MULTIDIMENSIONAL QUASI-CYCLIC AND CONVOLUTIONAL CODES

by

BUKET ÖZKAYA

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
2014

Multidimensional Quasi-Cyclic and Convolutional Codes

APPROVED BY

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

Prof. Dr. Alev Topuzoğlu ....

Prof. Dr. Henning Stichtenoth ....

Assoc. Prof. Dr. Erkay Savaş ....

Prof. Dr. Ferruh Özbudak ....

DATE OF APPROVAL: 18.07.2014

©Buket Özkaya 2014

All Rights Reserved

to perseverance, endeavor and love

Multidimensional Quasi-Cyclic and Convolutional Codes

Buket Özkaya

Mathematics, Doctorate Thesis, 2014

Thesis Supervisor: Assoc. Prof. Dr. Cem Güneri

Keywords: Quasi-cyclic code, multidimensional quasi-cyclic code, convolutional code

Abstract

We introduce multidimensional generalizations of quasi-cyclic codes and investigate their algebraic properties as well as their links to multidimensional convolutional codes. We call these generalized codes n-dimensional quasi-cyclic (QnDC) codes. We provide a concatenated structure for QnDC codes in the sense that they can be decomposed into shorter codes over extensions of their base field. This structure allows us to prove that these codes are asymptotically good.

Then, we extend the relation between quasi-cyclic and convolutional codes to multidimensional case. Lally has shown that the free distance of a convolutional code is lower bounded by the minimum distance of an associated quasi-cyclic code. We show that a QnDC code can be associated to a given nD convolutional code. Moreover, we prove that the relation between distances of convolutional and quasi-cyclic codes extend to a class of 1-generator 2D convolutional codes and the associated Q2DC codes. Along the way, an alternative new description of noncatastrophic polynomial encoders is given for 1-generator 1D convolutional codes and a sufficient condition for noncatastrophic nD polynomial encoders is obtained for 1-generator nD convolutional codes.

Çok Boyutlu Sanki-Devirsel ve Konvolusyonel Kodlar

Buket Özkaya

Matematik, Doktora Tezi, 2014

Tez Danışmanı: Doç. Dr. Cem Güneri

Anahtar Kelimeler: Sanki-devirsel kodlar, çok boyutlu sanki-devirsel kodlar, konvolusyonel kodlar.

Özet

Bu tez çalışmasında, sanki-devirsel kodların çok boyutlu genellemeleri sunulup cebirsel özellikleri ile çok boyutlu konvolusyonel kodlarla olan ilişkileri ele alınmıştır. Bu genelleştirilmiş kodlara n-boyutlu sanki-devirsel kodlar adı verilmiştir. Çok boyutlu sanki-devirsel kodların birleşik yapısı tanımlandıkları cismin genişlemeleri üzerindeki daha kısa kodlar cinsinden verilmiştir. Bu birleşik yapı sayesinde n-boyutlu sanki-devirsel kodların asimptotik iyi oldukları gösterilmiştir.

Daha sonra sanki-devirsel ve konvolusyonel kodların bilinen ilişkisi cok boyuta genellenmiştir. Bir boyutlu durumda her konvolusyonel kodun serbest uzaklığının ilişkili sanki-devirsel kodun minimum uzaklığı tarafından alttan sınırlı olduğu Lally tarafından ispatlanmıştır. Verilen her n-boyutlu konvolusyonel kodla ilişkili bir n-boyutlu sanki-devirsel kod olduğu gösterilmiştir. Benzer bir sonucun çok boyutlu durumda da geçerli olduğu özel bir 2-boyutlu tek üreteçli konvolusyonel kod sınıfı için gösterilmiştir. Ayrıca, 1-boyutlu tek üreteçli konvolusyonel kodların polinom üreteç matrislerinin katastrofik olmaması için yeni bir tarif bulunmuş, n-boyutlu tek üreteçli konvolusyonel kodların polinom üreteç matrislerinin katastrofik olması için ise yeterli koşul elde edilmiştir.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my thesis advisor Cem Güneri for his patience, encouragement and motivation. Besides his immense contribution to my academic experience, he treated me not only as a student but also as a colleague along the way. Without his guidance and tremendous support this dissertation would not be possible.

I would also like to thank my thesis committee members: Alev Topuzoğlu, Henning Stichtenoth, Erkay Savaş and Ferruh Özbudak. My sincere appreciations also go to Joachim Rosenthal and Florian Hess for their valuable remarks and comments on this study.

Being a member of Sabancı University was a great experience, I am thankful to all the graduate students for the joyful moments we shared. I would like to acknowledge all the distinguished professors of the Mathematics Department, especially the members of the Algebra Group, for the care, support and knowledge they provided.

During the last two years I was very fortunate to have my cousin Fulya Kurtuluş as flatmate and I am grateful to her for her care and friendship. Last but not the least, I would like to thank my parents Behiye Özkaya and Ali Özkaya for their never-ending love and support.

I was supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) under the Project Grant 111T234 partly last year and fully during my last term.

Contents

Introduction

The main goal of coding and information theory is to provide a reliable communication over a noisy channel. Any information sent across a noisy channel may be received with possible transmission errors. The communication system has to be designed in such a way that these errors are first detected and then corrected. This is obtained by redundancy, i.e. the messages are sent with some extra information so that the receiver can recover the original message. That operation is done via encoding which has to be done efficiently: the message is supposed to be encoded with least possible amount of redundancy and be capable of a certain error correction level with a suitable decoding process. The design and the implementation of such a system are the fundamental issues in the theory of error-correcting-codes. From theoretical point of view, the research on efficient information transmission is directed towards studying well-performing error-correcting codes with a nice algebraic structure. This dissertation is aimed at developing algebraic coding theory in this direction.

In this work, we focus on a specific class of linear block codes, namely quasi-cyclic codes. They yield explicit codes with good parameters (see [3, 5, 10, 11]) and they are asymptotically good ([6, 20, 24, 28]). For m, ℓ integers with $\gcd(m, q) = 1$, a quasi-cyclic (QC) code of length $m\ell$ and index ℓ over $\mathbb{F}_q$ is a linear code $C \subset \mathbb{F}_q^{m\ell}$ which is invariant under the shift of codewords by ℓ positions (where ℓ is the minimal such number). It is well-known that such a QC code can be viewed algebraically as an R-module of R^ℓ, where $R = \mathbb{F}_q[x]/\langle x^m - 1\rangle$. Alternatively, we can let $S = \mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$ and view a QC code of length $m\ell$ and index ℓ as an R-submodule of S.

One can decompose a QC code over $\mathbb{F}_q$ into its constituent codes, which are shorter linear codes over certain extensions of $\mathbb{F}_q$ ([23]). Also, a concatenated decomposition can be described for QC codes where the inner codes in the decomposition are minimal cyclic codes ([19]). It has been shown in [16] that the constituents in the sense of Ling-Solé and the outer codes in the concatenated structure given by Jensen are the same.

Convolutional codes are also an important class of codes which are extensively studied. An (ℓ, k) convolutional code C over $\mathbb{F}_q$ is defined as a k-dimensional $\mathbb{F}_q(x)$-subspace of $\mathbb{F}_q(x)^\ell$ in general (see [29]). In this sense, convolutional codes are also linear codes, but they are not block codes since the symbol field is no more the finite field $\mathbb{F}_q$, but the rational function field $\mathbb{F}_q(x)$, which produces codewords of different lengths over $\mathbb{F}_q$. The reason for taking that field as the alphabet is that convolutional codes are codes with memory. The message is not sent in a fixed-length block but in a data stream where each codeword is loaded with the information of some previous codewords. Given a sequence of information words $u_0(x), u_1(x), \ldots$ they are mapped to a sequence of codewords $c_0(x), c_1(x), \ldots$ such that $c_i(x) = u_i(x) \cdot G$ for each $i = 0, 1, \ldots$, where G is the corresponding encoder for C and given as a $k \times \ell$ matrix over $\mathbb{F}_q(x)$. In particular, if we consider a so-called basic encoder for a convolutional code, then all polynomial codewords are produced from polynomial input sequences. Hence, such a convolutional code can be defined as an $\mathbb{F}_q[x]$-submodule of $\mathbb{F}_q[x]^\ell$. The degrees of the entries of G determine the memory of the convolutional code. Hence, convolutional codes generalize block codes in the sense that block codes are memoryless convolutional codes.

The first chapter of the thesis contains all the required background about quasi-cyclic and convolutional codes for the next chapters. Quasi-cyclic codes are naturally related to convolutional codes. It has been shown by Lally that the free distance of a convolutional code can be lower bounded by the minimum distance of an associated QC code (see [21]).

In the second chapter, we define multidimensional generalizations of QC codes and investigate their properties. For $n \geq 1$, we consider the quotient ring $R_n = \mathbb{F}_q[x_1, x_2, \ldots, x_n]/\langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle$ and define the nD quasi-cyclic (QnDC) code of size $m_1 \times \cdots \times m_{n+1}$ as an R_n-submodule of R_{n+1}. It is clear the for $n = 1$, we obtain QC codes (of length $m_1 m_2$ and index m_2). QnDC codes are linear codes of length $m_1 \cdots m_{n+1}$ over $\mathbb{F}_q$ and they can also be viewed as QC codes of index $l = m_2 \cdots m_{n+1}$. However, they have extra shift-invariance properties than ordinary QC codes.

Being QC codes, we can talk about the decomposition of QnDC codes into constituents (or the concatenated structure). We prove that the constituents (or the outer codes in Jensen's concatenated decomposition) of a length $m_1 \cdots m_{n+1}$ QnDC code are Q$(n-1)$DC codes (over various extensions of $\mathbb{F}_q$) of length $m_2 \cdots m_{n+1}$. We also prove that the family of QnDC codes are asymptotically good for any $n \geq 1$.

Multidimensional versions of convolutional codes have been studied by Weiner in his PhD thesis ([33]), although they have not been as extensively investigated as the 1D convolutional codes. In the last chapter, we show that one can naturally associate a QnDC code to any nD convolutional code, which is defined as an $\mathbb{F}_q[x_1, x_2, \ldots, x_n]$-submodules of $\mathbb{F}_q[x_1, x_2, \ldots, x_n]^\ell$. Then we prove an analogue of Lally's result for a particular class of 1-generator 2D convolutional codes. In addition, we give a new alternative description for a polynomial generating matrix of a 1-generator 1D convolutional code to be noncatastrophic. For the 1-generator nD case, we obtain a sufficient condition for the polynomial encoder to be noncatastrophic.

Weiner mentions in the conclusion of his thesis that connections between multidimensional convolutional codes and algebraic geometry should be investigated. Let us note that the number of rational points on Artin-Schreier type hypersurfaces over finite fields helps us estimate the minimum distance of multidimensional cyclic codes via the trace representation of this class of codes (see [13, 15], and also [32] for another relation between algebraic geometry and multidimensional cyclic codes). Multidimensional cyclic codes are closely related to multidimensional QC codes, as we will explain in this thesis. Moreover, QnDC codes can be viewed as QC codes and there is a trace representation for QC codes ([23, Thereom 5.1]). So, an analysis similar to those in [13, 15] can be in principal applied to QnDC codes and the relation with certain nD convolutional codes can be used to write a lower bound on the free distance of nD convolutional codes in terms of rational points on Artin-Schreier hypersurfaces. This remains as a work to be done in the future.

Chapter 1

Preliminaries

In this first chapter, we will give a brief background on quasi-cyclic, 2D cyclic and convolutional codes, along with the notation and some important results used throughout this study.

1.1 QC and 2D cyclic codes

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

$$c = \begin{pmatrix} c_{00} & \dots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \dots & c_{m-1,\ell-1} \end{pmatrix}, \tag{1.1.1}$$

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

Now consider the principal ideal $I=\langle x^m-1\rangle$ of $\mathbb{F}_q[x]$ and let $R:=\mathbb{F}_q[x]/I$. If T denotes the shift-by-1 operator on $\mathbb{F}_q^{m\ell}$, let us denote its action on $c\in\mathbb{F}_q^{m\ell}$ by $T\cdot c$. Then $\mathbb{F}_q^{m\ell}$ has an $\mathbb{F}_q[x]$-module structure given by the following multiplication

$$\begin{aligned} \mathbb{F}_q[x]\times\mathbb{F}_q^{m\ell} &\longrightarrow \mathbb{F}_q^{m\ell} \\ (a(x),c) &\mapsto a(T^\ell)\cdot c \end{aligned}$$

For instance, if $a(x) = a_0 + a_1x + a_2x^2$, then

$$a(T^\ell) \cdot (c_{ij}) = a_0(c_{ij}) + a_1(T^\ell \cdot (c_{ij})) + a_2(T^{2\ell} \cdot (c_{ij})).$$

Observe that the ideal I annihilates $\mathbb{F}_q^{m\ell}$:

$$(x^m - 1) \cdot (c_{ij}) = T^{m\ell} \cdot (c_{ij}) - (c_{ij}) = 0.$$

Therefore $\mathbb{F}_q^{m\ell}$ can also be viewed as an R-module and a QC code $C \subset \mathbb{F}_q^{m\ell}$ of index ℓ is an R-submodule of $\mathbb{F}_q^{m\ell}$.

To an element $c \in \mathbb{F}_q^{m\times\ell}$ as in (1.1.1), we associate an element of R^ℓ

$$\vec{c}(x) := (c_0(x), c_1(x), \ldots, c_{\ell-1}(x)) \in R^\ell, \tag{1.1.2}$$

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

$$c_j(x) := c_{0,j} + c_{1,j}x + c_{2,j}x^2 + \cdots + c_{m-1,j}x^{m-1} \in R. \tag{1.1.3}$$

Then, the following map is an R-module isomorphism

$$\begin{array}{rccc} \phi : & \mathbb{F}_q^{m\ell} & \longrightarrow & R^\ell \\ & c = \begin{pmatrix} c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-1,0} & \cdots & c_{m-1,\ell-1} \end{pmatrix} & \longmapsto & \vec{c}(x). \end{array} \tag{1.1.4}$$

Note that the case $\ell = 1$ amounts to the classical polynomial representation of cyclic codes where 1-shift on $\mathbb{F}_q^m$ corresponds to multiplication by x in R. Observe that ℓ-shift on $\mathbb{F}_q^{m\ell}$ corresponds to componentwise multiplication by x in R^ℓ. Namely, if $c \in \mathbb{F}_q^{m\times\ell}$ corresponds to $\vec{c}(x) \in R^\ell$ (as in (1.1.2) and (1.1.3)), then

$$\phi(T^\ell \cdot (c_{ij})) = \phi \begin{pmatrix} c_{m-1,0} & \cdots & c_{m-1,\ell-1} \\ c_{00} & \cdots & c_{0,\ell-1} \\ \vdots & & \vdots \\ c_{m-2,0} & \cdots & c_{m-2,\ell-1} \end{pmatrix} = (x \cdot c_0(x), \ldots, x \cdot c_{\ell-1}(x)) = x \cdot \vec{c}(x).$$

Thus, a QC code $C \subset R^\ell$ is an R-submodule of R^ℓ.

Now, let $J = \langle x^m - 1, y^\ell - 1 \rangle$ be an ideal of $\mathbb{F}_q[x, y]$ and set $S := \mathbb{F}_q[x, y]/J$. The ring S is clearly an R-module and the following map is an R-module isomorphism (cf. (1.1.2) and (1.1.3)).

$$\begin{aligned} \psi : R^\ell &\longrightarrow S \\ \vec{c}(x) = (c_j(x))_j &\mapsto \sum_{j=0}^{\ell-1} c_j(x) y^j = \sum_{j=0}^{\ell-1} \sum_{i=0}^{m-1} c_{i,j} x^i y^j \end{aligned} \tag{1.1.5}$$

Hence, $\mathbb{F}_q^{m\ell}$, R^ℓ and S are all isomorphic as R-modules and a q-ary QC code C of length $m\ell$ and index ℓ can be considered as an R-submodule in any of these rings.

