THE CONCATENATED STRUCTURE OF QUASI-ABELIAN CODES

Martino Borello, Cem Güneri, Elif Saçikara, Patrick Solé

THE CONCATENATED STRUCTURE OF QUASI-ABELIAN CODES

Martino Borello[1], Cem Güneri[2], Elif Saçıkara[2], Patrick Solé[1]

[1] Université Paris 13, Sorbonne Paris Cité, LAGA, CNRS, UMR 7539, Université Paris 8, F-93430, Villetaneuse, France
borello@math.univ-paris13.fr, sole@math.univ-paris13.fr

[2] Sabancı University, Faculty of Engineering and Natural Sciences, 34956 Istanbul, Turkey
guneri@sabanciuniv.edu, elifsacikara@sabanciuniv.edu

Abstract. The decomposition of a quasi-abelian code into shorter linear codes over larger alphabets was given in (Jitman, Ling, (2015)), extending the analogous Chinese remainder decomposition of quasi-cyclic codes (Ling, Solé, (2001)). We give a concatenated decomposition of quasi-abelian codes and show, as in the quasi-cyclic case, that the two decompositions are equivalent. The concatenated decomposition allows us to give a general minimum distance bound for quasi-abelian codes and to construct some optimal codes. Moreover, we show by examples that the minimum distance bound is sharp in some cases. In addition, examples of large strictly quasi-abelian codes of about a half rate are given. The concatenated structure also enables us to conclude that strictly quasi-abelian linear complementary dual codes over any finite field are asymptotically good.

Keywords: Quasi-abelian codes, concatenated codes, linear complementary dual codes, optimal codes, additive abelian codes.

1. Introduction

The well-known family of quasi-cyclic (QC) codes contains examples of good codes ([13, 14]) and it is also asymptotically good ([19, 25]). As shown by Ling and Solé in [18], a QC code over $\mathbb{F}_q$ (the finite field with q elements, where q is a prime power) can be decomposed into shorter linear codes over various extensions of $\mathbb{F}_q$, using the Chinese Remainder Theorem (so-called CRT decomposition). Moreover, QC codes can also be decomposed into concatenated codes as shown by Jensen ([15]). It was observed in [9] that these two decompositions are equivalent. More specifically, the CRT components (constituents) of a QC code and the outer codes in its concatenated structure are the same.

The family of quasi-abelian (QA) codes has been introduced by Wasan ([24]) in order to generalize the algebraic structure of QC codes. Jitman and Ling reconsidered QA codes ([17]) giving, among other things, the decomposition of QA codes by extending the CRT decomposition for QC introduced by Ling-Solé (see also [6]). Let us note that a special class of QA codes is also studied in [11], which is called by the authors multidimensional QC codes, or quasi nD cyclic codes. In the general case, the family of QA codes coincides with the family QC codes, but if one considers strictly QA codes, these form a proper subfamily of QC codes. Let us also note that QA codes are

a special class of codes over a group algebra $\mathbb{F}_q[H]$ in $\mathbb{F}_q[G]$, where H is a subgroup of a finite group G. In this work, we assume that G is a finite abelian group and $(q, |H|) = 1$, namely $\mathbb{F}_q[H]$ is a semisimple algebra. The cases in which G is nonabelian or the algebra is not semisimple are more difficult to be treated in full generality. For some results in this direction, the interested reader may refer to [3] and references therein.

Here, we contribute to the structural understanding of QA codes by giving their concatenated decomposition. As in the QC case, we show that the decomposition given by Jitman-Ling and the concatenated decomposition are equivalent. However, there are several advantages of viewing a code in the concatenated form. Firstly, we can transfer the general minimum distance bound for concatenated codes to QA codes. This is, to the best of our knowledge, the first general minimum distance bound on QA codes. Moreover, using Magma ([4]), we obtain numerical results for the minimum distance of some QA codes, based on their concatenated structure.

A q-ary linear code $\mathcal{C}$ is said to be linear complementary dual (LCD) if $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$. In [16], Jitman et al. showed that binary QA LCD codes of index 3 are asymptotically good by using the asymptotic goodness of binary self-dual QA codes of index 2, which was proved in [17]. We can show that the family of (strictly) QA LCD codes, over any finite field, are asymptotically good, using the concatenated structure obtained for QA codes.

The sections are arranged as follows. Introductory material are presented in Section 2. The concatenated structure of QA codes is given in Section 3, which is followed by consequences on the minimum distance. Numerical results and asymptotic conclusions are presented in Section 4.

2. Preliminaries

In this section, we give the background materials used in this work. We assume that the reader is familiar with the definition and general theory of linear codes ([20]).

2.1. **Asymptotics.** Let $B_q(n, d)$ denote the maximum cardinality of a linear code $\mathcal{C}$, for given positive integers n and d, such that a q-ary linear code $\mathcal{C}$ with parameters $[n, k, d]$ exists. In general, we have $k := \log_q |\mathcal{C}|$, where $|\mathcal{C}|$ denotes the cardinality of $\mathcal{C} \subseteq \mathbb{F}_q^n$. A linear code $\mathcal{C}$ is said to be *optimal* if it contains exactly $B_q(n, d)$ elements.

If we consider a family of q-ary linear codes $\mathcal{C}_{(n)}$ with parameters $[n, k_n, d_n]$, then recall that the rate and the relative distance of the family is defined, respectively, as

$$r := \liminf_{n\to\infty} k_n/n,$$

$$\delta := \liminf_{n\to\infty} d_n/n.$$

A family of q-ary linear codes $\mathcal{C}_{(n)}$ is called *asymptotically good* if its rate r and relative distance δ are both nonzero.

2.2. **Generalized Concatenated Codes.** Throughout the paper, by the concatenated structure, we mean generalized concatenated codes (GCC) introduced by Block-Zyablov ([2]). Since our main results are based on this structure, we find it useful to remind the structure of GCC, following [7]. The idea of this construction is to extend a simple concatenation to a general concatenation with

more than one outer code, which are of the same length but defined over possibly different finite extensions of $\mathbb{F}_q$.

