda = 1$ or $q = 2$, then C is QC of index ℓ. For a codeword $\vec{c} \in C$, seen as an $m \times \ell$ array

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

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

To an element $\vec{c} \in \mathbb{F}_q^{m\times\ell} \simeq \mathbb{F}_q^{m\ell}$ in (3), we associate an element of R^ℓ (cf. (1))

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

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

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

The isomorphism ϕ in (1) extends naturally to

$$\begin{array}{rcl} \Phi : \mathbb{F}_q^{m\ell} & \longrightarrow & R^\ell \\ \vec{c} & \longmapsto & \vec{c}(x). \end{array} \tag{5}$$

The row λ-constashift in $\mathbb{F}_q^{m\times\ell}$ corresponds to componentwise multiplication by x in R^ℓ. The map Φ above is, therefore, an R-module isomorphism and a λ-QT code $C \subseteq \mathbb{F}_q^{m\ell}$ of index ℓ can be viewed as an R-submodule of R^ℓ.

Lally and Fitzpatrick proved in [11] that every QC code has a polynomial generator in the form of a reduced matrix. We provide an easy adaptation of their findings for QT codes.

Consider the ring homomorphism

$$\begin{array}{rcl} \Psi \ : \ \mathbb{F}_q[x]^\ell & \longrightarrow & R^\ell \\ (f_0(x), \ldots, f_{\ell-1}(x)) & \longmapsto & (f_0(x) + I, \ldots, f_{\ell-1}(x) + I). \end{array} \tag{6}$$

Let each $\vec{e}_j$ denote the standard basis vector of length ℓ with 1 at the j^{th} coordinate and 0 elsewhere. Given a λ-QT code $C \subseteq R^\ell$, the preimage $\widetilde{C}$ of C in $\mathbb{F}_q[x]^\ell$ is an $\mathbb{F}_q[x]$-submodule containing $\widetilde{K} = \{(x^m - \lambda)\vec{e}_j : 0 \leq j \leq \ell - 1\}$. From here on, the tilde indicates structures over $\mathbb{F}_q[x]$.

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

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

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

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

generate $\widetilde{C}$. We triangularise $\mathcal{G}$ by elementary row operations to obtain another equivalent generating set from the rows of an upper-triangular $\ell \times \ell$ matrix with entries in $\mathbb{F}_q[x]$

$$\widetilde{G}(x) = \begin{pmatrix} g_{0,0}(x) & g_{0,1}(x) & \dots & g_{0,\ell-1}(x) \\ 0 & g_{1,1}(x) & \dots & g_{1,\ell-1}(x) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & g_{\ell-1,\ell-1}(x) \end{pmatrix}, \quad (7)$$

where $\widetilde{G}(x)$ satisfies (see [11, 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 $\widetilde{G}(x)$ has nonzero rows and each nonzero element of $\widetilde{C}$ can be expressed as $(0, \dots, 0, c_j(x), \dots, c_{\ell-1}(x))$, where $j \ge 0$, $c_j(x) \ne 0$ and $g_{j,j}(x) \mid c_j(x)$. Moreover, Condition 2) implies that the rows of $\widetilde{G}(x)$ is a reduced basis of $\widetilde{C}$, 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 Ψ in (6). Then, the rows of $G(x)$ are an R-generating set for C. We say that C, generated as an R-submodule, is an r-generator QT code if $G(x)$ has r (nonzero) rows. The $\mathbb{F}_q$-dimension of C, as shown in [11, Corollary 2.4], is

$$m\ell - \sum_{j=0}^{\ell-1} \deg(g_{j,j}(x)) = \sum_{j=0}^{\ell-1} [m - \deg(g_{j,j}(x))]. \quad (8)$$

In [15], Semenov and Trifonov use the polynomial matrix $\widetilde{G}(x)$ in (7) to develop a spectral theory for QC codes. This gives rise to a BCH-like minimum distance bound. Their bound is improved by Zeh and Ling in [16] by using the HT bound ([8]). We 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 (7) with entries in $\mathbb{F}_q[x]$. The *determinant* of $\widetilde{G}(x)$ is

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

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

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

where $\mathbb{F}$ is the splitting field of $x^m - \lambda$, as before. It was shown in [15] 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 without the proof, since it can be shown in exactly the same way.

