STRUCTURE AND PERFORMANCE OF GENERALIZED QUASI-CYCLIC CODES

Cem Güneri[1], Ferruh Özbudak[3], Buket Özkaya[1], Elif Saçıkara [1],
Zahra Sepasdar[4], Patrick Solé[2]

[1] Sabancı University, Istanbul, Turkey
[2] CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France,
[3] Middle East Technical University, Ankara, Turkey
[4] Department of Pure Mathematics, Ferdowsi University of Mashhad, Iran

Abstract. Generalized quasi-cyclic (GQC) codes form a natural generalization of quasi-cyclic (QC) codes. They are viewed here as mixed alphabet codes over a family of ring alphabets. Decomposing these rings into local rings by the Chinese Remainder Theorem yields a decomposition of GQC codes into a sum of concatenated codes. This decomposition leads to a trace formula, a minimum distance bound, and to a criteria for the GQC code to be self-dual or to be linear complementary dual (LCD). Explicit long GQC codes that are LCD, but not QC, are exhibited.

Keywords: GQC codes, QC codes, LCD codes, self-dual codes.

1. Introduction

Quasi-cyclic codes (QC) have been known for more than fifty years. They have been shown to be asymptotically good, which is in marked contrast with the subclass of cyclic codes. Even in short length (less than a hundred) they contain more optimal codes than cyclic codes. Still, their structure is more complex than that of cyclic codes. Let q denote a prime power and $\mathbb{F}_q$ be the finite field of that order. A linear code over $\mathbb{F}_q$ is said to be a quasi-cyclic code of index ℓ and length $n = \ell m$, if and only if it is held invariant by T^ℓ, where T is the standard coordinate shift on n digits and ℓ is the smallest number with this property. The approach of [9] is to view such a code as mapped from a code of length ℓ over the ring

$$R = \mathbb{F}_q[x]/\langle x^m - 1\rangle.$$

In recent years a super class of quasi cyclic codes has appeared: generalized quasi-cyclic codes ([5, 13]). Up to coordinate permutation a QC code is equivalent to a linear code with block circulant generator matrix. More specifically, the circulant blocks will have the same size, namely the co-index m. The idea of Generalized Quasi-Cyclic (GQC) codes is to relax this requirement to allow blocks of different sizes. The immediate benefit is to construct codes whose lengths are not multiple of the index. For instance a GQC code might very well have prime length. The CRT decomposition has been extended to GQC codes at the price of a more complicated notation ([5]).

The aim of this paper is twofold. First, we aim to extend the structural theory of [9] to GQC codes, a program partially done in [5]. In particular the trace formula of [9] is extended to GQC codes. Concatenated description of GQC codes is presented and the results for QC codes in [6] is extended to GQC codes. Moreover, multilevel (generalized) concatenated description of GQC codes is obtained, which yields a minimum distance bound for GQC codes, extending Jensen's bound for QC codes. Let us note that there is a minimum distance bound on GQC codes due to Esmaeili and Yari ([5]) but it only applies to one generator GQC codes. Our bound applies to all GQC codes. Criteria for self-duality bearing on the component codes are given. In a recent paper [7], a similar criterion for a QC code to intersect its dual trivially (LCD code as Linear Complementary Dual) was derived. This criterion is generalized here to GQC codes.

Next, we study the asymptotic performance of GQC codes. Explicit long GQC codes that are LCD, but not QC, are exhibited. These codes have only finitely many distinct co-indices in the spirit of [11], but have a length going to infinity. The proof rests on the existence of families of good QC codes that are LCD [7].

The material is organized as follows. The next section collects the necessary definitions and notations. Section 3 develops the concatenated structure and a trace expression. Section 4 derives the minimum distance bound. Section 5 derives criteria for self-duality and LCDness. Asymptotic results are given in Section 6. Section 7 concludes the article and points out directions for future research.

2. Background on QC and GQC codes

Let $\mathbb{F}_q$ denote the finite field with q elements, where q is a prime power. A linear code C of length $m\ell$ over $\mathbb{F}_q$ is called a quasi-cyclic (QC) code of index ℓ if it is invariant under shift of codewords by ℓ positions and ℓ is the minimal number with this property. Note that if $\ell = 1$, then C is a cyclic code. If we view codewords of C as $m \times \ell$ arrays as follows

$$c = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix}, \tag{2.1}$$

then being invariant under shift by ℓ units amounts to being closed under row shift.

Let us define the quotient ring $R := \mathbb{F}_q[x]/\langle x^m - 1\rangle$. To an element $c \in \mathbb{F}_q^{m\times\ell} \simeq \mathbb{F}_q^{m\ell}$ as in (2.1), we associate an element of R^ℓ

$$\vec{c}(x) := (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) \in R^\ell, \tag{2.2}$$

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

$$c_j(x) := c_{0,j} + c_{1,j}x + c_{2,j}x^2 + \cdots + c_{m-1,j}x^{m-1} \in R. \tag{2.3}$$

Then, the following map is an $\mathbb{F}_q$-linear isomorphism.

$$\begin{array}{rccc} \phi: & \mathbb{F}_q^{m\ell} & \longrightarrow & R^\ell \\ & c=\begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \longmapsto & \vec{c}(x). \end{array} \tag{2.4}$$

Note that for $\ell = 1$, this amounts to the classical polynomial representation of cyclic codes. Observe that ℓ shift on $\mathbb{F}_q^{m\ell}$ corresponds to componentwise multiplication by x in R^ℓ and a q-ary QC code C of length $m\ell$ and index ℓ can be considered as an R-submodule in R^ℓ.

Let us now recall the decomposition of a length $m\ell$ QC code over $\mathbb{F}_q$ into shorter codes over extensions of $\mathbb{F}_q$. We follow the brief presentation in [6] and refer the reader to [9] for details. We assume that $\gcd(m, q) = 1$ and factor the polynomial $x^m - 1$ into pairwise distinct irreducible polynomials in $\mathbb{F}_q[x]$ as

$$x^m - 1 = f_1(x)f_2(x)\cdots f_s(x). \tag{2.5}$$

By Chinese Remainder Theorem, we have the following ring isomorphism:

$$R \cong \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle f_i(x)\rangle. \tag{2.6}$$

Since each $f_i(x)$ divides $x^m - 1$, their roots are powers of some fixed primitive m^{th} root of unity ξ. For each $i = 1, \ldots, s$, let u_i be the smallest nonnegative integer such that $f_i(\xi^{u_i}) = 0$. Since $f_i(x)$'s are irreducible, direct summands in (2.6) are field extensions of $\mathbb{F}_q$. If $\mathbb{E}_i := \mathbb{F}_q[x]/\langle f_i(x)\rangle$ for $1 \le i \le s$, then we have

$$R^\ell \cong \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell. \tag{2.7}$$

Hence, a QC code $\mathcal{C} \subset R^\ell$ 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 decomposes as

$$C = C_1 \oplus \cdots \oplus C_s, \tag{2.8}$$

where C_i is a linear code of length ℓ over $\mathbb{E}_i$, for each i. These length ℓ linear codes over various extensions of $\mathbb{F}_q$ are called the constituents of C.

If $C \subset R^\ell$ is generated as an R-module by

$$\{\big(a_0^1(x), \ldots, a_{\ell-1}^1(x)\big), \ldots, \big(a_0^r(x), \ldots, a_{\ell-1}^r(x)\big)\} \subset R^\ell,$$

then

$$C_i = \mathrm{Span}_{\mathbb{E}_i}\big\{\big(a_0^b(\xi^{u_i}), \ldots, a_{\ell-1}^b(\xi^{u_i})\big) : 1 \le b \le r\big\}, \text{ for } 1 \le i \le s. \tag{2.9}$$

Another way of decomposing QC codes is given by Jensen ([8]) by the concatenation method. For each $1 \le i \le s$, consider the minimal cyclic code of length m over $\mathbb{F}_q$, whose check polynomial is $f_i(x)$. Let θ_i denote the generating primitive idempotent for each minimal cyclic code in consideration. Jensen showed the following.

Theorem 2.1. [8] *(i) Let C be a length $m\ell$ and index ℓ QC code over $\mathbb{F}_q$. Then there exist linear codes $\mathfrak{C}_i$ of length ℓ over $\mathbb{E}_i$ such that $C = \bigoplus_{i=1}^{s} \langle\theta_i\rangle \square \mathfrak{C}_i$.*

(ii) Conversely, let $\mathfrak{C}_i$ be an $\mathbb{E}_i$-linear code of length ℓ for each $i \in \{1, \ldots, s\}$. Then, $C = \bigoplus_{i=1}^{s} \langle\theta_i\rangle \square \mathfrak{C}_i$ is a q-ary QC code of length $m\ell$ and index ℓ.