Definition 2.1. For $i \in \{1, \ldots, s\}$, let $\mathcal{C}_i$'s be linear codes (called *outer codes*) with parameters $[N, K_i, d(\mathcal{C}_i)]$ over $\mathbb{F}_{q^{k_i}}$, where $\mathbb{F}_{q^{k_i}}$ are extensions of degree k_i of the finite field $\mathbb{F}_q$. Consider the set $\mathcal{C}$ of $s \times N$- matrices defined as follows

$$\mathcal{C} := \left\{ c = \begin{pmatrix} c_1^1 & \ldots & c_N^1 \\ \vdots & \ldots & \vdots \\ c_1^s & \ldots & c_N^s \end{pmatrix} : \ (c_1^i, \ldots, c_N^i) \in \mathcal{C}_i \text{ for } 1 \leq i \leq s \right\}. \tag{2.1}$$

For $k_1 + \ldots + k_s \leq n$, suppose that $\pi : \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_s}} \mapsto {\mathbb{F}_q}^n$ is an $\mathbb{F}_q$-linear injection whose image $A := \mathrm{im}(\pi)$ is a linear code (called an *inner code*) of parameters $[n, \sum_{i=1}^s k_i, d(A)]$. Then the set

$$\pi(\mathcal{C}) = \{(\pi(c_1), \ldots, \pi(c_N)) : c_j\text{'s are columns of } c \in \mathcal{C}, \text{ for } j = 1, \ldots, N\}, \tag{2.2}$$

is called a *generalized concatenated code* (*GCC*).

This concatenation of an inner code A with an outer code $\mathcal{C}$ is denoted throughout by $A \square \mathcal{C}$. Let us note that *simple concatenation* is obtained if we choose a GCC with only one outer code.

With the following statement, we observe the relation between a GCC with at least two outer codes and a simple concatenation, and we give the parameters of a GCC.

Theorem 2.2. *Let $\pi(\mathcal{C})$ be a GCC as described above. Then the following conditions hold:*

(i) *A generalized concatenated code $\pi(\mathcal{C})$ is a linear code of length nN, of dimension $\sum_{i=1}^{s} k_i K_i$ over $\mathbb{F}_q$.*

(ii) *A generalized concatenated code $\pi(\mathcal{C})$ can be written as a direct sum of simple concatenations. Namely,*

$$\pi(\mathcal{C}) = A_1 \square \mathcal{C}_1 \oplus \cdots \oplus A_s \square \mathcal{C}_s = \bigoplus_{i=1}^{s} A_i \square \mathcal{C}_i, \tag{2.3}$$

where $A_i = \pi(0, \ldots, 0, x_i, 0, \ldots, 0)$'s are k_i-dimensional subcodes of A and $x_i \in \mathbb{F}_{q^{k_i}}$. Here, A_i's are also called inner codes in the concatenation (2.2).

(iii) *Conversely, let A_i's be q-ary linear codes of parameters $[n, k_i, d(A_i)]$ with $A_j \cap \sum_{i \neq j} A_i = \{0\}$, and let $\mathcal{C}_i$'s be $\mathbb{F}_{q^{k_i}}$-linear codes with parameters $[N, K_i, d(\mathcal{C}_i)]$, for each $i \in \{1, \ldots, s\}$. Then the direct sum of simple concatenations $\bigoplus_{i=1}^{s} A_i \square \mathcal{C}_i$ can be redescribed as a* GCC *code.*

(iv) *For a given GCC in the form of $\pi(\mathcal{C}) = A_1 \square \mathcal{C}_1 \oplus \cdots \oplus A_s \square \mathcal{C}_s$, we have*

$$d(\pi(\mathcal{C})) \geq \min_{1 \leq i \leq s} \{d(\mathcal{C}_i) d(A_1 \oplus \cdots \oplus A_i)\},$$

if $d(\mathcal{C}_1) \leq d(\mathcal{C}_2) \leq \cdots \leq d(\mathcal{C}_s)$.

2.3. **Background on Quasi-Abelian Codes.** We review the structure of quasi-abelian codes in this section, following [17] closely (see also [6]). We refer the reader to these articles for further details. Let us note that in the special case of quasi-cyclic codes, the material presented in this section has analogies with that presented in [18].

Let G be a finite (additive) abelian group of order n. Consider the group algebra $\mathbb{F}_q[G]$, whose elements are of the form $\sum_{g\in G}\alpha_g Y^g$ for $\alpha_g \in \mathbb{F}_q$. The multiplicative identity of $\mathbb{F}_q[G]$ is Y^0. Note that $\mathbb{F}_q[G]$ can be considered as a vector space over $\mathbb{F}_q$ of dimension $|G|$.

We call $\mathcal{C}$ a linear code in $\mathbb{F}_q[G]$ of length n if it is an $\mathbb{F}_q$-subspace of $\mathbb{F}_q[G]$. Note that such a code can be viewed as a linear code of length n over $\mathbb{F}_q$ by indexing the symbols in codewords with the elements in G. Hence, the Hamming weight $\mathrm{wt}(v)$ of $v=\sum_{g\in G} v_g Y^g \in \mathbb{F}_q[G]$ is the number of nonzero terms v_g and the minimum distance of $\mathcal{C}$ is

$$d(\mathcal{C}) := \min\{\mathrm{wt}(v) | v\in\mathcal{C}, v\neq 0\}.$$

Definition 2.3. A code $\mathcal{C}$ in $\mathbb{F}_q[G]$ is called an H *quasi-abelian code* (H-QA) of index ℓ if $\mathcal{C}$ is an $\mathbb{F}_q[H]$-module, where H is a subgroup of G with $[G:H]=\ell$. We will only refer to these codes as QA codes, unless it is needed to specify the subgroup H and the index.