Lemma 6. *[15, Lemma 1] The algebraic multiplicity of any eigenvalue of a λ-QT code C is equal to its geometric multiplicity.*

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

$$V_i := \begin{pmatrix} \vec{v}_{i,0} \\ \vdots \\ \vec{v}_{i,n_i-1} \end{pmatrix} = \begin{pmatrix} v_{i,0,0} & \dots & v_{i,0,\ell-1} \\ \vdots & \vdots & \vdots \\ v_{i,n_i-1,0} & \dots & v_{i,n_i-1,\ell-1} \end{pmatrix}, \quad (9)$$

having the basis elements as its rows. We let

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

$$H := \begin{pmatrix} H_1 \\ \vdots \\ H_t \end{pmatrix} = \begin{pmatrix} V_1 & \beta_1 V_1 & \dots & (\beta_1)^{m-1} V_1 \\ \vdots & \vdots & \vdots & \vdots \\ V_t & \beta_t V_t & \dots & (\beta_t)^{m-1} V_t \end{pmatrix}. \quad (10)$$

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 Lemma 7 below, it remains to show the linear independence of these n rows, which was already shown in [15, Lemma 2].

Lemma 7. *The matrix H in (10) has rank $m\ell - \dim_{\mathbb{F}_q}(C)$.*

It is immediate to confirm that $H\vec{c}^\top = \vec{0}_n$ for any codeword $\vec{c} \in C$. Together with Lemma 7, we obtain the following easily.

Proposition 8. *[15, Theorem 1] The $n \times m\ell$ matrix H in (10) is a parity-check matrix for C.*

Remark 9. Note that if $\overline{\Omega} = \emptyset$, then the construction of H in (10) is impossible. Hence, we have assumed $\overline{\Omega} \ne \emptyset$ and we can always say $H = \vec{0}_{m\ell}$ if $C = \mathbb{F}_q^{m\ell}$. The other extreme case is when $\overline{\Omega} = \Omega$. By using Lemma 7 above, one can easily deduce that a given QT code $C = \{\vec{0}_{m\ell}\}$ 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 eigenvalue in Ω has multiplicity ℓ.

Definition 10. Let $\mathcal{V} \subseteq \mathbb{F}^\ell$ be an eigenspace. We define the *eigencode* corresponding to $\mathcal{V}$ by

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

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

The BCH-like minimum distance bound of Semenov and Trifonov for a given QC code in [15, Theorem 2] 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 [16, Theorem 1] without using the parity-check matrix in their proof. The

eigencode, however, is still needed. In the next section we will prove the analogues of these bounds for QT codes in terms of the Roos and shift bounds.

III. Spectral Bounds for QT Codes

First, we establish a general spectral bound on the minimum distance of a given QT code. Let $C \subseteq \mathbb{F}_q^{m\ell}$ be a λ-QT code of index ℓ with nonempty eigenvalue set $\overline{\Omega} \subsetneq \Omega$. Let $P \subseteq \overline{\Omega}$ be a nonempty subset of eigenvalues such that $P = \{\alpha\xi^{u_1}, \alpha\xi^{u_2}, \ldots, \alpha\xi^{u_r}\}$, where $0 < r \leq |\overline{\Omega}|$. We define

$$\widetilde{H}_P := \begin{pmatrix} 1 & \alpha\xi^{u_1} & (\alpha\xi^{u_1})^2 & \ldots & (\alpha\xi^{u_1})^{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha\xi^{u_r} & (\alpha\xi^{u_r})^2 & \ldots & (\alpha\xi^{u_r})^{m-1} \end{pmatrix}. \quad (11)$$

Let d_P be a nonnegative integer such that any λ-constacyclic code $C_P \subseteq \mathbb{F}_q^m$, whose defining set contains P, has a minimum distance at least d_P. We have $\widetilde{H}_P \vec{c}_P^{\top} = \vec{0}_r$, for any $\vec{c}_P \in C_P$. In particular, if P is equal to the defining set of C_P, then $\widetilde{H}_P$ is a parity-check matrix for C_P.