Note that each field $\mathbb{E}_i$ is isomorphic to $\langle\theta_i\rangle$, for each $1 \leq i \leq s$, via the maps

$$\begin{array}{ccc} \varphi_i : \langle\theta_i\rangle & \longrightarrow & \mathbb{E}_i \\ a(x) & \longmapsto & a(\xi^{u_i}) \end{array} \qquad \begin{array}{ccc} \psi_i : \mathbb{E}_i & \longrightarrow & \langle\theta_i\rangle \\ \delta & \longmapsto & \sum_{k=0}^{m-1} a_k x^k \end{array}, \tag{2.10}$$

where

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

It is easy to observe that φ_i and ψ_i are inverse to each other. Let us note that for each i, the concatenation of the minimal cyclic code $\langle\theta_i\rangle$ and the linear code $\mathfrak{C}_i$ over $\mathbb{E}_i$ is carried out by the map ψ_i, which identifies the field $\mathbb{E}_i$ with the minimal cyclic code. In other words, a codeword $(c_0, \ldots, c_{\ell-1})$ in some $\mathfrak{C}_i$ is mapped to $(\psi_i(c_0), \ldots, \psi_i(c_{\ell-1}))$ in R^ℓ.

It is proved in [6] that for a given QC code C, the constituents C_i's in (2.8) and the outer codes $\mathfrak{C}_i$'s in the concatenated structure are equal to each other (see [6, Theorem 4.1]).

By (2.10), the concatenated structure of QC codes can be used to demonstrate the trace representation of QC codes given by Ling-Solé, which provides a vectorial representation of codewords equivalent to (2.1), when the constituents are known.

Theorem 2.2. [9, Theorem 5.1] [6, Theorem 4.2] *Consider the QC code C with the constituents $C = C_1 \oplus \cdots \oplus C_s$, where $C_i \subset \mathbb{E}_i^\ell = \mathbb{F}_q(\xi^{u_i})^\ell$ is linear over $\mathbb{E}_i$ of length ℓ for each $1 \leq i \leq s$. Then an arbitrary codeword $c \in C$ as an $m \times \ell$ array has the form*

$$c = \begin{pmatrix} c_0(\lambda_1, \ldots, \lambda_s) \\ c_1(\lambda_1, \ldots, \lambda_s) \\ \vdots \\ c_{m-1}(\lambda_1, \ldots, \lambda_s) \end{pmatrix},$$

where $\lambda_i = (\lambda_{i,0}, \ldots, \lambda_{i,\ell-1})$ is a codeword in C_i for each i and

$$c_k(\lambda_1, \ldots, \lambda_s) = \left(\sum_{i=1}^{s} \mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q} \left(\lambda_{i,j} \xi^{-ku_i} \right) \right)_{0 \leq j \leq \ell-1},$$

for each $0 \leq k \leq m-1$.

If we set $\ell = 1$ above, then we get the trace representation of a q-ary cyclic code of length m.

Generalized quasi-cyclic (GQC) codes were introduced in [13], where their description is given as follows.

Definition 2.3. Let $m_0, \ldots, m_{\ell-1}$ be positive integers and set $R_j := \mathbb{F}_q[x]/\langle x^{m_j} - 1\rangle$ for each $j = 0, \ldots, \ell - 1$. An $\mathbb{F}_q[x]$-submodule of $R' := R_0 \times \cdots \times R_{\ell-1}$ is called a generalized quasi-cyclic (GQC) code of block lengths $(m_0, \ldots, m_{\ell-1})$, which is a linear code of length $m_0 + \cdots + m_{\ell-1}$ over $\mathbb{F}_q$.

Note that if $m_0 = \cdots = m_{\ell-1} = m$, then we obtain a quasi-cyclic code of length $m\ell$ and index ℓ.

Example 2.4. For any finite field $\mathbb{F}_q$ and any positive integer n, the q-ary repetition code of length n is a GQCCD code for any partition of n. Its dual, namely the parity check code of length n is also GQCCD. A nontrivial example is the class of binary Cordaro-Wagner codes([3]), which are, by definition, two dimensional codes attaining the best possible distance. Given an $[n, 2, d]$ Cordaro-Wagner code with the column partition (h, j, k), each h, j and k gives the number of the nonzero binary columns, namely $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in the generator matrix. Note that this code is self-orthogonal if n is multiple of 6 and complementary-dual otherwise (see Table I in [3]).

Consider the binary $[16, 2, 10]$ Cordaro-Wagner code C generated by

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

where $h = 6$, $j = k = 5$.

If we set $m_1 = h$, $m_2 = j$, $m_3 = k$ and $\ell = 3$, then C is a binary GQC code with:

$$C = \langle (x^5 + x^4 + x^3 + x^2 + x + 1, 0, x^4 + x^3 + x^2 + x + 1), (0, x^4 + x^3 + x^2 + x + 1, x^4 + x^3 + x^2 + x + 1) \rangle.$$

It is easy to observe that any Cordaro-Wagner code will give a binary 2-generator GQC code, where the polynomial coordinates of the generators will be either 0 or $\frac{x^m-1}{x-1}$ for $m = h, j, k$.

The factorization of GQC codes into constituents is given by Esmaeili and Yari in [5]. We will review this decomposition and introduce a notation which is suitable for presentation of our results in the rest of the article.

Let $\gcd(m_j, q) = 1$ for each $j = 0, \ldots, \ell - 1$, then each $x^{m_j} - 1$ factors into distinct irreducible polynomials. Suppose that the total number of distinct irreducible factors over all $x^{m_j} - 1$ decompositions is s and let $f_1(x), \ldots, f_s(x)$ denote these irreducible polynomials. Then for each j we have

$$x^{m_j} - 1 = f_1(x)^{v_{1,j}} f_2(x)^{v_{2,j}} \cdots f_s(x)^{v_{s,j}}, \tag{2.11}$$

where $v_{i,j} \in \{0, 1\}$. Since $f_i(x)$'s are irreducible, $\mathbb{F}_q[x]/\langle f_i(x)\rangle$ is a finite field extension of $\mathbb{F}_q$. Set $\mathbb{E}_i := \mathbb{F}_q[x]/\langle f_i(x)\rangle$ for $1 \le i \le s$ and for $1 \le i \le s$, $0 \le j \le \ell - 1$, define

$$\mathbb{E}_{i,j} := \begin{cases} \mathbb{E}_i, \text{ if } v_{i,j} = 1, \\ \{0\}, \text{ if } v_{i,j} = 0. \end{cases} . \tag{2.12}$$

Let us fix a root α_i of each f_i $(1 \le i \le s)$. For $a(x) \in R_j$ and $1 \le i \le s$, set

$$a_{i,j} = \begin{cases} a(\alpha_i), & \text{if } \mathbb{E}_{i,j} = \mathbb{E}_i, \\ 0, & \text{if } \mathbb{E}_{i,j} = \{0\}. \end{cases} \tag{2.13}$$

By (2.11), (2.12) and the Chinese Remainder Theorem, we get the following ring isomorphism for each $j = 0, \ldots, \ell - 1$:

$$R_j \cong \bigoplus_{i=1}^{s} \mathbb{E}_{i,j}, \tag{2.14}$$

where the isomorphism maps $a(x) \in R_j$ to $(a_{1,j} + \cdots + a_{s,j})$ (cf. (2.13)). Therefore we have

$$R' = R_0 \times \cdots \times R_{\ell-1} \cong \left(\bigoplus_{i=1}^{s} \mathbb{E}_{i,0} \right) \times \cdots \times \left(\bigoplus_{i=1}^{s} \mathbb{E}_{i,\ell-1} \right) \cong \bigoplus_{i=1}^{s} (\mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}), \tag{2.15}$$

where $\left(a^0(x), \ldots, a^{\ell-1}(x)\right) \in R'$ is mapped to $\sum_{i=1}^{s} \left(a^0_{i,0}, a^1_{i,1}, \ldots, a^{\ell-1}_{i,\ell-1}\right)$. In particular, a GQC code $C \subset R'$ can be viewed inside $\bigoplus_{i=1}^{s} \mathbb{E}_i^{\ell}$ since for each j, $\mathbb{E}_{i,j}$ is either $\mathbb{E}_i$ or $\{0\} \subset \mathbb{E}_i$.