Let us now introduce 2D cyclic codes (see [13, 17, 18] for further information) as a special case of QC codes. Again, let C be a length $m\ell$ linear code over $\mathbb{F}_q$ whose codewords are written as in (1.1.1). Then, C is called 2D cyclic, if it is closed under not only row shifts of codewords but also under column shifts:

$$\begin{pmatrix} c_{00} & \cdots & c_{0,\ell-2} & \boldsymbol{c_{0,\ell-1}} \\ \vdots & & \vdots & \vdots \\ c_{m-2,0} & \cdots & c_{m-2,\ell-2} & \boldsymbol{c_{m-2,\ell-1}} \\ \boldsymbol{c_{m-1,0}} & \cdots & \boldsymbol{c_{m-1,\ell-2}} & \boldsymbol{c_{m-1,\ell-1}} \end{pmatrix} \in C$$

$$\Rightarrow \begin{pmatrix} \boldsymbol{c_{m-1,0}} & \cdots & \boldsymbol{c_{m-1,\ell-2}} & \boldsymbol{c_{m-1,\ell-1}} \\ c_{00} & \cdots & c_{0,\ell-2} & c_{0,\ell-1} \\ \vdots & & \vdots & \vdots \\ c_{m-2,0} & \cdots & c_{m-2,\ell-2} & c_{m-2,\ell-1} \end{pmatrix} \in C$$

$$\Rightarrow \begin{pmatrix} \boldsymbol{c_{0,\ell-1}} & c_{00} & \cdots & c_{0,\ell-2} \\ \vdots & \vdots & \cdots & \vdots \\ \boldsymbol{c_{m-2,\ell-1}} & c_{m-2,0} & & c_{m-2,\ell-2} \\ \boldsymbol{c_{m-1,\ell-1}} & c_{m-1,0} & \cdots & c_{m-1,\ell-2} \end{pmatrix} \in C$$

Clearly, a length $m\ell$ 2D cyclic code is also an index ℓ QC code. Hence, it is also an R-submodule of S. The extra column-shift invariance property amounts to being closed under multiplication by y. Thus, 2D cyclic codes are ideals of S.

Remark 1.1.1. Note that both QC and 2D cyclic codes are 2-dimensional codes, where the former has one shift invariance and the latter has two shift invariances.

Remark 1.1.2. Let C_1 and C_2 be length $m\ell$ QC and 2D cyclic codes, respectively, and assume that they have the same generator set in S (or in R^ℓ). Since C_2 is an S-submodule in S and C_1 is an R-submodule in S, C_2 contains C_1. Hence $d(C_1) \geq (C_2)$. In other words, given a QC code, the 2D cyclic code with the same generating elements provide a lower bound for its minimum distance.

1.2 Encoding of QC Codes

After presenting QC codes in vectorial and polynomial terminologies, we now move onto the two equivalent encoding schemes based on these descriptions. We will illustrate the idea first on 1-generator QC codes.

Let $C = \langle \vec{g}(x) \rangle = \langle (g_0(x), \ldots, g_{\ell-1}(x)) \rangle$ be a 1-generator QC code in R^ℓ, where $R = \mathbb{F}_q[x]/\langle x^m - 1 \rangle$ as before. In vectorial presentation, C is a length $m\ell$, index ℓ QC code. Let us write each $g_j(x)$ as

$$g_j(x) = g_{j0} + g_{j1}x + \cdots + g_{j,m-1}x^{m-1}.$$

By (1.1.4), we have the following $m \times \ell$ array (or, length $m\ell$ vector) over $\mathbb{F}_q$ which corresponds to $\vec{g}(x)$

$$\vec{g} := \begin{pmatrix} g_{00} & g_{10} & \cdots & g_{\ell-1,0} \\ g_{01} & g_{11} & \cdots & g_{\ell-1,1} \\ \vdots & \vdots & & \vdots \\ g_{0,m-1} & g_{1,m-1} & \cdots & g_{\ell-1,m-1} \end{pmatrix}$$

Being an R-module, the codewords of C are $\mathbb{F}_q$-linear combinations of the polynomials $\{\vec{g}(x), x\vec{g}(x), \ldots, x^{m-1}\vec{g}(x)\}$ in R^ℓ. Recall that the multiplication of $\vec{g}(x)$ by x in R^ℓ amounts to row shift of $\vec{g}$. Hence, as a subspace in $\mathbb{F}_q^{m\times\ell}$, C is generated by $\mathbb{F}_q$-linear combinations of $\{\vec{g}, x\cdot\vec{g}, \ldots, x^{m-1}\cdot\vec{g}\}$, where for $0 \leq j \leq m-1$, we have

$$x^j \cdot \vec{g} := \begin{pmatrix} g_{0,m-j} & g_{1,m-j} & \cdots & g_{\ell-1,m-j} \\ g_{0,m-j+1} & g_{1,m-j+1} & \cdots & g_{\ell-1,m-j+1} \\ \vdots & \vdots & & \vdots \\ g_{0,m-j-1} & g_{1,m-j-1} & \cdots & g_{\ell-1,m-j-1} \end{pmatrix}$$

Note that the indices are considered mod m so that $g_{0,m}$ should actually be g_{00}, $g_{0,m+1}$ should be g_{01}, and so on. Let us now write each $m \times \ell$ array $x^j \cdot \vec{g}$ as a length $m\ell$ vector over $\mathbb{F}_q$ by listing the entries in columns one after the other:

$$x^j \cdot \vec{g} := (g_{0,m-j}, \ldots, g_{0,m-j-1}; g_{1,m-j}, \ldots, g_{1,m-j-1}; \cdots ; g_{\ell-1,m-j}, \ldots, g_{\ell-1,m-j-1}) \tag{1.2.1}$$

Remark 1.2.1. Note that when we say C is closed under ℓ-shift, we are expanding $m \times \ell$ codewords in C into length $m\ell$ vectors by listing the entries in rows one after the other. So, the vectors in (1.2.1) are in fact obtained from actual codewords in C by a fixed permutation. In other words, the $\mathbb{F}_q$-space generated by vectors in (1.2.1) will be a code which is equivalent to C.

Now let us write each vector in (1.2.1) as a row of an $m \times m\ell$ matrix. Since the $\mathbb{F}_q$-span of these rows generate (a code equivalent to) C, this matrix will be thought of as a generating matrix of C:

$$G := \left(\begin{array}{ccc|ccc|c|ccc} g_{00} & \cdots & g_{0,m-1} & g_{10} & \cdots & g_{1,m-1} & \cdots & g_{\ell-1,0} & \cdots & g_{\ell-1,m-1} \\ g_{0,m-1} & \cdots & g_{0,m-2} & g_{1,m-1} & \cdots & g_{1,m-2} & \cdots & g_{\ell-1,m-1} & \cdots & g_{\ell-1,m-1} \\ \vdots & & \vdots & \vdots & & \vdots & \cdots & \vdots & & \vdots \\ g_{01} & \cdots & g_{00} & g_{00} & \cdots & g_{11} & \cdots & g_{\ell-1,1} & \cdots & g_{\ell-1,0} \end{array} \right)$$

Let each $m \times m$ block in G be denoted by G_j:

$$G_j = \begin{pmatrix} g_{j0} & g_{j1} & \cdots & g_{j,m-1} \\ g_{j,m-1} & g_{j0} & \cdots & g_{j,m-2} \\ \vdots & \vdots & & \vdots \\ g_{j1} & g_{j2} & \cdots & g_{j0} \end{pmatrix}, \quad 0 \leq j \leq \ell - 1. \tag{1.2.2}$$

Note that the rows of G_j are obtained from the previous row by a cyclic shift. Such a matrix is called an $m \times m$ circulant matrix. Hence, a scalar generator matrix for the QC code

$$C = \langle \vec{g}(x) \rangle = \langle (g_0(x), \ldots, g_{\ell-1}(x)) \rangle$$

can be given as

$$G = \begin{pmatrix} G_0 & G_1 & \cdots & G_{\ell-1} \end{pmatrix}, \tag{1.2.3}$$

where each G_j is an $m \times m$ circulant matrix and these blocks are associated to the polynomial entries $g_j(x)$'s in $\vec{g}(x)$.

We will call the $1 \times \ell$ matrix

$$G = \big(g_0(x) \ldots g_{\ell-1}(x) \big) \tag{1.2.4}$$

a polynomial generating matrix (PGM) of C, since

$$C = \{b(x)(g_0(x), \dots, g_{\ell-1}(x)) : b(x) \in R\}. \tag{1.2.5}$$

So, we have introduced a scalar and polynomial generating matrix for a 1-generator QC code.

Remark 1.2.2. The scalar matrix G in (1.2.3) may have linearly independent rows, since it is not expected that every index ℓ, length $m\ell$ QC code has dimension m. So, the actual generating matrix, which has as many rows as the dimension of C, can be obtained by removing the linearly dependent rows from G.

Equivalently, the R-module isomorphism (1.1.5) allows us to view $C \subseteq S$ as an R-submodule generated by $g(x, y) = \psi(\vec{g}(x))$ in S and (1.2.5) becomes

$$C = \{c(x, y) = b(x)G : b(x) \in R\}, \tag{1.2.6}$$

where $G = \big(g(x, y)\big)$ is the corresponding PGM over S.

Now let us extend these notions to the r-generator case. Let $C \subseteq R^\ell$ be generated by $\{\vec{g}_1(x), \dots, \vec{g}_r(x)\}$, then

$$\begin{aligned} C &= \langle \vec{g}_1(x), \dots, \vec{g}_r(x) \rangle \\ &= \langle \big(g_{10}(x), \dots, g_{1,\ell-1}(x)\big), \dots, \big(g_{r0}(x), \dots, g_{r,\ell-1}(x)\big) \rangle \\ &= \left\{ \vec{c}(x) = \sum_{i=1}^{r} b_i(x)\big(g_{i0}(x), \dots, g_{i,\ell-1}(x)\big) : b_i(x) \in R \right\}. \end{aligned} \tag{1.2.7}$$

Hence,

$$C = \big\{\vec{c}(x) = \big(b_1(x), \dots, b_r(x)\big)G : b_i(x) \in R\big\}, \tag{1.2.8}$$

where G is the following PGM:

$$G = \begin{pmatrix} \vec{g}_1(x) \\ \vec{g}_2(x) \\ \vdots \\ \vec{g}_r(x) \end{pmatrix} = \begin{pmatrix} g_{10}(x) & \cdots & g_{1,\ell-1}(x) \\ g_{20}(x) & \cdots & g_{2,\ell-1}(x) \\ \vdots & & \vdots \\ g_{r0}(x) & \cdots & g_{r,\ell-1}(x) \end{pmatrix} \tag{1.2.9}$$

As in 1-generator case, we can write a scalar generator matrix for C as

$$G = \begin{pmatrix} G_{10} & G_{11} & \cdots & G_{1,\ell-1} \\ G_{20} & G_{21} & \cdots & G_{2,\ell-1} \\ \vdots & \vdots & & \vdots \\ G_{r0} & G_{r1} & \cdots & G_{r,\ell-1} \end{pmatrix}, \tag{1.2.10}$$

where each G_{ij} is the circulant matrix corresponding to $g_{ij}(x)$ as in (1.2.2).

If C is considered as an R-submodule in S, then to $\vec{g}_j(x) \in R^\ell$ we associate $g_j(x, y) = \psi(\vec{g}_j(x)) \in S$ for each $0 \leq j \leq \ell - 1$ and then(1.2.9) becomes

$$G = \begin{pmatrix} g_1(x,y) \\ g_2(x,y) \\ \vdots \\ g_r(x,y) \end{pmatrix}.$$

1.3 Concatenated Structure of QC Codes

We now describe the decomposition of a q-ary QC code into shorter codes over extensions of $\mathbb{F}_q$. We follow the brief presentation in [16] and refer to [23] for details. Consider the factorization of $x^m - 1$ into irreducibles in $\mathbb{F}_q[x]$, say

$$x^m - 1 = f_1(x) f_2(x) \ldots f_s(x). \tag{1.3.1}$$

Since m is relatively prime to q, there are no repeating factors in (1.3.1). By Chinese Remainder Theorem we have the following ring isomorphism.

$$R \cong \bigoplus_{i=1}^{s} \mathbb{F}_q[x]/\langle f_i(x) \rangle. \tag{1.3.2}$$

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 $i = 1, 2, \ldots, s$, 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 (1.3.2) 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

$$\begin{aligned} R &\cong \mathbb{E}_1 \oplus \cdots \oplus \mathbb{E}_s \\ a(x) &\mapsto \left(a(\xi^{u_1}), \ldots, a(\xi^{u_s})\right). \end{aligned} \tag{1.3.3}$$

This implies that

$$\begin{array}{ccc} R^\ell & \cong & \mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell \\ \vec{a}(x) = (a_0(x), \ldots, a_{\ell-1}(x)) & \longmapsto & [(a_0(\xi^{u_1}), \ldots, a_{\ell-1}(\xi^{u_1})), \ldots, (a_0(\xi^{u_s}), \ldots, a_{\ell-1}(\xi^{u_s}))]\,. \end{array} \tag{1.3.4}$$

Hence, a QC code $C \subset R^\ell$ can be viewed as an $(\mathbb{E}_1 \oplus \cdots \oplus \mathbb{E}_s)$-submodule of $\mathbb{E}_1^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell$ and decomposes as

$$C = C_1 \oplus \cdots \oplus C_s, \tag{1.3.5}$$

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

For an r-generator QC code $C = \langle \vec{g}_1(x), \ldots, \vec{g}_r(x) \rangle \subset R^\ell$ we have

$$C_i = \text{span}_{\mathbb{E}_i}\{(g_{j,0}(\xi^{u_i}), \ldots, g_{j,\ell-1}(\xi^{u_i})) \in \mathbb{E}_i^\ell | 1 \leq j \leq r\}$$

by (1.3.4) and $C_i = 0$ if and only if $f_i(x) \mid g_{j,t}(x)$ for all $1 \leq j \leq r$, $0 \leq t \leq \ell - 1$.

Note that each field $\mathbb{E}_i$ is isomorphic to a minimal cyclic code of length m over $\mathbb{F}_q$. Namely, consider the cyclic code of length m whose check polynomial is $f_i(x)$ (i.e. the code is generated by $\frac{x^m-1}{f_i(x)}$). Let θ_i denote the generating primitive idempotent for the minimal cyclic code ([22, Theorem 6.4.1 and Definition 6.4.2]) The isomorphism between $\langle \theta_i \rangle$ and $\mathbb{E}_i$ is given by the maps

$$\begin{array}{rcl} \varphi_i : \langle \theta_i \rangle & \longrightarrow & \mathbb{E}_i \\ a(x) & \longmapsto & a(\xi^{u_i}) \end{array} \qquad \begin{array}{rcl} \psi_i : \mathbb{E}_i & \longrightarrow & \langle \theta_i \rangle \\ \delta & \longmapsto & \sum\limits_{k=0}^{m-1} a_k x^k \end{array} \quad , \tag{1.3.6}$$

where

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

If C_i is a length ℓ linear code over $\mathbb{E}_i$, we will denote its concatenation with $\langle \theta_i \rangle$ by $\langle \theta_i \rangle \Box C_i$ and the concatenation will be carried out by the map ψ_i. In other words, each entry of the codewords of C_i are mapped by ψ_i to length m codewords in $\langle \theta_i \rangle$ so that we obtain a length $m\ell$ vector over $\mathbb{F}_q$. If we apply this concatenation for each $i = 1, \ldots, s$, we get the following concatenated description for QC codes, which is given by Jensen.

Theorem 1.3.1. *([19]) (i) Let C be an R-submodule of S (i.e. a QC code). Then for some subset $\mathcal{I}$ of $\{1,\ldots,s\}$, there exist linear codes C_i of length ℓ over $\mathbb{E}_i$ (which can be explicitly described) such that $C = \oplus_{i\in\mathcal{I}}\langle\theta_i\rangle\Box C_i$.*

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

It is proved in [16] that for a given QC code C, the constituents C_i's in (1.3.5) and the outer codes C_i's in the concatenated structure are equal to each other (see [16, Theorem 4.1]).

1.4 Convolutional Codes

QC codes are not only closely related to cyclic and 2D cyclic codes, but also to another well-studied class of codes, namely convolutional codes. In this section we will cover some basic facts on convolutional codes and then present their link to QC codes.

An (ℓ, k) convolutional code C over $\mathbb{F}_q$ is defined as a k-dimensional $\mathbb{F}_q(x)$-subspace of $\mathbb{F}_q(x)^\ell$. The weight of an element $c(x) \in \mathbb{F}_q(x)$ is defined as the number of terms in $c(x)$ expressed as a Laurent series, since every rational function has a unique causal Laurent series representation. Therefore, the weight of a codeword $\vec{c}(x) = (c_0(x),\ldots,c_{\ell-1}(x)) \in C$ is the sum of the weights of its coordinates. The free distance of the convolutional code $d_f(C)$ is the minimum weight among nonzero codewords.