Let $\{g_1,\dots,g_\ell\}$ be a fixed set of representatives of the cosets of H in G. Note that a QA code of index ℓ in $\mathbb{F}_q[G]$ can be seen as an $\mathbb{F}_q[H]$-submodule of $\mathbb{F}_q[H]^\ell$ by the following $\mathbb{F}_q[H]$-module isomorphism.

$$\begin{array}{rccc} \Phi: & \mathbb{F}_q[G] & \longrightarrow & \mathbb{F}_q[H]^\ell \\ & \displaystyle\sum_{i=1}^{\ell}\sum_{h\in H}\alpha_{h+g_i}Y^{h+g_i} & \longmapsto & \displaystyle\left(\sum_{h\in H}\alpha_{h+g_1}Y^h,\dots,\sum_{h\in H}\alpha_{h+g_\ell}Y^h\right). \end{array} \tag{2.4}$$

Remark 2.4. It is clear that an H-QA code is QC if H is cyclic. Moreover, if $H=J\times K$ with J cyclic and $|K|=t$, then an H-QA code of index ℓ is a QC code of index $t\ell$. By the fundamental theorem of finite abelian groups, every abelian group H decomposes into products of cyclic groups. Hence the class of QA codes is a subclass of QC codes. For instance, if we choose $H=C_{m_1}\times C_{m_2}$, where C_{m_i} denotes the cyclic group $\mathbb{Z}/m_i\mathbb{Z}$ of order m_i for $i=1,2$, then an H-QA code can be viewed as a QC code of co-index m_1 or co-index m_2. Moreover, as mentioned before in [11] and [15] for certain special cases, we have various QA structures with different indices for a given QA code, since an $\mathbb{F}_q[H]$-module in $\mathbb{F}_q[H]^\ell$ is also an $\mathbb{F}_q[H']$-module, for any $H'\leq H\leq G$.

Jitman and Ling ([17]) call a QA code $\mathcal{C}$ strictly QA (SQA) if H is not a cyclic group. Similarly, if $\ell=1$ and H is not cyclic, we refer to strictly abelian (SA) codes.

We continue with recalling the CRT decomposition of H-QA codes of index ℓ, which is introduced in [17] (see also [6]). For a semisimple algebra $\mathbb{F}_q[H]$, where H is a subgroup of a finite abelian G with $|H|=m$, let M be the exponent of H and let $\mathbb{K}$ be an extension of $\mathbb{F}_q$ which contains a primitive M-th root of unity ξ. We set $R:=\mathbb{F}_q[H]$ throughout.

A character χ from H to the multiplicative group of $\mathbb{K}$ is a group homomorphism. The set $\mathrm{Hom}(H,\mathbb{K}^*)$ of characters forms a group which is isomorphic to H. So, we can denote the characters

in $\mathrm{Hom}(H, \mathbb{K}^*)$ as χ_a, $a \in H$. If we view the abelian group H as a direct product of finite cyclic groups,

$$H = \prod_{i=1}^{s} C_{m_i},$$

then an element $h \in H$ can be represented as $h = (h_1, \cdots, h_s)$, where $h_i \in C_{m_i}$ and C_{m_i} denotes the additive cyclic group $\mathbb{Z}/m_i\mathbb{Z}$ of order m_i. In this case, it is well-known that the character χ_a can be written as

$$\chi_a(h) = \xi^{\sum_{i=1}^{s} a_i h_i M/m_i}, \tag{2.5}$$

for any $a \in H$.

Recall that a primitive idempotent of a ring is a nonzero element e such that $e^2 = e$ and for any other idempotent f, either $ef = 0$ or $ef = e$. To present the decomposition of QA codes, we will need to use idempotents in $R = \mathbb{F}_q[H]$. For this purpose, one first considers the group algebra $\mathbb{K}[H]$, whose primitive idempotents are given by

$$E_x = \frac{1}{m} \sum_{a \in H} \chi_x(-a) Y^a \in \mathbb{K}[H], \tag{2.6}$$

for each $x \in H$. The primitive idempotents of $\mathbb{K}[H]$ are orthogonal, i.e. $E_x E_y = 0$ if $x, y \in H$ and $x \neq y$.

The *q-cyclotomic class* of H containing $h \in H$ is defined as

$$S_q(h) := \{q^i h : 0 \leq i < v_h\}, \tag{2.7}$$

where $q^i h$ denotes addition of h with itself q^i times (recall that G and hence H are additive groups), and v_h is the smallest positive integer such that $q^{v_h} \equiv 1$ (ord h). Primitive idempotents in $\mathbb{F}_q[H]$ are of the form

$$e_h = \sum_{x \in S_q(h)} E_x, \tag{2.8}$$

where $h \in H$ and E_x is a primitive idempotent in $\mathbb{K}[H]$ as in (2.6). The idempotent e_h is called the primitive idempotent induced by $S_q(h)$. Orthogonality of the primitive idempotents of $\mathbb{K}[H]$ implies orthogonality of the primitive idempotents in $\mathbb{F}_q[H]$:

$$e_h e_{h'} = 0, \quad \text{if } h, h' \in H \text{ have distinct } q\text{-cyclotomic classes.} \tag{2.9}$$

If $S_q(h_1), \ldots, S_q(h_t)$ are all q-cyclotomic classes of H and $e_{h_1}, \ldots, e_{h_t}$ are the corresponding primitive idempotents of $\mathbb{F}_q[H]$, then we have

$$\sum_{i=1}^{t} e_{h_i} = 1. \tag{2.10}$$

Moreover, primitive idempotents of $R = \mathbb{F}_q[H]$ yields the decomposition

$$R = \bigoplus_{i=1}^{t} R e_{h_i}. \tag{2.11}$$

The ideal Re_{h_i} generated by e_{h_i} in the group algebra R is an abelian code ([15]). Moreover, Re_{h_i} is an extension field of $\mathbb{F}_q$ with the extension degree $S_q(h_i)$ (for all $1 \leq i \leq t$). The maps yielding the identification of Re_{h_i} with the extension $\mathbb{E}_i$ of $\mathbb{F}_q$ are

$$\begin{array}{rccc} \varphi_i : & Re_{h_i} & \longrightarrow & \mathbb{E}_i \\ & \left(\sum_{h\in H} \alpha_h Y^h\right) e_{h_i} & \longmapsto & \sum_{h\in H} \alpha_h \chi_{h_i}(h), \end{array} \tag{2.12}$$

$$\begin{array}{rccc} \psi_i : & \mathbb{E}_i & \longrightarrow & Re_{h_i} \\ & \delta & \longmapsto & \sum_{k\in H} \alpha_k Y^k, \end{array} \tag{2.13}$$

where $\alpha_k = \frac{1}{m}\mathrm{Tr}(\delta\chi_{h_i}(-k))$. Here, Tr denotes the trace map from $\mathbb{E}_i$ to $\mathbb{F}_q$. Note that φ_i and ψ_i are nontrivial ring homomorphisms and they are inverse to each other for every $1 \leq i \leq t$. Moreover, $\varphi_i(e_{h_i}) = 1$ and hence $\psi_i(1) = e_{h_i}$.

