CONCATENATED STRUCTURE AND CONSTRUCTION OF CERTAIN CODE FAMILIES

by
Elif Saçıkara

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

Sabancı University
2018

CONCATENATED STRUCTURE AND CONSTRUCTION OF CERTAIN CODE FAMILIES

APPROVED BY:

Prof. Dr. Cem Güneri
(Thesis Supervisor) .....

Prof. Dr. Erkay Savaş .....

Assoc. Prof. Dr. Kağan Kurşungöz .....

Prof. Dr. Ferruh Özbudak .....

Dr. Martino Borello .....

DATE OF APPROVAL: 25.07.2018

to my family

Concatenated Structure and Construction of Certain Code Families

Elif Saçıkara

Mathematics, Doctorate Thesis, 2018

Thesis Supervisor: Prof. Dr. Cem Güneri

Keywords: Concatenated codes, generalized concatenated codes, quasi-cyclic codes, generalized quasi-cyclic codes, quasi-abelian codes, linear complementary dual codes, linear complementary pair of codes.

Abstract

In this thesis, we consider concatenated codes and their generalizations as the main tool for two different purposes. Our first aim is to extend the concatenated structure of quasi-cyclic codes to its two generalizations: generalized quasi-cyclic codes and quasi-abelian codes. Concatenated structure have consequences such as a general minimum distance bound. Hence, we obtain minimum distance bounds, which are analogous to Jensen's bound for quasi-cyclic codes, for generalized quasi-cyclic and quasi-abelian codes. We also prove that linear complementary dual quasi-abelian codes are asymptotically good, using the concatenated structure. Moreover, for generalized quasi-cyclic and quasi-abelian codes, we prove, as in the quasi-cyclic codes, that their concatenated decomposition and the Chinese Remainder decomposition are equivalent.

The second purpose of the thesis is to construct a linear complementary pair of codes using concatenations. This class of codes have been of interest recently due to their applications in cryptography. This extends the recent result of Carlet et al. on the concatenated construction of linear complementary dual codes.

Bazı Kod Ailelerinin Birleştirmeli Yapıları ve İnşaları

Elif Saçıkara

Matematik, Doktora Tezi, 2018

Tez Danışmanı: Prof. Dr. Cem Güneri

Anahtar Kelimeler: Birleştirmeli kodlar, genelleştirilmiş birleştirmeli kodlar, sanki devirsel kodlar, genelleştirilmiş sanki devirsel kodlar, sanki değişmeli kodlar, doğrusal bütünleyici dual kodlar, doğrusal bütünleyici kod ikilileri.

Özet

Bu tez çalışmasında birleştirmeli kodlar ve genelleştirmeleri iki ana amaç için kullanılmışlardır. İlk amacımız sanki devirsel kodların birleştirmeli yapılarını, bu kodların iki farklı genellemesi için genişletmektir: genelleştirilmiş sanki devirsel kodlar ve sanki değişmeli kodlar. Birleştirmeli yapının genel minimum uzaklık sınırı gibi sonuçları vardır. Dolayısıyla, genelleştirilmiş sanki devirsel kodlar ve sanki değişmeli kodlar için, Jensen'in sanki devirsel kodlarda elde ettiği sınıra benzer minimum uzaklık sınırları elde edilmiştir. Ayrıca, birleştirmeli yapı kullanılarak, doğrusal bütünleyici dual sanki değişmeli kodların asimptotik olarak iyi oldukları kanıtlanmıştır. Bunlara ek olarak, sanki devirsel kodlarda olduğu gibi, genelleştirilmiş sanki devirsel kodlar ve sanki değişmeli kodların birleştirmeli ayrışmaları ile Çinlilerin Kalan ayrışmalarının denk oldukları gösterilmiştir.

Tezin ikinci amacı, birleştirme kullanarak doğrusal bütünleyici kod ikilileri inşasıdır. Bu kod ailesi son zamanlarda şifrelemedeki uygulamaları sebebiyle ilgi çekmiştir. Bu sonucumuz Carlet ve diğerlerinin birleştirme yoluyla elde ettikleri doğrusal bütünleyici dual kod inşalarını genişletmiştir.

ACKNOWLEDGEMENTS

A Ph.D. student is considered "lucky" if s/he has a chance to work with a professor who is a great researcher and teacher, who is genuinely kind and an understanding, and who encourages their graduate students and makes them smile with his jokes. I feel more than lucky to complete my Ph.D. research under the supervision of Prof. Cem Güneri and I would like to express my deep gratitude to him for his continuous support throughout my Ph.D. journey.

I would also like to thank my jury members Prof. Kağan Kurşungöz, Prof. Erkay Savaş, and my previous committee member Prof. Alev Topuzoğlu. My sincere thanks to Prof. Ferruh Özbudak and Prof. Martino Borello, not only for being my jury members, but also for familiarizing me with the Magma software and for their important contributions to my Ph.D. research. I would also like to thank Prof. Patrick Solé for his guidance and hospitality during my five month research stay at the University of Paris 8, as a visitor within the team MTII (Mathématiques du traitemantde l'Information et de l'Image) of CNRS lab LAGA.

It was a nice experience to take my first steps into the academia as a member of Sabancı University. I would also like to thank my fellow graduate students and all professors in the Department of Mathematics at Sabancı University. I would especially like to thank Prof. Henning Stichtenoth, whose lectures were important to me as a student who changed her research direction from time scale calculus to algebra.

Last but not least, I would like to thank my parents and my brother for their endless love and support. I am fortunate to have Can Deha by my side during almost all of my Ph.D. years, hence my special thanks to him for encouraging me under any condition. Finally, I would like to send my regards to all my friends who have shared my joy and burden throughout this process.

I was supported by The Scientific and Technological Research Council of Turkey

(TÜBİTAK) under the Project Grant 114F432 from September 2016 until December 2017, and 2214/A International Doctoral Research Fellowship Programme from January 2018 till June 2018; thereby I would like to thank TÜBİTAK for their support during the last two years of my Ph.D. research.

Contents

Abstract **v**

Özet **vi**

Acknowledgements **vii**

Introduction **1**

1 Preliminaries **5**

1.1 Linear Codes 5

1.2 Generalized Concatenated Codes 7

1.2.1 Quasi-Cyclic Codes 11

1.2.2 Concatenated Structure of QC Codes 13

1.3 A Variant of Concatenated Codes and Its Generalized Version . . . 15

1.4 Dual of Concatenated Codes 17

2 Generalized Quasi-Cyclic Codes **25**

2.1 Concatenated Structure of GQC codes 28

2.2 Multilevel View of GQC Codes and a Minimum Distance Bound . . 35

3 Quasi-Abelian Codes **39**

3.1 Concatenated Structure of QA Codes 44

3.2 Asymptotic Results on QA Codes 49

4 Linear Complementary Pair of Codes **51**

4.1 Concatenation for LCP of codes 51

4.2 Generalized Concatenation for LCP of codes 53

4.3 Numerical Results 54

Introduction

To obtain a new code either from an old one, or as a combination of two codes is a common technique in algebraic coding theory, and concatenation is one of the methods for this purpose. Defined by Forney ([16]), the idea of concatenation is to construct a new code by combining two component codes. In other words, for an $[N, K, D]$ linear code $\mathcal{C}$ over $\mathbb{F}_{q^k}$, and an $[n, k, d]$ linear code $\mathcal{A}$ over $\mathbb{F}_q$, consider an $\mathbb{F}_q$-linear isomorphism between $\mathbb{F}_{q^k}$ and $\mathcal{A}$. Via this isomorphism, each symbol in $\mathcal{C}$ can be identified by a codeword of $\mathcal{A}$. Carrying out this operation for every codeword of $\mathcal{C}$, a linear code over $\mathbb{F}_q$ with parameters $[nN, kK, D^*]$ can be obtained, where $D^* \geq dD$. Here, $\mathcal{C}$ is called the outer code, $\mathcal{A}$ is called the inner code and the resulting code, which is usually denoted by $\mathcal{A}\square\mathcal{C}$, is the concatenated code.

Later, generalized concatenated codes were introduced by Blokh and Zyablov ([2]), extending the construction of Forney from one inner and one outer code to several inner and outer codes. A generalized concatenated code can be written as a direct sum of "simple" concatenations (in the sense of Forney). Moreover, the minimum distance of a generalized concatenated code is also bounded from below by a quantity determined by the minimum distances of the inner and outer codes in the construction.

A variant of concatenation, among other things, has been introduced by Chen et al. ([10]), where a single outer code $\mathcal{C}$ over $\mathbb{F}_{q^k}$ is considered, but each symbol in a codeword is identified with codewords of varying lengths. Description of the dual code in this construction is also obtained in the same work.

In addition to constructing new codes via concatenation, describing a family of codes, defined by other means, in concatenated form is also of interest. On one hand, a concatenated view yields a general minimum distance bound for the code family in consideration. On the other hand, asymptotic conclusions can be made using the concatenated structure. Moreover, examples of good codes in the family

could be searched using the concatenated structure.

This thesis studies both the concatenated description of certain code families and a concatenated construction of new codes which have applications in cryptography. The content of the thesis comes from parts of three articles, one of which is published ([19]), and the other two are submitted ([3], [20]). Parts of these articles which are not directly related to the concatenation theme are not included in this thesis.

The starting point for this thesis is the family of quasi-cyclic (QC) codes, which is one of the various generalizations of classical cyclic codes. As it is well-known, cyclic codes are one of the central topics in coding theory and their structure is very well-understood. One way of defining algebraically an index ℓ and co-index m QC code over $\mathbb{F}_q$ is to consider $\mathbb{F}_q[C_m]$ submodules in $\mathbb{F}_q[C_m \times C_\ell]$, where C_m and C_ℓ are cyclic groups of order m and ℓ respectively. Note that when $\ell = 1$, one has an ideal in the group algebra $\mathbb{F}_q[C_m]$, which is nothing but a cyclic code of length m. Alternatively, a length $m\ell$ and index ℓ QC code can be viewed as an $\mathbb{F}_q[C_m]$ submodule of $\mathbb{F}_q[C_m]^\ell$.

Two generalizations of QC codes are considered in this thesis. The first of these is the generalized quasi-cyclic (GQC) codes, which are introduced in [15] and in [33]. The main difference is that GQC codes have several co-indices rather than one co-index m as described above for QC codes. Hence, the length of a GQC code need not be a multiple of co-index m (or index ℓ) as in the QC case. In particular, there are GQC codes of prime length.

The second generalization of QC codes we study is quasi-abelian (QA) codes, which are introduced by Wasan ([34]). If G is a finite abelian group and H is a subgroup of index ℓ in G, then an $\mathbb{F}_q[H]$ submodule of $\mathbb{F}_q[G]$ (equivalently, $\mathbb{F}_q[H]$ submodule of $\mathbb{F}_q[H]^\ell$) is a QA code of index ℓ. Note that $H = C_m$ and $G = C_m \times C_\ell$ case amounts to a QC code. As described in Chapter 3, it is also possible to view a QA code in QC form, so they coincide as a class. Let us note that in the study of both QC and QA codes, the order of the group H is assumed to be relatively prime to q (i.e. $\mathbb{F}_q[H]$ is semisimple). This is similar to the assumption usually made on the length of cyclic codes in order to avoid repeated roots (inseparability). Let us note that a special class of QA codes is also studied in [21], which are called multidimensional QC codes, or quasi nD cyclic codes.

The concatenated decomposition of QC codes is given by Jensen ([23]). Another decomposition of QC codes is given by Ling and Solé in [26], which is based on the Chinese Remainder Theorem (so-called CRT decomposition). It is shown in [18] that the CRT components (constituents) of a QC code in the CRT decomposition and the outer codes in its concatenated structure are the same. On the other hand, the CRT decomposition for GQC codes and a CRT type decomposition for QA codes are obtained in [15] and [24], respectively.

Here, we obtain the concatenated description for GQC and QA codes and prove, as in [18], that the concatenated structures are compatible with the CRT or CRT type decompositions of these codes. Hence, consequences of the concatenated structure follow for both code families as a general minimum distance bound. A minimum distance bound on GQC codes is obtained by Esmaeili and Yari ([15]) but it only applies to one generator GQC codes. Our bound applies to all GQC codes. For QA codes, our minimum distance bound is, to the best of our knowledge, the first general minimum distance bound on QA codes. In addition, the concatenated structure of QA codes also allows us to obtain asymptotic results.

The last chapter of the thesis contains our contribution in the direction of construction of codes using concatenation, hence has a different goal compared to the other chapters. Namely, we use concatenation and generalized concatenation to construct linear complementary pair (LCP) of codes. Linear complementary dual (LCD) and LCP of codes have been proposed, in the context of masking schemes, as a protection against side channel and fault injection attacks ([1, 5]). A pair of linear codes $(\mathcal{C}, \mathcal{D})$ of length n over $\mathbb{F}_q$ is called an LCP of codes if they intersect trivially and $\mathcal{C} \oplus \mathcal{D} = \mathbb{F}_q^n$. The security parameter of an LCP of codes is defined as the minimum of $d(\mathcal{C})$ and $d(\mathcal{D}^\perp)$, where the dual is considered with respect to the Euclidean inner product. Let us note that the special case of $\mathcal{D} = \mathcal{C}^\perp$ amounts to LCD codes, where the security parameter simply becomes $d(\mathcal{C})$.

LCD codes have been more extensively studied in the literature compared to LCP of codes. Carlet et al. showed that for $q > 3$ and for any $\mathbb{F}_q$-linear code $\mathcal{C}$, there is an LCD code equivalent to $\mathcal{C}$ ([9]). Hence, the search for LCD and LCP of codes is particularly interesting for binary and ternary fields. Moreover, by a result of Sendrier ([32]), the density of LCD codes over $\mathbb{F}_q$ among all $\mathbb{F}_q$-linear codes is much bigger for large values of q. Hence, it is natural to search for constructions

of LCD and LCP of codes from extension fields to smaller fields. For this purpose, certain concatenation methods are applied in the LCD case ([6, 22]), although the inner codes in these settings are poor (codes of minimum distance 1). Later, Carlet et al. constructed LCD codes via concatenation with potentially better inner codes (so-called isometry codes) in [8] and extended the results in [6, 22].

Here, we extend the result in [8] to LCP of codes. Namely, we obtain an LCP of codes over $\mathbb{F}_q$ from an LCP of codes over an extension field. Moreover, we also provide such a construction via generalized concatenated codes. Hence, our result here differs from the concatenated code constructions in [6, 22, 8]. Let us note that binary LCP QC codes are also studied and constructed in [7] with different methods. To obtain LCD codes via concatenation, a special class of inner codes called isometry codes are used in [8]. In our constructions, we show the existence of linear inner codes that guarantee to carry complementary codes to the base field. Finally, in order to have a generalized concatenated code construction of LCP of codes, we need to describe the dual code for a generalized concatenated code. This was done by Chen et al. in [10] for a simple concatenation (i.e., one inner, one outer code). So, we also extend the result of Chen et al. along the way.

Basic definitions from algebraic coding theory, background material on concatenated codes and their applications to the class of QC codes are presented in Chapter 1. Chapter 1 also contains the description of the dual of generalized concatenated codes, which extends the result of Chen et al. We study GQC codes in Chapter 2 and QA codes in Chapter 3. The final Chapter is on the construction of LCP of codes via concatenation and contains numerical results of this construction.