An encoder of C is a $k\times\ell$ matrix over $\mathbb{F}_q(x)$, which is called a generator matrix of C as usual. By clearing off the denominators of all the entries in any generating matrix, we can obtain a polynomial generator matrix (PGM) for C which is a $k\times\ell$ matrix G of rank k with entries from $\mathbb{F}_q[x]$ such that

$$C = \left\{(u_0(x),\ldots,u_{k-1}(x))\,G:\ (u_0(x),\ldots,u_{k-1}(x)) \in \mathbb{F}_q(x)^k\right\}. \tag{1.4.1}$$

Moreover, it is usually assumed that G is noncatastrophic in the sense that finite weight codewords of C can only be produced from finite weight information words. For instance, consider the following PGM

$$G = \left(x^2+1, x+1\right),$$

which generates a $(2,1)$-convolutional code C over $\mathbb{F}_2$. Let

$$u(x) = 1 + x + x^2 + \cdots = \frac{1}{x+1}.$$

Then $u(x)G = (x+1, 1)$ which is a codeword with weight 3 but $wt(u(x)) = \infty$. This may cause an infinite number of fails in the decoding, which is undesired.

Definition 1.4.1. ([26, 29]) Let G be a PGM for an (ℓ, k) convolutional code.

i. G is noncatastrophic if and only if the greatest common divisor of all $k \times k$ minors of G is x^b for some nonnegative integer b.

ii. G is basic if and only if the greatest common divisor of all $k \times k$ minors of G is 1.

In this sense, $G = \big(x+1, 1\big)$ is a basic (hence, noncatastrophic) PGM for the example above. Note that a basic PGM exists for any convolutional code (see [29, Section 3]).

Remark 1.4.2. If C is given with a basic PGM, then all finite weight codewords with polynomial coordinates come from information words with polynomial coordinates ([29]).

Viewing convolutional codes as linear codes over $\mathbb{F}_q(x)$ leads to codewords with infinite weight, which can not occur in practice and there is no reason to use this as the definition (see [8, 21]). Moreover, again due to practical purposes, finite weight codewords which are causal are of interest ([21, 29]). These are exactly the polynomial codewords. For this reason, we consider an (ℓ, k) convolutional code C as a rank k $\mathbb{F}_q[x]$-submodule of $\mathbb{F}_q[x]^\ell$. Note that C is necessarily a free module since $\mathbb{F}_q[x]$ is a principal ideal domain. Such convolutional codes are also called finite support convolutional codes ([4]) and in this case (1.4.1) turns out to be

$$C = \left\{ (u_0(x), \ldots, u_{k-1}(x))\, G : \ (u_0(x), \ldots, u_{k-1}(x)) \in \mathbb{F}_q[x]^k \right\}. \tag{1.4.2}$$

Observe that if G is a basic PGM for C, then (1.4.2) describes all the polynomial codewords (since polynomial output implies polynomial input for a basic PGM).

We are ready to associate a QC code to a given convolutional code. Let $R = \mathbb{F}_q[x]/\langle x^m - 1\rangle$ as before and consider the projection map

$$\begin{aligned} \Phi : \mathbb{F}_q[x] &\longrightarrow R \\ f(x) &\mapsto f'(x) := f(x) \mod \langle x^m - 1\rangle. \end{aligned} \tag{1.4.3}$$

It is clear that for a given (ℓ, k) convolutional code C, there is a natural QC code C' related to it (of length $m\ell$ and index ℓ, for any $m > 1$) as shown below. Note that we denote the map from C to C' also by Φ.

$$\begin{aligned} \Phi : C &\longrightarrow C' \\ \vec{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x)) &\mapsto \vec{c'}(x) = (c'_0(x), \ldots, c'_{\ell-1}(x)). \end{aligned} \tag{1.4.4}$$

In fact, the minimum distance of the QC code C' is a lower bound on the free distance of the convolutional code C, as shown by Lally ([21]). We will formulate several crucial findings of Lally in the following. Note that the last result below is a consequence of the first two.

Theorem 1.4.3. *([21, Theorem 2 and its proof]) Let C be an (ℓ, k) convolutional code over $\mathbb{F}_q$ with a basic PGM and C' be the related QC code in R^ℓ. Let $\vec{c}$ be a codeword in C and set $\vec{c'} = \Phi(\vec{c}) \in C'$.*

i. If $\vec{c'}(x) \neq 0$, then $wt(\vec{c}) \geq wt(\vec{c'})$.

ii. If $\vec{c'}(x) = \vec{0}$, let $\gamma \geq 1$ be the maximal positive integer such that $(x^m - 1)^\gamma$ divides each coordinate of $\vec{c}$. Write $\vec{c} = (x^m - 1)^\gamma\, (v_0(x), \ldots, v_{\ell-1}(x))$ and set $\vec{v} = (v_0(x), \ldots, v_{\ell-1}(x))$. Then, $\vec{v}$ is a codeword of C. Moreover, by using the weight preserving property proven in [25], we have $wt(\vec{c}) \geq wt(\vec{v'})$ for $\vec{v'} \in C' \setminus \{\vec{0}\}$

iii. By (i) and (ii), $d_f(C) \geq d(C')$.

An important fact to emphasize is that the assumption of a basic PGM for the given convolutional code is crucial in this theorem since a catastrophic PGM may violate the second result, as the following example shows.

Example 1.4.4. Let C be a $(2,1)$ convolutional code over $\mathbb{F}_2$ with the PGM below

$$G = \left(\begin{array}{cc} x^2+x+1 & x^2+x+1 \end{array} \right)$$

and suppose that C' is the related QC code in $(\mathbb{F}_2[x]/\langle x^3+1\rangle)^2$. Then $\vec{c}(x) = (x^3+1, x^3+1)$ is a codeword in C and $\vec{c'}(x) = \vec{0}$. But $\vec{c} = (x^3+1)\cdot(1,1)$ and $\vec{v} = (1,1)$ is not a codeword of C, which is considered as an $\mathbb{F}_2[x]$-submodule in $\mathbb{F}_2[x]^2$. Therefore we have to take the PGM $G = (1,1)$, which is basic.

Remark 1.4.5. Let us note that Lally uses an alternative module description of convolutional and QC codes in [21]. Namely, a basis $\{1, \alpha, \ldots, \alpha^{\ell-1}\}$ of $\mathbb{F}_{q^\ell}$ over $\mathbb{F}_q$ is fixed and the $\mathbb{F}_q[x]$-modules $\mathbb{F}_q[x]^\ell$ and $\mathbb{F}_{q^\ell}[x]$ are identified via the following map:

$$\begin{array}{rcl} \mathbb{F}_q[x]^\ell & \longrightarrow & \mathbb{F}_{q^\ell}[x] \\ \vec{c}(x) = (c_0(x), \ldots, c_{\ell-1}(x)) & \mapsto & c(x) = \displaystyle\sum_{i=0}^{\ell-1} c_i(x)\alpha^i \end{array}$$

With this identification, a length ℓ convolutional code is viewed as an $\mathbb{F}_q[x]$-module in $\mathbb{F}_{q^\ell}[x]$ and a length $m\ell$, index ℓ QC code is viewed as an $\mathbb{F}_q[x]$-module in $\mathbb{F}_{q^\ell}[x]/\langle x^m - 1\rangle$. However, all of Lally's findings can be translated to the module descriptions that we have been using for convolutional and QC codes and this is how they are presented in Theorem 1.4.3.

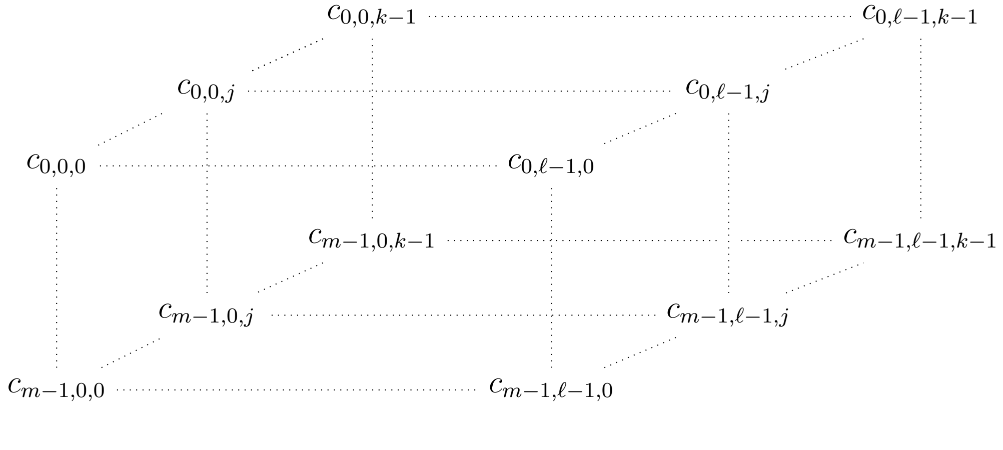
Chapter 2

Multidimensional Quasi-Cyclic Codes

In this chapter, multidimensional generalization of quasi-cyclic codes will be introduced. Due to the ease in visualization of the idea, we first focus on 3D codes in the following section. Generalization to arbitrary dimension as well as the study of their algebraic structure are given in later sections.

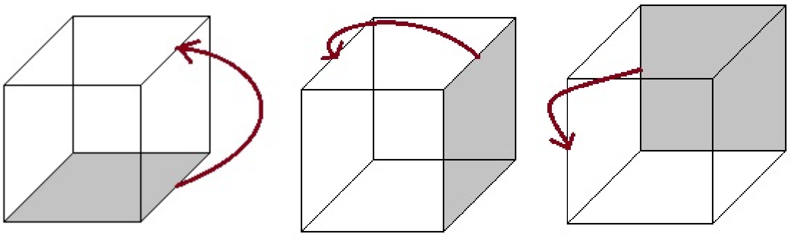
2.1 Quasi 2D Cyclic and 3D Cyclic Codes

Let C be a q-ary length $m\ell k$ linear code and view its codewords as $m \times \ell \times k$ cubes as follows:



(2.1.1)

A 3D code C is called a 3D cyclic if it is closed under bottom-to-top, right-to-left and back-to-front face shifts of its codewords (see the figures below). Let us note that multidimensional cyclic codes have been studied in the literature (see [13, 15, 17, 18, 32]).



(2.1.2)

Moreover, the codewords of a 3D cyclic code can be put into a 2D form. For this, let us write the cube (2.1.1) as a $m \times \ell k$ array in $\mathbb{F}_q^{m\times \ell k}$:

$$\left(\begin{array}{ccc|c|ccc}
c_{000} & \cdots & c_{0,\ell-1,0} & \cdots\ \cdots & c_{0,0,k-1} & \cdots & c_{0,\ell-1,k-1} \\
c_{100} & \cdots & c_{1,\ell-1,0} & \cdots\ \cdots & c_{1,1,k-1} & \cdots & c_{1,\ell-1,k-1} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
c_{m-1,0,0} & \cdots & c_{m-1,\ell-1,0} & \cdots\ \cdots & c_{m-1,0,k-1} & \cdots & c_{m-1,\ell-1,k-1}
\end{array}\right) \tag{2.1.3}$$

So, a length $m\ell k$ linear code $C \subset \mathbb{F}_q^{m\ell k}$ is called 3D cyclic if its codewords viewed as $m \times \ell k$ arrays are not only closed under row shift and column shifts in each $m \times \ell$ subarrays, but also under shift of $m \times \ell$ subarrays.

Remark 2.1.1. It is easy to see that the arrows in (2.1.3) correspond to face shifts in the 3D picture. Namely, the bottom-to-top, right-to-left and back-to-front face shifts in the 3D representation (2.1.2) correspond to row shift, column shift in each $m \times \ell$ subarrays and $m \times \ell$ block shift, respectively. Hence, the codewords of a 3D cyclic code are closed under shift by ℓk, mk and $m\ell$ positions.

Observe that for $k = 1$ we get a 2D cyclic code. Recall from Chapter 1 that a QC code is a 2D linear code which misses one of the shift invariances that a 2D cyclic code has. We proceed similarly to define quasi 2D cyclic codes.

Definition 2.1.2. A length $m\ell k$ linear code $C \subset \mathbb{F}_q^{m\ell k}$ is called a quasi 2D cyclic (Q2DC) code if its codewords viewed as $m \times \ell k$ arrays are closed under row shift and column shifts in each $m \times \ell$ subarrays.

$$\left(\begin{array}{ccc|c|ccc}
c_{000} & \cdots & c_{0,\ell-1,0} & \cdots\ \cdots & c_{0,0,k-1} & \cdots & c_{0,\ell-1,k-1} \\
c_{100} & \cdots & c_{1,\ell-1,0} & \cdots\ \cdots & c_{1,1,k-1} & \cdots & c_{1,\ell-1,k-1} \\
\vdots & \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\
c_{m-1,0,0} & \cdots & c_{m-1,\ell-1,0} & \cdots\ \cdots & c_{m-1,0,k-1} & \cdots & c_{m-1,\ell-1,k-1}
\end{array}\right) \tag{2.1.4}$$

In other words, the codewords of a Q2DC code $C \subset \mathbb{F}_q^{m\ell k}$ are closed under shift by ℓk and mk positions. Therefore, C can be viewed as an index ℓk QC code.

Remark 2.1.3. The codewords of a Q2DC cyclic code C viewed as $m \times \ell \times k$ cubes as in (2.1.1) are closed under bottom-to-top, right-to-left shifts (see 2.1.2). Therefore, just like the case in QC and 2D cyclic codes, 3D cyclic codes can also be viewed as a special case of Q2DC codes with one more shift invariance.

In order to realize the algebraic description of Q2DC cyclic codes, let $J = \langle x^m - 1, y^\ell - 1\rangle$ be an ideal of $\mathbb{F}_q[x, y]$ and set $S := \mathbb{F}_q[x, y]/J$ as before. For an $m \times \ell \times k$ cube $c \in \mathbb{F}_q^{m\times\ell\times k}$ as in (2.1.1), assign an element of S^k via the following analogue of the map ϕ in (1.1.4):

$$\begin{aligned}
\phi' : \mathbb{F}_q^{m\times\ell\times k} &\longrightarrow S^k \\
(c_{i,j,t}) &\mapsto \vec{c}(x, y) = (c_0(x, y), \ldots, c_{k-1}(x, y)) ,
\end{aligned} \tag{2.1.5}$$

where for each $0 \le t \le k - 1$,

$$c_t(x, y) = \sum_{i=0}^{m-1}\sum_{j=0}^{\ell-1} c_{i,j,t}x^i y^j \in S. \tag{2.1.6}$$

Now, let $U = \langle x^m - 1, y^\ell - 1, z^k - 1\rangle$ be an ideal of $\mathbb{F}_q[x, y, z]$ and define the quotient ring $P := \mathbb{F}_q[x, y, z]/U$. Then we define the following analogue of the map ψ in (1.1.5):

$$\begin{aligned}
\psi' : S^k &\longrightarrow P \\
\vec{c}(x, y) &\mapsto c(x, y, z),
\end{aligned} \tag{2.1.7}$$

where

$$c(x, y, z) = \sum_{t=0}^{k-1} c_t(x, y)z^t = \sum_{t=0}^{k-1}\sum_{i=0}^{m-1}\sum_{j=0}^{\ell-1} c_{i,j,t}x^i y^j z^t. \tag{2.1.8}$$

Note that under these identifications, bottom-to-top and right-to-left face shifts of $(c_{i,j,t}) \in \mathbb{F}_q^{m\times\ell\times k}$ correspond, respectively, to multiplication by x and y (componentwise) in S^k and in P. The back-to-front shift of $(c_{i,j,t})$ corresponds to cyclic shift of $\vec{c}(x,y)$ in S^k and to multiplication by z in P.

The following is immediate after the preparation provided above.

Proposition 2.1.4. *A Q2DC code as in Definition 2.1.2 is an S-submodule in S^k and in P. Moreover, a 3D cyclic code is an ideal in P.*

Remark 2.1.5. It has been noted by Ling and Solé in [23] that a QC code C of length $m\ell$ and index ℓ can be characterized algebraically by the automorphism group $\mathrm{Perm}(C)$ of the code, which is a subgroup of the symmetric group $S_{m\ell}$. Namely, C is QC of length $m\ell$ and index ℓ if and only if there exists a fixed point free permutation in $\mathrm{Perm}(C)$ that consists of ℓ disjoint cycles of length m. With our notation so far, a 3D linear code C of length $m \times \ell \times k$ is a Q2DC code if and only if there exists a fixed point free permutation in $\mathrm{Perm}(C)$ which consists of ℓk disjoint cycles of length m and there exists another fixed point free permutation in $\mathrm{Perm}(C)$ which consists of mk disjoint cycles of length ℓ.