By (2.10), any element $r \in R$ can be written as $r = re_{h_1} + \cdots + re_{h_t}$. For an element $(r_1, \ldots, r_\ell) \in R^\ell$, we have

$$\begin{aligned} (r_1, \ldots, r_\ell) &= (r_1 e_{h_1} + \cdots + r_1 e_{h_t}, \ldots, r_\ell e_{h_1} + \cdots + r_\ell e_{h_t}) \\ &= (r_1 e_{h_1}, \ldots, r_\ell e_{h_1}) + \cdots + (r_1 e_{h_t}, \ldots, r_\ell e_{h_t}). \end{aligned}$$

Using the isomorphisms $\varphi_1, \ldots, \varphi_t$, we can identify R^ℓ and $\oplus_{i=1}^t \mathbb{E}_i^\ell$:

$$\begin{array}{rcl} R^\ell & \longrightarrow & \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_t^\ell \\ (r_1, \ldots, r_\ell) & \longmapsto & \big(\varphi_1(r_1 e_{h_1}), \ldots, \varphi_1(r_\ell e_{h_1})\big) + \cdots + \big(\varphi_t(r_1 e_{h_t}), \ldots, \varphi_t(r_\ell e_{h_t})\big) \end{array}$$

Consequently, an R-submodule of R^ℓ can be viewed as $\oplus_{i=1}^t \mathbb{E}_i$-submodule of $\oplus_{i=1}^t \mathbb{E}_i^\ell$. Therefore, a QA code $C \subseteq R^\ell$ decomposes as

$$\mathcal{C} = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_t, \tag{2.14}$$

where $\mathcal{C}_i \subset \mathbb{E}_i^\ell$ is a linear code of length ℓ over the field $\mathbb{E}_i$ for every $1 \leq i \leq t$. We call $\mathcal{C}_i$'s the constituents of $\mathcal{C}$. The preceding arguments yield the explicit description of the constituents (for $1 \leq i \leq t$):

$$\mathcal{C}_i = \Big\{ \big(\varphi_i(c_1 e_{h_i}), \ldots, \varphi_i(c_\ell e_{h_i})\big) : (c_1, \ldots, c_\ell) \in C \Big\}. \tag{2.15}$$

3. The Concatenated Structure of Quasi-Abelian Codes

Jensen gave the concatenated structure of abelian and QC codes in [15]. It was later shown in [9] that the CRT decomposition of a QC code in [18] and the code's concatenated decomposition by Jensen are equivalent. Here, we give the concatenated structure of QA codes and prove the analog of the result in [9].

Consider the rings $R^\ell = \mathbb{F}_q[H]^\ell$ and $\mathbb{E}_i^\ell$ (for $i \in \{1, \ldots, t\}$), where the ring operations are clearly componentwise addition and multiplication. Using the maps φ_i and ψ_i in (2.12) and (2.13), we define

$$\begin{array}{rccc} \Psi_i : & \mathbb{E}_i^\ell & \longrightarrow & R^\ell \\ & (a_1, \ldots, a_\ell) & \longmapsto & (\psi_i(a_1), \ldots, \psi_i(a_\ell)) \end{array} \tag{3.1}$$

and

$$\begin{array}{rccc} \Phi_i : & R^\ell & \longrightarrow & \mathbb{E}_i^\ell \\ & \left(\sum_{h \in H} \alpha_h^1 Y^h, \ldots, \sum_{h \in H} \alpha_h^\ell Y^h \right) & \longmapsto & \left(\sum_{h \in H} \alpha_h^1 \chi_{h_i}(h), \ldots, \sum_{h \in H} \alpha_h^\ell \chi_{h_i}(h) \right). \end{array} \tag{3.2}$$

Note that Ψ_i and Φ_i are $\mathbb{F}_q$-linear ring homomorphisms (for $i \in \{1, \ldots, t\}$). Moreover they are inverse to each other when Φ_i is restricted to the image of Ψ_i. Next we describe the primitive idempotents of R^ℓ.

Theorem 3.1. *For each $i \in \{1, \ldots, t\}$, let $\Theta_i := \Psi_i(1, \ldots, 1) = (e_{h_i}, \ldots, e_{h_i})$. Then $\langle \Theta_i \rangle = \Psi_i(\mathbb{E}_i^\ell)$ and $R^\ell = \bigoplus_{i=1}^{t} \langle \Theta_i \rangle$. Moreover,*

$$\Theta_i \Theta_j = \begin{cases} \Theta_i & \text{if } i = j, \\ 0 & \text{if } i \neq j, \end{cases}$$

and $\sum_{i=1}^{t} \Theta_i = (1, \ldots, 1)$ in R^ℓ.

Proof. The equality $\langle \Theta_i \rangle = \Psi_i(\mathbb{E}_i^\ell)$ follows immediately from the definitions of ψ_i and Ψ_i. Suppose $(f_1, \ldots, f_\ell)$ in R^ℓ belongs to the intersection of $\langle \Theta_i \rangle$ and $\langle \Theta_j \rangle$ for $i \neq j$. This implies that for all $u \in \{1, \ldots, \ell\}$, $f_u \in Re_{h_i} \cap Re_{h_j}$, which is trivial by (2.11). So, $\bigoplus_{i=1}^{t} \langle \Theta_i \rangle$ is indeed a direct sum in R^ℓ. Since $\langle \Theta_i \rangle = \Psi_i(\mathbb{E}_i^\ell)$, we have $\dim_{\mathbb{F}_q} \langle \Theta_i \rangle = \ell[\mathbb{E}_i : \mathbb{F}_q]$. Hence,

$$\begin{aligned} \dim_{\mathbb{F}_q} \bigoplus_{i=1}^{t} \langle \Theta_i \rangle &= \ell \sum_{i=1}^{t} [\mathbb{E}_i : \mathbb{F}_q] \\ &= \ell \sum_{i=1}^{t} \dim_{\mathbb{F}_q} Re_{h_i} \quad \text{by (2.12)} \\ &= \ell \dim_{\mathbb{F}_q} R \quad \text{by (2.11)}. \end{aligned}$$

Hence, $R^\ell = \bigoplus_{i=1}^{t} \langle \Theta_i \rangle$. The other assertions easily follow from (2.9) and (2.10). □

Next, we describe the concatenated structure of QA codes. We denote the concatenation operation by $\square$ as commonly done in the literature. In the following, we use the set defined as

$$\mathcal{C}s := \{cs : \ c \in \mathcal{C}\},$$

for $\mathcal{C} \subseteq R^\ell$ and an element $s \in R^\ell$.