Proposition 2.5. *Suppose the GQC code $C \subset R'$ is generated as an $\mathbb{F}_q[x]$-module by*

$$\left\{ \left(a^{1,0}(x), \ldots, a^{1,\ell-1}(x)\right), \ldots, \left(a^{r,0}(x), \ldots, a^{r,\ell-1}(x)\right) \right\} \subset R'.$$

Then C, as a subset of $\bigoplus_{i=1}^{s} \mathbb{E}_i^{\ell}$, can be written as

$$C = C_1 \oplus \cdots \oplus C_s, \tag{2.16}$$

where each C_i (constituent) is an $\mathbb{E}_i$-linear code of length ℓ and described as

$$C_i = \mathrm{Span}_{\mathbb{E}_i} \left\{ \left(a^{b,0}_{i,0}, \ldots, a^{b,\ell-1}_{i,\ell-1} \right) : 1 \le b \le r \right\}, \text{ for } 1 \le i \le s. \tag{2.17}$$

Proof. Observe that C, as a subset of R', can be written as

$$C = \left\{ g_1(x) \left(a^{1,0}(x), \ldots, a^{1,\ell-1}(x)\right) + \cdots + g_r(x) \left(a^{r,0}(x), \ldots, a^{r,\ell-1}(x)\right) : \ g_1, \ldots, g_r \in \mathbb{F}_q[x] \right\}.$$

Then by (2.15), C_i is of the form

$$C_i = \left\{ g_1(\alpha_i) \left(a^{1,0}_{i,0}, \ldots, a^{1,\ell-1}_{i,\ell-1}\right) + \cdots + g_r(\alpha_i) \left(a^{r,0}_{i,0}, \ldots, a^{r,\ell-1}_{i,\ell-1}\right) : \ g_1, \ldots, g_r \in \mathbb{F}_q[x] \right\}.$$

Since α_i is a root of $f_i(x)$, we have $\mathbb{E}_i = \mathbb{F}_q(\alpha_i)$. Therefore the elements $g_1(\alpha_i), \ldots, g_r(\alpha_i)$ take all possible values in $\mathbb{E}_i$ as the polynomials $g_1, \ldots, g_r$ range over $\mathbb{F}_q[x]$. Hence the result follows. □

Remark 2.6. Depending on $v_{i,j}$'s in the factorization (2.11), some $\mathbb{E}_{i,j}$'s can be $\{0\}$ and hence corresponding coordinates of all the codewords in the related constituent will be 0.

Example 2.7. Let $q = 2$, $m_0 = 3$, $m_1 = 5$, $m_2 = 9$ and hence $\ell = 3$. We have

$$R' = R_0 \times R_1 \times R_2 = \mathbb{F}_2[x]/\langle x^3 - 1\rangle \times \mathbb{F}_2[x]/\langle x^5 - 1\rangle \times \mathbb{F}_2[x]/\langle x^9 - 1\rangle$$

and

$$\begin{aligned} x^3 - 1 &= (x+1)(x^2 + x + 1), \\ x^5 - 1 &= (x+1)(x^4 + x^3 + x^2 + x + 1), \\ x^9 - 1 &= (x+1)(x^2 + x + 1)(x^6 + x^3 + 1). \end{aligned}$$

Let $f_1(x) = x + 1$, $f_2(x) = x^2 + x + 1$, $f_3(x) = x^4 + x^3 + x^2 + x + 1$ and $f_4(x) = x^6 + x^3 + 1$. Then we have $\mathbb{E}_1 \simeq \mathbb{F}_2$, $\mathbb{E}_2 \simeq \mathbb{F}_4$, $\mathbb{E}_3 \simeq \mathbb{F}_{16}$ and $\mathbb{E}_4 \simeq \mathbb{F}_{64}$. Moreover, with the notation in (2.12), we have the following:

$$\begin{array}{llll} \mathbb{E}_{1,0} = \mathbb{E}_1 & \mathbb{E}_{2,0} = \mathbb{E}_2 & \mathbb{E}_{3,0} = \{0\} & \mathbb{E}_{4,0} = \{0\} \\ \mathbb{E}_{1,1} = \mathbb{E}_1 & \mathbb{E}_{2,1} = \{0\} & \mathbb{E}_{3,1} = \mathbb{E}_3 & \mathbb{E}_{4,1} = \{0\} \\ \mathbb{E}_{1,2} = \mathbb{E}_1 & \mathbb{E}_{2,2} = \mathbb{E}_2 & \mathbb{E}_{3,2} = \{0\} & \mathbb{E}_{4,2} = \mathbb{E}_4 \end{array}$$

Hence,

$$R' \simeq (\mathbb{E}_1 \times \mathbb{E}_1 \times \mathbb{E}_1) \oplus (\mathbb{E}_2 \times \{0\} \times \mathbb{E}_2) \oplus (\{0\} \times \mathbb{E}_3 \times \{0\}) \oplus (\{0\} \times \{0\} \times \mathbb{E}_4).$$

Let us fix roots of $f_1, \ldots, f_4$ as $\alpha_1 = 1, \alpha_2, \alpha_3, \alpha_4$. If $C \subset R'$ is a GQC code generated by $\langle \vec{g}_1(x), \ldots, \vec{g}_r(x)\rangle$, where

$$\vec{g}_b(x) = \left(g^{b,0}(x), g^{b,1}(x), g^{b,2}(x)\right),\ 1 \le b \le r,$$

then C has the following constituents:

$$\begin{aligned} C_1 &= \mathrm{Span}_{\mathbb{F}_2}\left\{\left(g^{b,0}(1), g^{b,1}(1), g^{b,2}(1)\right)\ :\ 1 \le b \le r\right\}, \\ C_2 &= \mathrm{Span}_{\mathbb{F}_4}\left\{\left(g^{b,0}(\alpha_2), 0, g^{b,2}(\alpha_2)\right)\ :\ 1 \le b \le r\right\}, \\ C_3 &= \mathrm{Span}_{\mathbb{F}_{16}}\left\{\left(0, g^{b,1}(\alpha_3), 0\right)\ :\ 1 \le b \le r\right\}, \\ C_4 &= \mathrm{Span}_{\mathbb{F}_{64}}\left\{\left(0, 0, g^{b,2}(\alpha_4)\right)\ :\ 1 \le b \le r\right\}. \end{aligned}$$

3. Concatenated Structure and Trace Representation

Our goal is to obtain, as in the QC codes, a concatenated description and its relation to constituent decomposition for GQC codes. For this purpose, some further notation needs to be introduced. We will also continue using the notation of the previous section.

For i, j such that $f_i(x) \mid x^{m_j} - 1$, let $\theta_{i,j}$ denote the primitive idempotent generator of the minimal cyclic code of length m_j in R_j, whose check polynomial is $f_i(x)$. Let 0_j denote the zero codeword of length m_j (or the zero polynomial in R_j). Then define the following polynomials for each i and j:

$$I_{i,j} := \begin{cases} \theta_{i,j}(x), & \text{if } f_i(x) \mid x^{m_j} - 1, \\ 0_j & \text{otherwise.} \end{cases} \tag{3.1}$$

Now we can define the following analogues of the maps in (2.10) for each block of length m_j and each $1 \leq i \leq s$:

$$\begin{array}{rccc} \varphi_{i,j}: & \langle I_{i,j}\rangle & \longrightarrow & \mathbb{E}_{i,j} \\ & a(x) & \longmapsto & a_{i,j} \end{array} \qquad \begin{array}{rccc} \psi_{i,j}: & \mathbb{E}_{i,j} & \longrightarrow & \langle I_{i,j}\rangle \\ & \delta & \longmapsto & \sum_{k_j=0}^{m_j-1} a_{k_j} x^{k_j} \end{array}, \tag{3.2}$$

where

$$a_{k_j} = \frac{1}{m_j}\mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}(\delta\alpha_i^{-k_j}).$$

Note that $\langle I_{i,j}\rangle = \langle 0_j\rangle$, $\mathbb{E}_{i,j} = \{0\}$ and $a_{i,j} = 0$ are equivalent and all amount to $f_i(x) \nmid x^{m_j} - 1$. Then, $\varphi_{i,j}$ and $\psi_{i,j}$ are well-defined $\mathbb{E}_i$-linear isomorphisms and they are inverses to each other for all i and j. Moreover, when $\mathbb{E}_{i,j} = \mathbb{E}_i$, hence $I_{i,j} = \theta_{i,j}$, $\psi_{i,j}$ and $\phi_{i,j}$ are known to be field isomorphisms. In particular, if $m_0 = \cdots = m_{\ell-1}$, then we obtain the isomorphisms in (2.10) for the QC case.

Note that $R' = R_0 \times \cdots \times R_{\ell-1}$ and $\mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}$ (for each $1 \leq i \leq s$) are rings with coordinate-wise addition and multiplication. The multiplicative identity of R' is clearly $1_{R'} := (1, \ldots, 1)$. For all $1 \leq i \leq s$, $0 \leq j \leq \ell - 1$, set

$$1_{i,j} := \begin{cases} 1_{\mathbb{E}_i}, & \text{if } \mathbb{E}_{i,j} = \mathbb{E}_i, \\ 0, & \text{if } \mathbb{E}_{i,j} = \{0\}. \end{cases} \tag{3.3}$$

Then, $1_i := (1_{i,0}, \ldots, 1_{i,\ell-1})$ is the multiplicative identity of $\mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}$ for each $1 \leq i \leq s$. Note also that $\psi_{i,j}(1_{i,j}) = I_{i,j}$ for all i, j.