Let $\mathcal{V}_P$ denote the common eigenspace of the eigenvalues in P and let V_P be the matrix, say of size $t \times \ell$, consisting of a basis for $\mathcal{V}_P$ (cf. (9)). If we set $\widehat{H}_P = \widetilde{H}_P \otimes V_P$, then $\widehat{H}_P \vec{c}^{\top} = \vec{0}_{m\ell}$, for all $\vec{c} \in C$. In other words, $\widehat{H}_P$ is a submatrix of H in (10) if $\mathcal{V}_P \neq \{\vec{0}_\ell\}$. If $\mathcal{V}_P = \{\vec{0}_\ell\}$, then $\widehat{H}_P$ does not exist. We first handle this case separately so that the bound is valid even if we have $\mathcal{V}_P = \{\vec{0}_\ell\}$, before the cases where we can use $\widehat{H}_P$ in the proof.

In the rest, we consider the quantity $\min(d_P, d(\mathbb{C}_P))$, where $\mathbb{C}_P$ is the eigencode corresponding to $\mathcal{V}_P$. We have assumed $P \neq \emptyset$ so that $\widetilde{H}_P$ is defined, and we also have $P \neq \Omega$ as $P \subseteq \overline{\Omega} \subsetneq \Omega$ so that d_P is well-defined. If $|P| \geq 1$, then the BCH bound implies $d_P \geq 2$. On the other hand, if $\mathcal{V}_P = \{\vec{0}_\ell\}$, then $\mathbb{C}_P = \mathbb{F}_q^\ell$ and $d(\mathbb{C}_P) = 1$. Hence, $\min(d_P, d(\mathbb{C}_P)) = 1$ only if $d(\mathbb{C}_P) = 1$ (including the case $\mathcal{V}_P = \{\vec{0}_\ell\}$), where $d(C) \geq 1$ holds for any nonzero QT code C.

Now let $\emptyset \neq P \subseteq \overline{\Omega} \subsetneq \Omega$ and $d(\mathbb{C}_P) \geq 2$. Assume that there exists a codeword $\vec{c} \in C$ of weight ω such that $0 < \omega < \min(d_P, d(\mathbb{C}_P))$. For each $0 \leq k \leq m-1$, let $\vec{c}_k = (c_{k,0}, ..., c_{k,\ell-1})$ be the k^{th} row of the codeword $\vec{c}$ given as in (3) and we set $\vec{s}_k := V_P \vec{c}_k^{\top}$. Since $d(\mathbb{C}_P) > \omega$, we have $\vec{c}_k \notin \mathbb{C}_P$ and therefore $\vec{s}_k = V_P \vec{c}_k^{\top} \neq \vec{0}_t$, for all $\vec{c}_k \neq \vec{0}_\ell$, $k \in \{0, \ldots, m-1\}$. Hence, $0 < |\{\vec{s}_k : \vec{s}_k \neq \vec{0}_t\}| \leq \omega < \min(d_P, d(\mathbb{C}_P))$. Let $S := [\vec{s}_0\ \vec{s}_1 \cdots \vec{s}_{m-1}]$. Then $\widetilde{H}_P S^{\top} = 0$, which implies that the rows of the matrix S lies in the right kernel of $\widetilde{H}_P$. But this is a contradiction since any row of S has weight at most $\omega < d_P$, showing the following.