Theorem 3.2. *With the notation above, the following conditions hold:*

(i) *Let $\mathcal{C}$ be an R-submodule of R^ℓ and $\tilde{\mathcal{C}}_i := \mathcal{C}\Theta_i \subseteq R^\ell$ for all $i = 1, \ldots, t$. Then, for some subset $\mathfrak{I} \subseteq \{1, \ldots, t\}$, we have $\mathcal{C} = \bigoplus_{i\in\mathfrak{I}} \tilde{\mathcal{C}}_i$. Moreover, $\tilde{\mathcal{C}}_i = Re_{h_i}\Box\mathfrak{C}_i$, where $\mathfrak{C}_i = \Phi_i(\tilde{\mathcal{C}}_i)$ is an $\mathbb{E}_i$-linear code of length ℓ for each i.*

(ii) *Conversely, let $\mathfrak{C}_i$ be a linear code over $\mathbb{E}_i$ of length ℓ for all i in some subset $\mathfrak{I}$ of $\{1, \ldots, t\}$. Then, $\mathcal{C} = \bigoplus_{i\in\mathfrak{I}} Re_{h_i}\Box\mathfrak{C}_i$ is an H-QA code of index ℓ.*

Proof. (i) By Theorem 3.1 we have

$$\mathcal{C} = \mathcal{C}\sum_{i=1}^{t}\Theta_i = \sum_{i\in\mathfrak{I}}\tilde{\mathcal{C}}_i,$$

where $\mathfrak{I}$ consists of indices i for which $\tilde{\mathcal{C}}_i \neq \{0\}$. Since $\tilde{\mathcal{C}}_i$ lies in the ideal $\langle\Theta_i\rangle$ and the sum of these ideals is direct, the sum $\sum_{i\in\mathfrak{I}}\tilde{\mathcal{C}}_i$ is also direct.

On the other hand, for all $i \in \mathfrak{I}$, we have

$$\begin{aligned}\tilde{\mathcal{C}}_i &= \mathcal{C}\Theta_i \\ &= \{(c_1, \ldots, c_\ell)\,(e_{h_i}, \ldots, e_{h_i}) : (c_1, \ldots, c_\ell) \in \mathcal{C}\} \\ &= \{(c_1e_{h_i}, \ldots, c_\ell e_{h_i}) : (c_1, \ldots, c_\ell) \in \mathcal{C}\}.\end{aligned}$$

Hence,

$$\mathfrak{C}_i = \Phi_i\left(\tilde{\mathcal{C}}_i\right) = \left\{\left(\varphi_i(c_1e_{h_i}), \ldots, \varphi_i(c_\ell e_{h_i})\right) : (c_1, \ldots, c_\ell) \in \mathcal{C}\right\}. \tag{3.3}$$

Since $\tilde{\mathcal{C}}_i$ and Φ_i are $\mathbb{F}_q$-linear, each $\mathfrak{C}_i$ is an $\mathbb{F}_q$-linear code of length ℓ. The map φ_i in (2.12) is bijective. Therefore for any $\delta \in \mathbb{E}_i$, there exists $f \in R$ such that $\varphi_i(fe_{h_i}) = \delta$. So, for any $(\varphi_i(c_1e_{h_i}), \ldots, \varphi_i(c_\ell e_{h_i})) \in \mathfrak{C}_i$, we have

$$\begin{aligned}\delta(\varphi_i(c_1e_{h_i}), \ldots, \varphi_i(c_\ell e_{h_i})) &= (\varphi_i(fe_{h_i})\varphi_i(c_1e_{h_i}), \ldots, \varphi_i(fe_{h_i})\varphi_i(c_\ell e_{h_i})) \\ &= (\varphi_i(fc_1e_{h_i}), \ldots, \varphi_i(fc_\ell e_{h_i})). \qquad (3.4)\end{aligned}$$

Since $\mathcal{C}$ is an R-module, $(fc_1, \ldots, fc_\ell)$ lies in $\mathcal{C}$. Therefore, (3.4) belongs to $\mathfrak{C}_i$, which shows that $\mathfrak{C}_i$ is $\mathbb{E}_i$-linear.

Now, consider the concatenated code $Re_{h_i}\Box\mathfrak{C}_i$ determined by $\psi_i : \mathbb{E}_i \to Re_{h_i}$ in (2.13):

$$Re_{h_i}\Box\mathfrak{C}_i = \{(\psi_i(\varphi_i(c_1e_{h_i})), \ldots, \psi_i(\varphi_i(c_\ell e_{h_i}))) : (c_1, \ldots, c_\ell) \in \mathcal{C}\}.$$

Since ψ_i and ϕ_i are inverse to each other, we have

$$Re_{h_i}\Box\mathfrak{C}_i = \{(c_1e_{h_i}, \ldots, c_\ell e_{h_i}) : (c_1, \ldots, c_\ell) \in \mathcal{C}\} = \tilde{\mathcal{C}}_i,$$

which completes the proof.