For $i = 1, \ldots, s$, we now define two other maps (cf. (2.13) and (3.2)).

$$\begin{array}{rccc} \Phi_i: & R_0 \times \cdots \times R_{\ell-1} & \longrightarrow & \mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1} \\ & \left(a^0(x), \ldots, a^{\ell-1}(x)\right) & \longmapsto & \left(a_{i,0}^0, \ldots, a_{i,\ell-1}^{\ell-1}\right) \end{array} \tag{3.4}$$

$$\begin{array}{rccc} \Psi_i: & \mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1} & \longrightarrow & R_0 \times \cdots \times R_{\ell-1} \\ & (\delta_0, \ldots, \delta_{\ell-1}) & \longmapsto & (\psi_{i,0}(\delta_0), \ldots, \psi_{i,\ell-1}(\delta_{\ell-1})) \end{array} \tag{3.5}$$

Note that for each i, Φ_i and Ψ_i are $\mathbb{F}_q$-linear maps and they are also ring homomorphisms. Moreover, when Φ_i is restricted to $\langle I_{i,0}\rangle \times \cdots \times \langle I_{i,\ell-1}\rangle$, they are inverse to each other (cf. (3.2)). For $i = 1, \ldots, s$, we set $I_i := (I_{i,0}, \ldots, I_{i,\ell-1}) \in R'$. We have $\Psi_i(1_i) = I_i$ and the ideal generated by I_i in R' is nothing but $\langle I_{i,0}\rangle \times \cdots \times \langle I_{i,\ell-1}\rangle$. The next result follows immediately from the definition of I_i's and the analogous results on primitive idempotents of cyclic codes (cf. [12, Theorem 6.4.4]). Recall that the multiplication and addition in R' are coordinate-wise.

Lemma 3.1. *The following identities hold in R':*

i. $I_i \cdot I_i = I_i$, *for all* $i = 1, \ldots, s$.
ii. $I_u \cdot I_v = 0$, *if* $u \neq v$.
iii. $I_1 + \cdots + I_s = 1_{R'}$.

The next result will be used in proving the concatenated structure of GQC codes.

Theorem 3.2. *With the notation above, we have*

$$R' = \bigoplus_{i=1}^{s} \langle I_i \rangle.$$

Proof. We first show that the sum is direct in R'. Let $(g_0(x), \ldots, g_{\ell-1}(x))$ be an element of $\langle I_u \rangle \cap \langle I_v \rangle$ for some $u \neq v \in \{1, \ldots, s\}$. Since $\langle I_u \rangle = \langle I_{u,0} \rangle \times \cdots \times \langle I_{u,\ell-1} \rangle$ and $\langle I_v \rangle = \langle I_{v,0} \rangle \times \cdots \times \langle I_{v,\ell-1} \rangle$, we have $g_j(x) \in \langle I_{u,j} \rangle \cap \langle I_{v,j} \rangle$ for all $0 \leq j \leq \ell - 1$. If one of the irreducible polynomials $f_u(x)$ or $f_v(x)$ does not divide $x^{m_j} - 1$, say f_u, then $\langle I_{u,j} \rangle = \langle 0_j \rangle$. Therefore $g_j(x) = 0$ in this case. If both $f_u(x)$, $f_v(x)$ divide $x^{m_j} - 1$, then $\langle I_{u,j} \rangle$ (respectively, $\langle I_{v,j} \rangle$) is the minimal cyclic code generated by $(x^{m_j} - 1)/f_u(x)$ (respectively, $(x^{m_j} - 1)/f_v(x)$). Since these minimal cyclic codes intersect trivially, we have $g_j(x) = 0$ in this case too. Hence, $(g_0(x), \ldots, g_{\ell-1}(x)) = (0, \ldots, 0)$ and the sum is direct.

Clearly $\langle I_i \rangle \subset R'$ for each i. Recall that when Φ_i is restricted to $\langle I_i \rangle$, Φ_i and Ψ_i are inverse $\mathbb{F}_q$-linear maps. Hence, $\Psi_i \left(\mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1} \right) = \langle I_i \rangle$ and

$$\dim_{\mathbb{F}_q} \langle I_i \rangle = \dim_{\mathbb{F}_q} \left(\mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1} \right) = \sum_{\substack{0 \leq j \leq \ell - 1 \\ f_i(x) \mid (x^{m_j} - 1)}} \deg f_i,$$

for all $1 \leq i \leq s$. Then,

$$\begin{aligned} \dim_{\mathbb{F}_q} \bigoplus_{i=1}^{s} \langle I_i \rangle &= \sum_{i=1}^{s} \sum_{\substack{0 \leq j \leq \ell - 1 \\ f_i(x) \mid (x^{m_j} - 1)}} \deg f_i \\ &= \sum_{j=0}^{\ell-1} \sum_{\substack{1 \leq i \leq s \\ f_i(x) \mid (x^{m_j} - 1)}} \deg f_i. \end{aligned}$$

For each $0 \leq j \leq \ell - 1$, we have

$$\sum_{\substack{1 \leq i \leq s \\ f_i(x) \mid (x^{m_j} - 1)}} \deg f_i = m_j,$$

since $\gcd(q, m_j) = 1$ and hence $x^{m_j} - 1$ is separable. Therefore

$$\dim_{\mathbb{F}_q} \bigoplus_{i=1}^{s} \langle I_i \rangle = \sum_{j=0}^{\ell-1} m_j.$$

Note that $(m_0 + m_1 + \cdots + m_{\ell-1})$ is also the $\mathbb{F}_q$-dimension of R' and therefore the result follows. □

Remark 3.3. For any $i \in \{1, \ldots, s\}$ and an $\mathbb{E}_i$-linear code $\mathfrak{C}_i \subset \mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}$ of length ℓ, concatenation with $\langle I_i \rangle = \langle I_{i,0} \rangle \times \cdots \times \langle I_{i,\ell-1} \rangle \subset R'$ is carried out by the map Ψ_i in (3.5). Namely,

$$\langle I_i \rangle \square \mathfrak{C}_i := \left\{ (\psi_{i,0}(c_0), \ldots, \psi_{i,\ell-1}(c_{\ell-1})) : (c_0, \ldots, c_{\ell-1}) \in \mathfrak{C}_i \right\}.$$

After this preparation, we can now generalize Theorem 2.1 for a GQC code $C \subset R'$ of length $m_0 + \cdots + m_{\ell-1}$ over $\mathbb{F}_q$.

Theorem 3.4. *(i) Let $C \subset R'$ be a GQC code and $\tilde{C}_i := C \cdot I_i \subset R'$ for each $1 \leq i \leq s$. Then,*

$$C = \bigoplus_{i=1}^{s} \tilde{C}_i.$$

Moreover, for the $\mathbb{E}_i$-linear code $\mathfrak{C}_i := \Phi_i(\tilde{C}_i) \subset \mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}$ of length ℓ, we have $\tilde{C}_i = \langle I_i \rangle \square \mathfrak{C}_i$ (for all i), so that

$$C = \bigoplus_{i=1}^{s} \langle I_i \rangle \square \mathfrak{C}_i.$$

(ii) Conversely, let $\mathfrak{C}_i \subseteq (\mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1})$ be an $\mathbb{E}_i$-linear code of length ℓ for each $i \in \{1, \ldots, s\}$. Then, $C = \bigoplus_{i=1}^{s} \langle I_i \rangle \square \mathfrak{C}_i$ is a q-ary GQC code of length $m_0 + \cdots + m_{\ell-1}$.

Proof. (i) By Lemma 3.1, we have

$$C = C \cdot 1_{R'} = C \cdot \sum_{i=1}^{s} I_i = \sum_{i=1}^{s} \tilde{C}_i.$$

Since $\tilde{C}_i \subset \langle I_i \rangle$ for each i and $\langle I_i \rangle$'s are pairwise intersecting trivially (Theorem 3.2), we conclude that $C = \oplus_i \tilde{C}_i$.

We have

$$\begin{aligned} \tilde{C}_i &= \left\{ \left(c^0(x), \ldots, c^{\ell-1}(x) \right) \cdot (I_{i,0}(x), \ldots, I_{i,\ell-1}(x)) : \ \left(c^0(x), \ldots, c^{\ell-1}(x) \right) \in C \right\} \\ &= \left\{ \left(c^0(x) I_{i,0}(x), \ldots, c^{\ell-1}(x) I_{i,\ell-1}(x) \right) : \ \left(c^0(x), \ldots, c^{\ell-1}(x) \right) \in C \right\} \subset \langle I_i \rangle. \end{aligned}$$

Since Φ_i restricted to $\langle I_i \rangle$ is an isomorphism ((3.4) and (3.5)), the last expression is equal to

$$\left\{ \left(\psi_{i,0}\left(d_{i,0}^0\right), \ldots, \psi_{i,\ell-1}\left(d_{i,\ell-1}^{\ell-1}\right) \right) : \ \left(d^0(x), \ldots, d^{\ell-1}(x) \right) \in \Phi_i(\tilde{C}_i) \right\},$$

which is nothing but $\langle I_i \rangle \square \Phi_i(\tilde{C}_i)$ (cf. (Remark 3.3).