2.2 QnDC Codes

We have extended the definition of QC codes to Q2DC codes, which are 3D codes with 2 shift invariances, and described their algebraic structure in the previous section. We now move onto the higher dimensional generalizations of QC codes. For this, let us first define certain rings:

$$\begin{aligned}
R_1 &= \mathbb{F}_q[x_1]/\langle x_1^{m_1}-1\rangle \\
R_2 &= \mathbb{F}_q[x_1,x_2]/\langle x_1^{m_1}-1, x_2^{m_2}-1\rangle \\
\vdots\ & \ \ \vdots \\
R_n &= \mathbb{F}_q[x_1,\dots,x_n]/\langle x_1^{m_1}-1,\dots,x_n^{m_n}-1\rangle \\
R_{n+1} &= \mathbb{F}_q[x_1,\dots,x_{n+1}]/\langle x_1^{m_1}-1,\dots,x_{n+1}^{m_{n+1}}-1\rangle
\end{aligned} \tag{2.2.1}$$

Here, m_i's are positive integers and m_1 will be assumed to be relatively prime to q. Note that the rings R, S and P in Section 2.1 are the first three rings above.

Keeping the analogy with QC and Q2DC codes, a quasi nD cyclic code will be an $(n+1)$D linear code with n shift invariances. Algebraically, the natural definition that corresponds to this is as follows.

Definition 2.2.1. A quasi nD cyclic code (QnDC) C over $\mathbb{F}_q$ of length $m_1 \times \cdots \times m_{n+1}$ is an R_n-submodule of R_{n+1}. Alternatively, C can be defined as an R_n-module in $R_n^{m_{n+1}}$ (this was done for $n = 2$ case (Proposition 2.1.4) via the identification given in (2.1.7)).

Let us note that an $(n+1)$D cyclic code of length $m_1 \times \cdots \times m_{n+1}$ is an ideal in R_{n+1} ([15, 32]). In particular, it is also a QnDC code.

Remark 2.2.2. We can characterize QnDC codes via their automorphism groups as we did for $n = 2$ case in Remark 2.1.5. Namely, an $(n+1)D$ linear code C of length $m_1 \times \cdots \times m_{n+1}$ is QnDC if and only if $\mathrm{Perm}(C)$ contains n fixed point free automorphisms $\sigma_1, \ldots, \sigma_n$, where each σ_i consists of $m_1 \cdots m_{i-1} m_{i+1} \cdots m_{n+1}$ disjoint cycles of length m_i.

Remark 2.2.3. We can extend the distance relation given in Remark 1.1.2 to nD case as well. If C_1 and C_2 are QnDC and $(n+1)$D cyclic codes given with the same generator set in R_{n+1}, respectively, then $C_1 \subseteq C_2$ and hence $d(C_1) \geq d(C_2)$.

Now let us generalize the encoding of the QC codes given in Section 1.2 to QnDC codes. We begin with 1-generator Q2DC codes: let $C = \langle \vec{g}(x,y) \rangle = \langle \big(g_0(x,y), \ldots, g_{k-1}(x,y)\big) \rangle$ be an S-submodule in S^k where $S = \mathbb{F}_q[x,y]/\langle x^m - 1, y^\ell - 1 \rangle$ as in Section 2.1. Then

$$C = \big\{ \vec{c}(x,y) = \big(b(x,y)g_0(x,y), \ldots, b(x,y)g_{k-1}(x,y) \big) : b(x,y) \in S \big\}$$

and $G = \big(g_0(x,y), g_1(x,y), \ldots, g_{k-1}(x,y)\big)$ is the corresponding PGM for C in S^k.

Equivalently, $C = \langle g(x,y,z) \rangle \subset P$, where $P \simeq S^k = \mathbb{F}_q[x,y,z]/\langle x^m - 1, y^\ell - 1, z^k - 1 \rangle$ as before and $g(x,y,z) = \psi'(\vec{g}(x,y))$. From this point of view,

$$C = \{ c(x,y,z) = b(x,y)g(x,y,z) : b(x,y) \in S \}$$

and $\big(g(x,y,z)\big)$ is the PGM of C in P.

If $C = \langle \vec{g}_1(x,y), \ldots, \vec{g}_r(x,y) \rangle$ is an r-generator Q2DC code in S^k, where

$$\begin{aligned} \vec{g}_1(x,y) &= \big(g_{10}(x,y), \ldots, g_{1,k-1}(x,y)\big) \\ \vdots \quad & \quad \vdots \\ \vec{g}_r(x,y) &= \big(g_{r0}(x,y), \ldots, g_{r,k-1}(x,y)\big), \end{aligned}$$

then

$$C = \left\{ \vec{c}(x,y) = \left(\sum_{t=1}^{r} b_t(x,y) g_{t0}(x,y), \ldots, \sum_{t=1}^{r} b_t(x,y) g_{t,k-1}(x,y) \right) : b_t(x,y) \in S \right\}.$$

In this case, the PGM for C over S is given by

$$G = \begin{pmatrix} g_{10}(x,y) & g_{11}(x,y) & \cdots & g_{1,k-1}(x,y) \\ g_{20}(x,y) & g_{21}(x,y) & \cdots & g_{2,k-1}(x,y) \\ \vdots & \vdots & & \vdots \\ g_{r0}(x,y) & g_{r1}(x,y) & \cdots & g_{r,k-1}(x,y) \end{pmatrix}. \tag{2.2.2}$$

Clearly, by setting $g_i(x,y,z) = \psi'(\vec{g}_i(x,y))$, we get the following PGM in T:

$$G = \begin{pmatrix} g_1(x,y,z) \\ \vdots \\ g_r(x,y,z) \end{pmatrix}.$$

Now we describe the encoders for QnDC codes. Let C be a 1-generator QnDC code with $C = \langle g(x_1, ..., x_{n+1}) \rangle \subset R_{n+1}$. Then, as we did for $n = 2$ case in (1.2.6),

$$C = \{c(x_1, ..., x_{n+1}) = b(x_1, ..., x_n)G : b(x_1, ..., x_n) \in R_n\} \tag{2.2.3}$$

and $G = \big(g(x_1, ..., x_{n+1})\big)$ is the corresponding PGM for C in R_{n+1}.

There exists a uniquely determined element $\vec{g}(x_1, ..., x_n) \in R_n^{m_{n+1}}$, which is obtained by the following analogue of the maps (1.1.5) and (2.1.7)

$$\begin{aligned} \Psi : R_n^{m_{n+1}} &\longrightarrow R_{n+1} \\ \vec{g}(x_1, ..., x_n) &\mapsto g(x_1, ..., x_{n+1}) = \sum_{i=0}^{m_{n+1}-1} g_i(x_1, ..., x_n) x_{n+1}^i. \end{aligned} \tag{2.2.4}$$

Obviously, Ψ is an isomorphism and therefore we have the following PGM for C over R_n, which generalizes (1.2.4):

$$G = \begin{pmatrix} g_0(x_1, ..., x_n) & g_1(x_1, ..., x_n) & \cdots & g_{m_{n+1}-1}(x_1, ..., x_n) \end{pmatrix} \tag{2.2.5}$$

Now let $C = \langle g_1(x_1, ..., x_{n+1}), \ldots, g_r(x_1, ..., x_{n+1}) \rangle \in R_{n+1}$ be an r-generator QnDC code. In this case (2.2.3) turns out to be

$$C = \left\{ c(x_1, ..., x_{n+1}) = \sum_{t=1}^{r} b_t(x_1, ..., x_n) g_t(x_1, ..., x_{n+1}) : b_t(x_1, ..., x_n) \in R_n \right\}$$

where

$$G = \begin{pmatrix} g_1(x_1, ..., x_{n+1}) \\ \vdots \\ g_r(x_1, ..., x_{n+1}) \end{pmatrix}$$

and

$$G = \begin{pmatrix} g_{10}(x_1, ..., x_n) & g_{11}(x_1, ..., x_n) & \cdots & g_{1,m_{n+1}-1}(x_1, ..., x_n) \\ g_{20}(x_1, ..., x_n) & g_{21}(x_1, ..., x_n) & \cdots & g_{2,m_{n+1}-1}(x_1, ..., x_n) \\ \vdots & \vdots & & \vdots \\ g_{r0}(x_1, ..., x_n) & g_{r1}(x_1, ..., x_n) & \cdots & g_{r,m_{n+1}-1}(x_1, ..., x_n) \end{pmatrix} \tag{2.2.6}$$

are the corresponding PGM's for C in R_{n+1} and R_n, respectively. We have $C = \langle \vec{g}_1(x_1, ..., x_n), \ldots, \vec{g}_1(x_1, ..., x_n) \rangle \in R_n^{m_{n+1}}$ where $g_t(x_1, ..., x_{n+1}) = \Psi(\vec{g}_t(x_1, ..., x_n))$ for all $1 \leq t \leq n$. By using (1.2.1) for each x_j and $\vec{g}_t(x_1, ..., x_n)$ with $1 \leq j \leq n$ and $1 \leq t \leq r$, we can also get a generator matrix for C over $\mathbb{F}_q$.

2.3 Concatenated Structure and Asymptotics

Being a QC code, both QnDC and $(n+1)$D cyclic codes have concatenated structures. It was proved in [16, Theorem 4.3] that outer codes (or constituents) of an $(n+1)$D cyclic code are nD cyclic codes. We now prove the analogue of that statement for QnDC codes. We assume that $x^{m_1} - 1$ factors into irreducibles over $\mathbb{F}_q[x]$ as in (1.3.1) (setting $m = m_1$) and use the notations in (1.3.2), (1.3.3), (1.3.4) and (1.3.5). We let ξ be a primitive m_1^{th} root of unity over $\mathbb{F}_q$.

Theorem 2.3.1. *Let $n \geq 2$ and $(m_1, q) = 1$. For each $1 \leq i \leq s$, let $\langle\theta_i\rangle$ be the minimal cyclic code of length m_1 over $\mathbb{F}_q$, whose parity check polynomial is $f_i(x)$ and which is generated by the primitive idempotent θ_i.*

i. If C is a QnDC code of length $m_1 \times \cdots \times m_{n+1}$ over $\mathbb{F}_q$, then it can be decomposed as

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

where each C_i is a Q(n-1)DC code of length $m_2 \times \cdots \times m_{n+1}$ over $\mathbb{E}_i$.

ii. Conversely, if C_i is a Q(n-1)DC code of length $m_2 \times \cdots \times m_{n+1}$ over $\mathbb{E}_i$ (for each i), then

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

is a QnDC code of length $m_1 \times \cdots \times m_{n+1}$ over $\mathbb{F}_q$.

Proof. View C as a QC code of index $m_2 \cdots m_{n+1}$ and note by [16, Theorem 4.3] that its constituents lie in

$$\mathbb{E}_i^{m_2 \times \cdots \times m_{n+1}} \simeq \mathbb{E}_i[x_2, \ldots, x_{n+1}]/\langle x_2^{m_2} - 1, \ldots, x_{n+1}^{m_{n+1}} - 1\rangle.$$

Each constituent C_i (for $1 \leq i \leq s$) is of the form

$$C_i = \left\{ \sum_{a_2=0}^{m_2-1} \cdots \sum_{a_{n+1}=0}^{m_{n+1}-1} \left[\sum_{k=0}^{m_1-1} c_{ka_2 \ldots a_{n+1}} \xi^{ku_i} \right] x_2^{a_2} \ldots x_{n+1}^{a_{n+1}} : \left(c_{ka_2 \ldots a_{n+1}} \right) \in \mathcal{C} \right\}.$$

Since C is an R_n-submodule in R_{n+1}, it is closed under multiplication by $x_2, ..., x_n$ and by elements of $\mathbb{F}_q$. Hence, C_i is closed under multiplication by $x_2, ..., x_n$ and by elements of $\mathbb{F}_q$. It remains to show that $\mathcal{C}_i$ is also closed under multiplication by ξ^{u_i} to conclude that it is a $\mathbb{E}_i[x_2, \ldots, x_n]/\langle x_2^{m_2} - 1, \ldots, x_n^{m_n} - 1\rangle$-submodule in $\mathbb{E}_i[x_2, \ldots, x_{n+1}]/\langle x_2^{m_2} - 1, \ldots, x_{n+1}^{m_{n+1}} - 1\rangle$ (i.e. C_i is a Q$(n-1)$DC code over $\mathbb{E}_i$). If we take an arbitrary codeword from C_i and multiply it with ξ^{u_i}, it takes the form

$$\sum_{a_2=0}^{m_2-1} \cdots \sum_{a_{n+1}=0}^{m_{n+1}-1} \left(\sum_{k=0}^{m_1-1} c_{ka_2 \ldots a_{n+1}} \xi^{(k+1)u_i} \right) x_2^{a_2} \cdots x_{n+1}^{a_{n+1}}.$$

This polynomial is obtained from the polynomial $x_1c(x_1,\ldots,x_{n+1})$, where

$$c(x_1,\ldots,x_{n+1}) = \sum_{a_2=0}^{m_2-1}\cdots\sum_{a_{n+1}=0}^{m_{n+1}-1}\left[\sum_{k=0}^{m_1-1} c_{ka_2\ldots a_{n+1}}x_1^k\right] x_2^{a_2}\cdots x_{n+1}^{a_{n+1}}.$$

Note that we have not used the fact that C is closed under multiplication by x_1 so far. Using this fact, $x_1c(x_1,\ldots,x_{n+1}) \in C$ and part i is proved.

For the converse recall that C_i is a $\mathbb{E}_i[x_2,\ldots,x_n]/\langle x_2^{m_2}-1,\ldots,x_n^{m_n}-1\rangle$- submodule in $\mathbb{E}_i[x_2,\ldots,x_{n+1}]/\langle x_2^{m_2}-1,\ldots,x_{n+1}^{m_{n+1}}-1\rangle$ for each i. Moreover, the concatenation is of the form (cf. (1.3.6))

$$\langle\theta_i\rangle\Box C_i = \left\{\sum_{a_2=0}^{m_2-1}\cdots\sum_{a_{n+1}=0}^{m_{n+1}-1}\psi_i(c_{a_2\ldots a_{n+1}})x_2^{a_2}\cdots x_{n+1}^{a_{n+1}} : \left(c_{a_2,\ldots,a_{n+1}}\right)\in C_i\right\}.$$

Since $\langle\theta_i\rangle$ is a cyclic code of length m_1 over $\mathbb{F}_q$, $\psi_i(c_{a_2\ldots a_{n+1}})$ lies in $\mathbb{F}_q[x_1]/\langle x_1^{m_1}-1\rangle$ and hence $\langle\theta_i\rangle\Box C_i \subset \mathbb{E}_i[x_1,\ldots,x_{n+1}]/\langle x_1^{m_1}-1,\ldots,x_{n+1}^{m_{n+1}}-1\rangle$ which is closed under multiplication by $x_2,\ldots,x_{n+1}$ and by constants in $\mathbb{E}_i$ due to the fact that C_i is Q$(n-1)$DC. Moreover, it is also closed under multiplication by x_1 since $\psi_i(c_{a_2\ldots a_{n+1}}) \in \langle\theta_i\rangle$ and $\langle\theta_i\rangle$ is an ideal of $\mathbb{F}_q[x_1]/\langle x_1^{m_1}-1\rangle$. This finishes the proof. □

It is known that QC codes and various special families of QC codes are asymptotically good ([6, 20, 24, 28]). Our goal in this section is to show that for any $n \geq 2$, QnDC codes are also asymptotically good. For this, we will utilize the concatenated structure of these codes.

Theorem 2.3.2. *For every $n \geq 2$ and any finite field $\mathbb{F}_q$, there exists an asymptotically good sequence of QnDC codes over $\mathbb{F}_q$. When these codes are viewed as QC codes, their index is $N/(q+1)$ where N denotes the length of the codes.*

Proof. Note that for any prime power r, the polynomial $f(x) = x^{r+1}-1$ has exactly one linear factor $(x-1)$ and all other irreducible factors of f over $\mathbb{F}_r[x]$ are quadratic with roots β and $\beta^r = \beta^{-1}$. In particular, $\mathbb{F}_{r^2}$ is the splitting field of f over $\mathbb{F}_r$.