(ii) Let $\mathfrak{C}_i$ be an $\mathbb{E}_i$ linear code of length ℓ and consider the concatenation

$$Re_{h_i}\Box\mathfrak{C}_i = \{(\psi_i(\lambda_1), \ldots, \psi_i(\lambda_\ell)) : (\lambda_1, \ldots, \lambda_\ell) \in \mathfrak{C}_i\}$$

for each $i \in \mathfrak{I}$. By linearity of $\mathfrak{C}_{\mathfrak{i}}$ and ψ_i, this set becomes an additive subgroup of R^ℓ. We need to show that $Re_{h_i}\Box\mathfrak{C}_i$ is closed under multiplication by elements of R. For this, it is enough to show that it is closed under multiplication by $Y^x \in R$, for any $x \in H$. Since φ_i is surjective, we can write an element $(\lambda_1, \ldots, \lambda_\ell) \in \mathfrak{C}_i$ as $(\varphi_i(f_1 e_{h_i}), \ldots, \varphi_i(f_\ell e_{h_i}))$ for some $f_1, \ldots, f_\ell \in R$. Then,

$$\begin{aligned} Y^x(\psi_i(\lambda_1), \ldots, \psi_i(\lambda_\ell)) &= Y^x(f_1 e_{h_i}, \ldots, f_\ell e_{h_i}) \quad (\psi_i \text{ and } \varphi_i \text{ are inverse}) \\ &= \left(Y^x e_{h_i} f_1 e_{h_i}, \ldots, Y^x e_{h_i} f_\ell e_{h_i}\right) \quad (\text{using } e_{h_i} e_{h_i} = e_{h_i}) \\ &= \left(\psi_i\Big(\varphi_i\big(Y^x e_{h_i} f_1 e_{h_i}\big)\Big), \ldots, \psi_i\Big(\varphi_i\big(Y^x e_{h_i} f_\ell e_{h_i}\big)\Big)\right) \\ &= \left(\psi_i\Big(\varphi_i\big(Y^x e_{h_i}\big)\varphi_i\big(f_1 e_{h_i}\big)\Big), \ldots, \psi_i\Big(\varphi_i\big(Y^x e_{h_i}\big)\varphi_i\big(f_\ell e_{h_i}\big)\Big)\right). \end{aligned} \tag{3.5}$$

Since $\varphi_i\big(Y^x e_{h_i}\big)$ is in $\mathbb{E}_i$ and $\mathfrak{C}_i$ is $\mathbb{E}_i$-linear, $\Big(\varphi_i\big(Y^x e_{h_i}\big)\varphi_i\big(f_1 e_{h_i}\big), \ldots, \varphi_i\big(Y^x e_{h_i}\big)\varphi_i\big(f_\ell e_{h_i}\big)\Big)$ belongs to $\mathfrak{C}_i$. Therefore (3.5) is in $Re_{h_i}\Box\mathfrak{C}_i$.

Finally, $Re_{h_i}\Box\mathfrak{C}_i$ lies in $(Re_{h_i})^\ell$ (for each i) and Re_{h_i}'s intersect trivially (cf. (2.11)). Therefore the sum of the concatenations $Re_{h_i}\Box\mathfrak{C}_i$, for $i \in \mathfrak{I}$, is direct. Hence the result follows. □

Remark 3.3. For a QA code $\mathcal{C}$, the constituent $\mathcal{C}_i$ and the outer code $\mathfrak{C}_i$ in its concatenated form coincide, for each i. This follows from (2.15) and (3.3).

The minimum distance bound which is valid for all concatenated codes (see [2, 7], and part *iv* in Theorem 2.2,) apply to QA codes by Theorem 3.2. So, we do not prove the next result.

Corollary 3.4. *Let $\mathcal{C}$ be a QA code of index ℓ in R^ℓ with the concatenated structure*

$$C = \bigoplus_{j=1}^{g} Re_{h_{i_j}}\Box\mathfrak{C}_{i_j},$$

where $\mathfrak{C}_{i_j}$'s are the nonzero outer codes (constituents) of $\mathcal{C}$, and $Re_{h_{i_j}}$'s are minimal abelian codes generated by primitive idempotents in R^ℓ for $\{i_1, \ldots, i_g\} \subseteq \{1, \ldots, t\}$. Assume that $d(\mathfrak{C}_{i_1}) \leq d(\mathfrak{C}_{i_2}) \leq \cdots \leq d\left(\mathfrak{C}_{i_g}\right)$. Then, we have

$$d(C) \geq \min_{1 \leq v \leq g} \left\{ d(\mathfrak{C}_{i_v}) d(Re_{h_{i_1}} \oplus \cdots \oplus Re_{h_{i_v}}) \right\}.$$

4. Numerical Results and Asymptotics

The concatenated structure of QA codes in Section 3 allows us to obtain numerical results and asymptotic conclusions for QA codes, as it is shown here.

4.1. **Numerical Results.** Corollary 3.4 gives a theoretical bound for the minimum distance of QA codes. As we have already observed, the class of SQA codes forms a subfamily of the class of QC and this last class contains many optimal codes. In this part, we present some numerical results to see how good the bound obtained is and to show the existence of some optimal SQA codes, different from those found by Jitman and Ling in [17]. In the first three examples, particularly, we show some examples of optimal SQA codes of index 3 and 4, while in the last two examples we present certain SQA codes of rate close to 1/2.

We develop an algorithm in MAGMA to compute, given a finite group H, all H-QA codes of a fixed index ℓ with a minimum distance bounded below by certain constant d. The algorithm follows the following steps:

- compute all q-cyclotomic classes $S_q(h)$ in $\mathbb{F}_q[H]$, whose cardinalities give the degrees of the extension fields;
- for each extension $\mathbb{F}_{q^k}$, where $k = |S_q(h)|$, compute all linear codes of length ℓ over $\mathbb{F}_{q^k}$;
- for each element h in a q-cyclotomic class $S_q(h)$ and for each linear code $\mathcal{C}$ of length ℓ over $\mathbb{F}_{q^k}$, by using DFT, which is written explicitly in 2.13 and chosen as a concatenation map, we compute the concatenation of $\mathcal{C}$ with the minimal abelian code given by h. We put the obtained codes in a list S if their minimum distance is greater than or equal to d;
- we sum pairs of elements of S, always checking if their minimum distance is greater than or equal to d, and we put the obtained codes in a list S'. We repeat the process to obtain codes with a higher dimension.

The complexity of this algorithm strongly depends on ℓ, on the size of the q-cyclotomic classes and on the chosen d.

We applied this algorithm in some cases and obtained some optimal codes. As an example, we first give here three cases, of index 2, 3 and 4 respectively, for which the codes obtained have the best-known minimum distance for their dimension. Moreover, in the second and the third, the minimum distance obtained meets the lower bound given by Corollary 3.4.