(ii) The concatenation has the form

$$\langle I_i \rangle \square \mathfrak{C}_i = \{ (\psi_{i,0}(c_0), \ldots, \psi_{i,\ell-1}(c_{\ell-1})) : \ (c_0, \ldots, c_{\ell-1}) \in \mathfrak{C}_i \}.$$

Note that each $\psi_{i,j}(c_j)$ is an element of $\langle I_{i,j} \rangle$. By $\mathbb{F}_q$-linearity of $\mathfrak{C}_i$ and $\psi_{i,j}$'s, it is clear that the concatenation is an additive subgroup of R' which is closed under scalar multiplication by elements of $\mathbb{F}_q$. Note that for a nonzero coordinate c_j of a codeword in $\mathfrak{C}_i$, $\psi_{i,j}$ identifies $\alpha_i c_j \in \mathbb{E}_{i,j} = \mathbb{E}_i$ with $x\psi_{i,j}(c_j) \in I_{i,j}$, since it is a field isomorphism between $\mathbb{E}_i$ and $\langle I_{i,j} \rangle = \langle \theta_{i,j} \rangle$ in this case (see (3.2) and the discussion following it). Therefore we have

$$\begin{aligned} x \cdot (\psi_{i,0}(c_0), \ldots, \psi_{i,\ell-1}(c_{\ell-1})) &= (\psi_{i,0}(\alpha_i c_0), \ldots, \psi_{i,\ell-1}(\alpha_i c_{\ell-1})) \\ &= \alpha_i \left(\psi_{i,0}(c_0), \ldots, \psi_{i,\ell-1}(c_{\ell-1}) \right) \end{aligned}$$

Since $\mathfrak{C}_i$ is an $\mathbb{E}_i$-linear code, $\alpha_i(c_0,\ldots,c_{\ell-1})$ is also a codeword of $\mathfrak{C}_i$. Hence,

$$x\cdot(\psi_{i,0}(c_0),\ldots,\psi_{i,\ell-1}(c_{\ell-1}))=x\cdot\Psi_i\left(c_0,\ldots,c_{\ell-1}\right)$$

is also a codeword of $\langle I_i\rangle\square\mathfrak{C}_i$ and this concatenation is an $\mathbb{F}_q[x]$-submodule of R'. If we take the direct sum of several such concatenations, the result is again an submodule of R', i.e. a GQC code. □

Remark 3.5. Note from the proof of Theorem 3.4 (i) that the outer codes of the GQC code C are of the form (for each $1\le i\le s$):

$$\begin{aligned}\mathfrak{C}_i &= \left\{\left(\varphi_{i,0}\left(c^0(x)I_{i,0}(x)\right),\ldots,\varphi_{i,\ell-1}\left(c^{\ell-1}(x)I_{i,\ell-1}(x)\right)\right):\ \left(c^0(x),\ldots,c^{\ell-1}(x)\right)\in C\right\}\\ &= \left\{\left(\varphi_{i,0}\left(c^0(x)\right),\ldots,\varphi_{i,\ell-1}\left(c^{\ell-1}(x)\right)\right):\ \left(c^0(x),\ldots,c^{\ell-1}(x)\right)\in C\right\},\end{aligned}$$

where the last equality follows from $\varphi_{i,j}(I_{i,j}(x))=1_{i,j}$. The outer code $\mathfrak{C}_i$ is nothing but the constituent C_i of C (Proposition 2.5). Hence, the analogous result for QC codes extends to GQC codes.

As in Theorem 2.2, we can obtain a trace representation for the codewords of a given GQC code, which is straightforward by using the isomorphism (concatenation map) in (3.5).

Theorem 3.6. *Consider the q-ary GQC code C of length $m_0+\cdots+m_{\ell-1}$ with the constituents $C=C_1\oplus\cdots\oplus C_s$, where $C_i\subset\mathbb{E}_i^{\ell}$ is linear over $\mathbb{E}_i$ of length ℓ for each $1\le i\le s$. Assume that each m_j is relatively prime to q and let $\alpha_1,\ldots,\alpha_s$ be fixed roots of the polynomials $f_1,\ldots,f_s$, describing the fields $\mathbb{E}_1,\ldots,\mathbb{E}_s$. Then an arbitrary codeword $c\in C$ has the form*

$$c=\left(c_0(\lambda_1,\ldots,\lambda_s)\mid c_1(\lambda_1,\ldots,\lambda_s)\mid\cdots\mid c_{\ell-1}(\lambda_1,\ldots,\lambda_s)\right),$$

where $\lambda_i=(\lambda_{i,0},\ldots,\lambda_{i,\ell-1})$ is a codeword in C_i, for each $i=1,\ldots,s$, and for $j\in\{0,\ldots,\ell-1\}$, the j^{th} column has length m_j and it is of the form

$$c_j(\lambda_1,\ldots,\lambda_s)=\frac{1}{m_j}\left(\sum_{i=1}^{s}\mathrm{Tr}_{\mathbb{E}_i/\mathbb{F}_q}\left(\lambda_{i,j}\alpha_i^{-k_j}\right)\right)_{0\le k_j\le m_j-1}.$$

Remark 3.7. Note that for $m_0=\cdots=m_{\ell-1}$, this coincides with the trace representation of a length $m\ell$ QC code (cf. Theorem 2.2). However, the trace representation in Theorem 2.2 describes codewords by their rows whereas Theorem 3.6 provides a column-wise description of codewords in a GQC code.

Example 3.8. Let $m_0=3$, $m_1=5$ and $q=2$. We will consider a binary GQC code C of length $3+5=8$. We have

$$R'=R_0\times R_1=\mathbb{F}_2[x]/\langle x^3-1\rangle\times\mathbb{F}_2[x]/\langle x^5-1\rangle$$

and

$$x^3-1=(x+1)(x^2+x+1)\qquad x^5-1=(x+1)(x^4+x^3+x^2+x+1). \tag{3.6}$$

Therefore, $s = 3$ and R' decomposes as follows:

$$\begin{aligned} R' &\cong (\mathbb{F}_2[x]/\langle x+1\rangle \times \mathbb{F}_2[x]/\langle x+1\rangle) \\ &\oplus \left(\mathbb{F}_2[x]/\langle x^2+x+1\rangle \times \{0\}\right) \\ &\oplus \left(\{0\} \times \mathbb{F}_2[x]/\langle x^4+x^3+x^2+x+1\rangle\right). \end{aligned}$$

Let $1, \xi_1, \xi_2$ be the fixed roots of the irreducible factors in (3.6), respectively. Let $C_1 \subseteq \mathbb{F}_2^2$, $C_2 \subseteq \mathbb{F}_4^2$, $C_3 \subseteq \mathbb{F}_{16}^2$ be the constituents of C. Note that the second (first) coordinate of every codeword in C_2 (in C_3) must be zero due to the decomposition R' above. We write $\mathrm{Tr}_{\mathbb{F}_{16}/\mathbb{F}_2}(\alpha) = \mathrm{Tr}(\alpha)$ as short. Then, by Theorem 3.6, the codewords of C are of the form (cf. Theorem 6.7 and 6.14 in [9])

$$(z_1+2a-b|z_1-a+2b|z_1-a-b|z_2+\mathrm{Tr}(y)|z_2+\mathrm{Tr}(y\xi_2^{-1})|z_2+\mathrm{Tr}(y\xi_2^{-2})|z_2+\mathrm{Tr}(y\xi_2^{-3})|z_2+\mathrm{Tr}(y\xi_2^{-4})),$$

where $(z_1, z_2) \in C_1$, $a + \xi_1 b \in C_2$ $(a, b \in \mathbb{F}_2)$ and $y \in C_3$.

Moreover, we can simplify this expression further, by using the fact $2a = 2b = 0$ in $\mathbb{F}_2$ and by setting $y = c + \xi_2 d + \xi_2^2 e + \xi_2^3 f$, for some $c, d, e, f \in \mathbb{F}_2$, as follows:

$$(z_1+b|z_1+a|z_1+a+b|z_2+d+e+f|z_2+c+e+f|z_2+c+d+f|z_2+c+d+e|z_2+c+d+e+f),$$

where $(z_1, z_2) \in C_1$, $a + \xi_1 b \in C_2$ and $c + \xi_2 d + \xi_2^2 e + \xi_2^3 f \in C_3$.

4. Multilevel Concatenated View of GQC Codes and a Minimum Distance Bound

A direct sum of concatenated codes can be seen as a multilevel (generalized) concatenation. Linear generalized concatenated codes were introduced by Blokh and Zyablov ([1]), which enabled Jensen to obtain a minimum distance bound for QC codes ([8, Theorem 4]; see also [6, Theorem 3.3]). We refer to Section 2 in Dumer's chapter [4] for more information on multilevel concatenation.

Note however that for a QC code, or multilevel concatenations as described in [4, Section 2], symbols in the codewords of outer codes are mapped to inner codes of the same length (length m in Theorem 2.1), whereas this is not the case for the concatenated structure of GQC codes ($m_0, \ldots, m_{\ell-1}$ in Theorem 3.4). Our goal is to adapt the multilevel approach to GQC codes and obtain a minimum distance bound as Jensen did for QC codes. We will first define multilevel concatenation in a setting applicable to GQC codes. We continue with the notation introduced so far.