Theorem 11. *Let $C \subseteq R^\ell$ be a λ-QT code of index ℓ with nonempty eigenvalue set $\overline{\Omega} \subsetneq \Omega$. Let $P \subseteq \overline{\Omega}$ be a nonempty subset of eigenvalues and let $C_P \subseteq \mathbb{F}_q^m$ be any λ-constacyclic code with defining set $L \supseteq P$ and minimum distance at least d_P. We define $\mathcal{V}_P := \bigcap_{\beta \in P} \mathcal{V}_\beta$ as the common eigenspace of the eigenvalues in P and let $\mathbb{C}_P$ denote the eigencode corresponding to $\mathcal{V}_P$. Then,*

$$d(C) \geq \min\{d_P, d(\mathbb{C}_P)\}. \quad (12)$$

Theorem 11 allows us to use any minimum distance bound derived for constacyclic codes based on their defining set. The following special cases are immediate after the preparation that we have done in Section II (cf. Theorems 1 and 4).

Corollary 12. *Let $C \subseteq R^\ell$ be a λ-QT code of index ℓ with $\overline{\Omega} \subsetneq \Omega$ 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' containing 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 $T_A := A \cap \overline{\Omega}$.

Proof.

i) Let $N = \{\alpha\xi^{u_1}, \ldots, \alpha\xi^{u_r}\}$ and $M = \{\alpha\xi^{v_1}, \ldots, \alpha\xi^{v_s}\}$ be such that there exists a consecutive set $M' = \{\alpha\xi^z : v_1 \leq z \leq v_s\} \subseteq \Omega$ containing M with $|M'| \leq |M| + d_N - 2$. We define the matrices

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

$$\widetilde{H}_M := \begin{pmatrix} 1 & \alpha\xi^{v_1} & (\alpha\xi^{v_1})^2 & \ldots & (\alpha\xi^{v_1})^{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha\xi^{v_s} & (\alpha\xi^{v_s})^2 & \ldots & (\alpha\xi^{v_s})^{m-1} \end{pmatrix}.$$

Consider the joint subset $MN = \{\alpha\xi^{u_i+v_j} : 1 \leq i \leq r, 1 \leq j \leq s\} \subseteq \overline{\Omega}$. Let B_k be the k^{th} column of $\widetilde{H}_N$ for $k \in \{0, \ldots, m-1\}$. We create the joint matrix

$$\widetilde{H}_{MN} = \begin{pmatrix} B_0 & \alpha^{v_1}B_1 & (\alpha^{v_1})^2 B_2 & \ldots & (\alpha^{v_1})^{m-1}B_{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ B_0 & \alpha^{v_s}B_1 & (\alpha^{v_s})^2 B_2 & \ldots & (\alpha^{v_s})^{m-1}B_{m-1} \end{pmatrix}.$$

Now let $\mathcal{V}_{MN} := \bigcap_{\beta \in MN} \mathcal{V}_\beta$ denote the common eigenspace of the eigenvalues in MN and let V_{MN} be the matrix consisting of a basis for $\mathcal{V}_{MN}$, built as in (9). Let $\mathbb{C}_{MN}$ be the eigencode corresponding to $\mathcal{V}_{MN}$. Setting $\widehat{H}_{MN} := \widetilde{H}_{MN} \otimes V_{MN}$ implies $\widehat{H}_{MN}\vec{c}^{\top} = \vec{0}$ for all $\vec{c} \in C$. The rest of the proof is identical with the proof of Theorem 11, where P is replaced by MN, and the result follows by the Roos bound (Theorem 1).

ii) For each independent $A \subseteq \Omega$ with respect to $\overline{\Omega}$, let $T_A = A \cap \overline{\Omega} = \{\alpha\xi^{w_1}, \alpha\xi^{w_2}, \ldots, \alpha\xi^{w_y}\}$. Since $\overline{\Omega}$ is a proper subset of Ω, a nonempty T_A can be obtained by the recursive construction of A. We define

$$\widetilde{H}_{T_A} = \begin{pmatrix} 1 & \alpha\xi^{w_1} & (\alpha\xi^{w_1})^2 & \ldots & (\alpha\xi^{w_1})^{m-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha\xi^{w_y} & (\alpha\xi^{w_y})^2 & \ldots & (\alpha\xi^{w_y})^{m-1} \end{pmatrix}.$$

Let V_{T_A} be the matrix corresponding to a basis of $\mathcal{V}_{T_A}$, which is the intersection of the eigenspaces belonging to the eigenvalues in T_A. Let $\mathbb{C}_{T_A}$ be the eigencode corresponding to the eigenspace $\mathcal{V}_{T_A}$. We again set $\widehat{H}_{T_A} := \widetilde{H}_{T_A} \otimes V_{T_A}$ and the result follows in a similar way by using the shift bound (Theorem 4).