We looked for QA codes in $R := \mathbb{F}_2[C_5 \times C_5]^2$ of minimum distance at least 18 and, for the dimension 12, we got only one $[50, 12, 18]$ code $\mathcal{C}$, up to equivalence, which is the direct sum

$$\mathcal{C} = (Re_{(1,0)} \square \mathcal{C}_1) \oplus (Re_{(1,1)} \square \mathcal{C}_1) \oplus (Re_{(2,4)} \square \mathcal{C}_2)$$

with $\mathcal{C}_1$ of generator matrix $G_1 := [1, \alpha^7]$ and $\mathcal{C}_2$ of generator matrix $G_2 := [1, \alpha^{12}]$, where α is a primitive element in $\mathbb{F}_{16}$ such that $\alpha^4 = \alpha + 1$.

Note that 18 is the best known minimum distance for a code of length 50 and dimension 12, according to Grassl's tables [8]. Moreover, in this case the lower bound given by Corollary 3.4 is 12.

Secondly, we looked for QA codes in $R := \mathbb{F}_2[C_3 \times C_3]^3$ of minimum distance at least 12 and, for the dimension 6, we got only one $[27, 6, 12]$ code $\mathcal{C}$, up to equivalence, with two outer codes, namely

$$\mathcal{C} = (Re_{(2,2)} \square \mathcal{C}_1) \oplus (Re_{(1,0)} \square \mathcal{C}_2)$$

with $\mathcal{C}_1$ of generator matrix $G_1 := \left[\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{smallmatrix}\right]$ and $\mathcal{C}_2$ of generator matrix $G_2 := [1, \alpha, 1]$, where α is a primitive element in $\mathbb{F}_4$.

Note that 12 is the best known minimum distance for a code of length 27 and dimension 6, by the Griesmer bound [8]. Moreover, in this case the lower bound given by Corollary 3.4 is exactly 12.

Now, we looked for QA codes in $R := \mathbb{F}_2[C_3 \times C_3]^4$ of minimum distance at least 16 and, for the dimension 6, we got only one $[36, 6, 16]$ code $\mathcal{C}$, up to equivalence, with two outer codes, namely

$$\mathcal{C} = (Re_{(2,2)} \square \mathcal{C}_1) \oplus (Re_{(1,0)} \square \mathcal{C}_2)$$

with $\mathcal{C}_1$ of generator matrix $G_1 := \left[\begin{smallmatrix} 1 & 0 & \alpha^2 & \alpha \\ 0 & 1 & 1 & \alpha \end{smallmatrix}\right]$ and $\mathcal{C}_2$ of generator matrix $G_2 := [1, \alpha, \alpha, \alpha]$, where α is a primitive element in $\mathbb{F}_4$.
Note that 16 is the best known minimum distance for a code of length 36 and dimension 6, by the Griesmer bound [8]. Moreover, in this case the lower bound given by Corollary 3.4 is exactly 16.

In the last two examples, in order to show the effectiveness the concatenation method for QA codes, we consider a binary QA in $\mathbb{F}_2[C_5 \times C_5]^{256}$ of minimum distance at least 48 and of rate $\approx 1/2$, with the concatenated structure

$$\mathcal{C} = \bigoplus_{i=1}^{4} (Re_{h_i} \square \mathcal{C}_i),$$

where all $\mathcal{C}_i$'s are Reed-Muller codes $\mathcal{RM}_{\mathbb{F}_{16}}(20, 2)$ of parameters $[256, 201, 12]$ over $\mathbb{F}_{16}$ ([1]), and h_i's are $(1, 0), (0, 1), (1, 1)$, and $(1, 2)$ in $H = C_5 \times C_5$, respectively. In fact, since each inner code R_{h_i}, for the corresponting h_i, has parameters $[25, 4, 10]$ over binary field, and since their sum has minimum distance 4, the QA code with the given concatenated structure is of parameters $[6400, 3216, \geq 48]$.

Finally, we consider a QA code in $R := \mathbb{F}_3[C_5 \times C_5]^{6561}$ of minimum distance at least 220 and of rate close to $1/2$, with the concatenated structure

$$\mathcal{C} = \bigoplus_{i=1}^{4} (Re_{h_i} \square \mathcal{C}_i),$$

where all $\mathcal{C}_i$'s are Reed-Muller codes $\mathcal{RM}_{81}(106, 2)$ of parameters $[6561, 5076, 55]$ over $\mathbb{F}_{3^4}$ ([1]), and h_i's are $(1, 0), (1, 1), (0, 1)$, and $(1, 2)$ in $H = C_5 \times C_5$, respectively. In fact, using the same arguments as before, we obtain that the QA code with the given concatenated structure has parameters $[164025, 81216, \geq 220]$.

4.2. **Asymptotic Results.** The class of binary self-dual doubly even strictly QA codes has been shown to be asymptotically good ([17, Theorem 7.2]), followed by the asymptotical goodness of binary complementary dual QA (QA LCD) codes of index 3 ([16]). Recall that, by a strictly QA code, the authors mean a QA code which is not QC. Note that H being a noncyclic abelian group is enough for this purpose (cf. Remark 2.4). We first show that strictly QA codes are asymptotically good over any finite field $\mathbb{F}_q$.

Theorem 4.1. *For any prime power q, the class of strictly QA codes over $\mathbb{F}_q$ is asymptotically good.*

Proof. Let p be a prime different than $\mathrm{char}(\mathbb{F}_q)$ and set $H = C_p \times C_p$ so that it is not cyclic and $\gcd(|H|, q) = 1$. Note that the q-cyclotomic class of $0 \in H$ consists of itself only. Let us denote the primitive idempotent corresponding to this cyclotomic class by e_0. Hence in the decomposition (2.11) of $\mathbb{F}_q[H]$, there exists the field $\mathbb{F}_q$, which is isomorphic to the ideal $\mathbb{F}_q[H]e_0$. This implies that an H-QA code over $\mathbb{F}_q$ of any index ℓ has a constituent which lies in $\mathbb{F}_q^{\ell}$.