Let C be a q-ary GQC code of length $m_0 + \cdots + m_{\ell-1}$ with the outer codes (or constituents) $C_1, \ldots, C_s$. Recall that $C_i \subset \mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}$ is an $\mathbb{E}_i$-linear code of length ℓ for each i. Consider the following set:

$$B := \left\{ \begin{pmatrix} c_{1,0} & \ldots & c_{1,\ell-1} \\ \vdots & \vdots & \vdots \\ c_{s,0} & \ldots & c_{s,\ell-1} \end{pmatrix} : (c_{i,0}, \ldots, c_{i,\ell-1}) \in C_i \text{ for } 1 \le i \le s \right\}.$$

We can view B as a length ℓ code over a mixed alphabet $(\mathbb{E}_{1,0}\times\cdots\times\mathbb{E}_{s,0})\times\cdots\times(\mathbb{E}_{1,\ell-1}\times\cdots\times\mathbb{E}_{s,\ell-1})$, which is $\mathbb{F}_q$-linear with $|B| = \prod_{i=1}^{s}|C_i|$. We note that B will be the outer code in the multilevel concatenation scheme.

For each $j = 0,\ldots,\ell-1$, we use the maps $\psi_{i,j}$'s in (3.2) to define the following $\mathbb{F}_q$-linear isomorphisms:

$$\begin{array}{rccl} \psi_j & : & \mathbb{E}_{1,j}\times\cdots\times\mathbb{E}_{s,j} & \to & \langle I_{1,j}\rangle\oplus\cdots\oplus\langle I_{s,j}\rangle\subset R_j \\ & & (a_{1,j},\ldots,a_{s,j}) & \mapsto & \psi_{1,j}(a_{1,j})+\cdots+\psi_{s,j}(a_{s,j}) \end{array} \tag{4.1}$$

The multilevel concatenated code is defined as

(4.2)

$$\psi(B) := \left\{ \left(\psi_0\left(c_{1,0},\ldots,c_{s,0}\right),\ldots,\psi_{\ell-1}\left(c_{1,\ell-1},\ldots,c_{s,\ell-1}\right)\right) : \begin{pmatrix} c_{1,0} & \cdots & c_{1,\ell-1} \\ \vdots & \vdots & \vdots \\ c_{s,0} & \cdots & c_{s,\ell-1} \end{pmatrix} \in B \right\}.$$

Observe that the maps $\psi_0,\ldots,\psi_{\ell-1}$ concatenate each symbol in the codewords of B, which comes from mixed cross-product alphabets as described above, to length $m_0,\ldots,m_{\ell-1}$ words respectively. It is also clear that $\dim_{\mathbb{F}_q}\psi(B) = \sum_{i=1}^{s}\dim_{\mathbb{F}_q}C_i = \dim_{\mathbb{F}_q}C$.

Proposition 4.1.

$$\psi(B) = \bigoplus_{i=1}^{s}\langle I_i\rangle\square C_i.$$

Proof. A codeword in $\psi(B)$ is of the form

$$\Big(\big(\psi_{1,0}(c_{1,0})+\cdots+\psi_{s,0}(c_{s,0})\big),\ldots,\big(\psi_{1,\ell-1}(c_{1,\ell-1})+\cdots+\psi_{s,\ell-1}(c_{s,\ell-1})\big)\Big),$$

which can be rewritten as

$$\big(\psi_{1,0}(c_{1,0}),\ldots,\psi_{1,\ell-1}(c_{1,\ell-1})\big)+\cdots+\big(\psi_{s,0}(c_{s,0}),\ldots,\psi_{s,\ell-1}(c_{s,\ell-1})\big).$$

This expression also belongs to $\bigoplus_{i=1}^{s}\langle I_i\rangle\square C_i$ (cf. Remark 3.3), hence $\psi(B)\subseteq\bigoplus_{i=1}^{s}\langle I_i\rangle\square C_i$. The result follows since both codes have the same $\mathbb{F}_q$-dimension. □

So, we obtained another way of presenting the GQC code C. The advantage of this is that it makes it possible to prove the minimum distance bound on GQC codes

Theorem 4.2. *Let C be a GQC code with nonzero constituents $C_{i_1},\ldots,C_{i_g}$, where $\{i_1,\ldots,i_g\}\subseteq\{1,\ldots,s\}$. Let d_u denote the minimum distance of C_{i_u}, for each $1\le u\le g$ and assume that $d_1\le d_2\le\cdots\le d_g$. If we set*

$$D_u := \min_{\substack{J\subset\{0,1,\ldots,\ell-1\}\\ |J|=d_u}}\left\{\sum_{t\in J} d\Big(\langle I_{i_1,t}\rangle\oplus\langle I_{i_2,t}\rangle\oplus\cdots\oplus\langle I_{i_u,t}\rangle\Big)\right\}$$

for $1 \le u \le g$, *then*

$$d(C) \ge \min\{D_1, D_2, \ldots, D_g\}.$$

Proof. Codewords in B have g rows coming from the constituents of C. For any $u \in \{1, \ldots, g\}$, consider a codeword $b \in B$ whose first u rows are nonzero codewords from the corresponding constituents and the remaining rows are the zero codewords. Let us denote the columns (symbols in the mixed alphabets) of b by $(b_0, \ldots, b_{\ell-1})$. By assumption on the ordering of minimum distances of the constituents, b has at least d_u nonzero columns. By linearity of Ψ, a zero (nonzero) column in b is mapped to the zero (nonzero) codeword in the corresponding image. Again due to linearity, zero entries in nonzero columns (e.g. the last $g-u$ entry in each nonzero column) are also mapped to zeros in the image. Therefore, if $0 \le t_1, \ldots, t_{d_u} \le \ell - 1$ denotes nonzero columns of b, then $\Psi(b) = \big(\psi_0(b_0), \ldots, \psi_{\ell-1}(b_{\ell-1})\big)$ lies in

$$\Big(\langle I_{i_1,t_1}\rangle \oplus \cdots \oplus \langle I_{i_u,t_1}\rangle\Big) \times \cdots \times \Big(\langle I_{i_1,t_{d_u}}\rangle \oplus \cdots \oplus \langle I_{i_u,t_{d_u}}\rangle\Big) \text{ (cf. (4.1) and (4.2))}.$$

Hence the weight of $\Psi(b)$ is at least

$$\sum_{k=1}^{d_u} d\Big(\langle I_{i_1,t_k}\rangle \oplus \cdots \oplus \langle I_{i_u,t_k}\rangle\Big).$$

If we consider all possible choices of d_u nonzero columns for $b \in B$ as above, codewords obtained this way in the image of Ψ (i.e. C) have weights greater than or equal to D_u. Applying the same argument with each $u = 1, \ldots, g$, we see that codewords of C arising this way from B have weights at least $D := \min\{D_1, D_2, \ldots, D_u\}$.

Now suppose $c = \Psi(b)$ is a codeword in C, where $b \in B$ has different configuration of nonzero rows, $\mu_1 < \mu_2 < \cdots < \mu_e \in \{1, \ldots, g\}$. Arguing as above, for some subset J of $\{0, 1, \ldots, \ell - 1\}$ of cardinality $|J| = d_{\mu_e}$, the weight $w(c)$ of such c is at least

$$\sum_{t \in J} d\Big(\langle I_{i_{\mu_1},t}\rangle \oplus \langle I_{i_{\mu_2},t}\rangle \oplus \cdots \oplus \langle I_{i_{\mu_e},t}\rangle\Big).$$

For each $t \in J$ we have

$$\Big(\langle I_{i_{\mu_1},t}\rangle \oplus \langle I_{i_{\mu_2},t}\rangle \oplus \cdots \oplus \langle I_{i_{\mu_e},t}\rangle\Big) \subset \Big(\langle I_{i_1,t}\rangle \oplus \langle I_{i_2,t}\rangle \oplus \cdots \oplus \langle I_{i_{\mu_e},t}\rangle\Big).$$

Hence $w(c) \ge D_{\mu_e} \ge D$. Therefore D is a lower bound for the weights of all codewords in C. □

Remark 4.3. Suppose C is a QC code with nonzero constituents $C_{i_1}, \ldots, C_{i_g}$, whose minimum distances are ordered as in Theorem 4.2. If C is of length $m\ell$ and index ℓ, then $m_0 = \cdots = m_{\ell-1} = m$ and $\langle I_{i_u,t}\rangle = \langle \theta_{i_u}\rangle$ for any $t \in \{0, \ldots, \ell - 1\}$ and any $u \in \{1, \ldots, g\}$. (cf. Section 2). Then for any $J \subset \{0, 1, \ldots, \ell - 1\}$ with $|J| = d(C_{i_u})$, we have

$$\begin{aligned}\sum_{t \in J} d\Big(\langle I_{i_1,t}\rangle \oplus \langle I_{i_2,t}\rangle \oplus \cdots \oplus \langle I_{i_u,t}\rangle\Big) &= \sum_{t \in J} d\Big(\langle \theta_{i_1}\rangle \oplus \langle \theta_{i_2}\rangle \oplus \cdots \oplus \langle \theta_{i_u}\rangle\Big) \\ &= d(C_{i_u}) d\Big(\langle \theta_{i_1}\rangle \oplus \langle \theta_{i_2}\rangle \oplus \cdots \oplus \langle \theta_{i_u}\rangle\Big).\end{aligned}$$

Hence the bound in Theorem 4.2 takes the form

$$d(C) \geq \min_{1\leq u\leq g} \left\{ d(C_{i_u}) d\Big(\langle \theta_{i_1} \rangle \oplus \langle \theta_{i_2} \rangle \oplus \cdots \oplus \langle \theta_{i_u} \rangle \Big) \right\},$$

for a QC code C, which is exactly Jensen's bound (see [8, Theorem 4], [6, Theorem 3.3]).