Chapter 1

Preliminaries

In the beginning of this dissertation, we find it useful to recall some fundamental definitions in algebraic coding theory. Then, we recall the generalized concatenated code construction due to Blokh and Zyablov ([2]). We present its application structural understanding of quasi-cyclic codes, which motivates our work in Chapters 2 and 3. A variant of the concatenation idea, due to Chen et al. [10] is also presented. In the aforementioned work, the authors describe the dual of a concatenated code with only one outer code. We extend the dual description to the generalized concatenated codes with more than one outer code in Section 1.4.

1.1 Linear Codes

In this first section, we briefly review certain well-known definitions in algebraic coding theory. We refer the reader to [29] for further details.

From now on, $\mathbb{F}_q$ denotes a finite field of order q, where q is a prime power, and $\mathbb{F}_q^n$ denotes the n dimensional vector space over $\mathbb{F}_q$ for $n \in \mathbb{Z}^+$. The Hamming distance on $\mathbb{F}_q^n$ is defined as

$$d(x, y) := |\{0 \leq i \leq n-1 : x_i \neq y_i\}|,$$

for vectors $x = (x_0, x_1, \ldots, x_{n-1}), y = (y_0, y_1, \ldots, y_{n-1})$ in $\mathbb{F}_q^n$, where $|.|$ denotes the cardinality of a finite set. Similarly, the Hamming weight of a vector x is defined

as

$$wt(x) := d(x, \mathbf{0}),$$

where $\mathbf{0}$ denotes the zero vector in $\mathbb{F}_q^n$.

A linear code $\mathcal{C}$ is defined to be a subspace in $\mathbb{F}_q^n$. We call $\mathcal{C} \subset \mathbb{F}_q^n$ an $[n, k, d]$ code if it has dimension k and minimum distance d. By the minimum distance, we mean

$$d = d(\mathcal{C}) := \min_{x \neq y} \{d(x, y) : x, y \in \mathcal{C}\},$$

where $d(x, y)$ denotes the Hamming distance. Let us note that the minimum distance of a linear code $\mathcal{C}$ is nothing but the minimum nonzero weight of it, that is

$$d = d(\mathcal{C}) := \min_{x \neq 0} \{wt(x) : x \in \mathcal{C}\}.$$

Each vector in $\mathcal{C}$ is called a codeword in $\mathcal{C}$.

Let us note that the parameters n, k, and d of a linear code $\mathcal{C}$ over $\mathbb{F}_q$ depend upon each other. One of the bounds which explains this dependence is the Griesmer bound, which is stated as

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

for a linear $[n, k, d]$ code $\mathcal{C}$ over $\mathbb{F}_q$ ([17]).

An $[n, k, d]$ code $\mathcal{C}$ is also defined as a row space of a given $k \times n$ full rank matrix and such a matrix is called a generator matrix of $\mathcal{C}$ and denoted by $G_{\mathcal{C}}$.

The (Euclidean) dual of a linear code $\mathcal{C}$ is given by

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}_q^n : \langle x, c \rangle = 0 \text{ for all } c \in \mathcal{C}\},$$

where $\langle c, x \rangle := \sum_{i=0}^{n-1} c_i x_i$ denotes the Euclidean inner product of $x = (x_0, \ldots, x_{n-1})$ and $c = (c_0, \ldots, c_{n-1})$ in $\mathbb{F}_q^n$.

Let $B_q(n, d)$ denote the maximum cardinality of a linear code $\mathcal{C}$ of length n and minimum distance d over $\mathbb{F}_q$. A linear code $\mathcal{C}$ over $\mathbb{F}_q$ of length n and distance d is said to be optimal if it contains exactly $B_q(n, d)$ codewords.

If we consider a family of q-ary linear codes $\{\mathcal{C}_{(n)}\}_{n=1}^{\infty}$ with parameters $[n, k_n, d_n]$, then the relative rate and the relative distance of the family are defined, respec-

tively, as

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

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

A family of q-ary linear codes $\{\mathcal{C}_{(n)}\}_{n=1}^{\infty}$ is called asymptotically good if r and δ are both nonzero. The asymptotic conclusions proved in Section 3.2 are based on this definition.

1.2 Generalized Concatenated Codes

In this section, we recall a generalized concatenated (GC) codes, which are also referred to as multilevel codes, introduced by Blokh and Zyablov, ([2]). Our presentation follows that of Dumer in [14]. The idea of this construction is to extend simple concatenation with one inner and outer code to several outer codes, which are of the same length but defined over possibly different finite extensions of $\mathbb{F}_q$.

Definition 1.2.1. [14] For $i = 1, \ldots, s$, let $\mathcal{C}_i$ be linear codes over $\mathbb{F}_{q^{k_i}}$ of length N and dimension K_i. Consider the set

$$\mathcal{C} := \left\{ c = \begin{pmatrix} c_1^1 & \ldots & c_N^1 \\ \vdots & \vdots & \vdots \\ c_1^s & \ldots & c_N^s \end{pmatrix} : \ (c_1^i, \ldots, c_N^i) \in \mathcal{C}_i \text{ for } 1 \leq i \leq s \right\}. \tag{1.2.1}$$

Denote by $c_1, \ldots, c_N$ the columns of an element c in $\mathcal{C}$ and note that c_j lies in $\mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_s}}$ for all j. Let $\pi : \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_s}} \to \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear injection whose image $\mathcal{A} = im(\pi)$ is a linear code over $\mathbb{F}_q$ of length n and dimension $k_1 + \cdots + k_s$. Then the set

$$\pi(\mathcal{C}) = \{(\pi(c_1), \ldots, \pi(c_N)) : c \in \mathcal{C}\},$$

is called a GC code with outer codes $\mathcal{C}_1, \ldots, \mathcal{C}_s$ and the inner code $\mathcal{A}$.

This concatenation of an inner code $\mathcal{A}$ with outer codes $\mathcal{C}_i$'s is denoted throughout by $\pi(\mathcal{C})$. Let us note that simple concatenation is obtained if we choose a GC

code with only one outer code $\mathcal{C}$, which is denoted by $\mathcal{A}\square\mathcal{C}$.

In the next proposition, we present some properties of a GC code. The proofs are outlined for completeness.

Proposition 1.2.2. *([14])*

Let $\pi(\mathcal{C})$ be a GC code as described above. Then the following conditions hold:

(i) The GC code $\pi(\mathcal{C})$ is a linear code over $\mathbb{F}_q$ with parameters $[nN, \sum_{i=1}^{s} k_i K_i]$.

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

$$\pi(\mathcal{C}) = (\mathcal{A}_1\square\mathcal{C}_1) \oplus \cdots \oplus (\mathcal{A}_s\square\mathcal{C}_s),$$

where $\mathcal{A}_i = \pi(0, \ldots, 0, \mathbb{F}_{q^{k_i}}, 0, \ldots, 0)$ is a k_i-dimensional subcode of $\mathcal{A}$ for all i.

(iii) Conversely, let $\mathcal{A}_i$'s be q-ary linear codes of parameters $[n, k_i, d(\mathcal{A}_i)]$ with $\mathcal{A}_g \cap \sum_{i\neq g} \mathcal{A}_i = \{0\}$, 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 $i, g \in \{1, \ldots, s\}$. Then the direct sum of simple concatenations $\bigoplus_{i=1}^{s} \mathcal{A}_i\square\mathcal{C}_i$ can be described as a GC code.

(iv) If the outer codes are arranged such that $d(\mathcal{C}_1) \leq \cdots \leq d(\mathcal{C}_s)$, then

$$d(\pi(\mathcal{C})) \geq \min\{d(\mathcal{A}_1 \oplus \cdots \oplus \mathcal{A}_i)d(\mathcal{C}_i) : \ i = 1, \ldots, s\}.$$

Proof. (i) Let $\pi(c)$ be a codeword from a GC code which is obtained from an $s \times N$-matrix $c \in \mathcal{C}$. Since there exists N columns in c and the image of each column is a codeword in $\mathcal{A} \subseteq \mathbb{F}_q^n$, the length of $\pi(c)$ is equal to $n \times N$.

On the other hand, injectivity of π yields

$$|\pi(\mathcal{C})| = |\mathcal{C}| = |\mathcal{C}_1| \times \cdots \times |\mathcal{C}_s| = q^{\sum_{i=1}^{s} k_i K_i}.$$

Hence, the dimension of $\pi(\mathcal{C})$ is $\sum_{i=1}^{s} k_i K_i$, which is the sum of dimensions of outer codes over $\mathbb{F}_q$.

(ii) Note that $\mathcal{A} = im(\pi)$ is a linear code with parameters $[n, \sum_{i=1}^{s} k_i, d(\mathcal{A})]$. It

is clear that $\mathcal{A}$ can be written as a direct sum of its subcodes A_i's, where

$$\mathcal{A}_i := im\{\pi(0,\ldots,0,\alpha_i,0,\ldots,0) : \alpha_i \in \mathbb{F}_{q^{k_i}}\}$$

is an $[n, k_i, d(\mathcal{A}_i)]$ code for each i. Since π is an $\mathbb{F}_q$-linear map, for any $(\alpha_1, \alpha_2, \ldots, \alpha_s) \in \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_s}}$, we have

$$\pi(\alpha_1, \alpha_2, \ldots, \alpha_s) = \pi(\alpha_1, 0, \ldots, 0) + \pi(0, \alpha_2, 0, \ldots, 0) + \cdots + \pi(0, 0, \ldots, 0, \alpha_s).$$

Moreover, the image of π has unique such representation for every $(\alpha_1, \alpha_2, \ldots, \alpha_s)$ since π is injective. Using this observation, one can show that any element of $\pi(\mathcal{C})$ is an element of the direct sum of $\mathcal{A}_i \square \mathcal{C}_i$'s. Since these two codes have the same dimension the result follows.

(iii) For $1 \leq i \leq s$, let $\pi_i : \mathbb{F}_{q^{k_i}} \to \mathcal{A}_i$ be the concatenation map for $\mathcal{A}_i \square \mathcal{C}_i$, for each $i = 1, \ldots, s$. If we define $\mathcal{C}$ as in (1.2.1) using $\mathcal{C}_i$'s and set

$$\begin{array}{ccc} \pi : \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_s}} & \longrightarrow & \mathbb{F}_q^n \\ (\alpha_1, \ldots, \alpha_s) & \longmapsto & \pi_1(\alpha_1) + \cdots + \pi_s(\alpha_s) \end{array}, \tag{1.2.2}$$

then the result follows.

(iv) For ease of the notation, we explain how to obtain a lower bound for the minimum distance of a GC code with two outer codes $\mathcal{C}_1$ over $\mathbb{F}_{q^{k_1}}$ and $\mathcal{C}_2$ over $\mathbb{F}_{q^{k_2}}$ under the assumption $d(\mathcal{C}_1) \leq d(\mathcal{C}_2)$. However, the same idea can be extended to arbitrary number of outer codes.

In order to count nonzero components of a codeword $\pi(c) \in \pi(\mathcal{C})$ with a concatenation map $\pi : \mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_1}} \mapsto \mathbb{F}_q^n$, we discuss the following three cases for $c \in \mathcal{C}$.

Case 1: Assume that a nonzero codeword $\pi(c)$ comes from $c \in \mathcal{C}$ in the form of

$$c = \begin{pmatrix} 0 & \ldots & 0 \\ c_1^2 & \ldots & c_N^2 \end{pmatrix},$$

where $(c_1^2, \ldots, c_N^2)$ is a nonzero codeword in $\mathcal{C}_2$. Hence, there exists at least $d(\mathcal{C}_2)$ columns in $c \in \mathcal{C}$. Here, also note that the images of columns in $\mathcal{C}$ under π are codewords in the subcode $\mathcal{A}_2$. Hence the weight of $\pi(c)$ in this case is bounded

from below by $d(\mathcal{C}_2)d(\mathcal{A}_2)$.

Case 2: Following the argument in Case 1, it is easy to see that the image of

$$c = \begin{pmatrix} c_1^1 & \dots & c_N^1 \\ 0 & \dots & 0 \end{pmatrix},$$

under π contains at least $d(\mathcal{C}_1)d(\mathcal{A}_1)$ nonzero entries.

Case 3: Now consider

$$c = \begin{pmatrix} c_1^1 & \dots & c_N^1 \\ c_1^2 & \dots & c_N^2 \end{pmatrix},$$

where both $(c_1^1, \dots, c_N^1)$ and $(c_1^2, \dots, c_N^2)$ are nonzero codewords from $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively. By the assumption $d(\mathcal{C}_1) \leq d(\mathcal{C}_2)$, there exits at least $d(\mathcal{C}_2)$ nonzero columns in c whose images under π belongs to $\mathcal{A}$. Hence, we have $wt(\pi(c)) \geq d(\mathcal{C}_2)d(\mathcal{A})$, where $\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2$.

These three cases cover the type of any codeword $c \in \mathcal{C}$. Hence,

$$wt(\pi(c)) \geq \min\{d(\mathcal{C}_1)d(\mathcal{A}_1), d(\mathcal{C}_2)d(\mathcal{A}_2), d(\mathcal{C}_2)d(\mathcal{A}_1 \oplus \mathcal{A}_2)\}.$$

On the other hand, since $\mathcal{A}_2$ is a subcode of $\mathcal{A}$ we have $d(\mathcal{A}_2) \geq d(\mathcal{A}_1 \oplus \mathcal{A}_2)$. Therefore the weight of a codeword $\pi(c)$, for any $c \in \mathcal{C}$, is at least

$$\min\{d(\mathcal{C}_1)d(\mathcal{A}_1), d(\mathcal{C}_2)d(\mathcal{A}_1 \oplus \mathcal{A}_2)\}.$$

□

Example 1.2.3. Let $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ be a degree 3 extension of the binary field, where α is a root of the irreducible polynomial $x^3 + x + 1$ over $\mathbb{F}_2$. Let $\beta = \{1, \alpha, \alpha^2\}$ be a basis for $\mathbb{F}_2(\alpha)$ over $\mathbb{F}_2$. Consider a GC code with a binary $[2, 2, 1]$ outer code $\mathcal{C}_1$ and an outer code $\mathcal{C}_2$ over $\mathbb{F}_8$ with the generator matrix $[1\ \alpha]$, which is a $[2, 1, 2]$ code.

As a concatenation map, consider an $\mathbb{F}_2$-linear isomorhism π from $\mathbb{F}_2 \times \mathbb{F}_8$ to $\mathbb{F}_2^8$ which maps the elements of the basis $\{(1, 0), (0, 1), (0, \alpha), (0, \alpha^2)\}$ for $\mathbb{F}_2 \times \mathbb{F}_8$

to the rows of the generator matrix

$$G_{\mathcal{A}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

for the linear code $\mathcal{A}$, respectively. By setting $\mathcal{A}_1 := \pi(\mathbb{F}_2 \times \{0\})$, which is the binary repetition code of length 8 and $\mathcal{A}_2 := \pi(\{0\} \times \mathbb{F}_8)$, which is the linear code with the generator matrix

$$G_{\mathcal{A}_2} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{bmatrix},$$

we can observe that the GC code $\pi(\mathcal{C}) = \mathcal{A}_1 \square \mathcal{C}_1 \oplus A_2 \square \mathcal{C}_2$ is a binary linear code of length 16, and of dimension 5. By the minimum distance bound, we have $d(\pi(\mathcal{C})) \geq \min\{d(\mathcal{A}_1)d(\mathcal{C}_1), d(\mathcal{A}_1 \oplus \mathcal{A}_2)d(\mathcal{C}_2)\} = 8$. Let us note that 8 is the best known minimum distance for a linear code of length 16, and of dimension 5, by the Griesmer bound ([17]). Hence, the minimum distance bound is sharp in this example.