Let $\mathcal{F} := (\mathcal{F}_1, \mathcal{F}_2, \ldots)$ be an asymptotically good family of $\mathbb{F}_q$-linear codes and let the parameters of any member $\mathcal{F}_i$ in the family be (n_i, k_i, d_i). Define the groups

$$G_i := H \times C_{n_i},$$

for all $i \geq 1$. We can construct H-QA codes $\mathcal{E}_i$ in $\mathbb{F}_q[G_i]$ (or, in $\mathbb{F}_q[H]^{n_i}$) for all i using Theorem 3.2 as follows:

$$\mathcal{E}_i := \mathbb{F}_q[H]e_0 \square \mathcal{F}_i.$$

Note that any member $\mathcal{E}_i$ of the family $\mathcal{E} := (\mathcal{E}_1, \mathcal{E}_2, \ldots)$ of H-QA codes has parameters $(p^2 n_i, k_i, \geq dd_i)$, where d is the minimum distance of the fixed abelian code $\mathbb{F}_q[H]e_0$ of length p^2. Hence, the relative parameters of $\mathcal{E}_i$'s also have positive limit, namely $1/p^2$ multiple of the limit relative rate of $\mathcal{F}$ and at least d/p^2 multiple of the limit relative distance of $\mathcal{F}$. □

We can extend the preceding asymptotic conclusion to the linear complementary dual (LCD) class over any finite field. Let us note that the decomposition of the dual of a QA code is given in [17]. Based on this, a characterization of self-dual QA codes is obtained in terms of the constituents of the code ([17, Corollary 4.1]). The analogous result for QA LCD codes can be obtained in a straightforward way, so we do not prove it. One can consult [12, Theorem 3.1] for the special case of LCD QC codes.

Theorem 4.2. *For any prime power q, the class of strictly QA LCD codes over $\mathbb{F}_q$ is asymptotically good.*

Proof. Let H be as in the proof of Theorem 4.1 and choose $\mathcal{F}$ to be an asymptotically good family of LCD codes this time. Such codes exist by [21] and [22]. Consider the family $\mathcal{E}$ of strictly QA codes as in the same proof. The fact that this family is asymptotically good follows as above. For any $i \geq 1$, the code $\mathcal{E}_i$ has unique nonzero constituent (namely, $\mathcal{F}_i$) which is LCD by construction. All other constituents of $\mathcal{E}_i$ are $\{0\}$, which is trivially LCD with respect to the Euclidean inner product. Hence, by the dual QA code description [17, p. 519], and the discussion preceding this theorem, each $\mathcal{E}_i$ is LCD. Therefore $\mathcal{E}$ is an asymptotically good family of strictly QA LCD codes. □

We note that the codes presented in Theorems 4.1 and 4.2 resemble the asymptotically good QC codes presented in [19], since the "co-index" (i.e. length/index) of each code in the families considered is fixed (unlike the asymptotically good family presented in [16, 17]).

5. Acknowledgments

The first author was partially supported by PEPS - Jeunes Chercheur-e-s - 2018. The second author was supported by TÜBİTAK Project no. 114F432. The third author was supported by TÜBİTAK 2214/A Fellowship program.

References

[1] E. F. Assmuss, and J. D. Key, *Designs and their Codes*, No. 103, Cambridge University Press, 1992.

[2] E.L. Blokh and V.V. Zyablov, *Coding of generalized concatenated codes*, Problemy Peredachi Informatsii, 10 (1974), no. 3, pp. 45-50.

[3] M. Borello, *On the automorphism groups of binary linear codes*, Topics in Finite Fields, Contemporary Mathematics 632, 2015.

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

[5] C. Carlet and S. Guilley, *Complementary dual codes for counter-measures to side-channel attacks*, Adv. Math. Commun., 10 (2016), pp. 131-150.

[6] C. Ding, D.R. Kohel, and S. Ling, *Split group codes*, IEEE Trans. Inform. Theory, 46 (2000), pp. 485-495.

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

[8] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*, Online available at `http://www.codetables.de`, accessed on 2018-06-18.

[9] C. Güneri and F. Özbudak, *The concatenated structure of quasi-cyclic codes and an improvement of Jensen's bound*, IEEE Trans. Inform. Theory, 59 (2013), 979-985.

[10] C. Güneri, B. Özdemir, and P. Solé, *On additive cyclic structure of quasi-cyclic codes*, Discrete Math, 341 (2018), no. 10, pp. 2735-2741.

[11] C. Güneri and B. Özkaya, *Multidimensional quasi-cyclic and convolutional codes*, IEEE Trans. Inform. Theory, 62 (2016), pp. 6772-6785.

[12] C. Güneri, B. Özkaya, and P. Solé, *Quasi-cyclic complementary dual codes*, Finite Fields Appl., 42 (2016), pp. 67-80.

[13] T.A. Gulliver, M. Harada, and H. Miyabayashi, *Double circulant and quasi-twisted self-dual codes over and* $\mathbb{F}_5$ *and* $\mathbb{F}_7$, Adv. Math. Commun., 1 (2007), pp. 223-238.

[14] S. Han, J.L. Kim, H. Lee, and Y. Lee, *Construction of quasi-cyclic self-dual codes*, Finite Fields Appl., 18 (2012), pp. 613-633.

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

[16] S. Jitman, H.S. Palines, R.B. dela Cruz, *On Quasi-Abelian Complementary Dual Codes*, Barbero Á., Skachek V., Ytrehus Ø. (eds) Coding Theory and Applications, ICMCTA, Lecture Notes in Computer Science, vol 10495. Springer, Cham, 2017.

[17] S. Jitman, and S. Ling, *Quasi-abelian codes*, Des. Codes Cryptogr., 74 (2015), pp. 511-531.

[18] S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes I: Finite Fields*, IEEE Trans. Inform. Theory, 47 (2001), pp. 2751-2760.

[19] S. Ling and P. Solé, *Good self-dual quasi-cyclic codes exist*, IEEE Trans. Inform. Theory, 49 (2003), pp. 1052-1053.

[20] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, I. North-Holland Publishing Co., Amsterdam-New York-Oxford. North-Holland Mathematical Library, Vol. 16, 1977.

[21] J.L. Massey, *Linear codes with complementary duals*. Discrete Math., 106-107 (1992), pp. 337-342.

[22] N. Sendrier. *Linear codes with complementary dual meet the Gilbert-Varshamov bound*, Discrete Math.,285 (2004), pp. 345-347.

[23] M. Shi, R. Wu, and P. Solé, *Long cyclic codes are good*, arXiv:1709.09865v3.

[24] S.K. Wasan, *Quasi abelian codes*, Publ. Inst. Math., 35 (1977), pp. 201206.

[25] E.J. Weldon, *Long quasi-cyclic codes are good*, IEEE Trans. Inform. Theory, 13 (1970), pp.130.