Remark 4.4. Esmaeili and Yari also found a minimum distance bound for GQC codes but their bound only applies to one-generator GQC codes ([5, Theorem 4]).

5. Self-Dual and LCD Cases

Let us write the factorization of the polynomials $x^{m_j} - 1$ (for all $0 \leq j \leq \ell - 1$) into irreducible polynomials in $\mathbb{F}_q[x]$ as follows, which is needed for dual code analysis (see also [9]):

$$x^{m_j} - 1 = g_1(x)^{v_{1,j}} \cdots g_r(x)^{v_{r,j}} h_1(x)^{w_{1,j}} h_1^*(x)^{w_{1,j}} \cdots h_p(x)^{w_{p,j}} h_p^*(x)^{w_{p,j}}, \tag{5.1}$$

Here, g_i's are self-reciprocal, h_t^* denotes the reciprocal of h_t and $v_{i,j}, w_{t,j} \in \{0, 1\}$, for all i, j, t.

Let $\mathbb{G}_i = \mathbb{F}_q[x]/\langle g_i(x) \rangle$, $\mathbb{H}'_t = \mathbb{F}_q[x]/\langle h_t(x) \rangle$ and $\mathbb{H}''_t = \mathbb{F}_q[x]/\langle h_t^*(x) \rangle$ for each i and t. Let us define (cf.(2.12))

$$\mathbb{G}_{i,j} = \begin{cases} \mathbb{G}_i, \text{ if } v_{i,j} = 1, \\ \{0\}, \text{ if } v_{i,j} = 0. \end{cases} \quad \mathbb{H}'_{t,j} = \begin{cases} \mathbb{H}'_t, \text{ if } w_{t,j} = 1, \\ \{0\}, \text{ if } w_{t,j} = 0. \end{cases} \quad \mathbb{H}''_{t,j} = \begin{cases} \mathbb{H}''_t, \text{ if } w_{t,j} = 1, \\ \{0\}, \text{ if } w_{t,j} = 0. \end{cases} \tag{5.2}$$

By Chinese Remainder Theorem, decomposition of R_j in (2.14) now becomes:

$$R_j \cong \left(\bigoplus_{i=1}^{r} \mathbb{G}_{i,j} \right) \oplus \left(\bigoplus_{t=1}^{p} \Big(\mathbb{H}'_{t,j} \oplus \mathbb{H}''_{t,j} \Big) \right), \text{ for } 0 \leq j \leq \ell - 1. \tag{5.3}$$

Hence, we get the following isomorphism for $R' = R_0 \times \cdots \times R_{\ell-1}$:

$$R' \cong \left(\bigoplus_{i=1}^{r} (\mathbb{G}_{i,0} \times \cdots \times \mathbb{G}_{i,\ell-1}) \right) \oplus \left(\bigoplus_{t=1}^{p} (\mathbb{H}'_{t,0} \times \cdots \times \mathbb{H}'_{t,\ell-1}) \right) \oplus \left(\bigoplus_{t=1}^{p} (\mathbb{H}''_{t,0} \times \cdots \times \mathbb{H}''_{t,\ell-1}) \right), \tag{5.4}$$

which implies

$$R' \subseteq \left(\bigoplus_{i=1}^{r} \mathbb{G}_i^{\ell} \right) \oplus \left(\bigoplus_{t=1}^{p} (\mathbb{H}'_t)^{\ell} \right) \oplus \left(\bigoplus_{t=1}^{p} (\mathbb{H}''_t)^{\ell} \right),$$

since for each j, $\mathbb{G}_{i,j} \subset \mathbb{G}_i$, $\mathbb{H}'_{t,j} \subset \mathbb{H}'_t$ and $\mathbb{H}''_{t,j} \subset \mathbb{H}''_t$ by (5.2).

Hence, a GQC code $C \subset R' = R_0 \times \cdots \times R_{\ell-1}$ viewed as an $\mathbb{F}_q[x]$-submodule of R' now decomposes as (cf. (2.16))

$$C = \left(\bigoplus_{i=1}^{r} C_i \right) \oplus \left(\bigoplus_{t=1}^{p} \Big(C'_t \oplus C''_t \Big) \right). \tag{5.5}$$

where C_i's are the $\mathbb{G}_i$-linear constituents of C of length ℓ, for all $i = 1, \ldots, r$, C'_t's and C''_t's are the $\mathbb{H}'_t$-linear and $\mathbb{H}''_t$-linear constituents of C of length ℓ, respectively, for all $t = 1, \ldots, p$. By fixing roots corresponding to irreducible factors g_i, h_j, h_j^* and via Chinese Remainder Theorem (cf. Section 2), one can write explicitly the constituents as in (2.17) in this setting as well.

It is clear that the cardinality of each $\mathbb{G}_i$, say q_i, is an even power of q. Each $\mathbb{G}_i^\ell$ is equipped with the Hermitian inner product, which is defined for $\vec{c} = (c_{i,0}, \ldots, c_{i,\ell-1}), \vec{d} = (d_{i,0}, \ldots, d_{i,\ell-1}) \in \mathbb{G}_i^\ell$ as

$$\langle \vec{c}, \vec{d} \rangle := \sum_{j=0}^{\ell-1} c_{i,j} d_{i,j}^{\sqrt{q_i}}. \tag{5.6}$$

For $1 \leq t \leq p$, $\mathbb{H}_t'^\ell$ and $\mathbb{H}_t''^\ell$ are equipped with the usual Euclidean inner product.

The dual of a GQC code is also GQC. The proof of the following result will be omitted, since it follows the same lines of the analogous result given for QC codes in [10].

Proposition 5.1. *Let C be a GQC code with CRT decomposition as in (5.5). Then its dual code $C^\perp$ is of the form*

$$C^\perp = \left(\bigoplus_{i=1}^{r} C_i^{\perp_h} \right) \oplus \left(\bigoplus_{t=1}^{p} \left(C_t''^{\perp_e} \oplus C_t'^{\perp_e} \right) \right), \tag{5.7}$$

where $\perp_h$ denotes the Hermitian dual on G_i^ℓ (for all $1 \leq i \leq s$) and $\perp_e$ denotes the Euclidian dual on $\mathbb{H}_i'^\ell = \mathbb{H}_i''^\ell$ (for all $1 \leq i \leq t$).

Recall that a linear code C is said to be self dual, if $C = C^\perp$ and C is called linear complementary dual (LCD) if $C \cap C^\perp = \{0\}$. Let us now characterize self-dual and LCD GQC codes via their constituents (see [7, 14]).

Theorem 5.2. *Let C be a q-ary GQC code of length $m_0 + \cdots + m_{\ell-1}$, whose CRT decomposition is as in (5.5).*

1. *C is self-dual if and only if C_i is Hermitian self-dual over $\mathbb{G}_i$, for all $1 \leq i \leq r$, and $C_t'' = C_t'^{\perp_e}$ over $\mathbb{H}_t' = \mathbb{H}_t''$, for all $1 \leq t \leq p$.*
2. *C is LCD if and only if C_i is Hermitian LCD over $\mathbb{G}_i$, for all $1 \leq i \leq r$, and $C_t' \cap C_t''^{\perp_e} = \{0\}$, $C_t'' \cap C_t'^{\perp_e} = \{0\}$ over $\mathbb{H}_t' = \mathbb{H}_t''$, for all $1 \leq t \leq p$.*

Proof. Immediate from the CRT decompositions of C in (5.5) and of its dual $C^\perp$ in (5.7). □

The following special cases are easy to derive from Theorem 5.2 above.