1.2.1 Quasi-Cyclic Codes

A linear code over $\mathbb{F}_q$ is said to be a quasi-cyclic (QC) code of index ℓ and length $n = m\ell$, if it is closed under cyclic shifts of its codewords by ℓ units. Hence, QC codes are natural generalizations of cyclic codes, which amounts to the case $\ell = 1$. Recall that a cyclic code of length m also has a description as an ideal in the quotient ring $R := \mathbb{F}_q[x]/\langle x^m - 1\rangle$, which can also be viewed as the group algebra $\mathbb{F}_q[C_m]$ with the cyclic group C_m of order m. Similarly, QC codes can be described in an algebraic way.

For the vectorial view of a QC code $\mathcal{C}$ of index ℓ, and of length $m\ell$, we view

the codewords as $m \times \ell$ matrices as follows

$$c = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix}. \tag{1.2.3}$$

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

For the algebraic description of QC codes, consider the $\mathbb{F}_q$-linear isomorphism

$$\begin{aligned} \phi : \quad & \mathbb{F}_q^{m\ell} & \longrightarrow \quad & R^\ell \\ c = & \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \longmapsto \quad & \vec{c}(x), \end{aligned} \tag{1.2.4}$$

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

$$c_j(x) := c_{0,j} + c_{1,j}x + c_{2,j}x^2 + \cdots + c_{m-1,j}x^{m-1} \in R \tag{1.2.5}$$

for $0 \leq j \leq \ell - 1$.

Observe that componentwise multiplication by x in R^ℓ corresponds to row shift in $\mathbb{F}_q^{m\ell}$. Therefore QC codes, when viewed algebraically in R^ℓ, are nothing but R-submodules in R^ℓ.

One of the decomposition techniques for QC codes of length $m\ell$ and index ℓ over $\mathbb{F}_q$ into shorter codes over extensions of $\mathbb{F}_q$ was given by Ling and Solé ([26]) using the Chinese Remainder Theorem. This decomposition is also called the CRT decomposition. Assume that $\gcd(m, q) = 1$ and factor the polynomial $x^m - 1$ into pairwise distinct irreducible polynomials in $\mathbb{F}_q[x]$ as

$$x^m - 1 = f_1(x)f_2(x)\cdots f_s(x). \tag{1.2.6}$$

Hence, by Chinese Remainder Theorem, we have the following ring isomorphism:

$$R \cong \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle f_i(x)\rangle. \tag{1.2.7}$$

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 (1.2.7) are field extensions of $\mathbb{F}_q$. If $\mathbb{E}_i := \mathbb{F}_q[x]/\langle f_i(x)\rangle$ for $1 \leq i \leq s$, then we have

$$R^\ell \cong \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell. \tag{1.2.8}$$

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

$$\mathcal{C} = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_s, \tag{1.2.9}$$

where $\mathcal{C}_i$ is a linear code of length ℓ over $\mathbb{E}_i$, for each i. These length ℓ linear codes over extensions of $\mathbb{F}_q$ are called the constituents (or, CRT components) of $\mathcal{C}$.

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 it is not difficult to observe from the CRT isomorphism that

$$\mathcal{C}_i = \mathrm{Span}_{\mathbb{E}_i}\big\{\big(a_0^b(\xi^{u_i}), \ldots, a_{\ell-1}^b(\xi^{u_i})\big) : 1 \leq b \leq r\big\}, \text{ for } 1 \leq i \leq s. \tag{1.2.10}$$

1.2.2 Concatenated Structure of QC Codes

We present Jensen's concatenated description of QC codes in this section ([23]). We follow the notation so far.

Let $\mathcal{C}$ be an R-submodule in R^ℓ, where $R = \mathbb{F}_q[x]/\langle x^m - 1\rangle$ for $(m, q) = 1$. Let us recall that

$$R \cong \bigoplus_{i=1}^{s} \mathbb{E}_i, \tag{1.2.11}$$

where $\mathbb{E}_i = \mathbb{F}_q[x]/\langle f_i(x)\rangle$. For each $1 \leq i \leq s$, 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.

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

$$\begin{array}{ccccc} \varphi_i : \langle\theta_i\rangle & \longrightarrow & \mathbb{E}_i & \quad \psi_i : \mathbb{E}_i & \longrightarrow & \langle\theta_i\rangle \\ a(x) & \longmapsto & a(\xi^{u_i}) & \quad \delta & \longmapsto & \sum_{k=0}^{m-1} a_k x^k \end{array} , \tag{1.2.12}$$

where

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

The map ψ_i is commonly called the discrete Fourier transform (DFT). It can be observed that φ_i and ψ_i are inverse to each other. For each i, the concatenation of the minimal cyclic code $\langle\theta_i\rangle$ and a 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, by choosing the DFT ψ_i as a concatenation map, 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.

Theorem 1.2.4. *[23] With the notation so far, the following conditions hold:*

(i) Let $\mathcal{C}$ 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 $\mathcal{C} = \bigoplus_{i=1}^{s} \langle\theta_i\rangle \square \mathfrak{C}_i$.

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

By Proposition 1.2.2, the concatenated view of QC codes leads a general minimum distance bound. So, we give the following corollary without a proof.

Corollary 1.2.5. *Let $\mathcal{C}$ be a QC code of index ℓ with the concatenated structure*

$$\mathcal{C} = \bigoplus_{t=1}^{g} \langle\theta_{i_t}\rangle \square \mathfrak{C}_{i_t},$$

where $\mathfrak{C}_{i_t}$'s are the nonzero outer codes of $\mathcal{C}$ for $\{i_1, \ldots, i_g\} \subseteq \{1, \ldots, s\}$. Assume that $d(\mathfrak{C}_{i_1}) \leq d(\mathfrak{C}_{i_2}) \leq \cdots \leq d(\mathfrak{C}_{i_g})$. Then, we have

$$d(\mathcal{C}) \geq \min_{1 \leq v \leq g} \left\{ d(\mathfrak{C}_{i_v}) d(\langle\theta_{i_1}\rangle \oplus \cdots \oplus \langle\theta_{i_v}\rangle) \right\}.$$

Remark 1.2.6. It is proved in [18] that for a given QC code $\mathcal{C}$, the constituents $\mathcal{C}_i$'s in (1.2.9) and the outer codes $\mathfrak{C}_i$'s in the concatenated structure are equal to each

other (see [18, Theorem 4.1]). In other words, the concatenated decomposition and the CRT decomposition of QC codes are the same.

The concatenated structure of QC codes can be used to give the trace representation of QC codes, using the DFT concatenation maps.

Theorem 1.2.7. *[26, Theorem 5.1] [18, Theorem 4.2] Consider the QC code $\mathcal{C}$ with the constituents (outer codes) $\mathcal{C} = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_s$, where $\mathcal{C}_i \subset \mathbb{E}_i^\ell = \mathbb{F}_q(\xi^{u_i})^\ell$ is linear over $\mathbb{E}_i$ of length ℓ for each $1 \leq i \leq s$. Then an arbitrary codeword $c \in \mathcal{C}$ 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 $\mathcal{C}_i$ 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 $0 \leq k \leq m-1$.

1.3 A Variant of Concatenated Codes and Its Generalized Version

In [10], Chen, Ling and Xing study, among other things, a variant of concatenation. We introduce their concatenation in this Section. Moreover, we define this constructions generalized version, mimicing the GC code construction of Blokh and Zyablov.

Recall that in GC codes, symbols in the codewords of the outer codes are mapped to inner codes of the same length. The main difference here is that there will be inner codes of different lengths. This feature allows us to relax the length of inner codes, so does the length of the resulting concatenated code. Despite the aforementioned differences, we will refer to Chen-Ling-Xing construction as concatenation as well.

Definition 1.3.1. Let $\mathcal{C}$ be a linear code with parameters $[N, K, d(\mathcal{C})]$ over $\mathbb{F}_{q^k}$ for $k \geq 1$. For each $1 \leq i \leq N$, let $n_i \geq k$ and consider an $\mathbb{F}_q$-linear injection $\pi_i : \mathbb{F}_{q^k} \mapsto \mathbb{F}_q^{n_i}$, whose image $\mathcal{A}_i = im(\pi_i)$ is an $[n_i, k, d(\mathcal{A}_i)]$ linear code over $\mathbb{F}_q$. Then the set

$$\pi(\mathcal{C}) = \{(\pi_1(c_1), \ldots, \pi_N(c_N)) : (c_1, \ldots, c_N) \in \mathcal{C}\}, \tag{1.3.1}$$

is called a concatenated code with outer code $\mathcal{C}$, and inner codes $\mathcal{A}_i$'s.

Remark 1.3.2. (i) The concatenated code $\pi(\mathcal{C})$ described above is a linear code of length $\sum_{i=1}^{N} n_i$ and of dimension kK.

(ii) Note that if we choose identical $\mathbb{F}_q$-linear injections π_i's into $\mathbb{F}_q^n$ for each $1 \leq i \leq N$, a simple concatenated code $\pi(\mathcal{C}) = \mathcal{A}\square\mathcal{C}$ is obtained with length nN and dimension kK.

Example 1.3.3. Consider $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, where α is a root of the irreducible polynomial $x^2 + x + 1$ over $\mathbb{F}_2$. Let $\mathcal{C}$ be the $[2, 1, 2]$ linear code over $\mathbb{F}_4$ given as $\mathcal{C} = \{(0, 0), (1, \alpha), (\alpha, \alpha + 1), (\alpha + 1, 1)\}$. Define $\mathbb{F}_2$-linear injections

$$\begin{array}{rcl} \pi_1 : \mathbb{F}_4 & \longrightarrow & \mathbb{F}_2^2 \\ 0 & \longmapsto & (0,0) \\ 1 & \longmapsto & (1,0) \\ \alpha & \longmapsto & (0,1) \\ \alpha+1 & \longmapsto & (1,1) \end{array} \text{ , and } \quad \begin{array}{rcl} \pi_2 : \mathbb{F}_4 & \longrightarrow & \mathbb{F}_2^3 \\ 0 & \longmapsto & (0,0,0) \\ 1 & \longmapsto & (1,0,1) \\ \alpha & \longmapsto & (0,1,1) \\ \alpha+1 & \longmapsto & (1,1,0) \end{array} . \tag{1.3.2}$$

Note that images of π_1 and π_2 are binary codes with parameters $[2, 2, 1]$ and $[3, 2, 2]$, respectively.

If we apply π_1 and π_2 on the first and second coordinates of codewords in $\mathcal{C}$, we obtain the binary linear code

$$\pi(\mathcal{C}) = \{(\underbrace{0,0}_{\pi_1(0)}, \underbrace{0,0,0}_{\pi_2(0)}), (\underbrace{1,0}_{\pi_1(1)}, \underbrace{0,1,1}_{\pi_2(\alpha)}), (\underbrace{0,1}_{\pi_1(\alpha)}, \underbrace{1,1,0}_{\pi_2(\alpha+1)}), (\underbrace{1,1}_{\pi_1(\alpha+1)}, \underbrace{1,0,1}_{\pi_2(1)})\},$$

with parameters $[5, 2, 3]$.

We can extend Chen et al. concatenation in Definition 1.3.1 to a generalized

concatenation. We use the term generalized concatenation for this technique as well. This new construction plays an important role in the concatenated structure of GQC codes in Chapter 2.

Definition 1.3.4. For $i = 1, \ldots, s$, let $\mathcal{C}_i$'s be linear codes with parameters $[N, K_i, d(\mathcal{C}_i)]$ over $\mathbb{F}_{q^{k_i}}$, where $\mathbb{F}_{q^{k_i}}$ is a degree k_i extension of $\mathbb{F}_q$ for each i. Consider the set of $s \times N$- matrices

$$\mathcal{C} := \left\{ c = \begin{pmatrix} c_1^1 & \ldots & c_N^1 \\ \vdots & \ldots & \vdots \\ c_1^s & \ldots & c_N^s \end{pmatrix} : \ (c_1^i, \ldots, c_N^i) \in \mathcal{C}_i \text{ for } 1 \leq i \leq s \right\}. \tag{1.3.3}$$

For each $1 \leq j \leq N$, consider $\mathbb{F}_q$-linear injections $\pi_j : \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_s}} \mapsto \mathbb{F}_q^{n_j}$ whose image $\mathcal{A}_j = im(\pi_j)$ is a linear code with $[n_j, \sum_{i=1}^{s} k_i, d(\mathcal{A}_j)]$ with $k_1 + \ldots + k_s \leq n_j$. Then the set

$$\pi(\mathcal{C}) = \{(\pi_1(c_1), \ldots, \pi_N(c_N)) : c_j\text{'s are columns of } c \in \mathcal{C}, \text{ for } j = 1, \ldots, N\}, \tag{1.3.4}$$

is called a generalized concatenation code with outer codes $\mathcal{C}_i$'s and inner codes A_j's.

Remark 1.3.5. (i) The concatenated code $\pi(\mathcal{C})$ described above is an $\mathbb{F}_q$-linear code of length $\sum_{j=1}^{N} n_j$, and dimension $\sum_{i=1}^{s} k_i K_i$.

(ii) A GC-code in Definition 1.2.1 is obtained when $\pi_1 = \cdots = \pi_N$ and hence $n_1 = \cdots = n_N$.

(iii) A minimum distance bound for this extended concatenation can be obtained with the technique in the proof of Proposition 1.2.2. We will state this in Section 2.2 for GQC codes.

1.4 Dual of Concatenated Codes

The dual of a concatenated code (as in Definition 1.3.1) is described by Chen et al. in [10]. Here, we recall this result and also extend it to the generalized concatenated codes.

The following fact is needed for this description and also for the description

of various concatenations reviewed in Sections 1.2 and 1.3. It is also useful for explicit computations, hence we prove it.

Proposition 1.4.1. *Let $\{a_1, \ldots, a_k\} \subseteq \mathbb{F}_q^n$ be a linearly independent set over $\mathbb{F}_q$. Then there exists a linearly independent set of vectors $\{b_1, \ldots, b_k\} \subseteq \mathbb{F}_q^n$ over $\mathbb{F}_q$ such that*

$$b_j.a_i = \delta_{ij},$$

for all $1 \leq i, j \leq k$. Here, δ_{ij} denotes the Kronecker symbol which is defined as

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}.$$

Proof. For each $1 \leq i \leq k$, define the $\mathbb{F}_q$-linear maps

$$\begin{array}{rccc} \psi_i : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q \\ & x & \longmapsto & x.a_i \end{array}.$$

Linear independence of a_j's implies that $a_i \neq 0$ for all i. Hence, each ψ_i is surjective and if we denote $\mathrm{Ker}(\psi_i)$ by W_i, then $\dim_{\mathbb{F}_q}(W_i) = n - 1$, for all $1 \leq i \leq k$. Moreover, due to linear independence of a_j's again, we also have

$$\dim_{\mathbb{F}_q}(W_{i_1} \cap \ldots \cap W_{i_s}) \;=\; n - s, \tag{1.4.1}$$

for any $s \leq k$ and $\{i_1, \ldots, i_s\} \subseteq \{1, \ldots, k\}$. Therefore,

$$\bigcap_{i \neq j} W_i \not\subseteq W_j$$

for any j, since otherwise we would have (by (1.4.1))

$$n - k = \dim\left(W_j \cap \left(\bigcap_{i \neq j} W_i\right)\right) = \dim\left(\bigcap_{i \neq j} W_i\right) = n - (k - 1).$$

Hence, for each j, there exists a nonzero vector

$$x_j \in \left(\bigcap_{i \neq j} W_i\right) \setminus W_j,$$

which means, by definition of W_j's, that $x_j \cdot a_i = 0$ for all $i \neq j$ and $x_j \cdot a_j = u_j \neq 0$.