Let $f_0(x) = x^{q+1}-1 \in \mathbb{F}_q[x]$ and fix a root $1 \neq \alpha_0$ which is a root of one of the quadratic irreducible factors $f_0^*(x)$ of $f_0(x)$. Then, $\mathbb{F}_{q^2} = \mathbb{F}_q(\alpha_0)$. Now, consider $f_1(x) = x^{q^2+1}-1 \in \mathbb{F}_{q^2}[x]$ and fix a root $1 \neq \alpha_1$ which is a root of one of the quadratic irreducible factors $f_1^*(x)$ of $f_1(x)$. Then, $\mathbb{F}_{q^{2^2}} = \mathbb{F}_{q^2}(\alpha_1) = \mathbb{F}_q(\alpha_0, \alpha_1)$. More generally for $0 \leq j \leq n-1$, let $m_j = q^{2^j} + 1$ and note that each m_j is relatively prime to q. Consider the polynomials

$$f_j(x) = x^{m_j} - 1 \in \mathbb{F}_{q^{2^j}}[x] = \mathbb{F}_{m_j - 1}[x]$$

and fix a root α_j of each $f_j(x)$ as one of the roots of a chosen quadratic irreducible factor $f_j^*(x)$ of $f_j(x)$. Then, a sequence of field extensions is obtained:

$$\mathbb{F}_q \subset \mathbb{F}_{q^2} = \mathbb{F}_q(\alpha_0) \subset \mathbb{F}_{q^{2^2}} = \mathbb{F}_q(\alpha_0, \alpha_1) \subset \cdots \subset \mathbb{F}_{q^{2^n}} = \mathbb{F}_q(\alpha_0, \ldots, \alpha_{n-1}).$$

Let $\langle \theta_j^* \rangle$ be the minimal cyclic code over $\mathbb{F}_{q^{2^j}}$, which is generated by the primitive idempotent θ_j^* and whose parity check polynomial is $f_j^*(x)$. Note that $\langle \theta_j^* \rangle$ has dimension 2 and length m_j (for each $0 \leq j \leq n-1$). We denote the minimum distance of $\langle \theta_j^* \rangle$ by d_j^*.

Now start with an asymptotically good sequence of linear codes (C_i) over $\mathbb{F}_{q^{2^n}} = \mathbb{F}_q(\alpha_0, \ldots, \alpha_{n-1})$ and assume that N_i, d_i and k_i denote respectively the length, minimum distance and dimension of C_i, for all i. Let

$$\delta := \lim_i \frac{d_i}{N_i} \quad \text{and} \quad \alpha := \lim_i \frac{k_i}{N_i}$$

denote the limit distance and the limit rate of the sequence (C_i) and note that both quantities are positive, since (C_i) is asymptotically good.

Consider the sequence of codes $(\langle \theta_{n-1}^* \rangle \Box C_i)$. By Theorem 1.3.1, this sequence consists of QC codes over $\mathbb{F}_{q^{2^{n-1}}} = \mathbb{F}_q(\alpha_0, \ldots, \alpha_{n-2})$, where for each i the length and the dimension of $\langle \theta_{n-1}^* \rangle \Box C_i$ are, respectively, $m_{n-1} N_i$ and $2k_i$. Moreover, the minimum distance of $\langle \theta_{n-1}^* \rangle \Box C_i$ is at least $d_{n-1}^* d_i$. Now, take the members of this sequence of QC codes as outer codes and concatenate each with the code $\langle \theta_{n-2}^* \rangle$ to obtain a sequence of Q2DC codes $\left(\langle \theta_{n-2}^* \rangle \Box \left(\langle \theta_{n-1}^* \rangle \Box C_i\right)\right)$ over $\mathbb{F}_{q^{2^{n-2}}} = \mathbb{F}_q(\alpha_0, \ldots, \alpha_{n-3})$ (Theorem 2.3.1). Note that the i^{th} code in this new sequence has length $m_{n-2} m_{n-1} N_i$ and its dimension is $2^2 k_i$. The minimum distance of this i^{th} code is at least $d_{n-2}^* d_{n-1}^* d_i$. Continue this way to form the sequence of codes

$$\left(\langle \theta_0^* \rangle \Box \left(\langle \theta_1^* \rangle \Box \left(\cdots \Box \left(\langle \theta_{n-1}^* \rangle \Box C_i\right)\right)\right)\right). \tag{2.3.1}$$

By Theorem 2.3.1, the sequence (2.3.1) consists of QnDC codes over $\mathbb{F}_q$. The length and the dimension of the i^{th} code in this last sequence are respectively,

$$m_0 \cdots m_{n-1} N_i \text{ and } 2^n k_i.$$

The minimum distance of the i^{th} code is at least $d_0^* \cdots d_{n-1}^* d_i$. If we denote the limit parameters of the sequence of QnDC codes in (2.3.1) as δ^* and α^*, we have

$$\delta^* \geq \frac{d_0^* \cdots d_{n-1}^*}{m_0 \cdots m_{n-1}} \delta > 0 \text{ and } \alpha^* = \frac{2^n}{m_0 \cdots m_{n-1}} \alpha > 0.$$

It is clear that the i^{th} code in this sequence can be viewed as a QC code of index $m_1 \cdots m_{n-1} N_i$. □

Remark 2.3.3. Whether cyclic codes are asymptotically good or not is an important open problem in coding theory ([27]). As in Theorem 2.3.2, a sequence of nD cyclic codes can be obtained by starting with a sequence of cyclic codes and continuing with consecutive concatenations. Hence, if cyclic codes are asymptotically good, so are nD cyclic codes for any $n \geq 2$. We are not aware of any result on the asymptotic performance of nD cyclic codes.

Chapter 3

Multidimensional Convolutional Codes and Their Relation to QnDC Codes

We have shown in the first chapter that QC codes are naturally related to convolutional codes and they yield a lower bound on the free distance of convolutional codes. Our aim in this chapter is to provide an analogous relation between multidimensional quasi-cyclic and multidimensional convolutional codes. For this, we will first recall some basic facts on multidimensional convolutional codes.

3.1 Multidimensional Convolutional Codes

Suppose that G is a $k \times \ell$ full rank polynomial matrix G with entries from $\mathbb{F}_q[x_1, \ldots, x_n]$. An n-dimensional (nD) convolutional code over $\mathbb{F}_q$ of length ℓ is defined in general as an $\mathbb{F}_q[[x_1, \ldots, x_n]]$-module in $\mathbb{F}_q[[x_1, \ldots, x_n]]^\ell$ generated by the rows of G ([7, 33]):

$$C = \{(u_0, \ldots, u_{k-1})\, G : \; u_i \in \mathbb{F}_q[[x_1, \ldots, x_n]] \; \forall i\}\,.$$

Here, $\mathbb{F}_q[[x_1, \ldots, x_n]]$ denotes the ring of formal power series.

Analogous to the 1D case, we define the weight of a power series $c(x_1, \ldots, x_n)$ as the number of its terms and the weight of a codeword $\vec{c}(x_1, \ldots, x_n) = (c_0(x_1, \ldots, x_n), \ldots, c_{\ell-1}(x_1, \ldots, x_n))$ as the sum of the weights of its coordinates. The free distance of code $d_f(C)$ is the minimum nonzero weight in C.

Furthermore, as in the 1D case, it is generally assumed that C is encoded by a noncatastrophic PGM G, again in the sense that finite weight outputs can only come from finite weight inputs. Noncatastrophicity for G means that if a polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]$ divides all $(k \times k)$ minors of G, then this polynomial is a constant polynomial or a polynomial with zero constant term ([33, Proposition 5.1.7]). Finite weight power series are clearly polynomials. Again for the purpose of weight analysis infinite weight codewords are not of interest and hence we will focus on codes with polynomial representations. Therefore, we will consider

$$C = \{(u_0, \ldots, u_{k-1})\, G : \ u_i \in \mathbb{F}_q[x_1, \ldots, x_n] \ \forall i\} \tag{3.1.1}$$

and such a code will be referred to as (ℓ, k) nD convolutional code. In other words, an nD convolutional code will be an $\mathbb{F}_q[x_1, \ldots, x_n]$-module in $\mathbb{F}_q[x_1, \ldots, x_n]^\ell$. This is also the point of view taken in [4, 9, 33]. Unlike the classical case ($n = 1$), not every such module is necessarily free when $n \geq 2$ (see [9, Example 8.3]), although only free nD convolutional codes are studied in some articles (e.g. [4]).

Recall that a QnDC code of size $m_1 \times \cdots \times m_{n+1}$ can be viewed as an R_n-module in $R_n^{m_{n+1}}$. Set $\ell = m_{n+1}$ and define the analogue of the projection in (1.4.3) as:

$$\begin{aligned} \Phi : \mathbb{F}_q[x_1, x_2, \ldots, x_n] &\longrightarrow R_n \\ f &\mapsto f' := f \mod \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1 \rangle \end{aligned} \tag{3.1.2}$$

Then, for an nD convolutional code C of length ℓ, we can associate a size $m_1 \times \cdots \times m_n \times \ell$ QnDC code C', which is viewed as an R_n-module in R_n^ℓ, as was done for $n = 1$ case in (1.4.4):

$$\begin{aligned} \Phi : C &\longrightarrow C' \\ \vec{c} = (c_0, \ldots, c_{\ell-1}) &\mapsto \vec{c'} = \left(c'_0, \ldots, c'_{\ell-1}\right). \end{aligned} \tag{3.1.3}$$

3.2 Background on Gröbner Bases

Before proceeding further on the relation of multidimensional QC and convolutional codes, let us go over some facts about Gröbner bases. For details and proofs of the following statements, we refer to [1].

Let K be a field and fix a term order on $K[x_1, \ldots, x_n]$. A power product $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ will be denoted by X^α. Any element $f \in K[X] \backslash \{0\}$ can be written as

$$f = a_1 X^{\alpha_1} + \ldots + a_r X^{\alpha_r},$$

where $a_i \in K^*$ and $X^{\alpha_1} > \ldots > X^{\alpha_r}$.

We will use the following the notation:

$$\ell p(f) = X^{\alpha_1} : \text{the leading power product of } f$$
$$\ell c(f) = a_1 : \text{the leading coefficient of } f$$
$$\ell t(f) = a_1 X^{\alpha_1} : \text{the leading term of } f$$

Definition 3.2.1. Let $f, g \in K[X]$ with $g \neq 0$. We say that f reduces to h modulo g in one step ($f \xrightarrow{g} h$) if $\ell p(g)$ divides a nonzero term X that appears in f and

$$h = f - \frac{X}{\ell t(g)} g.$$

Definition 3.2.2. Let $f, h, f_1, \ldots, f_s \in K[X]$ and let $F = \{f_1, \ldots, f_s\}$. We say that f reduces to h mod F ($f \xrightarrow{F} h$) if there exists a sequence of indices $i_1, \ldots, i_t \in \{1, \ldots, s\}$ (not necessarily distinct) and a sequence of polynomials $h_1, \ldots, h_{t-1} \in K[X]$ such that

$$f \xrightarrow{f_{i_1}} h_1 \xrightarrow{f_{i_2}} h_2 \xrightarrow{f_{i_3}} \cdots \xrightarrow{f_{i_{t-1}}} h_{t-1} \xrightarrow{f_{i_t}} h.$$

Definition 3.2.3. A polynomial $r \in K[X]$ is called reduced with respect to $F = \{f_1, \ldots, f_s\}$ if $r = 0$ or no power product that appears in r is divisible by one of the $\ell p(f_i)$'s ($i = 1, \ldots, s$), i.e. r cannot be reduced mod F.

Definition 3.2.4. If $f \xrightarrow{F} r$ and r is reduced with respect to F, then r is called a remainder for f with respect to F.

Definition 3.2.5. A set of nonzero polynomials $G = \{g_1, \ldots, g_t\}$ contained in an ideal I is called a Gröbner basis for I, if for any nonzero element $f \in I$ there exists $i \in \{1, \ldots, s\}$ such that $\ell p(g_i) | \ell p(f)$.

Theorem 3.2.6. *i. G is a Gröbner basis for the ideal I if and only if*

$$f \in I \Leftrightarrow f \xrightarrow{G} 0.$$

ii. If G is a Gröbner basis for I then $I = \langle g_1, \dots, g_t \rangle$.

iii. Every nonzero ideal in $K[X]$ has a Gröbner basis.

Definition 3.2.7. We say that $G = \{g_1, \dots, g_t\}$ is a Gröbner basis if it is a Gröbner basis for the ideal $\langle G \rangle$ that it generates.

Theorem 3.2.8. *G is a Gröbner basis if and only if for all $f \in K[X]$ the remainder of the division of f with respect to G is unique.*

Definition 3.2.9. Let $f, g \in K[X]$ be nonzero and let $L = \operatorname{lcm}(\ell p(f), \ell p(g))$. The polynomial

$$S(f,g) = \frac{L}{\ell t(f)} f - \frac{L}{\ell t(g)} g$$

is called the S-polynomial of f and g.

Theorem 3.2.10. *Let $G = \{g_1, \dots, g_t\}$ be a set of nonzero polynomials in $K[X]$. Then G is a Gröbner basis if and only if for each $i \neq j$ we have $S(g_i, g_j) \xrightarrow{G} 0$.*

The following observations are immediate from the facts stated so far.

Proposition 3.2.11. *For any $n \in \mathbb{N}$ and $m_i \geq 1$ $(i = 1, \dots, n)$, $\{x_1^{m_1} - 1, \dots, x_n^{m_n} - 1\}$ is a Gröbner basis.*

Proposition 3.2.12. *Let $G = \{g_1, \dots, g_n\}$, where $g_i = x_i^{m_i} - 1$ for all $i = 1, \dots, n$. Let $f \in K[X]$ be nonzero and reduce f by g_1 as much as possible, then by g_2 as much as possible and so on. Then, f can be written as*

$$f = a_1 g_1 + \cdots + a_n g_n + r,$$

where

i. r is the unique remainder of f with respect to G,

ii. For $i > 1$, a_i is reduced with respect to $\{g_1, \dots, g_{i-1}\}$. In particular, a_i is not divisible by g_t for any $t \in \{1, \dots, i-1\}$.

3.3 On Noncatastrophicity for 1-Generator Convolutional Codes

Let $C \subset \mathbb{F}_q[x_1, \ldots, x_n]^\ell$ be a 1-generator nD convolutional code with the PGM

$$G = \big(\vec{g}(x_1, \ldots, x_n)\big) = \big(g_1(x_1, \ldots, x_n), \ldots, g_\ell(x_1, \ldots, x_n)\big). \tag{3.3.1}$$

Consider the set

$$J_{m_1,\ldots,m_n} = \{u(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]; ug_i \in \langle x_1^{m_1}-1, \ldots, x_n^{m_n}-1\rangle, \forall i = 1, \ldots, \ell\}$$

Note that $J_{m_1,\ldots,m_n}$ is an ideal of $\mathbb{F}_q[x_1, \ldots, x_n]$. Moreover,

$$\langle x_1^{m_n} - 1, \ldots, x_n^{m_n} - 1\rangle \subseteq J_{m_1,\ldots,m_n}$$

holds in general.

We will study 1-generator nD convolutional codes given with a PGM $G = \big(g_1(x_1, \ldots, x_n), \ldots, g_\ell(x_1, \ldots, x_n)\big)$ which satisfies

$$J_{m_1,\ldots,m_n} = \langle x_1^{m_n} - 1, \ldots, x_n^{m_n} - 1\rangle, \tag{3.3.2}$$

for all $m_i \geq 1$ relatively prime to q. For 1D convolutional codes, condition (3.3.2) is equivalent to noncatastrophicity.

Proposition 3.3.1. *Let $g_1(x), \ldots, g_\ell(x)$ be nonzero polynomials in $\mathbb{F}_q[x]$. Let*

$$J_m = \{h(x) \in \mathbb{F}_q[x] : h(x)g_i(x) \in \langle x^m - 1\rangle,\ \forall i = 1, \ldots, \ell\}.$$

Then, the encoder $G = \big(g_1(x), \ldots, g_\ell(x)\big)$ is noncatastrophic for the convolutional code C that it generates if and only if $J_m = \langle x^m - 1\rangle$ for all $m \geq 1$, relatively prime to q.

Proof. ($\Leftarrow$) Suppose $a(x) \in \mathbb{F}_q[x]$ is a common divisor of each $g_i(x)$. If $a(x)$ is not a constant polynomial or not of the form cx^d for $c \in \mathbb{F}_q^*$ and $d \geq 1$, then it has a root $\alpha \in \mathbb{F}_{q^u} \subset \bar{\mathbb{F}}_q$ in some extension of $\mathbb{F}_q$. Let m be the multiplicative order of α in $\mathbb{F}_{q^u}^*$ and note that being a divisor of $q^u - 1$, m is relatively prime to q. Let $f_\alpha(x) \in \mathbb{F}_q[x]$ denote the minimal polynomial of α over $\mathbb{F}_q$. Then $f_\alpha(x)|a(x)$ in $\mathbb{F}_q[x]$. Moreover, being an m'th root of unity, α is also a root of $x^m - 1$. Hence $f_\alpha(x)|(x^m - 1)$ also holds. Therefore,

$$\frac{x^m - 1}{f_\alpha(x)} \in \mathbb{F}_q[x] \text{ and } \frac{x^m - 1}{f_\alpha(x)} g_i \in \langle x^m - 1 \rangle \ \forall i.$$

However, $\dfrac{x^m - 1}{f_\alpha(x)} \notin \langle x^m - 1 \rangle$ by Definition 3.2.5 and Proposition 3.2.11. This contradicts the assumption and hence $a(x)$ is constant or a monomial.