Corollary 5.3.
1. *If the CRT decomposition of C is as in (5.5) with Hermitian self-dual codes C_i over $\mathbb{G}_i$, for all $1 \leq i \leq r$, and $C_t' = C_t'' = \{0\}$ over $\mathbb{H}_t' = \mathbb{H}_t''$, for all $1 \leq t \leq p$, then C is self-dual.*
2. *If the CRT decomposition of C is as in (5.5) with Euclidean LCD codes $C_t' = C_t''$ over $\mathbb{H}_t' = \mathbb{H}_t''$, for all $1 \leq t \leq p$ and Hermitian LCD codes C_i over $\mathbb{G}_i$, for all $1 \leq i \leq r$, then C is LCD.*

6. Asymptotics

The existence of the asymptotically good self-dual GQC codes is shown in [14]. In this section, we will analyze the asymptotic performance of the complementary dual GQC codes, which are constructed by using asymptotically good QC complementary dual (QCCD) codes (see [7]). We need the following results.

Lemma 6.1. [2, Proposition 10] *Suppose that C_1 and C_2 are two q-ary LCD codes with parameters $[n_1, k_1, d_1]$ and $[n_2, k_2, d_2]$ respectively. Let $E = [C_1|C_2] := \{[u|v] : u \in C_1, v \in C_2\}$. Then E satisfies the following:*

(i) *$E \subseteq \mathbb{F}_q^{n_1+n_2}$ is an LCD code.*
(ii) $\dim E = k_1 + k_2$.
(iii) $d(E) = \min\{d_1, d_2\}$.

Note that for more than two codes over the same alphabet, say $C_1, \ldots, C_a$, one can similarly define $[C_1|\cdots|C_a]$ and the parameters are also determined similarly. Moreover, it is also clear that if each C_i is LCD, then the same also holds for $[C_1|\cdots|C_a]$.

Theorem 6.2. [7, Corollary 3.8] *For any pair q and m, which are relatively prime, there exists an asymptotically good sequence of QCCD codes over $\mathbb{F}_q$ where each QC code in the sequence has index length/m.*

The construction in Lemma 6.1 with QC component codes yields a GQC code.

Lemma 6.3. *Suppose that C_i is a QC code of length $m_i\ell_i$ and index ℓ_i for each $1 \le i \le a$, where m_i's are pairwise distinct. Then $[C_1|\cdots|C_a]$ is a GQC code of block lengths $(\underbrace{m_1, \ldots, m_1}_{\ell_1}, \ldots, \underbrace{m_a, \ldots, m_a}_{\ell_a})$.*

Proof. Let $R_i = \mathbb{F}_q[x]/\langle x^{m_i} - 1\rangle$ for each i and recall that C_i is an R_i-submodule in $R_i^{\ell_i}$. In polynomial representation, codewords are of the form $[u_1(x)|\cdots|u_a(x)]$, where

$$u_i(x) = (u_{i,0}(x), \ldots, u_{i,\ell_i-1}(x)) \in C_i \subset R_i^{\ell_i}.$$

It is enough to show that $[C_1|\cdots|C_a]$ is closed under multiplication by x in $R_1^{\ell_1} \times \cdots \times R_a^{\ell_a}$, which is true since each C_i is a QC code and hence closed under multiplication by x. The claim about the block lengths of the resulting GQC code is also clear. □

Let m_1 and m_2 be distinct positive integers coprime to q. Take two asymptotically good sequences of QCCD codes over $\mathbb{F}_q$, say $(C_i)_{i\ge1}$ and $(D_i)_{i\ge1}$, with parameters $[m_1\ell_i, k_i, d_i]$ and $[m_2\ell_i, k_i', d_i']$ for members of these sequences, respectively. We have

$$\begin{array}{rclcrcl} R_{C_i} &=& \lim\limits_{i\to\infty} \dfrac{k_i}{m_1\ell_i} > 0, & & R_{D_i} &=& \lim\limits_{i\to\infty} \dfrac{k_i'}{m_2\ell_i} > 0, \\ \delta_{C_i} &=& \lim\limits_{i\to\infty} \dfrac{d_i}{m_1\ell_i} > 0, & \text{and} & \delta_{D_i} &=& \lim\limits_{i\to\infty} \dfrac{d_i'}{m_2\ell_i} > 0. \end{array} \tag{6.1}$$

Note that the existence of such sequences is guaranteed by Theorem 6.2. For each $i \ge 1$, set $E_i = [C_i|D_i]$. Then by Lemmas 6.1 and 6.3, E_i is a GQCCD code of length $(m_1+m_2)\ell_i$, and block lengths $(\underbrace{m_1, \ldots, m_1}_{\ell_i}, \underbrace{m_2, \ldots, m_2}_{\ell_i})$. We have

$$\begin{aligned} R_{E_i} &= \lim_{i\to\infty} \frac{k_i + k_i'}{(m_1+m_2)\ell_i} = \frac{m_1}{(m_1+m_2)} R_{C_i} + \frac{m_2}{(m_1+m_2)} R_{D_i} > 0, \\ \delta_{E_i} &= \lim_{i\to\infty} \frac{\min\{d_i, d_i'\}}{(m_1+m_2)\ell_i} = \min\left\{ \frac{m_1}{(m_1+m_2)}\delta_{C_i}, \frac{m_2}{(m_1+m_2)}\delta_{D_i} \right\} > 0. \end{aligned} \tag{6.2}$$

Hence, we obtain a GQCCD code sequence $(E_i)_{i\geq 1}$ over $\mathbb{F}_q$ where each member of the sequence has block lengths $(\underbrace{m_1,\ldots,m_1}_{\ell_i},\underbrace{m_2,\ldots,m_2}_{\ell_i})$. This argument can be generalized from two component codes to many and the following can be similarly obtained.

Theorem 6.4. *Let q be a prime power and assume that $m_1, m_2, \ldots, m_a$ are pairwise distinct positive integers relatively prime to q. Then there exists an asymptotically good sequence of q-ary GQCCD codes $(E_i)_{i\geq 1}$, where each GQC code in the sequence has block lengths $(\underbrace{m_1,\ldots,m_1}_{\ell_i},\ldots,\underbrace{m_a,\ldots,m_a}_{\ell_i})$ for some ℓ_i.*

7. Conclusion and open problems

We have provided a concatenated structure for GQC codes in the sense of [6] and [8], which gives rise to their trace representation covering the trace representations of QC and cyclic subclasses. Moreover, a multilevel concatenated view of GQC codes is introduced, which leads to a minimum distance bound that extends Jensen's bound for QC codes. By extending the CRT decomposition of the base ring into self-reciprocal polynomials and reciprocal pairs of polynomials, as done in [9] for QC case, we have obtained criteria for GQC codes to be self-dual or, respectively, LCD. We have then showed that long GQCCD codes are good. The enumeration of GQC codes that are LCD should be studied, with the potential application of deriving a Gilbert-Varshamov bound. Tabulating GQC codes parameters in modest lengths is also a worthy goal.

8. Acknowledgment

Özbudak and Özkaya are supported by TÜBİTAK project 215E200, which is associated with the SECODE project in the scope of CHIST-ERA Program. Solé is supported by the SECODE Project too. Güneri is supported partly by TÜBİTAK 215E200 (SECODE) and by TÜBİTAK 114F432 projects. Saçıkara is supported by TÜBİTAK project 114F432.

References

[1] E.L. Blokh and V.V. Zyablov, "Coding of generalized concatenated codes", *Probl. Inform. Transm.*, vol. 10, 218-222, 1974.

[2] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks", *Adv. in Math. of Comm.*, vol. 10, no 1, 131-150, 2016.

[3] J.T. Cordaro and T.J Wagner, "Optimum $(n, 2)$ codes for small values of channel error probability", *PGIT*, vol. 13, 349-350, 1967.

[4] I. Dumer, "Concatenated codes and their multilevel generalizations", *Handbook of Coding Theory*, North-Holland, Amsterdam, 1911-1988, 1998.

[5] M. Esmaeili and S. Yari, "Generalized quasi-cyclic codes: structural properties and code construction", *Applicable Algebra in Engineering, Communications and Computing*, vol. 20, 159-173, 2009.

[6] C. Güneri and F. Özbudak, "The concatenated structure of quasi-cyclic codes and an improvement of Jensen's bound", *IEEE Trans. on Inform. Theory*, vol. 59, no. 2, 979-985, 2013.

[7] C. Güneri, B. Özkaya and P. Solé, "Quasi-cyclic complementary dual codes", *Finite Fields Appl.*, vol. 42, 67-80, 2016.

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

[9] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: finite fields", *IEEE Trans. Inform. Theory*, vol. 47, 2751-2760, 2001.

[10] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes III: generator theory", *IEEE Trans. Inform. Theory*, vol. 51, 2692-2700, 2005.

[11] S. Ling and P. Solé, "Good self-dual quasi-cyclic codes exist", *IEEE Trans. Inform. Theory*, vol. 49, 1052-1053, 2003.

[12] J.H. van Lint, *Introduction to Coding Theory*, Springer, (1982).

[13] I. Siap and N. Kulhan, "The structure of generalized quasi-cyclic codes", *Applied Mathematics E-Notes*, vol. 5, 24-30, 2005.

[14] M. Shi, Y. Liu and P. Solé, "Good self-dual generalized quasi-cyclic codes exist", Information Proc. Letters, 2017. Available from `http://arxiv.org/abs/1601.02437`.