Setting $b_j := u_j^{-1}x_j$, we have the desired list of nonzero elements $b_1, \ldots, b_k$.

Suppose β_i's are elements in $\mathbb{F}_q$ such that

$$\beta_1 b_1 + \ldots + \beta_k b_k = 0.$$

Then taking the inner product with a_j for any j, and noting that a_j's and b_i's are all nonzero, we obtain $\beta_j = 0$. Hence, the set $\{b_1, \ldots, b_k\}$ is linearly independent over $\mathbb{F}_q$. □

Now, assume that $\beta = \{e_1, \ldots, e_k\}$ is an ordered basis for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$ and let $\beta' = \{e'_1, \ldots, e'_k\}$ be its dual basis. Recall that this means

$$\mathrm{Tr}_k(e_i.e'_j) = \delta_{ij}, \tag{1.4.2}$$

for $1 \leq i, j \leq k$, where Tr_k denotes the trace map from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$.

Since π is a linear injection, the set $\{\pi(e_1), \ldots, \pi(e_k)\}$ is $\mathbb{F}_q$-independent in $\mathbb{F}_q^n$. Let $b_1, \ldots, b_k$ be an $\mathbb{F}_q$-independent list of elements in $\mathbb{F}_q^n$ as in Proposition 1.4.1. Define another $\mathbb{F}_q$-linear injection π' from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q^n$ by setting $\pi'(e'_j) = b_j$ for all $1 \leq j \leq k$. By construction, we have

$$\pi(e_i).\pi'(e'_j) = \delta_{ij}. \tag{1.4.3}$$

Moreover, $im(\pi^{'})$ can be considered as a linear $[n, k]$ code over $\mathbb{F}_q$, which we will denote by $\mathcal{A}^{'}$. The following is a consequence of (1.4.3) and it is stated in [10, Lemma 2.2].

Lemma 1.4.2. *[10] Let $\beta = \{e_0, \ldots, e_{k-1}\}$ be a basis for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, and let $\beta' = \{e'_1, \ldots, e'_k\}$ be its dual basis. Let $\mathcal{A}$ be a linear code which is generated by the image set $\{\pi(e_1), \ldots, \pi(e_k)\}$ of β under an $\mathbb{F}_q$ linear injection $\pi : \mathbb{F}_{q^k} \mapsto \mathbb{F}_q^n$. Consider a linear code $\mathcal{A}^{'}$, which is generated by the image set $\{\pi^{'}(e_1^{'}), \ldots, \pi^{'}(e_k^{'})\}$, where $\pi^{'} : \mathbb{F}_{q^k} \mapsto \mathbb{F}_q^n$ is a map satisfying*

$$\pi(e_i).\pi'(e'_j) = \delta_{ij}.$$

Then, $\mathcal{A}^{\perp} \cap \mathcal{A}^{'} = \{0\}$.

The next result is due to Chen et al. ([10, Theorem 2.3]) and it uses the

preparation so far to describe the dual of the concatenated code $\pi(\mathcal{C})$.

Theorem 1.4.3. *[10] With the notation so far, the dual of $\pi(\mathcal{C})$ is*

$$\pi(\mathcal{C})^{\perp} = (A\square\mathcal{C})^{\perp} = E \oplus \pi'(\mathcal{C}^{\perp}) = E \oplus (\mathcal{A}'\square\mathcal{C}^{\perp}),$$

where $E = \mathcal{A}^{\perp} \times \cdots \times \mathcal{A}^{\perp} := (\mathcal{A}^{\perp})^N$.

In a similar way, now we extend the dual code of a simple concatenation to concatenations described in Section 1.3. For ease of notation, we will consider $\mathcal{C}$ with two outer codes $\mathcal{C}_1$ and $\mathcal{C}_2$, and we assume that inner codes are of the same length. Hence, we will study an $[nN, k_1K_1 + k_2K_2]$ GC-code $\pi(\mathcal{C}) = (\mathcal{A}_1\square\mathcal{C}_1) \oplus (\mathcal{A}_2\square\mathcal{C}_2)$, where $\mathcal{A}_1, \mathcal{A}_2 \subseteq \mathbb{F}_q^n$. However, our results can be extended to the all variants of concatenations considered in Definition 1.3.4.

Let $\{e_1, \ldots, e_{k_1}\}$ be an ordered basis of $\mathbb{F}_{q^{k_1}}$ and consider its dual basis $\{e'_1, \ldots, e'_{k_1}\}$. Similarly, let $\{f_1, \ldots, f_{k_2}\}$ be an ordered basis of $\mathbb{F}_{q^{k_2}}$ and $\{f'_1, \ldots, f'_{k_2}\}$ be its dual basis. Note that the sets

$$\{(e_1, 0), \ldots, (e_{k_1}, 0), (0, f_1), \ldots, (0, f_{k_2})\},$$

and

$$\{(e'_1, 0), \ldots, (e'_{k_1}, 0), (0, f'_1), \ldots, (0, f'_{k_2})\}$$

are bases for $\mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_2}}$ over $\mathbb{F}_q$. Hence, $\{\pi(e_1, 0), \ldots, \pi(e_{k_1}, 0), \pi(0, f_1), \ldots, \pi(0, f_{k_2})\}$ is linearly independent in $\mathbb{F}_q^n$. If we name $\pi(e_i, 0) = a_i$ for $1 \leq i \leq k_1$ and $\pi(0, f_j) = a_{k_1+j}$ for $1 \leq j \leq k_2$, then by Proposition 1.4.1, there exist linearly independent vectors $b_1, \ldots, b_{k_1}, b_{k_1+1}, \ldots, b_{k_1+k_2}$ in $\mathbb{F}_q^n$ such that $a_u \cdot b_v = \delta_{uv}$ for all $1 \leq u, v \leq k_1 + k_2$.

Define an $\mathbb{F}_q$-linear map $\pi' : \mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_2}} \to \mathbb{F}_q^n$ by setting

$$\pi'(e'_i, 0) = b_i \text{ for } 1 \leq i \leq k_1 \text{ and } \pi'(0, f'_j) = b_{k_1+j} \text{ for } 1 \leq j \leq k_2,$$

and extending linearly. By linear independence of b_i's, the map π' is an $\mathbb{F}_q$-linear injection and by construction we have

$$\begin{aligned} \pi(e_i, 0) \cdot \pi'(e'_u, 0) &= \delta_{iu}, \\ \pi(0, f_j) \cdot \pi'(e'_u, 0) &= 0, \end{aligned} \tag{1.4.4}$$

and

$$\begin{aligned} \pi(e_i, 0) \cdot \pi'(0, f'_v) &= 0, \\ \pi(0, f_j) \cdot \pi'(0, f'_v) &= \delta_{jv}, \end{aligned} \tag{1.4.5}$$

for all i, j, u, v. Let us denote the image of π' by $\mathcal{A}'$, which is an $\mathbb{F}_q$-linear code of length n and dimension $k_1 + k_2$.

Consider the set

$$\bar{\mathcal{C}} := \left\{ c = \begin{pmatrix} c_1^1 & \dots & c_N^1 \\ c_1^2 & \dots & c_N^2 \end{pmatrix} : \ (c_1^i, \dots, c_N^i) \in \mathcal{C}_i^{\perp} \text{ for } i = 1, 2 \right\}, \tag{1.4.6}$$

and the GC-code

$$\pi'(\bar{\mathcal{C}}) = \{(\pi'(c_1), \dots, \pi'(c_N)) : c \in \bar{\mathcal{C}}\} \text{ (cf. Definition 1.2.1)},$$

which is a linear code over $\mathbb{F}_q$ of length nN and dimension $k_1.(N-K_1)+k_2.(N-K_2)$. Note that $\pi'(\bar{\mathcal{C}})$ can also be written in the form of $(\mathcal{A}'_1 \square \mathcal{C}_1^{\perp}) \oplus (\mathcal{A}'_2 \square \mathcal{C}_2^{\perp})$, where $\mathcal{A}'_1 = \pi'(\mathbb{F}_{q^{k_1}}, 0)$ and $\mathcal{A}'_2 = \pi'(0, \mathbb{F}_{q^{k_2}})$ are subcodes of $\mathcal{A}'$.

The following is a generalization of Lemma 1.4.2.

Lemma 1.4.4. *Let β be a basis for $\mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_2}}$ and β' be its dual basis. Let $\mathcal{A} = im\pi$ and $\mathcal{A}' = im\pi'$ be linear codes which are generated by the images of the elements of the basis β and its dual β' under $\mathbb{F}_q$-linear injections π and π', respectively, which are introduced as in the equations 1.4.4 and 1.4.5. Then $\mathcal{A}^{\perp} \cap \mathcal{A}' = \{0\}$.*

Proof. Let x be an element in $\mathcal{A}^{\perp} \cap \mathcal{A}'$ and write it as $x = \pi'(\alpha, \beta)$ for $(\alpha, \beta) \in \mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_2}}$. Let

$$\alpha = \sum_{j=1}^{k_1} \alpha_j e'_j \text{ and } \beta = \sum_{j=1}^{k_2} \beta_j f'_j,$$

where $\alpha_j, \beta_j \in \mathbb{F}_q$, so that

$$x = \pi'(\alpha, \beta) = \sum_{j=1}^{k_1} \alpha_j \pi'(e'_j, 0) + \sum_{j=1}^{k_2} \beta_j \pi'(0, f'_j).$$

Since x belongs to $\mathcal{A}^{\perp}$, we also have $\pi(a, b) \cdot \pi'(\alpha, \beta) = 0$ for any $(a, b) \in \mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_2}}$.

In particular

$$\begin{aligned} \pi(e_i, 0) \cdot \pi'(\alpha, \beta) &= \alpha_i = 0, \\ \pi(0, f_i) \cdot \pi'(\alpha, \beta) &= \beta_i = 0, \end{aligned}$$

for all $1 \leq i \leq k_1$ and $1 \leq j \leq k_2$ (by (1.4.4) and (1.4.5)). Hence $x = 0$. □

We are ready to describe the dual of a GC code.

Theorem 1.4.5. *With the notation so far, the dual of $\pi(\mathcal{C})$ is*

$$\pi(\mathcal{C})^{\perp} = E \oplus \pi'(\bar{\mathcal{C}}),$$

where $E = \mathcal{A}^{\perp} \times \cdots \times \mathcal{A}^{\perp} = (\mathcal{A}^{\perp})^N$.

Proof. Note that $\pi(\mathcal{C})$ is an $[nN, k_1K_1 + k_2K_2]$ code in ${\mathbb{F}_q}^{nN}$. Hence we have

$$\dim_{\mathbb{F}_q} \pi(\mathcal{C})^{\perp} = nN - (k_1K_1 + k_2K_2). \tag{1.4.7}$$

Moreover,

$$\dim_{\mathbb{F}_q} E = N(n-(k_1+k_2)) \text{ and } \dim_{\mathbb{F}_q} \pi'(\bar{\mathcal{C}}) = k_1(N-K_1)+k_2(N-K_2). \tag{1.4.8}$$

By (1.4.7) and (1.4.8), we have

$$\dim_{\mathbb{F}_q} \pi(\mathcal{C})^{\perp} = \dim_{\mathbb{F}_q} E + \dim_{\mathbb{F}_q} \pi'(\bar{\mathcal{C}}). \tag{1.4.9}$$

Since $\pi(\mathcal{C}) \subseteq \mathcal{A} \times \cdots \times \mathcal{A}$, we clearly have

$$E = \mathcal{A}^{\perp} \times \cdots \times \mathcal{A}^{\perp} \subseteq \pi(\mathcal{C})^{\perp}. \tag{1.4.10}$$

Let $\pi'(c) = (\pi'(c_1), \ldots, \pi'(c_N)) \in \pi'(\bar{\mathcal{C}})$, with $c = \begin{bmatrix} c_1^1 \ldots c_N^1 \\ c_1^2 \ldots c_N^2 \end{bmatrix} \in \bar{\mathcal{C}}$, where the first row is a codeword in $\mathcal{C}_1^{\perp}$ and the second row is a codeword in $\mathcal{C}_2^{\perp}$. Let $\pi(x) = (\pi(x_1), \ldots, \pi(x_N))$ be an arbitrary element of $\pi(\mathcal{C})$, where $x = \begin{bmatrix} x_1^1 \ldots x_N^1 \\ x_1^2 \ldots x_N^2 \end{bmatrix} \in \mathcal{C}$ whose first row is in $\mathcal{C}_1$ and the second row is in $\mathcal{C}_2$. With our earlier notation for

bases of $\mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_2}}$, we can write

$$x_g^1 = \sum_{i=1}^{k_1} x_{g,i}^1 e_i \text{ and } c_g^1 = \sum_{j=1}^{k_1} c_{g,j}^1 e'_j \text{ in } \mathbb{F}_{q^{k_1}},$$
$$x_g^2 = \sum_{s=1}^{k_2} x_{g,s}^2 f_s \text{ and } c_g^2 = \sum_{t=1}^{k_2} c_{g,t}^2 f'_t \text{ in } \mathbb{F}_{q^{k_2}},$$

where $x_{g,i}^1, x_{g,s}^2, c_{g,j}^1, c_{g,t}^2$ are elements in $\mathbb{F}_q$ for all $g \in \{1, \ldots, N\}$. Then we have

$$\begin{aligned}
\pi(x) \cdot \pi'(c) &= \sum_{g=1}^{N} \pi(x_g^1, x_g^2) \cdot \pi'(c_g^1, c_g^2) \\
&= \sum_{g=1}^{N} (\pi(x_g^1, 0) + \pi(0, x_g^2)) \cdot (\pi'(c_g^1, 0) + \pi'(0, c_g^2)) \\
&= \sum_{g=1}^{N} \left(\left[\sum_{i=1}^{k_1} x_{g,i}^1 \pi(e_i, 0) + \sum_{s=1}^{k_2} x_{g,s}^2 \pi(0, f_s) \right] \cdot \left[\sum_{j=1}^{k_1} c_{g,j}^1 \pi'(e'_j, 0) + \sum_{t=1}^{k_2} c_{g,t}^2 \pi'(0, f'_t) \right] \right) \\
&= \sum_{g=1}^{N} (\sum_{i=1}^{k_1} x_{g,i}^1 c_{g,i}^1 + \sum_{s=1}^{k_2} x_{g,s}^2 c_{g,s}^2) \quad \text{(by (1.4.4) and (1.4.5))}
\end{aligned}$$

On the other hand, we have $x^1 \cdot c^1 = x_1^1 c_1^1 + \cdots + x_N^1 c_N^1 = 0$, since $x^1 \in \mathcal{C}_1$ and $c^1 \in \mathcal{C}_1^\perp$. Hence

$$\begin{aligned}
0 &= \mathrm{Tr}_{k_1}(x_1^1 c_1^1) + \cdots + \mathrm{Tr}_{k_1}(x_N^1 c_N^1) \\
&= \mathrm{Tr}_{k_1}\left(\left(\sum_{i=1}^{k_1} x_{1,i}^1 e_i \right) \left(\sum_{j=1}^{k_1} c_{1,j}^1 e'_j \right) \right) + \cdots + \mathrm{Tr}_{k_1}\left(\left(\sum_{i=1}^{k_1} x_{N,i}^1 e_i \right) \left(\sum_{j=1}^{k_1} c_{N,j}^1 e'_j \right) \right) \\
&= \left(x_{1,1}^1 c_{1,1}^1 + \cdots + x_{1,k_1}^1 c_{1,k_1}^1 \right) + \cdots + \left(x_{N,1}^1 c_{N,1}^1 + \cdots + x_{N,k_1}^1 c_{N,k_1}^1 \right),
\end{aligned}$$

where the last equality follows from the duality of the bases of $\mathbb{F}_{q^{k_1}}$ ((1.4.2)). One can similarly conclude that

$$\left(x_{1,1}^2 c_{1,1}^2 + \cdots + x_{1,k_2}^2 c_{1,k_2}^2 \right) + \cdots + \left(x_{N,1}^2 c_{N,1}^2 + \cdots + x_{N,k_2}^2 c_{N,k_2}^2 \right) = 0.$$

Hence we have

$$\pi'(\bar{\mathcal{C}}) \subseteq \pi(\mathcal{C})^\perp \tag{1.4.11}$$

Combining Equations 1.4.9, 1.4.10 and 1.4.11, it only remains to show that $E \cap \pi'(\bar{\mathcal{C}})$

is trivial. This follows from Lemma 1.4.4 since $\pi'(\bar{\mathcal{C}})$ lies in $(\mathcal{A}')^N$. $\square$

Chapter 2

Generalized Quasi-Cyclic Codes

In this chapter we present the concatenated structure of generalized QC (GQC) codes and its consequences. The work in this chapter appeared in [19]. Let us note that the article [19] also contains results on characterization of self-dual and linear complementary dual GQC codes, and asymptotic conclusions which are not presented here.