($\Rightarrow$) Since J_m is an ideal in the PID $\mathbb{F}_q[x]$, $J_m = \langle f(x) \rangle$ for some $f(x) \in \mathbb{F}_q[x]$. Moreover, $\langle x^m - 1 \rangle \subseteq J_m = \langle f(x) \rangle$ implies $f(x)|(x^m - 1)$. Say $x^m - 1 = f(x)k(x)$ for some $k(x) \in \mathbb{F}_q[x]$. Then for all i we have

$$f(x)g_i(x) = (x^m - 1)u_i(x) = f(x)k(x)u_i(x)$$

for some $u_i(x) \in \mathbb{F}_q[x]$. Hence, $k(x)$ is a common divisor for each $g_i(x)$. This means by assumption that $k(x)$ is a constant polynomial or a monomial of the form cx^d. Since $k(x)|(x^m - 1)$, we conclude that $k(x)$ is constant. Therefore, $J_m = \langle f(x) \rangle = \langle x^m - 1 \rangle$.

□

We would like to see the relation between Condition (3.3.2) and noncatastrophicity for 1-generator nD convolutional codes. The 2D case will be studied in detail first and for this, we need some preparation.

Lemma 3.3.2. *Let $a(x, y) \in \mathbb{F}_q[x, y]$ be a nonconstant polynomial with a nonzero constant term. Then $a(x, y)$ has a root $(u, v) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ with $u \neq 0 \neq v$.*

Proof. If a is a single-variable polynomial (say in x) with a nonzero constant term, then it has a nonzero root $u \in \overline{\mathbb{F}}_q$ and then for any $v \in \overline{\mathbb{F}}_q^*$, (u, v) can be thought of as a root of $a(x) = a(x, y)$.

So, assume that a is bivariate and write

$$a(x, y) = \sum_{i=0}^{n} f_i(x) y^i$$

where $f_i(x) \in \mathbb{F}_q[x]$ for all i and $f_0(x)$ has a nonzero constant term.

Let $u \in \overline{\mathbb{F}}_q^*$ be such that

$$f_0(u) \neq 0 \text{ and } f_i(u) \neq 0$$

for at least one $i \in \{1, \ldots, n\}$. Consider $a(u, y)$, which has coefficients in some extension $\mathbb{F}_{q^s}$ of $\mathbb{F}_q$ and by the choice of u,

i. it has a nonzero constant term (since $f_0(u) \neq 0$)

ii. it is not a constant polynomial (since $f_i(u) \neq 0$ for some $1 \leq i \leq n$).

Then, $a(u, y) \in \mathbb{F}_{q^s}[y]$ has a nonzero root in $\overline{\mathbb{F}}_q$, say v, and the proof is finished. □

Definition 3.3.3. Let $I \subseteq K[x_1, \ldots, x_n]$ be an ideal, where K is a field. I is called zero-dimensional if

$$V_{\overline{K}}(I) := \{(u_1, \ldots, u_n) \in \overline{K}^n : f(u_1, \ldots, u_n) = 0, \forall f \in I\}$$

is a finite set.

Lemma 3.3.4 (Seidenberg's Lemma 92)**.** *([2, Proposition 8.14],[31]) Let K be a perfect field and $I \subseteq K[x_1, \ldots, x_n]$ be a zero-dimensional ideal. Then, I is a radical ideal if and only if it contains a univariate, square-free polynomial in each variable x_i ($i = 1, \ldots, n$).*

Example 3.3.5. If $(m_i, q) = 1$ for all $1 \leq i \leq n$, then $I_n = \langle x_1^{m_1} - 1, \ldots, x_n^{m_n} - 1\rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_n]$ is a radical ideal. Moreover, any ideal J of $\mathbb{F}_q[x_1, \ldots, x_n]$ which contains I_n is also radical.

Let m_1, m_2 be positive integers relatively prime to q and let α_1, α_2 be primitive m_1'th, m_2'th roots of unity over $\mathbb{F}_q$, respectively. Define the set

$$\Omega = \{(\alpha_1^i, \alpha_2^j); 0 \leq i \leq m_1 - 1, 0 \leq j \leq m_2 - 1\}$$

in $\overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$. Note that $\Omega = V_{\overline{\mathbb{F}}_q}(\langle x^{m_1} - 1, y^{m_2} - 1\rangle)$.

For an element $(\alpha_1^i, \alpha_2^j) \in \Omega$, define its $\mathbb{F}_q$-conjugacy class as

$$[(\alpha_1^i, \alpha_2^j)] := \{(\alpha_1^i, \alpha_2^j), (\alpha_1^{qi}, \alpha_2^{qj}), \ldots, (\alpha_1^{q^{m-1}i}, \alpha_2^{q^{m-1}j})\},$$

where m is the least common multiple of $[\mathbb{F}_q(\alpha_1^i) : \mathbb{F}_q]$ and $[\mathbb{F}_q(\alpha_2^j) : \mathbb{F}_q]$. It is easy to see that Ω is a disjoint union of such $\mathbb{F}_q$-conjugacy classes. Also, if J is an ideal of $\mathbb{F}_q[x, y]$ that contains $\langle x^{m_1} - 1, y^{m_2} - 1\rangle$, then its zero set $V_{\overline{\mathbb{F}}_q}(J)$ is a union of conjugacy classes of Ω.

Convention: By a subset U of Ω, we mean a single $\mathbb{F}_q$-conjugacy class or a union of $\mathbb{F}_q$-conjugacy classes in Ω.

Definition 3.3.6. For a subset U of Ω, define the corresponding ideal

$$\mathcal{I}(U) := \{f \in \mathbb{F}_q[x, y]; f(u, v) = 0 \ \forall (u, v) \in U\}.$$

Note that $\mathcal{I}(U) \supseteq \langle x^{m_1} - 1, y^{m_2} - 1\rangle$.

Hilbert's Nullstellensatz ([1, Theorem 2.2.5]) implies that for any ideal I of $\mathbb{F}_q[x, y]$,

$$\mathcal{I}(V_{\overline{\mathbb{F}}_q}(I)) = \sqrt{I},$$

where $\sqrt{I}$ denotes the radical of I. By Lemma 3.3.4, $\mathcal{I}(U)$ is a radical ideal and hence

$$\mathcal{I}\left(V_{\overline{\mathbb{F}}_q}(\mathcal{I}(U))\right) = \mathcal{I}(U),$$

for any subset U of Ω.

Proposition 3.3.7. *With the notation so far, let U be a subset of Ω. Then,*

$$V_{\overline{\mathbb{F}}_q}(\mathcal{I}(U)) = U.$$

Proof. [14, Proposition 2.11]. □

Corollary 3.3.8. *If $U_1 \subsetneq U_2$ are subsets of Ω, then*

$$\mathcal{I}(U_1) \supsetneq \mathcal{I}(U_2) \supseteq \langle x^{m_1} - 1, y^{m_2} - 1\rangle.$$

Proof. It is clear that $\mathcal{I}(U_1) \supseteq \mathcal{I}(U_2) \supseteq \langle x^{m_1} - 1, y^{m_2} - 1\rangle$. If $\mathcal{I}(U_1) = \mathcal{I}(U_2)$, then using Proposition 3.3.7 we have

$$V_{\overline{\mathbb{F}}_q}(\mathcal{I}(U_1)) = U_1 = U_2 = V_{\overline{\mathbb{F}}_q}(\mathcal{I}(U_2)),$$

which is a contradiction. □

We are ready to prove a generalization of one implication in Proposition 3.3.1 to the 2D case.

Theorem 3.3.9. *Let $G = (g_1(x,y), \ldots, g_\ell(x,y))$ be a PGM for the 2D convolutional code C. Assume that $J_{m_1,m_2} = \langle x^{m_1} - 1, y^{m_2} - 1\rangle$ for all positive integers m_1 and m_2, which are relatively prime to q. Then G is noncatastrophic.*

Proof. Assume that there exists a nonconstant polynomial $a(x,y) \in \mathbb{F}_q[x,y]$, whose constant term is nonzero, which divides $g_i(x,y)$ for all $1 \leq i \leq \ell$. Let $g_i(x,y) = a(x,y)\tilde{g}_i(x,y)$ for some $\tilde{g}_i(x,y) \in \mathbb{F}_q[x,y]$, for all i. By Lemma 3.3.2, $a(x,y)$ has a root $(u,v) \in \overline{\mathbb{F}}_q \times \overline{\mathbb{F}}_q$ with $u \neq 0 \neq v$. Assume that m_1 and m_2 denote, respectively, the multiplicative orders of u and v. Note that since each m_i is a divisor of $q^s - 1$, for some $s \geq 1$, they are relatively prime to q.

If $a(x,y)$ vanishes on Ω, then $a(x,y)$ belongs to $\mathcal{I}(\Omega) = \langle x^{m_1} - 1, y^{m_2} - 1\rangle$. This would imply that $g_i(x,y) \in \langle x^{m_1} - 1, y^{m_2} - 1\rangle$ for each i, and hence

$$J_{m_1,m_2} = \mathbb{F}_q[x,y] \supsetneq \langle x^{m_1} - 1, y^{m_2} - 1\rangle,$$

which contradicts the assumption. Hence, there is a proper subset (i.e. a union of $\mathbb{F}_q$-conjugacy classes) $U \subsetneq \Omega$ such that $a(x,y) \in \mathcal{I}(U) \backslash \langle x^{m_1} - 1, y^{m_2} - 1\rangle$.

Let $U' := \Omega \backslash U$ be the complementary subset. By Corollary 3.3.8, $\mathcal{I}(U') \supsetneq \langle x^{m_1} - 1, y^{m_2} - 1\rangle$. Let $f(x,y)$ be a polynomial from $\mathcal{I}(U') \backslash \langle x^{m_1} - 1, y^{m_2} - 1\rangle$. Then the product $fa \in \mathbb{F}_q[x,y]$ vanishes on $U \bigcup U' = \Omega$ and hence belongs to $\mathcal{I}(\Omega) = \langle x^{m_1} - 1, y^{m_2} - 1\rangle$. Therefore, for each $1 \leq i \leq \ell$, $fg_i = fa\tilde{g}_i \in \langle x^{m_1} - 1, y^{m_2} - 1\rangle$ although $f \notin \langle x^{m_1} - 1, y^{m_2} - 1\rangle$. Hence, f belongs to $J_{m_1,m_2} \backslash \langle x^{m_1} - 1, y^{m_2} - 1\rangle$, which is a contradiction. □

Remark 3.3.10. For 2D convolutional codes, there are noncatastrophic encoders which do not satisfy condition (3.3.2). Namely, consider the 2D convolutional code of length 2 over $\mathbb{F}_2$, which is generated by the following PGM:

$$G = (x^2 + x + 1, y^4 + y^3 + y^2 + y + 1).$$

Then, G is clearly noncatastrophic but $J_{3,5} \neq \langle x^3 + 1, y^5 + 1\rangle$, since $(x+1)(y+1)G$ has its coordinates in the ideal $\langle x^3 + 1, y^5 + 1\rangle$ (hence $(x+1)(y+1) \in J_{3,5}$) but $(x+1)(y+1) \notin \langle x^3 + 1, y^5 + 1\rangle$.

Remark 3.3.11. The proof of Theorem 3.3.9 is based on Corollary 3.3.8, which relies on Proposition 3.3.7. Moreover, the proof of Proposition 3.3.7 uses Seidenberg's Lemma 92 (Lemma 3.3.4) and some basic facts on Commutative Algebra (see its proof in [14]). Both Seidenberg's Lemma and the facts from Commutative Algebra hold for ideals of $\mathbb{F}_q[x_1, \ldots, x_n]$ for any $n \geq 2$. Hence, Theorem 3.3.9's proof can be extended to n-variable case and one can write the same statement for 1-generator nD convolutional codes (i.e. a sufficient condition for noncatastrophicity of such nD convolutional codes).

3.4 A Distance Relation for 1-Generator 2D Convolutional Codes

We are ready to prove a generalization of Lally's result (Theorem 1.4.3 iii) to the multivariable case for a particular class of 1-generator 2D convolutional codes.

Theorem 3.4.1. *Let C be a 1-generator (ℓ, k) 2D convolutional code given with a PGM $G = (g_1(x,y), \ldots, g_\ell(x,y))$ satisfying (3.3.2) for some m_1, m_2 and let C' be the associated Q2DC code in $\left(\mathbb{F}_q[x,y]/\langle x^{m_1}-1, y^{m_2}-1\rangle\right)^\ell$. Then $d_f(C) \geq d(C')$.*

Proof. For any $a \geq 0$, let

$$C_a := \left\{ \vec{c}(x,y) = \big(c_1(x,y), \ldots, c_\ell(x,y)\big) \in C : \max_{1 \leq i \leq \ell}(\deg_y(c_i)) \leq a \right\}.$$

Note that

$$C_0 \subset C_1 \subset C_2 \subset \cdots \tag{3.4.1}$$

and

$$C = \bigcup_{a \geq 0} C_a.$$

We define a map, which will be called the unfolding map, that produces vectors over $\mathbb{F}_q[x]$ out of vectors in $\mathbb{F}_q[x,y]^\ell$:

$$\begin{array}{cccc} \varphi_x : & \mathbb{F}_q[x,y]^\ell & \longrightarrow & \bigcup_{d \geq 0} \mathbb{F}_q[x]^{(d+1)\ell} \\ & \left(\sum_{i=0}^{d} c_{1i}(x)y^i, \ldots, \sum_{i=0}^{d} c_{\ell i}(x)y^i\right) & \longmapsto & \big(c_{10}(x), \ldots, c_{1d}(x); \ldots; c_{\ell 0}(x), \ldots, c_{\ell d}(x)\big), \end{array}$$

where $d = \max_{1 \leq j \leq \ell}\big(\deg_y c_j(x,y)\big)$.