□

Remark 13. We can obtain the QT analogues of the BCH-like bound in [15, Theorem 2] and the HT-like bound in [16, Theorem 1] by using Remarks 3 and 5.

IV. Examples

We begin with two examples of QC codes ($\lambda = 1$) for which Corollary 12 yields the exact distances.

Example 14. Let γ be a primitive 23^{rd} root of unity. Let $C \subseteq \mathbb{F}_2^{92}$ be the binary QC code with $\ell = 4$, $d(C) = 7$ and eigenvalues $\overline{\Omega} = \{\gamma^i : i = 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. The common eigenspace is generated by $V_{\overline{\Omega}} = V = I_4$ over $\mathbb{F}_{2^{11}}$, which is the splitting field of $x^{23} - 1$. We have $\mathbb{C}_{\overline{\Omega}} = \{\vec{0}_4\}$ and therefore $d(\mathbb{C}_{\overline{\Omega}}) = \infty$. Hence, Theorem 11 yields $d(C) \geq d_P$, for $P = \overline{\Omega}$. The associated cyclic code $C_{\overline{\Omega}}$ is the well-known binary Golay code of length 23, which has minimum distance $d_{\overline{\Omega}} = 7$, which is equal to $d(C)$. Note that the shift bound yields the exact distance of binary Golay code (see [12, Example 7]) with $A = \{\gamma^i : i = 0, 1, 3, 4, 5, 6, 16, 18\}$ and $\mathbb{C}_{T_A} = \mathbb{C}_{\overline{\Omega}} = \{\vec{0}_4\}$, hence Corollary 12 ii. is sharp in this example. We also note that the Roos bound estimates 5 for $d(C_{\overline{\Omega}})$, as does the BCH bound.

Example 15. Let η be a primitive 26^{th} root of unity. Consider the ternary QC code $C \subseteq \mathbb{F}_3^{104}$ with $\ell = 4$, minimum distance 6 and eigenvalues $\overline{\Omega} = \{\eta^i : i = 0, 13, 14, 16, 17, 22, 23, 25\}$. The common eigenspace is generated by $V_{\overline{\Omega}} = V = I_4$ over $\mathbb{F}_{3^3}$, which is the splitting field of $x^{26}-1$. We again have $\mathbb{C}_{\overline{\Omega}} = \{\vec{0}_4\}$ and therefore $d(\mathbb{C}_{\overline{\Omega}}) = \infty$. Hence, Theorem 11 yields $d(C) \geq d_{\overline{\Omega}}$. The cyclic code $C_{\overline{\Omega}}$ has minimum distance $d_{\overline{\Omega}} = 6 = d(C)$. Note that the Roos bound yields the exact distance of $C_{\overline{\Omega}}$: let $N = \{\eta^{13}, \eta^{14}\}$ and $M = \{\eta^0, \eta^3, \eta^9, \eta^{12}\}$. Then $d_N = 3$ and $M' = \{\eta^0, \eta^3, \eta^6, \eta^9, \eta^{12}\} = \{\eta^{3i} : 0 \leq i \leq 4\}$, so $|M'| = 5 \leq 4 + 3 - 2$. We get $d_{MN} \geq 4 + 3 - 1$, where $\mathbb{C}_{MN} = \{\vec{0}_4\}$. However, the shift bound estimates 5 for $d(C_{\overline{\Omega}})$ (see [7, Example 26.7]), hence Corollary 12 i. is sharp here.