GQC codes were introduced in [33], where their description is given as follows.

Definition 2.0.1. 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.

The factorization of GQC codes into constituents, analogue of which is presented for QC codes in Section 1.2.1, is given by Esmaeili and Yari in [15]. We will review this decomposition and introduce a notation which is suitable for presentation of our results in the next section.

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

$$x^{m_j} - 1 = f_1(x)^{v_{1,j}} f_2(x)^{v_{2,j}} \cdots f_s(x)^{v_{s,j}}, \tag{2.0.1}$$

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

$$\mathbb{E}_{i,j} := \begin{cases} \mathbb{E}_i, \text{ if } v_{i,j} = 1, \\ \{0\}, \text{ if } v_{i,j} = 0. \end{cases} . \tag{2.0.2}$$

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

$$a_{i,j} = \begin{cases} a(\alpha_i), \text{ if } \mathbb{E}_{i,j} = \mathbb{E}_i, \\ 0, \qquad \text{if } \mathbb{E}_{i,j} = \{0\}. \end{cases} \tag{2.0.3}$$

By (2.0.1), (2.0.2) and the Chinese Remainder Theorem, we get the following ring isomorphism for each $j = 0, \ldots, \ell - 1$:

$$R_j \cong \bigoplus_{i=1}^{s} \mathbb{E}_{i,j}, \tag{2.0.4}$$

where the isomorphism maps $a(x) \in R_j$ to $(a_{1,j} + \cdots + a_{s,j})$ (cf. (2.0.3)). Therefore we have

$$R' = R_0 \times \cdots \times R_{\ell-1} \cong \left(\bigoplus_{i=1}^{s} \mathbb{E}_{i,0}\right) \times \cdots \times \left(\bigoplus_{i=1}^{s} \mathbb{E}_{i,\ell-1}\right) \cong \bigoplus_{i=1}^{s} (\mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}), \tag{2.0.5}$$

where $\big(a^0(x), \ldots, a^{\ell-1}(x)\big) \in R'$ is mapped to $\sum_{i=1}^{s} \big(a^0_{i,0}, a^1_{i,1}, \ldots, a^{\ell-1}_{i,\ell-1}\big)$. In particular, a GQC code $\mathcal{C} \subset R'$ 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 2.0.2. *Suppose the GQC code $\mathcal{C} \subset R'$ is generated as an $\mathbb{F}_q[x]$-module by*

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

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

$$\mathcal{C} = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_s, \tag{2.0.6}$$

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

$$\mathcal{C}_i = Span_{\mathbb{E}_i}\left\{\left(a_{i,0}^{b,0},\ldots,a_{i,\ell-1}^{b,\ell-1}\right) : 1 \le b \le r\right\},\ \textit{for } 1 \le i \le s. \tag{2.0.7}$$

Proof. Observe that $\mathcal{C}$, as a subset of R', can be written as

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

Then by (2.0.5), $\mathcal{C}_i$ is of the form

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

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 2.0.3. Depending on $v_{i,j}$'s in the factorization (2.0.1), 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 2.0.4. 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 (2.0.2), 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 $\mathcal{C} \subset R'$ is a GQC code generated by $\langle \vec{g}_1(x), \ldots, \vec{g}_r(x) \rangle$, where

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

then $\mathcal{C}$ has the following constituents:

$$\begin{aligned}
\mathcal{C}_1 &= \mathrm{Span}_{\mathbb{F}_2} \left\{ \left(g^{b,0}(1), g^{b,1}(1), g^{b,2}(1)\right) \ : \ 1 \leq b \leq r \right\}, \\
\mathcal{C}_2 &= \mathrm{Span}_{\mathbb{F}_4} \left\{ \left(g^{b,0}(\alpha_2), 0, g^{b,2}(\alpha_2)\right) \ : \ 1 \leq b \leq r \right\}, \\
\mathcal{C}_3 &= \mathrm{Span}_{\mathbb{F}_{16}} \left\{ \left(0, g^{b,1}(\alpha_3), 0\right) \ : \ 1 \leq b \leq r \right\}, \\
\mathcal{C}_4 &= \mathrm{Span}_{\mathbb{F}_{64}} \left\{ \left(0, 0, g^{b,2}(\alpha_4)\right) \ : \ 1 \leq b \leq r \right\}.
\end{aligned}$$

2.1 Concatenated Structure of GQC codes

Our goal is to obtain, as in the QC codes (Section 1.2.2), 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:

$$I_{i,j} := \begin{cases} \theta_{i,j}(x), & \text{if } f_i(x) \mid x^{m_j} - 1, \\ 0_j & \text{otherwise.} \end{cases} \tag{2.1.1}$$

Now, we can define the following analogues of the maps in (1.2.12) for each

block of length m_j and each $1 \leq i \leq s$:

$$\begin{array}{rccc} \varphi_{i,j}: & \langle I_{i,j} \rangle & \longrightarrow & \mathbb{E}_{i,j} \\ & a(x) & \longmapsto & a_{i,j} \end{array} \qquad \begin{array}{rccc} \psi_{i,j}: & \mathbb{E}_{i,j} & \longrightarrow & \langle I_{i,j} \rangle \\ & \delta & \longmapsto & \sum_{k_j=0}^{m_j-1} a_{k_j} x^{k_j} \end{array}, \tag{2.1.2}$$

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 (1.2.12) 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

$$1_{i,j} := \begin{cases} 1_{\mathbb{E}_i}, & \text{if } \mathbb{E}_{i,j} = \mathbb{E}_i, \\ 0, & \text{if } \mathbb{E}_{i,j} = \{0\}. \end{cases} \tag{2.1.3}$$

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. (2.0.3) and (2.1.2)).

$$\begin{array}{rccc} \Phi_i: & R_0 \times \cdots \times R_{\ell-1} & \longrightarrow & \mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1} \\ & \left(a^0(x), \ldots, a^{\ell-1}(x)\right) & \longmapsto & \left(a_{i,0}^0, \ldots, a_{i,\ell-1}^{\ell-1}\right) \end{array} \tag{2.1.4}$$

$$\begin{array}{rccc} \Psi_i: & \mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1} & \longrightarrow & R_0 \times \cdots \times R_{\ell-1} \\ & (\delta_0, \ldots, \delta_{\ell-1}) & \longmapsto & (\psi_{i,0}(\delta_0), \ldots, \psi_{i,\ell-1}(\delta_{\ell-1})) \end{array} \tag{2.1.5}$$

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. (2.1.2)). 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. [29,

Theorem 6.4.4]). Recall that the multiplication and addition in R' are coordinate-wise.

Lemma 2.1.1. *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 2.1.2. *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, $\Psi_i(\mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}) = \langle I_i \rangle$ and

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

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 2.1.3. 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 (2.1.5). Namely,

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

After this preparation, we can now generalize Theorem 1.2.4 for a GQC code $\mathcal{C} \subset R'$ of length $m_0 + \cdots + m_{\ell-1}$ over $\mathbb{F}_q$.

Theorem 2.1.4. *With the notation so far, the following conditions hold:*

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

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

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

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

(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, $\mathcal{C} = \bigoplus_{i=1}^{s} \langle I_i \rangle \square \mathfrak{C}_i$ is a q-ary GQC code of length $m_0 + \cdots + m_{\ell-1}$.

Proof. (i) By Lemma 2.1.1, we have

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

Since $\tilde{\mathcal{C}}_i \subset \langle I_i \rangle$ for each i and $\langle I_i \rangle$'s are pairwise intersecting trivially (Theorem 2.1.2), we conclude that $\mathcal{C} = \oplus_i \tilde{\mathcal{C}}_i$.

We have

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

Since Φ_i restricted to $\langle I_i \rangle$ is an isomorphism ((2.1.4) and (2.1.5)), the last expression is equal to

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

which is nothing but $\langle I_i \rangle \square \Phi_i(\tilde{C}_i)$ (cf. (Remark 2.1.3).

(ii) The concatenation has the form

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

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 (2.1.2) 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 2.1.5. Note from the proof of Theorem 2.1.4 (i) that the outer codes of the GQC code $\mathcal{C}$ are of the form (for each $1 \leq i \leq s$):

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

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 $\mathcal{C}$ of $\mathcal{C}$ (Proposition 2.0.2). Hence, the analogous result for QC codes extends to GQC codes.

As in Theorem 1.2.7, we can obtain a trace representation for the codewords of a given GQC code, which is straightforward by using the isomorphism (concatenation map) in (2.1.5).

Theorem 2.1.6. *Consider the q-ary GQC code $\mathcal{C}$ of length $m_0 + \cdots + m_{\ell-1}$ with the constituents $\mathcal{C} = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_s$, where $\mathcal{C}_i \subset \mathbb{E}_i^\ell$ is linear over $\mathbb{E}_i$ of length ℓ for each $1 \leq i \leq s$. 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 $c \in \mathcal{C}$ 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 $\mathcal{C}$, 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 2.1.7. Note that for $m_0 = \cdots = m_{\ell-1}$, this coincides with the trace representation of a length $m\ell$ QC code (cf. Theorem 1.2.7). However, the trace representation in Theorem 1.2.7 describes codewords by their rows whereas Theorem 2.1.6 provides a column-wise description of codewords in a GQC code.

Example 2.1.8. Let $m_0 = 3$, $m_1 = 5$ and $q = 2$. We will consider a binary GQC code $\mathcal{C}$ 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

$$x^3 - 1 = (x+1)(x^2 + x + 1) \qquad x^5 - 1 = (x+1)(x^4 + x^3 + x^2 + x + 1). \quad (2.1.6)$$

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 (2.1.6), respectively. Let $\mathcal{C}_1 \subseteq \mathbb{F}_2^2$, $\mathcal{C}_2 \subseteq \mathbb{F}_4^2$, $\mathcal{C}_3 \subseteq \mathbb{F}_{16}^2$ be the constituents of $\mathcal{C}$. Note that the second (first) coordinate of every codeword in $\mathcal{C}_2$ (in $\mathcal{C}_3$) 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 2.1.6, the codewords of $\mathcal{C}$ are of the form (cf. Theorem 6.7 and 6.14 in [26])

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

where $(z_1, z_2) \in \mathcal{C}_1$, $a + \xi_1 b \in \mathcal{C}_2$ $(a, b \in \mathbb{F}_2)$ and $y \in \mathcal{C}_3$.

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 $(z_1, z_2) \in \mathcal{C}_1$, $a + \xi_1 b \in \mathcal{C}_2$ and $c + \xi_2 d + \xi_2^2 e + \xi_2^3 f \in \mathcal{C}_3$.

2.2 Multilevel View of GQC Codes and a Minimum Distance Bound

Our goal is to adapt the multilevel concatenated approach to GQC codes and to obtain a minimum distance bound as Jensen did for QC codes (cf. Section 1.2.2). For this purpose, we adapt a variant of concatenation introduced in Section 1.3 (see Definition 1.3.4) to GQC codes. We continue with the notation introduced so far in this chapter.

Let $\mathcal{C}$ be a q-ary GQC code of length $m_0 + \cdots + m_{\ell-1}$ with the outer codes (or constituents) $\mathcal{C}_1, \ldots, \mathcal{C}_s$. Recall that $\mathcal{C}_i \subset \mathbb{E}_{i,0} \times \cdots \times \mathbb{E}_{i,\ell-1}$ is an $\mathbb{E}_i$-linear code of length ℓ for each i. Consider the following set:

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

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 $|B| = \prod_{i=1}^{s} |\mathcal{C}_i|$. 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 (2.1.2) as a concatenation map to define the following $\mathbb{F}_q$-linear isomorphisms:

$$\begin{array}{rcccl} \psi_j & : & \mathbb{E}_{1,j} \times \cdots \times \mathbb{E}_{s,j} & \to & \langle I_{1,j} \rangle \oplus \cdots \oplus \langle I_{s,j} \rangle \subset R_j \\ & & (a_{1,j}, \ldots, a_{s,j}) & \mapsto & \psi_{1,j}(a_{1,j}) + \cdots + \psi_{s,j}(a_{s,j}) \end{array} \tag{2.2.1}$$

By Definition 1.3.4, the multilevel concatenated code is defined as

$$\psi(B) := \left\{ \Big(\psi_0 \left(c_{1,0}, \ldots, c_{s,0}\right), \ldots, \psi_{\ell-1} \left(c_{1,\ell-1}, \ldots, c_{s,\ell-1}\right) \Big) : \begin{pmatrix} c_{1,0} & \ldots & c_{1,\ell-1} \\ \vdots & \vdots & \vdots \\ c_{s,0} & \ldots & c_{s,\ell-1} \end{pmatrix} \in B \right\}. \tag{2.2.2}$$

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 $\dim_{\mathbb{F}_q} \psi(B) = \sum_{i=1}^{s} \dim_{\mathbb{F}_q} \mathcal{C}_i = \dim_{\mathbb{F}_q} \mathcal{C}$.

Proposition 2.2.1.