Clearly, one can define an analogous unfolding map φ_y for y. The inverse of φ_x is called the folding map. Note that the unfolding map preserves weights; i.e.

$$wt\big(\vec{c}(x,y)\big) = wt\big(\varphi_x(\vec{c}(x,y))\big).$$

Consider the unfolded version of each C_a:

$$\begin{aligned} D_a := \varphi_x(C_a) = \big\{\vec{c}(x) = \big(c_{10}(x), \ldots, c_{1a}(x); \ldots; c_{\ell 0}(x), \ldots, c_{\ell a}(x)\big) : \\ \vec{c}(x) = \varphi_x(\vec{c}(x,y)) \text{ for some } \vec{c}(x,y) \in C_a\big\}. \end{aligned}$$

It is clear that D_a is closed under addition. Let $h(x) \in \mathbb{F}_q[x]$ and $\vec{c}(x) = \varphi_x(\vec{c}(x,y)) \in D_a$ for some $\vec{c}(x,y) \in C_a$. Consider the product

$$\begin{aligned} h(x)\vec{c}(x) &= \big(h(x)c_{10}(x), \ldots, h(x)c_{\ell a}(x)\big) \\ &= \varphi_x\left(h(x)\left(\sum_{i=0}^{a} c_{1i}(x)y^i, \ldots, \sum_{i=0}^{a} c_{\ell i}(x)y^i\right)\right) = \varphi_x\big(h(x)\vec{c}(x,y)\big). \end{aligned}$$

Multiplication of $\vec{c}(x,y)$ by $h(x)$ does not change the y-degrees of its coordinates. Hence, $h(x)\vec{c}(x,y) \in C_a$ again. Therefore, $h(x)\vec{c}(x)$ lies in D_a. This shows that $D_a \subset \mathbb{F}_q[x]^{(a+1)\ell}$ is an $\mathbb{F}_q[x]$-module. So, via unfolding, we obtain a family D_a $(a \geq 0)$ of length $(a+1)\ell$ 1D convolutional codes out of the 2D convolutional code C of length ℓ that we started with. For $a < b$, the length of D_a is less than the length of D_b. However, we can insert 0's at suitable positions of codewords of D_a and view it as a code of the same length as D_b. Then by (3.4.1) we have

$$D_0 \subset D_1 \subset D_2 \subset \cdots \tag{3.4.2}$$

For $a \geq 0$, let D'_a denote the associated QC code in $(\mathbb{F}_q[x]/\langle x^{m_1} - 1\rangle)^{(a+1)\ell}$. Namely,

$$D'_a = \big\{\vec{c'}(x) = (c'_{10}(x), \ldots, c'_{\ell a}(x)) : \vec{c}(x) \in D_a\big\}.$$

View elements of D'_a as vectors in $\mathbb{F}_q[x]^{(a+1)\ell}$ and fold them back into $\mathbb{F}_q[x,y]^\ell$:

$$\begin{array}{rcl} D'_a & \xrightarrow{\varphi_x^{-1}} & \mathbb{F}_q[x,y]^\ell \\ \vec{c'}(x) & \longmapsto & \vec{c'}(x,y) = \left(\sum\limits_{i=0}^{a} c'_{1i}(x)y^i, \ldots, \sum\limits_{i=0}^{a} c'_{\ell i}(x)y^i\right). \end{array}$$

Write the coordinates of folded vectors as polynomials in x

$$\vec{c'}(x,y) = \vec{c^t}(x,y) = \left(\sum_{i=0}^{m_1-1} c_{1i}^t(y)x^i, \dots, \sum_{i=0}^{m_1-1} c_{\ell i}^t(y)x^i\right),$$

and then unfold them by the map φ_y:

$$\vec{c^t}(x,y) \overset{\varphi_y}{\longmapsto} \vec{c^t}(y) = \left(c_{10}^t(y), \dots, c_{1,m_1-1}^t(y); \dots; c_{\ell 0}^t(y), \dots, c_{\ell,m_1-1}^t(y)\right)$$

Let us denote this operation by $\mathcal{T}$ and call it twisting, i.e. $\vec{c^t}(y) = \mathcal{T}(\vec{c'}(x))$. Note that twisting does not change weights of vectors:

$$wt(\vec{c'}(x)) = wt(\vec{c^t}(y)).$$

We set $E_a := \mathcal{T}(D'_a)$ for all $a \geq 0$. Namely,

$$E_a = \left\{\vec{c^t}(y) = \mathcal{T}(\vec{c'}(x)) : \vec{c'}(x) \in D'_a\right\}.$$

Note that E_a lies in $\mathbb{F}_q[y]^{m_1\ell}$ for all $a \geq 0$. On the other hand, coordinate degrees of elements in E_a are upper bounded by a, hence depend on a. Finally, let

$$E := \bigcup_{a\geq 0} E_a \subset \mathbb{F}_q[y]^{m_1\ell}.$$

We claim that E is an $\mathbb{F}_q[y]$-module, hence a 1D convolutional code of length $m_1\ell$. Let $\vec{e^t}(y) \in E_a$ and $\vec{f^t}(y) \in E_b$ be elements of E and suppose $a < b$. Then $\vec{e^t}(y) = \mathcal{T}(\vec{e'}(x))$ for some $\vec{e'}(x) \in D'_a$ and $\vec{e}(x) \in D_a$. Similarly, $\vec{f^t}(y) = \mathcal{T}(\vec{f'}(x))$ for some $\vec{f'}(x) \in D'_b$ and $\vec{f}(x) \in D_b$. Since $a < b$, both $\vec{e}(x)$ and $\vec{f}(x)$ can be viewed as elements of D_b by (3.4.2). Since D_b is a 1D convolutional code, $\vec{e}(x)+\vec{f}(x) \in D_b$ and hence $\vec{e'}(x) + \vec{f'}(x) \in D'_b$. Note that twisting respects addition. Hence,

$$\mathcal{T}\left(\vec{e'}(x) + \vec{f'}(x)\right) = \mathcal{T}\left(\vec{e'}(x)\right) + \mathcal{T}\left(\vec{f'}(x)\right) = \vec{e^t}(y) + \vec{f^t}(y).$$

Therefore, $\vec{e^t}(y) + \vec{f^t}(y) \in E_b \subset E$ and hence E is closed under addition.

Now we show that E is closed under scalar multiplication. Let $\vec{e^t}(y) \in E_a$ be as above and $k \in \mathbb{F}_q$. Then, $k\vec{e^t}(y) = \mathcal{T}(k\vec{e'}(x))$. Note that reduction mod $\langle x^{m_1} - 1\rangle$ respects scalar multiplication and hence $k\vec{e'}(x) = (k\vec{e})'(x)$ for $\vec{e}(x) \in D_a$. Since

D_a is a 1D convolutional code, $k\vec{e} \in D_a$ and hence $k\vec{e'}(x) \in D'_a$. Therefore $k\vec{e^t}(y)$, being the twist of $k\vec{e'}(x)$, lies in $E_a \subset E$.

Finally, we will show that E is closed under multiplication by y and this will prove our claim that E is an $\mathbb{F}_q[y]$-module. Let $\vec{e^t}(y) = \mathcal{T}(\vec{e'}(x)) \in E_a$ be as above and fold back $y\vec{e^t}(y)$:

$$\varphi_y^{-1}\left(y\vec{e^t}(y)\right) = \left(\sum_{i=0}^{m_1-1}\left(ye^t_{1i}(y)\right)x^i, \ldots, \sum_{i=0}^{m_1-1}\left(ye^t_{\ell i}(y)\right)x^i\right).$$

For any $1 \le j \le \ell$, we know that

$$\sum_{i=0}^{m_1-1} e^t_{ji}(y)x^i = \sum_{i=0}^{a} e'_{ji}(x)y^i.$$

Therefore

$$\sum_{i=0}^{m_1-1}\left(ye^t_{ji}(y)\right)x^i = \sum_{i=0}^{a} e'_{ji}(x)y^{i+1}$$

and

$$y\vec{e^t}(y) = \mathcal{T}\left(0, e'_{10}(x), \ldots, e'_{1a}(x); \ldots; 0, e'_{\ell 0}(x), \ldots, e'_{\ell a}(x)\right). \tag{3.4.3}$$

Let $\vec{e}(x) \in D_a$ be the vector whose reduction is $\vec{e'}(x) \in D'_a$ and let its folded version $\varphi_x^{-1}(\vec{e}(x))$ be $\vec{e}(x,y) \in C_a$. Note that $y\vec{e}(x,y)$ lies in $C_{a+1} \subset C$. Then $(\vec{ye})(x) = \varphi_x(y\vec{e}(x,y))$ is in D_{a+1} and the argument of $\mathcal{T}$ in (3.4.3) is an element of D'_{a+1}. Therefore $y\vec{e^t}(y)$ is the twist of some element in D'_{a+1} and hence lies in $E_{a+1} \subset E$. This proves the claim.

Consider the QC code

$$E' \subset \left(\mathbb{F}_q[y]/\langle y^{m_2} - 1\rangle\right)^{m_1\ell}$$

associated to the 1D convolutional code E. Let us note that E consists of unfolded versions of codewords of C after reduction mod $\langle x^{m_1} - 1\rangle$. Hence, if we view codewords of E' as polynomials in $\mathbb{F}_q[y]$ and fold them back by the map φ_y^{-1}, the resulting set corresponds to the codewords of C after reduction mod $\langle x^{m_1} - 1, y^{m_2} - 1\rangle$. In other words, $\varphi_y^{-1}(E')$ is the same as the Q2DC code C' associated to C.

We are ready to prove the assertion of the theorem. Note that any codeword of C is of the form $\vec{c}(x,y) = u(x,y)G$.

By Proposition 3.2.12 we can assume that

$$u(x,y) = a(x,y)(x^{m_1}-1) + b(x,y)(y^{m_2}-1) + r(x,y), \tag{3.4.4}$$

where $b(x,y)$ is reduced with respect to $(x^{m_1}-1)$ and $r(x,y)$ is reduced with respect to $\langle x^{m_1}-1, y^{m_2}-1\rangle$. For $\vec{c}(x,y) \in C_a$, let $\vec{c}(x) \in D_a$ denote its unfolded version. Then we have two possible outcomes for the associated QC codeword $\vec{c'}(x) \in D'_a$:
Case 1. If $\vec{c'}(x) \neq 0$, then $wt(\vec{c}(x,y)) = wt(\vec{c}(x)) \geq wt(\vec{c'}(x))$ by Theorem 1.4.3.
Case 2. If $\vec{c'}(x) = 0$, then $(x^{m_1}-1)|c_{ij}(x)$ for all i,j and therefore $(x^{m_1}-1)|c_i(x,y)$ for $1 \leq i \leq \ell$. Hence $c_i(x,y) = u(x,y)g_i(x,y) \in \langle x^{m_1}-1, y^{m_2}-1\rangle$ for all i.

By assumption (3.3.2) and Equation 3.4.4, we conclude that $r(x,y) = 0$, i.e. $u(x,y) \in \langle x^{m_1}-1, y^{m_2}-1\rangle$. Let γ_1 be the maximal power such that $(x^{m_1}-1)^{\gamma_1}$ divides all $c_{ij}(x)$. Then

$$\vec{c}(x) = (x^{m_1}-1)^{\gamma_1}\big(v_{10}(x), \ldots, v_{1a}(x); \ldots; v_{\ell,0}(x), \ldots, v_{\ell,a}(x)\big) \tag{3.4.5}$$

for some $v_{ij} \in \mathbb{F}_q[x]$.
By maximalitiy of γ_1, there exists i,j such that $v_{ij}(x)$ is not divisible by $(x^{m_1}-1)$. So,

$$\vec{c}(x,y) = \big(a(x,y)(x^{m_1}-1) + b(x,y)(y^{m_2}-1)\big)G = (x^{m_1}-1)^{\gamma_1}\vec{v}(x,y),$$

where $\vec{v}(x,y) = \varphi_x^{-1}(\vec{v}(x))$.

We claim that $\vec{v}(x,y) \in C_a \subset C$ and therefore $\vec{v}(x) \in D_a$. If so, $\vec{v'}(x) \in D'_a \backslash \{0\}$, since at least one coordinate of $\vec{v}(x)$ is not divisible by $x^{m_1}-1$. This, then implies by Theorem 1.4.3 that $wt(\vec{c}(x,y)) \geq wt(\vec{v'}(x))$.

By (3.4.5), $\vec{c}(x,y)$ is of the form

$$\begin{aligned}\vec{c}(x,y) &= (x^{m_1}-1)^{\gamma_1}\vec{v}(x,y)\\ &= u(x,y)(g_1(x,y), \ldots, g_\ell(x,y)).\end{aligned}$$

Thus, for all $i = 1, \ldots, \ell$ we have

$$(x^{m_1}-1)^{\gamma_1}v_i(x,y) = u(x,y)g_i(x,y).$$

Let $x^{m_1}-1=\prod p_i(x)\prod q_j(x)$ be the factorization of $x^{m_1}-1$ into irreducibles over $\mathbb{F}_q[x]$ and suppose that $\prod p_i(x)$ is the factor that divides $u(x,y)$. Then $(\prod q_j(x))\,|g_i(x)$ for all i and

$$\left(\frac{x^{m_1}-1}{\prod q_j(x)}\right)G=\left(\prod p_i(x)\right)G\in\langle x^{m_1}-1,y^{m_2}-1\rangle^{\ell}.$$

By assumption (3.3.2), $\prod p_i(x)$ must be in $J_{m_1,m_2}=\langle x^{m_1}-1,y^{m_2}-1\rangle$. However, this is not true unless $\prod p_i(x)=x^{m_1}-1$. Hence $(x^{m_1}-1)^{\gamma_1}$ has to divide $u(x,y)$ and therefore

$$\vec{v}(x,y)=\frac{u(x,y)}{(x^{m_1}-1)^{\gamma_1}}G,$$

where $\dfrac{u(x,y)}{(x^{m_1}-1)^{\gamma_1}}$ is a polynomial in $\mathbb{F}_q[x,y]$. This implies that $\vec{v}(x,y)\in C_a\subset C$.

Let us denote $\vec{c}(x)$ or $\vec{v}(x)$ (from Case 1 or 2, respectively) by $\vec{s}(x)\in D_a$ and let $\vec{s'}(x)$ be the reduction of $\vec{s}(x)$ mod $\langle x^{m_1}-1\rangle$. Note that $\varphi_x^{-1}(\vec{s}(x))=\vec{s}(x,y)\in C_a\subset C$ and

$$wt(\vec{c}(x,y))\geq wt(\vec{s'}(x)). \tag{3.4.6}$$

Moreover, the information word of $\vec{s}(x,y)$, which is $u(x,y)$ for $\vec{c}(x,y)$ and $\dfrac{u(x,y)}{(x^{m_1}-1)^{\gamma_1}}$ for $\vec{v}(x,y)$, is not divisible by $(x^{m_1}-1)$. Let us write $\vec{s}(x,y)$ as

$$\big(m(x,y)(x^{m_1}-1)+k(x,y)(y^{m_2}-1)+\tilde{r}(x,y)\big)G$$

following the convention in Proposition 3.2.12.

Consider the twist $\vec{s^t}(y)\in E$ of $\vec{s'}(x)$. Since twisting preserves weights, we have $wt(\vec{s'}(x))=wt(\vec{s^t}(y))$. Set $(\vec{s^t})'(y)\in E'$ as the reduction of $\vec{s^t}(y)$ mod $\langle y^{m_2}-1\rangle$. Observe that $\varphi_y^{-1}\big((\vec{s^t})'(y)\big)$ is the reduction of $\vec{s}(x,y)$ mod $\langle x^{m_1}-1,y^{m_2}-1\rangle$, i.e. $\varphi_y^{-1}\big((\vec{s^t})'(y)\big)\in C'$. After this second reduction, we again end up with two possible cases:

Case 1'. If $(\vec{s^t})'(y)\neq 0$, then $wt(\vec{s^t}(y))\geq wt((\vec{s^t})'(y))$. In this case, for $\vec{c}(x,y)\in C$ we found a nonzero codeword $\varphi_y^{-1}\big((\vec{s^t})'(y)\big)\in C'$ such that

$$wt(\vec{c}(x,y))\geq wt(\vec{s'}(x))=wt(\vec{s^t}(y))\geq wt((\vec{s^t})'(y))=wt(\varphi_y^{-1}\big((\vec{s^t})'(y)\big))$$

and the desired inequality of the theorem is obtained.

Case 2'. If $(\vec{s^t})'(y) = 0$, then $\vec{s}(x,y) \in C_a$ is congruent to 0 mod $\langle x^{m_1}-1, y^{m_2}-1\rangle$. By assumption (3.3.2), we have

$$\vec{s}(x,y) = \big(m(x,y)(x^{m_1}-1) + k(x,y)(y^{m_2}-1)\big)G.$$

Then,

$$\vec{s'}(x,y) = [k(x,y)(y^{m_2}-1)G'] \text{ mod } \langle x^{m_1}-1\rangle, \tag{3.4.7}$$

where $G' = (g'_1, \ldots, g'_\ell) = (g_1 \text{ mod } \langle x^{m_1}-1\rangle, \ldots, g_\ell \text{ mod } \langle x^{m_1}-1\rangle)$. Let us also recall that $k(x,y)$ is reduced mod $(x^{m_1}-1)$ by Proposition 3.2.12.

Let $(y^{m_2}-1)^{\gamma_2}$ be the maximal power that divides all coordinates of $\vec{s^t}(y)$. Then, there exists $\vec{w}(y) \in \mathbb{F}_q[y]^{m_1\ell}$ such that

$$\begin{aligned}\vec{s^t}(y) &= (y^{m_2}-1)^{\gamma_2}\vec{w}(y)\\ &= (y^{m_2}-1)^{\gamma_2}\big(w_{10}(x), \ldots, w_{1,m_1-1}(x); \ldots; w_{\ell,0}(x), \ldots, w_{\ell,m_1-1}(x)\big)\end{aligned}$$

and

$$\begin{aligned}\vec{s'}(x,y) = \vec{s^t}(x,y) &= (y^{m_2}-1)^{\gamma_2}\vec{w}(x,y)\\ &= (y^{m_2}-1)^{\gamma_2}(w_1(x,y), \ldots, w_\ell(x,y)).\end{aligned} \tag{3.4.8}$$

By maximalitiy of γ_2, at least one coordinate of $\vec{w}(y)$ is not divisible by $(y^{m_2}-1)$. We claim that $\vec{w}(x,y) \in C_a \subset C$ and therefore $\vec{w}(y) \in E$ with $(\vec{w})'(y) \in E'\backslash\{0\}$. This would yield $wt(\vec{s}(x,y)) \geq wt((\vec{w})'(y))$.