In [15], Semenov and Trifonov compared their BCH-like spectral bound with several other bounds given for QC codes. In Table I, we compare the estimates of the general spectral bound given in (12) with the ST and ZL bounds for a number of binary and ternary codes. The actual distance of the QT code and the estimates of the spectral, ST and ZL bounds are denoted by d, d_{SP}, d_{BCH} and d_{HT}, respectively. We consider the case $P = \overline{\Omega}$ so that $d_{\overline{\Omega}} = d(C_{\overline{\Omega}})$, and the search using Magma ([4]) is restricted to QT codes with $\mathbb{C}_{\overline{\Omega}} = \mathbb{C}_{BCH} = \mathbb{C}_{HT} = \{\vec{0}_\ell\}$ (*i.e.*, $d(\mathbb{C}_{\overline{\Omega}}) = d(\mathbb{C}_{BCH}) = d(\mathbb{C}_{HT}) = \infty$), due to their ease of computation. For each QT code listed, its eigenvalue set $\overline{\Omega}$ is given in terms of an index set $\mathcal{I}$, where $\overline{\Omega} = \{\xi^i : i \in \mathcal{I}\}$, for some primitive m^{th} root of unity ξ.

TABLE I
Spectral bound versus ST and ZL bounds

No	q	λ	m	ℓ	d_{BCH}	d_{HT}	d=d_{SP}	$\mathcal{I}$ for $\overline{\Omega}$
1	2	1	23	2	5	5	7	{1-4, 6, 8, 9, 12, 13, 16, 18}
2			33	2	8	10	12	{0, 3, 5-7, 9-15, 18-24, 26-28, 30}
3			39	2	7	8	12	{3, 6, 7, 9, 12-15, 17-19, 21, 23, 24, 26-31, 33-38}
4			21	3	5	6	8	{3, 5-7, 9, 10, 12-15, 17-20}
5			33	3	5	8	11	{1-4, 6, 8, 9, 11, 12, 15-18, 21, 22, 24, 25, 27, 29-32}
6	3	1	13	2	4	5	6	{0, 2, 4-6, 10, 12}
7			20	2	5	5	8	{0, 1, 3-5, 7-10, 12, 15, 16}
8			40	2	11	17	20	{0, 2, 4-8, 11-19, 21-26, 28, 29, 31-39}
9			26	3	5	8	10	{1-4, 6, 8-10, 12, 13, 17, 18, 20, 23-25}
10			44	3	10	11	18	{0-7, 9-13, 15-23, 25, 27, 29-31, 33, 35-37, 39, 41, 43}
11	3	-1	20	2	4	5	6	{3, 6, 10-12, 14, 15, 17-19}
12			28	2	4	6	9	{0-2, 4, 6, 7, 9, 11-13, 17, 19, 22, 24}
13			41	2	11	13	20	{0-4, 6, 7, 9-14, 17-19, 21-23, 26-31, 33, 34, 36-40}
14			28	3	3	4	6	{3, 10, 14, 15, 17, 18, 23, 24, 26, 27}
15			28	3	7	9	11	{0-2, 4-9, 11-13, 16, 17, 19-22, 24, 25}

References

[1] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaib and P. Solé, "On self-dual double negacirculant codes", *Disc. Appl. Math.*, vol. 222, 205–212, 2017.

[2] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaib and P. Solé, "On linear complementary-dual multinegacirculant codes", to appear in *Cryptog. Commun.*, 2019.

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

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

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

[6] R. Daskalov and P. Hristov, "New quasi-twisted degenerate ternary linear codes", *IEEE Trans. Inf. Theory*, vol. 49, 2259–2263, 2003.

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

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

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

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

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

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

[13] D. Radkova and A. J. van Zanten, "Constacyclic codes as invariant subspaces", *Linear Alg. Appl.*, vol. 430, no. 2–3, 855–864, 2009.

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

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

[16] A. Zeh and S. Ling, "Decoding of quasi-cyclic codes up to a new lower bound on the minimum distance", *Proc. ISIT*, Jun. 2014, 2584–2588.