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

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 $\bigoplus_{i=1}^{s} \langle I_i \rangle \square \mathcal{C}_i$ (cf. Proposition 1.2.2), hence $\psi(B) \subseteq \bigoplus_{i=1}^{s} \langle I_i \rangle \square \mathcal{C}_i$. The result follows since both codes have the same $\mathbb{F}_q$-dimension. □

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

Theorem 2.2.2. *Let $\mathcal{C}$ be a GQC code with nonzero constituents $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_g}$, where $\{i_1, \ldots, i_g\} \subseteq \{1, \ldots, s\}$. Let d_u denote the minimum distance of $\mathcal{C}_{i_u}$, for each $1 \leq u \leq g$ and assume that $d_1 \leq d_2 \leq \cdots \leq d_g$. 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 $1 \leq u \leq g$, *then*

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

Proof. Codewords in B have g rows coming from the constituents of $\mathcal{C}$. 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 $0 \leq t_1, \ldots, t_{d_u} \leq \ell - 1$ denotes nonzero columns of b, then $\Psi(b) = \big(\psi_0(b_0), \ldots, \psi_{\ell-1}(b_{\ell-1})\big)$ lies in

$$\Big(\langle I_{i_1,t_1}\rangle \oplus \cdots \oplus \langle I_{i_u,t_1}\rangle\Big) \times \cdots \times \Big(\langle I_{i_1,t_{d_u}}\rangle \oplus \cdots \oplus \langle I_{i_u,t_{d_u}}\rangle\Big) \text{ (cf. (2.2.1) and (2.2.2))}.$$

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. $\mathcal{C}$) have weights greater than or equal to D_u. Applying the same argument with each $u = 1, \ldots, g$, we see that codewords of $\mathcal{C}$ 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 $\mathcal{C}$, 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 $\mathcal{C}$ 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 $w(c) \geq D_{\mu_e} \geq D$. Therefore D is a lower bound for the weights of all codewords in $\mathcal{C}$. $\square$

Remark 2.2.3. Suppose $\mathcal{C}$ is a QC code with nonzero constituents $\mathcal{C}_{i_1}, \ldots, \mathcal{C}_{i_g}$, whose minimum distances are ordered as in Theorem 2.2.2. If $\mathcal{C}$ 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 1.2.2). Then for any $J \subset \{0, 1, \ldots, \ell-1\}$ with $|J| = d(\mathcal{C}_{i_u})$, we have

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

Hence the bound in Theorem 2.2.2 takes the form

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

for a QC code $\mathcal{C}$, which is exactly Jensen's bound (cf. Corollary 1.2.5; also see [23, Theorem 4], [18, Theorem 3.3]).

Remark 2.2.4. Esmaeili and Yari also found a minimum distance bound for GQC codes but their bound only applies to one-generator GQC codes ([15, Theorem 4]).

Chapter 3

Quasi-Abelian Codes

This chapter contributes to the structural understanding of quasi-abelian (QA) codes by giving their concatenated structure, presenting the relation of this structure with earlier decomposition of QA codes by Jitman and Ling ([24]), and consequences of the concatenated structure. The material in this chapter appears in [3]. Let us note that [3] also contains numerical results for examples of QA codes and the relation of QA codes to the so-called additive abelian codes, which are not presented here.

We first review basic facts on QA codes, following [24] closely (see also [12]). We refer the reader to these articles for further details. Let us note that in the special case of QC codes, the material presented in this chapter has analogues which are presented in Sections 1.2.1 and 1.2.2.

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.

For an element $v = \sum_{g\in G} v_g Y^g \in \mathbb{F}_q[G]$, the Hamming weight of v is defined to be the number of nonzero terms v_g and it is denoted by $\mathrm{wt}(v)$. As usual, the minimum distance of $\mathcal{C}$ is defined by

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

Definition 3.0.1. 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.

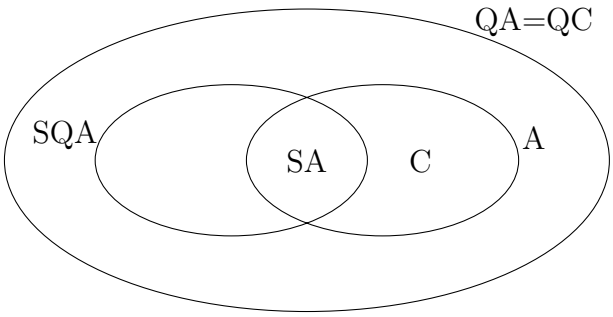
Let $\{g_1, \ldots, g_\ell\}$ be a fixed set of representatives of the cosets of H in G. Note that a QA code of index ℓ in $\mathbb{F}_q[G]$ can be seen as an $\mathbb{F}_q[H]$-submodule of $\mathbb{F}_q[H]^\ell$ by the following $\mathbb{F}_q[H]$-module isomorphism.

$$\begin{array}{ccccc} \Phi : & \mathbb{F}_q[G] & \longrightarrow & \mathbb{F}_q[H]^\ell & \\ & \displaystyle\sum_{i=1}^{\ell}\sum_{h\in H}\alpha_{h+g_i}Y^{h+g_i} & \longmapsto & \left(\displaystyle\sum_{h\in H}\alpha_{h+g_1}Y^h, \ldots, \sum_{h\in H}\alpha_{h+g_\ell}Y^h\right). \end{array} \tag{3.0.1}$$

Remark 3.0.2. It is clear that an H-QA code is QC if H is cyclic. Moreover, if $H = J \times K$ with $|K| = t$ and J is cyclic, then an H-QA code of index ℓ is a QC code of index $t \cdot \ell$. By Fundamental Theorem of finite abelian group, every abelian group H can be decomposed in such a way, so that the class of QA codes is a subclass of QC codes. For instance, if we choose $H = C_{m_1} \times C_{m_2}$, here C_{m_i}'s denote cyclic group $\mathbb{Z}/m_i\mathbb{Z}$ of order m_i, for $i = 1, 2$, such a 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 [23] and [21] 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 ([24]) call a QA code $\mathcal{C}$ strictly QA (SQA) if H is not a cyclic group. If H is a cyclic group then such a code has only one way of QC structure. Correspondingly, if $\ell = 1$ and H is not cyclic, we refer to strictly abelian (SA) codes.

The following diagram shows the relations among the families of codes that are discussed above. Here, A and C denote abelian codes and cyclic codes, respectively.



We find it useful to illustrate with a very explicit example how QA codes can be seen as QC codes.

Example 3.0.3. Let $H := C_2 \times C_2 = \{(0,0),(1,0),(0,1),(1,1)\}$. Consider an H-QA code of index 2, $\mathcal{C} \subseteq \mathbb{F}_q[C_2 \times C_2]^2$ with

$$\mathbb{F}_q[C_2 \times C_2] := \{a := a_0(0,0) + a_1(1,0) + a_2(0,1) + a_3(1,1) : a_i \in \mathbb{F}_q \text{ for } 0 \leq i \leq 3\},$$

where q is any odd prime power. Choose representatives $(0,0)$ and $(0,1)$ of the cosets of $C_2 \times \{0\}$ in $C_2 \times C_2$, and identify $C_2 \times \{0\}$ with C_2 in the following. Then by (3.0.1), we have the following $\mathbb{F}_q[C_2]$-module isomorphism:

$$\begin{aligned} \varphi : \ \mathbb{F}_q[C_2 \times C_2]^2 &\longrightarrow \mathbb{F}_q[C_2]^4 \\ (a,b) &\longmapsto (a_0(0,0) + a_1(1,0), a_2(0,1) + a_3(1,1), \\ &\qquad b_0(0,0) + b_1(1,0), b_2(0,1) + b_3(1,1)) \,. \end{aligned} \tag{3.0.2}$$

The image $\varphi(\mathcal{C})$ is clearly an $\mathbb{F}_q[C_2]$-module since (3.0.2) is an $\mathbb{F}_q[C_2]$-module isomorphism. Hence, $\varphi(\mathcal{C})$ is an index 4 and co-index 2 QC code over $\mathbb{F}_q$. Moreover, being closed under multiplication by $(0,1)$ in $\mathbb{F}_q[C_2 \times C_2]^2$ yields invariance under permutation $(1,2)(3,4)$ in $\mathbb{F}_q[C_2]^4$. Hence, the QC code $\varphi(\mathcal{C})$ corresponding to the SQA code $\mathcal{C}$ has additional symmetry that an arbitrary QC code does not have.

Now, we continue with explaining the CRT decomposition of H-QA codes of index ℓ, which is introduced in [24].

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. Finally, $R := \mathbb{F}_q[H]$ throughout.

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

H. So, we can denote the characters in $Hom(H, \mathbb{K}^*)$ 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

$$\chi_a(h) = \xi^{\sum_{i=1}^{s} a_i h_i M/m_i}, \tag{3.0.3}$$

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

$$E_x = \frac{1}{m} \sum_{a \in H} \chi_x(-a) Y^a \in \mathbb{K}[H], \tag{3.0.4}$$

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

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

$$S_q(h) := \{q^i h : 0 \leq i < v_h\}, \tag{3.0.5}$$

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

$$e_h = \sum_{x \in S_q(h)} E_x, \tag{3.0.6}$$

where $h \in H$ and E_x is a primitive idempotent in $\mathbb{K}[H]$ as in (3.0.4). 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 $\mathbb{F}_q[H]$:

$$e_h e_{h'} = 0, \quad \text{if } h, h' \in H \text{ have distinct } q\text{-cyclotomic classes.} \tag{3.0.7}$$

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

$$\sum_{i=1}^{t} e_{h_i} = 1. \tag{3.0.8}$$

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

$$R = \bigoplus_{i=1}^{t} Re_{h_i}. \tag{3.0.9}$$

The ideal Re_{h_i} generated by e_{h_i} in the group algebra R is an abelian code ([23]). 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

$$\begin{array}{rccc} \varphi_i : & Re_{h_i} & \longrightarrow & \mathbb{E}_i \\ & \left(\sum_{h\in H} \alpha_h Y^h\right) e_{h_i} & \longmapsto & \sum_{h\in H} \alpha_h \chi_{h_i}(h), \end{array} \tag{3.0.10}$$

$$\begin{array}{rccc} \psi_i : & \mathbb{E}_i & \longrightarrow & Re_{h_i} \\ & \delta & \longmapsto & \sum_{k\in H} \alpha_k Y^k, \end{array} \tag{3.0.11}$$

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 (3.0.8), 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 $\oplus_{i=1}^t \mathbb{E}_i^\ell$:

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

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

$$\mathcal{C} = \mathcal{C}_1 \oplus \cdots \oplus \mathcal{C}_t, \tag{3.0.12}$$

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 $\mathcal{C}$'s the constituents of $\mathcal{C}$. The preceding arguments yield the explicit description of the constituents (for $1 \leq i \leq t$):

$$\mathcal{C}_i = \Big\{ \big(\varphi_i(c_1 e_{h_i}), \ldots, \varphi_i(c_\ell e_{h_i})\big) : (c_1, \ldots, c_\ell) \in \mathcal{C} \Big\}. \tag{3.0.13}$$

3.1 Concatenated Structure of QA Codes

In this section, we explain the concatenated structure of QA codes in terms of GC codes. This structure can be seen as an extended version of Section 1.2.2. We continue with the notation used for QA codes so far.

Consider the rings $R^\ell = \mathbb{F}_q[H]^\ell$ and $\mathbb{E}_i^\ell$ (for $1 \leq i \leq t$), where the ring operations are clearly componentwise addition and multiplication. Using the maps φ_i and ψ_i in Equations 3.0.10 and 3.0.11, we define

$$\begin{array}{rccc} \Psi_i : & \mathbb{E}_i^\ell & \longrightarrow & R^\ell \\ & (a_1, \ldots, a_\ell) & \longmapsto & (\psi_i(a_1), \ldots, \psi_i(a_\ell)) \end{array} \tag{3.1.1}$$

and

$$\begin{array}{rccc} \Phi_i : & R^\ell & \longrightarrow & \mathbb{E}_i^\ell \\ & \left(\sum_{h \in H} \alpha_h^1 Y^h, \ldots, \sum_{h \in H} \alpha_h^\ell Y^h \right) & \longmapsto & \left(\sum_{h \in H} \alpha_h^1 \chi_{h_i}(h), \ldots, \sum_{h \in H} \alpha_h^\ell \chi_{h_i}(h) \right). \end{array} \tag{3.1.2}$$

Note that Ψ_i and Φ_i are $\mathbb{F}_q$-linear ring homomorphisms (for $1 \leq i \leq t$). 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 3.1.1. *For each $1 \le i \le t$, let $\Theta_i := \Psi_i(1, \dots, 1) = (e_{h_i}, \dots, e_{h_i})$. 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 $\sum_{i=1}^{t} \Theta_i = (1, \dots, 1)$ 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 $(f_1, \dots, f_\ell)$ 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 $1 \le u \le \ell$, $f_u \in Re_{h_i} \cap Re_{h_j}$, which is trivial by (3.0.9). 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,

$$\begin{aligned} \dim_{\mathbb{F}_q} \bigoplus_{i=1}^{t} \langle \Theta_i \rangle &= \ell \sum_{i=1}^{t} [\mathbb{E}_i : \mathbb{F}_q] \\ &= \ell \sum_{i=1}^{t} \dim_{\mathbb{F}_q} Re_{h_i} \quad \text{by (3.0.10)} \\ &= \ell \dim_{\mathbb{F}_q} R \quad \text{by (3.0.9)}. \end{aligned}$$

Hence, $R^\ell = \bigoplus_{i=1}^{t} \langle \Theta_i \rangle$. The other assertions easily follow from (3.0.7) and (3.0.8). □

Next, we describe the concatenated structure of QA codes. 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 3.1.2. *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 $i = 1, \dots, t$. Then, for some subset $\mathfrak{I} \subseteq \{1, \dots, t\}$, we have $\mathcal{C} = \bigoplus_{i \in \mathfrak{I}} \tilde{\mathcal{C}}_i$. Moreover, $\tilde{\mathcal{C}}_i = Re_{h_i} \square \mathfrak{C}_i$, 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, $\mathcal{C}=\bigoplus_{i\in\mathfrak{I}} Re_{h_i}\square\mathfrak{C}_i$ is an H-QA code of index ℓ.

Proof. (i) By Theorem 3.1.1 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,

$$\mathfrak{C}_i=\Phi_i\left(\tilde{\mathcal{C}}_i\right)=\left\{\left(\varphi_i(c_1e_{h_i}),\ldots,\varphi_i(c_\ell e_{h_i})\right):(c_1,\ldots,c_\ell)\in\mathcal{C}\right\}.\tag{3.1.3}$$

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 (3.0.10) 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

$$\begin{aligned}\delta(\varphi_i(c_1e_{h_i}),\ldots,\varphi_i(c_\ell e_{h_i}))&=(\varphi_i(fe_{h_i})\varphi_i(c_1e_{h_i}),\ldots,\varphi_i(fe_{h_i})\varphi_i(c_\ell e_{h_i}))\\&=(\varphi_i(fc_1e_{h_i}),\ldots,\varphi_i(fc_\ell e_{h_i})).\end{aligned}\tag{3.1.4}$$

Since $\mathcal{C}$ is an R-module, $(fc_1,\ldots,fc_\ell)$ lies in $\mathcal{C}$. Therefore, (3.1.4) belongs to $\mathfrak{C}_i$, which shows that $\mathfrak{C}_i$ is $\mathbb{E}_i$-linear.