By (3.4.7) and (3.4.8), we obtain

$$\begin{aligned}\vec{s'}(x,y) &= (y^{m_2}-1)^{\gamma_2}(w_1(x,y), \ldots, w_\ell(x,y))\\ &= (y^{m_2}-1)\left([k(x,y)g'_1(x,y)] \text{ mod } \langle x^{m_1}-1\rangle, \ldots, [k(x,y)g'_\ell(x,y)] \text{ mod } \langle x^{m_1}-1\rangle\right).\end{aligned}$$

Observe that even though both $k(x,y)$ and $g'_i(x,y)$'s are reduced mod $\langle x^{m_1}-1\rangle$, their product may require further reduction mod $\langle x^{m_1}-1\rangle$. Also $\vec{w}(x,y)$ is reduced mod $\langle x^{m_1}-1\rangle$ and at least one coordinate of $\vec{w}(x,y)$ is not divisible by $(y^{m_2}-1)$. Then, for all $i = 1, \ldots, \ell$ it follows that

$$(y^{m_2}-1)^{\gamma_2-1}w_i(x,y) = k(x,y)g'_i(x,y) \quad \text{mod } \langle x^{m_1}-1\rangle. \tag{3.4.9}$$

Therefore for some polynomials $t_i(x,y), K(x,y) \in \mathbb{F}_q[x,y]$ and for each $1 \leq i \leq \ell$, we have

$$k\big(g_i - t_i(x^{m_1}-1)\big) \bmod \langle x^{m_1}-1\rangle = (y^{m_2}-1)^{\gamma_2-1} w_i(x,y),$$

$$kg_i - kt_i(x^{m_1}-1) - K(x^{m_1}-1) = (y^{m_2}-1)^{\gamma_2-1} w_i(x,y).$$

Hence the following holds for all $i \in \{1,\dots,\ell\}$:

$$kg_i = [kt_i + K](x^{m_1}-1) + (y^{m_2}-1)^{\gamma_2-1} w_i \in \langle x^{m_1}-1, y^{m_2}-1\rangle.$$

Our assumption (3.3.2) implies that $k(x,y) \in \langle x^{m_1}-1, y^{m_2}-1\rangle$. Since $k(x,y)$ is reduced mod $\langle x^{m_1}-1\rangle$, $k(x,y) = \tilde{k}(x,y)(y^{m_2}-1)$ for some $\tilde{k}(x,y)$. Therefore, by (3.4.9) we have for all i

$$\tilde{k}(x,y)(y^{m_2}-1)g_i'(x,y) \bmod \langle x^{m_1}-1\rangle = (y^{m_2}-1)^{\gamma_2-1} w_i(x,y).$$

Hence,

$$\tilde{k}(x,y)g_i'(x,y) \bmod \langle x^{m_1}-1\rangle = (y^{m_2}-1)^{\gamma_2-2} w_i(x,y), \text{ for all } i.$$

We are back to the same situation. We repeat the same argument on $\tilde{k}(x,y)$ until $(y^{m_2}-1)$ disappears on the right side so that $k(x,y) = \bar{k}(x,y)(y^{m_2}-1)^{\gamma_2-1}$ for some $\bar{k}(x,y) \in \mathbb{F}_q[x,y]$ and $\bar{k}(x,y)g_i'(x,y) \bmod \langle x^{m_1}-1\rangle = w_i(x,y)$ for all i. Since at least one of the $w_i(x,y)$'s is not divisible by $(y^{m_2}-1)$ and every $w_i(x,y)$ is reduced mod $\langle x^{m_1}-1\rangle$, we no longer have $\bar{k}(x,y)g_i'(x,y) \bmod \langle x^{m_1}-1\rangle \in \langle x^{m_1}-1, y^{m_2}-1\rangle$ for every i. Hence, $\bar{k}(x,y)$ is no longer divisible by $(y^{m_2}-1)$. Therefore, if the information word of $\vec{s}(x,y) \in C$ is written as

$$m(x,y)(x^{m_1}-1) + \bar{k}(x,y)(y^{m_2}-1)^{\gamma_2-1}(y^{m_2}-1),$$

then $\vec{w}(x,y)$ is the reduction mod $\langle x^{m_1}-1\rangle$ of $\bar{k}(x,y)G \in C$. Hence, in the Case 2', we also have

$$wt(\vec{c}(x,y)) \geq wt(\vec{s'}(x)) = wt(\vec{s^t}(y)) \geq wt((\vec{w})'(y)).$$

□

Let us illustrate the idea of the proof in the following example.

Example 3.4.2. Let C be a 2D convolutional code of length 2 over $\mathbb{F}_2$ given with the PGM

$$G = (x, y)$$

and let C' be the associated QC code in $(\mathbb{F}_2[x,y]/\langle x^3+1, y^5+1\rangle)^2$. It is easy to see that $J_{3,5} = \langle x^3+1, y^5+1\rangle$, hence our assumption holds for $m_1 = 3$ and $m_2 = 5$.

For the information words $u_1(x,y) = x^4 + x \in \mathbb{F}_2[x,y]$ and $u_2(x,y) = x^3 + y^5 \in \mathbb{F}_2[x,y]$, consider the corresponding codewords $\vec{c}_1(x,y), \vec{c}_2(x,y) \in C$, respectively:

$$\vec{c}_1(x,y) = u_1(x,y)G = (x^5 + x^2, x^4y + xy),$$
$$\vec{c}_2(x,y) = u_2(x,y)G = (x^4 + xy^5, x^3y + y^6).$$

Let us begin with $\vec{c}_1(x,y)$. We have $\max\limits_{1\le j\le 2}\big(\deg_y c_{1j}(x,y)\big) = 1$. Therefore $\vec{c}_1(x,y) \in C_1 \subset C$. We unfold it by the map φ_x and get the following vector of length $(1+1)\cdot 2 = 4$:

$$\vec{c}_1(x) = \varphi_x(\vec{c}_1(x,y)) = (0, x^5 + x^2\ ; x^4 + x, 0)$$

such that $\vec{c}_1(x)$ is a codeword of the length 4 convolutional code $D_1 = \varphi_x(C_1)$ and $wt(\vec{c}_1(x,y)) = wt(\vec{c}_1(x)) = 4$.

Let D_1' denote the QC code in $(\mathbb{F}_2[x]/\langle x^3+1\rangle)^4$ associated to D_1, then

$$\vec{c'}_1(x) = \vec{c}_1(x) \mod \langle x^3 - 1\rangle = (0, 0\ ; 0, 0).$$

The maximal power of x^3+1 which divides the coordinates of $\vec{c}_1(x)$ is 1, so $\vec{c}_1(x) = (x^3+1)\vec{v}_1(x)$ with

$$\vec{v}_1(x) = (0, x^2\ ; x, 0)$$

and (x^3+1) does not divide the coordinates of $\vec{v}_1(x)$. So,

$$\vec{v}_1(x,y) = \varphi_x^{-1}(\vec{v}_1(x)) = (x^2, xy) \in C_1 \subset C,$$

where $\vec{v}_1(x,y) = x \cdot G$ and

$$\vec{v'}_1(x) = \vec{v}_1(x) \mod \langle x^3+1\rangle = (0, x^2\ ; x, 0)$$

is a nonzero codeword in D'_1 with $wt(\vec{v'}_1(x)) = 2$.

Next, we twist $\vec{v'}_1(x)$ to get a vector of length $3 \cdot 2 = 6$ such that

$$\vec{v_1^t}(y) = \mathcal{T}(\vec{v'}(x)) = (1, 0, 0\ ; 0, y, 0),$$

where $\vec{v_1^t}(y)$ is a codeword of E with $wt(\vec{v'}_1(x)) = wt(\vec{c_1^t}(y)) = 2$. Let E' be the associated QC code in $\left(\mathbb{F}_2[y]/\langle y^5 + 1\rangle\right)^6$, then we have

$$(\vec{v_1^t})'(y) = \vec{v_1^t}(y) \mod \langle y^5 + 1\rangle = (1, 0, 0\ ; 0, y, 0)$$

and $wt((\vec{v_1^t})'(y)) = 2$.

Now we fold it back by φ_y^{-1}:

$$\vec{v_1'}(x, y) = \varphi_y^{-1}(\vec{v_1^t}(y)) = (x^2, xy),$$

where $\vec{v_1'}(x, y) \in C'$ is the Q2DC codeword satisfying $wt(\vec{v_1'}(x, y)) = 2 \leq wt(\vec{c_1}(x, y))$.

We continue with $\vec{c}_2(x, y) = (x^4 + xy^5, x^3y + y^6)$. We have $\max\limits_{1 \leq j \leq 2}\big(\deg_y c_{2j}(x, y)\big) = 6$. Therefore $\vec{c}_2(x, y) \in C_6 \subset C$. Again, we unfold it by the map φ_x and get the following vector of length $(6 + 1) \cdot 2 = 14$:

$$\vec{c}_2(x) = \varphi_x(\vec{c}_2(x, y)) = (0, x, 0, 0, 0, 0, x^4\ ; 1, 0, 0, 0, 0, x^3, 0)$$

such that $\vec{c}_2(x) \in D_6 = \varphi_x(C_6)$ and $wt(\vec{c}_2(x, y)) = wt(\vec{c}_2(x)) = 4$.

Let D'_6 be associated the QC code in $\left(\mathbb{F}_2[x]/\langle x^3 + 1\rangle\right)^{14}$, then

$$\vec{c'}_2(x) = \vec{c}_2(x) \mod \langle x^3 - 1\rangle = (0, x, 0, 0, 0, 0, x\ ; 1, 0, 0, 0, 0, 1, 0)$$

is a nonzero codeword in D'_6 with $wt(\vec{c}_2(x)) = wt(\vec{c'}_2(x)) = 4$.

Then we twist $\vec{c'}_2(x)$ and obtain

$$\vec{c_2^t}(y) = \mathcal{T}(\vec{c'}_2(x)) = (0, y^5 + 1, 0\ ; 0, 0, y^6 + y),$$

where $\vec{c_2^t}(y) \in E$ with $wt(\vec{c'}_2(x)) = wt(\vec{c_2^t}(y)) = 4$. Let E' be the associated QC code in $\left(\mathbb{F}_2[y]/\langle y^5 + 1\rangle\right)^6$, then

$$(\vec{c_2^t})'(y) = \vec{c_2^t}(y) \mod \langle y^5 + 1\rangle = (0, 0, 0\ ; 0, 0, 0).$$

The maximal power of (y^5+1) which divides the coordinates of $\vec{c_2^t}(y)$ is 1, so $\vec{c_2^t}(y) = (y^5+1)\vec{w_2}(y)$ with

$$\vec{w_2}(y) = (0,1,0\ ;0,0,y)$$

and (y^5+1) does not divide the coordinates of $\vec{w_2}(y)$. So,

$$\vec{w_2}(x,y) = \phi_y^{-1}(\vec{w_2}(y)) = (x,y) \in C_1 \subset C,$$

where $\vec{w_2}(x,y) = 1 \cdot G$ and

$$\vec{(w_2)'}(y) = \vec{w_2}(y) \mod \langle y^5+1 \rangle = (0,1,0\ ;0,0,y)$$

is a nonzero codeword in E' with $wt(\vec{w_2}(x,y)) = wt(\vec{(w_2)'}(y)) = 2$.

Finally we fold it back by φ_y^{-1}:

$$\vec{(w_2)'}(x,y) = \varphi_y^{-1}(\vec{w_2}(y)) = (x,y),$$

where $\vec{(w_2)'}(x,y) \in C'$ and $wt(\vec{w_2'}(x,y)) = 2 \leq wt(\vec{c_2}(x,y))$.

Bibliography

[1] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, vol. 3, American Mathematical Society, Providence, RI, 1994.

[2] T. Becher and V. Weispfennig, “Gröbner Bases”, *Springer Verlag*, 1993.

[3] E.Z. Chen, “New quasi-cyclic codes from simplex codes”, *IEEE Trans. Inform. Theory*, vol. 53, pp. 1193-1196, 2007.

[4] J.-J. Climent, D. Napp, C. Perea and R. Pinto “A construction of MDS 2D convolutional codes of rate $1/n$ based on superregular matrices”, *Linear Algebra Appl.*, vol. 437, no. 3, 766–780, 2012.

[5] R.N. Daskalov and P. Hristov, “New binary one-generator quasi-cyclic codes”, *IEEE Trans. Inform. Theory*, vol. 49, pp. 3001-3005, 2003.

[6] B.K. Dey, “On existence of good self-dual quasi-cyclic codes”, *IEEE Trans. Inform. Theory*, vol. 50, no. 8, 1794–1798, 2004.

[7] E. Fornasini and M.E. Valcher, “Algebraic aspects of two-dimensional convolutional codes”, *IEEE Trans. Inform. Theory*, vol. 40, no. 4, pp. 1068-1082, 1994.

[8] H. Gluesing-Luerssen, J. Rosenthal and R. Smarandache, “Strongly-MDS convolutional codes”, *IEEE Trans. Inform. Theory*, vol. 52, no. 2, 584–598, 2006.

[9] H. Gluesing-Luerssen, J. Rosenthal and P. Weiner, “Duality between multidimensional convolutional codes and systems”, *Advances in Mathematical Systems Theory, Systems Control Found. Appl., Boston, MA*, pp. 135–150, 2001.

[10] T.A. Gulliver and V.K. Bhargava, “Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes”, *IEEE Trans. Inform. Theory*, vol. 37, pp. 552-555, 1991.

[11] T.A. Gulliver and V.K. Bhargava, “Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over GF(3) and GF(4)”, *IEEE Trans. Inform. Theory*, vol. 38, no. 4, pp. 1369-1374, 1992.

[12] T.A. Gulliver and V.K. Bhargava, “Nine good rate $(m-1)/pm$ and rate $(p-1)/p$ quasi-cyclic codes”, *IEEE Trans. Inform. Theory*, vol. 38, no. 4, pp. 1366-1369, 1992.

[13] C. Güneri, “Artin-Schreier curves and weights of two-dimensional cyclic codes”, *Finite Fields Appl.*, vol. 10, no. 4, pp. 481-505, 2004.

[14] C. Güneri, “Artin-Schreier Families and 2D Cyclic Codes”, PhD Thesis, Department of Mathematics, Louisiana State University, 2001.

[15] C. Güneri and F. Özbudak, “Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields”, *Finite Fields Appl.*, vol. 14, no. 1, pp. 44-58, 2008.

[16] C. Güneri and F. Özbudak, “The concatenated structure of quasi-cyclic codes and an improvement of Jensen’s bound”, *IEEE Trans. Inform. Theory*, vol. 59, no. 2, 979–985, 2013.

[17] T. Ikai, H. Kosako and Y. Kojima, “Two-dimensional cyclic codes”, *Electronics and Communications in Japan*, vol. 57-A, pp. 27-35, 1975.

[18] H. Imai, “A theory of two-dimensional cyclic codes”, *Information and Control*, vol. 34, pp. 1-21, 1977.

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

[20] T. Kasami, “A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2”, *IEEE Trans. Inform. Theory*, vol. 20, p. 679, 1974.

[21] K. Lally, “Algebraic lower bounds on the free distance of convolutional codes”, *IEEE Trans. Inform. Theory*, vol. 52, no. 5, pp. 2101–2110, 2006.

[22] J.H. van Lint, *Introdution to Coding Theory*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1999.

[23] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: finite fields", *IEEE Trans. Inform. Theory*, vol. 47, no. 7, pp. 2751–2760, 2001.

[24] S. Ling and P. Solé, "Good self-dual quasi-cyclic codes exist", *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 1052–1053, 2003.

[25] J.L. Massey, D.J. Costello, J. Justesen, "Polynomial weights and code constructions", *IEEE Trans. Inform. Theory*, vol. 19, no. 1, pp. 101-110, 1973.

[26] J.L. Massey and M.K. Sain, "Inverses of linear sequential circuits", *IEEE Trans. Comput.*, vol. C-17, no. 4, pp. 330-337, 1968.

[27] C. Martínez-Pérez and W. Willems, "Is the class of cyclic codes asymptotically good?" *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 696-700, 2006.

[28] C. Martínez-Pérez and W. Willems, "Self-dual doubly even 2-quasi-cyclic transitive codes are asymptotically good", *IEEE Trans. Inform. Theory*, vol. 53, no. 11, pp. 4302–4308, 2007.

[29] R.J. McEliece, "The algebraic theory of convolutional codes", *Handbook of Coding Theory, North-Holland, Amsterdam*, pp. 1065–1138, 1998.

[30] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 2006.

[31] A. Seidenberg, "Constructions in Algebra", *Trans. Amer. Math. Soc.*, vol. 197, pp. 272-313, 1974.

[32] K. Saints and C. Heegard, "Algebraic-geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases", *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1733-1751, 1993.

[33] P.A. Weiner, "Multidimensional Convolutional Codes", PhD Thesis, Department of Mathematics, University of Notre Dame, 1998.