Now, consider the concatenated code $Re_{h_i}\square\mathfrak{C}_i$ determined by $\psi_i:\mathbb{E}_i\to Re_{h_i}$ in (3.0.11):

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

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 $(\varphi_i(f_1e_{h_i}), \ldots, \varphi_i(f_\ell e_{h_i}))$ for some $f_1, \ldots, f_\ell \in R$. Then,

$$\begin{aligned} Y^x(\psi_i(\lambda_1), \ldots, \psi_i(\lambda_\ell)) &= Y^x(f_1e_{h_i}, \ldots, f_\ell e_{h_i}) \quad (\psi_i \text{ and } \varphi_i \text{ are inverse}) \\ &= \big(Y^x e_{h_i} f_1 e_{h_i}, \ldots, Y^x e_{h_i} f_\ell e_{h_i}\big) \quad (\text{using } e_{h_i}e_{h_i} = 1) \\ &= \Big(\psi_i\Big(\varphi_i\big(Y^x e_{h_i} f_1 e_{h_i}\big)\Big), \ldots, \psi_i\Big(\varphi_i\big(Y^x e_{h_i} f_\ell e_{h_i}\big)\Big)\Big) \\ &= \Big(\psi_i\Big(\varphi_i\big(Y^x e_{h_i}\big)\varphi_i\big(f_1 e_{h_i}\big)\Big), \ldots, \psi_i\Big(\varphi_i\big(Y^x e_{h_i}\big)\varphi_i\big(f_\ell e_{h_i}\big)\Big)\Big). \end{aligned} \tag{3.1.5}$$

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 (3.1.5) 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. (3.0.9)). 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 3.1.3. 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 (3.0.13) and (3.1.3).

The concatenated view of QA codes in Theorem 3.1.2 results in a general minimum distance bound (cf. Proposition 1.2.2), as will be shown in the following corollary.

Corollary 3.1.4. *Let $\mathcal{C}$ be a QA code of index ℓ in R^ℓ with the concatenated structure*

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

where $\mathfrak{C}_{i_j}$*'s are the nonzero outer codes (constituents) of* $\mathcal{C}$ *for* $\{i_1, \ldots, i_g\} \subseteq \{1, \ldots, t\}$*. Assume that* $d(\mathfrak{C}_{i_1}) \leq d(\mathfrak{C}_{i_2}) \leq \cdots \leq d(\mathfrak{C}_{i_g})$*. Then, we have*

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

Now, we find it useful to explain the concatenated structure of a strictly QA code and the resulting minimum distance bound with the following example, confirmed by MAGMA ([4]). In this example, we also aim to explain how good the bound obtained is and to show the existence of optimal strictly QA codes. We refer the reader to [3] for further examples.

Example 3.1.5. Let $\mathbb{F}_2[C_7 \times C_7]$ be a semisimple algebra. Then, all cyclotomic cosets in this semisimple algebra can be computed, and their cardinalities give the degrees of the extension fields over the binary field. Hence, this computation allows us to consider the extension field $\mathbb{F}_8 \simeq \mathbb{F}_2(\alpha)$ be a degree 3 extension field, where α is a roof of $x^3 + x + 1$ over $\mathbb{F}_2$. Now, consider a strictly QA $\mathcal{C}$ in $\mathbb{F}_2[C_7 \times C_7]^2$ which has the concatenated form

$$\mathcal{C} = Re_{(3,0)} \square \mathfrak{C}_1 \oplus Re_{(3,3)} \square \mathfrak{C}_2.$$

Here, (the outer codes) $\mathfrak{C}_1$ and $\mathfrak{C}_2$ are linear $[2, 1, 2]$ codes over $\mathbb{F}_8$, with respective generator matrices $[1\ 1]$ and $[1\ \alpha]$, and (the inner codes) $Re_{(3,0)}$ and $Re_{(3,3)}$ are binary $[49, 3, 28]$ abelian codes with respective generator matrix

$$G_{Re_{(3,0)}} := \left[\begin{array}{*{49}{c}} 1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1 \\ 0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0 \\ 0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1 \end{array}\right],$$

and

$$G_{Re_{(3,3)}} := \left[\begin{array}{*{49}{c}} 1&0&0&1&0&1&1&0&0&1&0&1&1&1&0&1&0&1&1&1&0&1&0&1&1&1&0&0&0&1&1&1&0&0&1&1&1&1&0&0&1&0&1&1&0&0&1&0&1 \\ 0&1&0&1&1&1&0&1&0&1&1&1&0&0&0&1&1&1&0&0&1&1&1&0&0&1&0&1&1&0&0&1&0&1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1 \\ 0&0&1&0&1&1&1&0&1&0&1&1&1&0&1&0&1&1&1&0&0&0&1&1&1&0&0&1&1&1&1&0&0&1&0&1&1&0&0&1&0&1&1&0&0&1&0&1&1 \end{array}\right].$$

Then, the minimum distance $d(\mathcal{C})$ is bounded from below by

$$\min\{d(Re_{(0,3)}) d(\mathcal{C}_1), d(Re_{(3,0)} \oplus Re_{(3,3)}) d(\mathcal{C}_2)\} = 48.$$

Note that 48 is the best known minimum distance for a linear code of length 98, and of dimension 6, by the Griesmer bound ([17]).

3.2 Asymptotic Results on QA Codes

The class of binary self-dual doubly even strictly QA codes has been shown to be asymptotically good ([24]).

We first show that strictly QA codes are asymptotically good over any finite field $\mathbb{F}_q$. Note that H being a non-cyclic abelian group is enough for this purpose (cf. Remark 3.0.2).

Theorem 3.2.1. *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 (3.0.9) 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 3.1.2 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 LCD class over any finite field. Let us note that the decomposition of the dual of a QA code is given in [24]. Based on this, a characterization of self-dual QA codes is obtained in terms of the constituents of the code ([24, 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 [22, Theorem 3.1] for the special case of LCD QC codes.

Theorem 3.2.2. *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 3.2.1 and choose $\mathcal{F}$ to be an asymptotically good family of LCD codes this time. Such codes exist by [31] and [32]. 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 [24, 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 3.2.1 and 3.2.2 resemble the asymptotically good QC codes presented in [28], since the "co-index" (i.e. length/index) of each code in the families considered is fixed (unlike the asymptotically good family presented in [24, 25]).

Chapter 4

Linear Complementary Pair of Codes

A concatenated construction for LCD codes was given by Carlet et al. using a special type of inner codes called isometry codes ([8]). The construction in [8] extends the earlier concatenated LCD code constructions in [6, 22], where the inner codes in consideration are poor from minimum distance perspective. Here, we extend the concatenated construction to linear complementary pair (LCP) of codes. Hence we develop a method to construct LCP of codes over small finite fields from LCP of codes over extension fields. The work in this chapter comes from [20].

Recall that a pair of linear codes $(\mathcal{C}, \mathcal{D})$ of length n over $\mathbb{F}_q$ is called an LCP of codes if $\mathcal{C} \oplus \mathcal{D} = \mathbb{F}_q^n$. As mentioned in the Introduction, the security parameter is defined as $\min\{d(\mathcal{C}), d(\mathcal{D}^\perp)\}$ due to their applications in cryptography. Here, the dual of a linear code is considered with respect to Euclidean inner product. The special case of $\mathcal{D} = \mathcal{C}^\perp$ amounts to LCD codes, where the security parameter simply becomes $d(\mathcal{C})$.

4.1 Concatenation for LCP of codes

We continue with the notation and definitions in Section 1.4, in particular about the maps π and π'. For this purpose, we find it useful to remind these notations again.

Let $\beta = \{e_0, \ldots, e_{k-1}\}$ be a basis for $\mathbb{F}_{q^k}$ over $\mathbb{F}_q$, and let $\beta' = \{e'_1, \ldots, e'_k\}$

be its dual basis. Let $(\mathcal{C}, \mathcal{D})$ be an LCP of codes in $\mathbb{F}_{q^k}^N$ (i.e. $\mathcal{C} \cap \mathcal{D} = \{0\}$ and $\mathcal{C} \oplus \mathcal{D} = \mathbb{F}_{q^k}^N$), with the security parameter $\min\{d(\mathcal{C}), d(\mathcal{D}^\perp)\}$. We concatenate $\mathcal{C}$ with the (inner) code $\mathcal{A}$, which is generated by the image set $\{\pi(e_1), \ldots, \pi(e_k)\}$ of β under a linear injection $\pi : \mathbb{F}_{q^k} \mapsto \mathbb{F}_q^n$. We also concatenate $\mathcal{D}^\perp$ with $\mathcal{A}'$, which is generated by the image set $\{\pi'(e_1'), \ldots, \pi'(e_k')\}$, where $\pi' : \mathbb{F}_{q^k} \mapsto \mathbb{F}_q^n$ is a map satisfying

$$\pi(e_i).\pi'(e_j') = \delta_{ij},$$

where δ_{ij} denotes the Kronecker delta.

Theorem 4.1.1. *Let $(\mathcal{C}, \mathcal{D})$ be an* LCP *of codes in $\mathbb{F}_{q^k}^N$ and let $\mathcal{A} = im(\pi), \mathcal{A}' = im(\pi')$, which are $\mathbb{F}_q$-linear codes of length n and dimension k. Then $(\pi(\mathcal{C}), \pi'(\mathcal{D}^\perp)^\perp) = (\mathcal{A}\square\mathcal{C}, (\mathcal{A}'\square\mathcal{D}^\perp)^\perp)$ is an* LCP *of codes of length nN over $\mathbb{F}_q$ with the security parameter*

$$d_{sec} = \min\{d(\pi(\mathcal{C})), d(\pi'(\mathcal{D}^\perp))\} \geq \min\{d(\mathcal{A})d(\mathcal{C}), d(\mathcal{A}')d(\mathcal{D}^\perp)\}.$$

Proof. Let K_1 and K_2 denote the dimensions of $\mathcal{C}$ and $\mathcal{D}$ over $\mathbb{F}_{q^k}$, respectively. Since these codes are complementary, we have $K_1 + K_2 = N$ and hence $\dim_{\mathbb{F}_{q^k}}(\mathcal{D}^\perp) = N - K_2 = K_1$. Therefore, $\pi(\mathcal{C})$ and $\pi'(\mathcal{D}^\perp)$ are both $[nN, kK_1]$ codes over $\mathbb{F}_q$ and we have

$$\dim_{\mathbb{F}_q}(\pi(\mathcal{C})) + \dim_{\mathbb{F}_q}(\pi'(\mathcal{D}^\perp)^\perp) = kK_1 + (nN - kK_1) = nN.$$

Hence, it remains to show that $\pi(\mathcal{C})$ and $\pi'(\mathcal{D}^\perp)^\perp$ intersect trivially.

Now, assume that there exists a codeword $\pi(c) \in \pi(\mathcal{C}) \cap \pi'(\mathcal{D}^\perp)^\perp$, where $c \in \mathcal{C}$. By Theorem 1.4.3, we have

$$\pi'(\mathcal{D}^\perp)^\perp = (\mathcal{A}'^\perp \times \cdots \times \mathcal{A}'^\perp) \oplus \pi(\mathcal{D}).$$

So, there exists $a' \in (\mathcal{A}'^\perp)^N$ and $d \in \mathcal{D}$ such that

$$\pi(c) = a' + \pi(d).$$

By linearity of π, we have $\pi(c - d) = a'$. Note that the left hand side is in $\mathcal{A}^N$ whereas the right hand side belongs to $(\mathcal{A}'^\perp)^N$. However, $\mathcal{A} \cap \mathcal{A}'^\perp = \{0\}$ by Lemma

1.4.4. Hence, $a' = 0$, and by injectivity of π, this implies $c = d$. Therefore $\mathcal{C}$ lies in $\mathcal{C} \cap \mathcal{D}$, which implies that $c = 0$.

The lower bound on d_{sec} follows from the lower bound on the minimum distances of the two concatenated codes $\pi(\mathcal{C})$ and $\pi'(\mathcal{D}^{\perp})$ (cf. Section 1.2). □

Remark 4.1.2. If $\mathcal{D} = \mathcal{C}^{\perp}$ and the concatenation map π' can be chosen equal to π, then Theorem 3.1 in [8] becomes a special case of Theorem 4.1.1, and one obtains an LCD code $\pi(\mathcal{C})$. Isometry maps and inner codes are introduced in [8], which guarantee $\pi = \pi'$. As noted in [8], an isometry code need not exist for any q, k and n.

4.2 Generalized Concatenation for LCP of codes

In this section, we extend the concatenated description for LCP of codes in Section 4.1, using the dual code description for GC codes in Section 1.4. Namely, starting with more than one LCP of codes over extension fields, we will obtain an LCP of codes over the base field. For simplicity, as in the case of dual description for GC codes, we will present the construction for two different pairs of complementary codes but our result holds for more pair of complementary codes.

We let $(\mathcal{C}_1, \mathcal{D}_1)$ be an LCP of codes of length N over $\mathbb{F}_{q^{k_1}}$ and $(\mathcal{C}_2, \mathcal{D}_2)$ be an LCP of codes of length N over $\mathbb{F}_{q^{k_2}}$. If we let $\dim_{\mathbb{F}_{q^{k_i}}} \mathcal{C}_i = K_i$ (for $i = 1, 2$), then it is clear that $\dim_{\mathbb{F}_{q^{k_i}}} \mathcal{D}_i = N - K_i$.

Consider the codes $\mathcal{C}$ and $\mathcal{D}$ over $\mathbb{F}_{q^{k_1}} \times \mathbb{F}_{q^{k_2}}$ as in Definition 1.2.1, where the rows of $\mathcal{C}$ come from $\mathcal{C}_1, \mathcal{C}_2$ and the rows of D come from $\mathcal{D}_1, \mathcal{D}_2$. Define $\bar{\mathcal{D}}$ as in (1.4.6) to be the code whose rows come from $\mathcal{D}_1^{\perp}$ and $\mathcal{D}_2^{\perp}$. Let the bases and the dual bases of $\mathbb{F}_{q^{k_1}}$ and $\mathbb{F}_{q^{k_2}}$ and the $\mathbb{F}_q$-linear injections π and π' be as in Section 1.4. Recall that the images of π and π', denoted by $\mathcal{A}$ and $\mathcal{A}'$ respectively, are $\mathbb{F}_q$-linear codes with parameters $[n, k_1 + k_2]$. Moreover, the subcodes of $\mathcal{A}$ and $\mathcal{A}'$ are defined as $\mathcal{A}_1 = \pi(\mathbb{F}_{q^{k_1}}, 0)$, $\mathcal{A}_2 = \pi(0, \mathbb{F}_{q^{k_2}})$, $\mathcal{A}'_1 = \pi'(\mathbb{F}_{q^{k_1}}, 0)$ and $\mathcal{A}'_2 = \pi'(0, \mathbb{F}_{q^{k_2}})$.

The following result generalizes Theorem 4.1.1.

Theorem 4.2.1. *Let $(\mathcal{C}_i, \mathcal{D}_i)$ be an LCP of codes in $\mathbb{F}_{q^{k_i}}^N$ for $i = 1, 2$. Then $(\pi(\mathcal{C}), (\pi'(\bar{\mathcal{D}}))^{\perp})$ is an LCP of codes of length nN over $\mathbb{F}_q$.*

Proof. If $\dim_{\mathbb{F}_q^{k_i}} \mathcal{C}_i = K_i$, then $\dim_{\mathbb{F}_q^{k_i}} \mathcal{D}_i = N - K_i$ for $i = 1, 2$. By Proposition

1.2.2, we have

$$\dim_{\mathbb{F}_q}(\pi(\mathcal{C})) = k_1K_1 + k_2K_2 \text{ and } \dim_{\mathbb{F}_q}(\pi'(\bar{\mathcal{D}})^{\perp}) = nN - (k_1K_1 + k_2K_2),$$

where both of the codes $\pi(\mathcal{C})$ and $\pi'(\bar{\mathcal{D}})^{\perp}$ lie in $\mathbb{F}_q^{nN}$. Hence it is enough to show that these codes intersect trivially.

Let $c \in C$ be such that $\pi(c)$ is an element in the intersection $\pi(\mathcal{C}) \cap \pi'(\bar{\mathcal{D}})^{\perp}$. By Theorem 1.4.5, we have

$$\pi'(\bar{\mathcal{D}}))^{\perp} = E \oplus \pi(\mathcal{D}),$$

where $E = (\mathcal{A}'^{\perp})^N$. So, there exists $a' \in (\mathcal{A}'^{\perp})^N$ and $d \in \mathcal{D}$ such that

$$\pi(c) = a' + \pi(d).$$

By linearity of π, we have $\pi(c - d) = a'$, where the left hand side is in $\mathcal{A}^N$ and the right hand side is in $(\mathcal{A}'^{\perp})^N$. Hence, by Lemma 1.4.4, we have $\pi(c - d) = 0$ and by injectivity of π, this implies that $c = d$. Then the first row of $\mathcal{C}$ belongs to $\mathcal{C}_1 \cap \mathcal{D}_1$ and the second row belongs to $\mathcal{C}_2 \cap \mathcal{D}_2$. Since $(\mathcal{C}_i, \mathcal{D}_i)$ is an LCP of codes (for $i = 1, 2$), we have $c = 0$ and this concludes the proof. □

4.3 Numerical Results

We present some numerical results, obtained using MAGMA ([4]), based on Proposition 1.4.1, Theorem 4, and Theorem 4.2.1.

The first two examples are based on the simple concatenated construction presented in Section 4.1.

Let $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ be a degree 2 extension field over the binary field, where α is a root of the irreducible polynomial $x^2 + x + 1$ over $\mathbb{F}_2$. Let $\beta = \{1, \alpha\}$ be a basis of $\mathbb{F}_4$ and $\beta' = \{\alpha^2, 1\}$ be its dual basis. In the following examples, we start with LCP of codes $(\mathcal{C}, \mathcal{D})$ over $\mathbb{F}_4$, concatenate $\mathcal{C}$ with an inner code $\mathcal{A}$ from the class of Cordaro-Wagner Codes ([11]), and concatenate $\mathcal{D}^{\perp}$ with an inner code $\mathcal{A}'$, which is suitably chosen to guarantee that the resulting concatenated codes are complementary over $\mathbb{F}_2$ (cf. Proposition 1.4.1 and Theorem 4).

Example 4.3.1. Consider LCP of codes $(\mathcal{C}, \mathcal{D})$ in $\mathbb{F}_4^3$ with respective generator matrices

$$G_{\mathcal{C}} = \begin{bmatrix} 1 & 0 & \alpha \\ 0 & \alpha & \alpha \end{bmatrix} \text{ and } G_{\mathcal{D}} = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}.$$

Choose the inner code $\mathcal{A}$ as the image of the map $\pi : \mathbb{F}_4 \to \mathbb{F}_2^3$ such that $\pi(1) = (1, 0, 1)$ and $\pi(\alpha) = (0, 1, 1)$. By Proposition 1.4.1, there exists π' which maps the elements of the dual basis $\{\alpha^2, 1\}$ to $(1, 0, 1)$ and $(0, 1, 1)$, respectively. Note that $\pi' = \pi$, hence it is an isometry map as introduced in [8]. Then, by Theorem 4, the concatenated codes $\pi(\mathcal{C}) = \mathcal{A}\square\mathcal{C}$, of dimension 4, and $(\pi(\mathcal{D}^\perp))^\perp$ yields a pair of binary complementary dual codes. Here, the security parameter is greater than or equal to $\min\{d(\mathcal{A})d(\mathcal{C}), d(\mathcal{A}')d(\mathcal{D}^\perp))\} = 4$. This is also the best known minimum distance of a linear code of length 9, and dimension 4. Let us note that an LCD code with parameters $[9, 4, 3]$ is obtained in Table 2 of [13], and an LCP of codes with parameters $[9, 3, 4]$ is obtained in Table 1 of [7].

Example 4.3.2. Consider LCP of codes $(\mathcal{C}, \mathcal{D})$ in $\mathbb{F}_4^2$ with respective generator matrices

$$G_{\mathcal{C}} = \begin{bmatrix} 1 & \alpha \end{bmatrix} \text{ and } G_{\mathcal{D}} = \begin{bmatrix} 1 & 1 \end{bmatrix}.$$

Choose the inner code $\mathcal{A}$ as the image of $\pi : \mathbb{F}_4 \to \mathbb{F}_2^8$, which maps $\{1, \alpha\}$ to the vectors

$$\{(1, 1, 1, 0, 0, 1, 1, 1), (0, 0, 0, 1, 1, 1, 1, 1)\}$$

(cf. [11]). By Proposition 1.4.1, there exists π', which maps the elements of the dual basis $\{\alpha^2, 1\}$ to $(0, 1, 1, 1, 0, 1, 1, 1), (1, 0, 1, 1, 1, 0, 0, 1)$, respectively. Here, $\pi' \neq \pi$ and hence π' differs from an isometry map as introduced in [8]. By Theorem 4, the concatenated codes $\pi(\mathcal{C}) = \mathcal{A}\square\mathcal{C}$, of dimension 2, and $(\pi(\mathcal{D}^\perp))^\perp = (\mathcal{A}'\square\mathcal{D}^\perp)^\perp$ yields a binary complementary pair of codes. The security parameter is bounded from below by $\min\{d(\mathcal{A})d(\mathcal{C}), d(\mathcal{A}')d(\mathcal{D}^\perp))\} = 10$. This is also the best known minimum distance of a linear code of length 16, and dimension 2. Note that Table 2 in [13] has an LCD code with parameters $[16, 2, \geq 6]$.

In a similar way, we can construct binary LCP of codes $(\pi(\mathcal{C}), (\pi'(\mathcal{D}^\perp))^\perp)$, with the guaranteed security parameters:

- 9, where $\pi(\mathcal{C})$ has parameters $[14, 2, 9]$, and note that $[14, 2, 7]$ is obtained in Table 2 of [13],

- 6, where $\pi(\mathcal{C})$ has parameters $[15, 4, 6]$, and note that $[15, 4, 5]$ is obtained in Table 2 of [13],

- 9, where $\pi(\mathcal{C})$ has parameters $[15, 2, 9]$, and note that $[15, 2, 7]$ is obtained in Table 2 of [13].

Next, we give an example of constructing LCP of codes in a generalized concatenated setting.

Let $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$ be a degree 4 extension field over the binary field, where α is a root of the irreducible polynomial $x^4 + x + 1$ over $\mathbb{F}_2$. Let $\beta = \{1, \alpha, \alpha^2, \alpha^3\}$ be a basis of $\mathbb{F}_{16}$ and $\beta' = \{\alpha^{14}, \alpha^2, \alpha, 1\}$ be its dual basis. In the following examples, we start with LCP of codes $(\mathcal{C}_1, \mathcal{D}_1)$ over $\mathbb{F}_2$, and $(\mathcal{C}_2, \mathcal{D}_2)$ over $\mathbb{F}_{16}$, concatenate

$$\mathcal{C} := \left\{ c = \begin{pmatrix} c_1^1 & c_2^1 \\ c_1^2 & c_2^2 \end{pmatrix} : \ (c_1^i, c_2^i) \in \mathcal{C}_i \text{ for } i = 1, 2 \right\}, \tag{4.3.1}$$

with an inner code $\mathcal{A} := \mathcal{A}_1 \oplus \mathcal{A}_2$ with parameters $[10, 5, 4]$, and concatenate

$$\bar{\mathcal{D}} := \left\{ d = \begin{pmatrix} d_1^1 & d_2^1 \\ d_1^2 & d_2^2 \end{pmatrix} : \ (d_1^i, d_2^i) \in \mathcal{D}_i^{\perp} \text{ for } i = 1, 2 \right\}, \tag{4.3.2}$$

with an inner code $\mathcal{A}' := \mathcal{A}_1' \oplus \mathcal{A}_2'$, which is suitably chosen to guarantee that the resulting concatenated codes are complementary over $\mathbb{F}_2$ (cf. Section 1.4 and Theorem 4.2.1).

Example 4.3.3. Consider LCP of codes $(\mathcal{C}_1, \mathcal{D}_1)$ in $\mathbb{F}_2^2$, and $(\mathcal{C}_2, \mathcal{D}_2)$ in $\mathbb{F}_{16}^2$, which have generator matrices

$$G_{\mathcal{C}_1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ G_{\mathcal{D}_1} = \begin{bmatrix} 0 & 0 \end{bmatrix}, \ G_{\mathcal{C}_2} = \begin{bmatrix} 1 & \alpha \end{bmatrix}, \text{ and } G_{\mathcal{D}_2} = \begin{bmatrix} 1 & 1 \end{bmatrix},$$

respectively.

By the settings (4.3.1) and (4.3.2), consider $(\mathcal{C}, \bar{\mathcal{D}})$ in $(\mathbb{F}_2 \times \mathbb{F}_{16})^2$. Choose the inner code $\mathcal{A}$ as the image of $\pi : \mathbb{F}_2 \times \mathbb{F}_{16} \to \mathbb{F}_2^{10}$, which maps the elements of

$$\{(1, 0), (0, 1), (0, \alpha), (0, \alpha^2), (0, \alpha^3)\}$$

to the corresponding rows of the matrix

$$G_{\mathcal{A}} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

By Proposition 1.4.1, there exists π', which maps the elements of

$$\beta^{'} = \{(1,0), (0,\alpha^{14}), (0,\alpha^2), (0,\alpha), (0,1)\}$$

to the corresponding rows of

$$G_{\mathcal{A}'} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Here, $\pi' \neq \pi$ and hence π' differs from an isometry map as introduced in [8]. By Theorem 4.2.1, the concatenated codes $\pi(\mathcal{C}) = \mathcal{A}_1 \square \mathcal{C}_1 \oplus \mathcal{A}_2 \square \mathcal{C}_2$, of dimension 6, and $(\pi(\bar{\mathcal{D}}))^{\perp} = (\mathcal{A}_1^{'} \square \mathcal{D}_1^{\perp} \oplus \mathcal{A}_2^{'} \square \mathcal{D}_2^{\perp})^{\perp}$ yields a binary complementary pair of codes. The security parameter is bounded from below by

$$\min\{d(\mathcal{A}_1)d(\mathcal{C}_1), d(\mathcal{A}_1 \oplus \mathcal{A}_2)d(\mathcal{C}_2), d(\mathcal{A}_1^{'})d(\mathcal{D}_1^{\perp}), d(\mathcal{A}_1^{'} \oplus \mathcal{A}_2^{'})d(\mathcal{D}_2^{\perp})\} = 6.$$

Note that Table 2 in [13] has an LCD code with parameters $[20, 5, \geq 6]$.

In a similar way, we can construct binary LCP of codes $(\pi(\mathcal{C}), (\pi'(\bar{\mathcal{D}}))^{\perp})$ with the guaranteed security parameters:

- 6, where $\pi(\mathcal{C})$ has parameters $[15, 5, 6]$, and note that $[14, 2, 7]$ is obtained in Table 2 of [13],
- 5, where $\pi(\mathcal{C})$ has parameters $[15, 6, 4]$, and note that $[15, 4, 4]$ is obtained in Table 2 of [13],

- 5, where $\pi(\mathcal{C})$ has parameters $[12, 5, 4]$, and note that $[12, 4, 4]$ is obtained in Table 2 of [13].

Bibliography

[1] S. Bhasin, J.-L. Danger, S. Guilley, Z. Najm, X.T. Ngo, "Linear complementary dual code improvement to strengthen encoded circuit against hardware Trojan horses", *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, May 5-7, 2015.

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

[3] M. Borello, C. Güneri, P. Solé, E. Saçıkara, "The concatenated structure of quasi-abelian codes", submitted, available from arXiv: 1807.01246.

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

[5] J. Bringer, C. Carlet, H. Chabanne, S. Guilley, H. Maghrebi, "Orthogonal direct sum masking - a smartcard friendly computation paradigm in a code with builtin protection against side-channel and fault attacks", *in WISTP, Springer*, Heraklion, 40-56, 2014.

[6] 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.

[7] C. Carlet, C. Güneri, F. Özbudak, B. Özkaya, P. Solé, "On linear complementary pairs of codes", *IEEE Trans. Inform. Theory*, to appear.

[8] C. Carlet, C. Güneri, F. Özbudak, P. Solé, "A new concatenated type construction for LCD codes and isometry codes", *Discrete Math.*, vol. 341, 830-835, 2018.

[9] C. Carlet, S. Mesnager, C. Tang, Y. Qi, R. Pellikaan, "Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$", *IEEE Trans. Inform. Theory*, vol. 64, 3010-3017, 2018.

[10] H. Chen, S. Ling, C. Xing "Asymptotically good quantum codes exceeding the AshikhminLitsynTsfasman bound", *IEEE Trans. Inform. Theory*, 47(5), 2055-2058, 2001.

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

[12] C. Ding, D.R. Kohel, and S. Ling. "Split group codes". *IEEE Trans. Inform. Theory*, vol. 46, 485-495, 2000.

[13] S.T. Dougherty, J.-L. Kim, B. Özkaya, L. Sok, P. Solé, "The Combinatorics of LCD Codes: Linear programming bound and orthogonal matrices", *Int. J. Inform. Coding Theory* 4 (2/3),116128, 2017.

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

[15] 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.

[16] G. D. Forney Jr., "Concatenated codes", *M.I.T. Research Monograph*, No. 37. The M.I.T. Press, Cambridge, Mass., 1966.

[17] J.H. Griesmer, "A bound for error-correcting codes", *IBM Journal of Res. and Dev.* 4 (5): 532-542, 1960.

[18] 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.

[19] C. Güneri, F. Özbudak, B. Özkaya, E. Saçıkara, Z. Sepasdar and P. Solé, "The structure and performance of generalized quasi-cyclic codes". *Finite Fields Appl.*, vol. 47, 183-202, 2017.

[20] C. Güneri, F. Özbudak and E. Saçıkara, "A concatenated construction of linear complementary pair of codes", submitted.

[21] C. Güneri, B. Özkaya, "Multidimensional quasi-cyclic and convolutional codes", *IEEE Trans. Inform. Theory*, vol. 62, 6772-6785, 2016.

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

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

[24] S. Jitman, S. Ling, "Quasi-abelian codes", *Des. Codes Cryptogr.*, vol. 74, 511-531, 2015.

[25] 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.

[26] 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.

[27] 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.

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

[29] J.H. van Lint, "Introduction to Coding Theory", *Springer*, 1982.

[30] 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.

[31] J.L. Massey, "Linear codes with complementary duals", *Discrete Math.*, vol. 106-107, 337-342, 1992.

[32] N. Sendrier, "Linear codes with complementary duals meet the Gilbert-Varshamov bound", *Discrete Math.*, vol. 285, 345-347, 2004.

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

[34] S.K. Wasan. "Quasi abelian codes". *Publ. Inst. Math.* 35, 201206, 1977.