CONCATENATED CODES, MATRIX-PRODUCT CODES AND THEIR SCHUR PRODUCT

by

Tuğçe Ulutaş

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Master of Arts

Sabancı University
July 2021

Concatenated Codes, Matrix-Product Codes and Their Schur Product

APPROVED BY

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

DATE OF APPROVAL: 13.07.2021

to my family

Concatenated Codes, Matrix-Product Codes and Their Schur Product

Tuğçe Ulutaş

Mathematics, Master Thesis, 2021

Thesis Supervisor: Prof. Dr. Cem Güneri

Keywords: Concatenated codes, matrix-product codes, Schur product.

Abstract

The aim of thesis is two-fold. Firstly, we introduce concatenated codes, matrix-product codes and elaborate on their relation. It is known that a matrix-product code can be seen as a concatenated code. We give a proof of this fact. Conversely, we show how a particular concatenated code can be viewed as a matrix-product code. The second goal is to study the Schur product of certain matrix-product codes, following the recent work of Cascudo et al. The Schur product of linear codes is a topic of interest in the context of code-based cryptography.

Bitiştirme Kodları, Matris-Çarpım Kodları ve Onların Schur Çarpımı

Tuğçe Ulutaş

Matematik, Yüksek Lisans Tezi, 2021

Tez Danışmanı: Prof. Dr. Cem Güneri

Anahtar Kelimeler: Bitiştirme kodları, matris-çarpım kodları, Schur çarpımı.

Özet

Bu tezin iki amacı bulunmaktadır. Öncelikle bitiştirme kodları, matris-çarpım kodları tanıtılarak aralarındaki ilişki üzerinde durulacaktır. Matris-çarpım kodlarının bitiştirme kodu olarak gösterilebilecekleri bilinmektedir. Bu gerçeğin ispatı sunulacaktır. Ters yönde ise özel bir bitiştirme kodunun nasıl matris-çarpım kodu olarak temsil edilebileceği gösterilecektir. İkinci amacımız ise Cascudo et al. çalışmasını takip ederek bazı matris-çarpım kodlarının Schur çarpımlarını çalışmaktır. Doğrusal kodların Schur çarpımları, kod tabanlı şifreleme açısından ilgi çeken bir konudur.

ACKNOWLEDGEMENTS

I would first like to thank my thesis advisor Prof. Dr. Cem Güneri for the continuous support of my study, for his patience, motivation, and immense knowledge. Without his passionate participation and input, this thesis could not have been successfully conducted. He guided me in the right direction whenever he thought I needed it.

Besides my advisor, I would like to thank the rest of my thesis jury: Prof. Dr. Ferruh Özbudak and Assist. Prof. Dr. Nurdagül Anbar Meidl. I am gratefully indebted to them for every valuable comments on this thesis.

I would also like to thank Dr. Elif Saçıkara for sharing notes herself to support our thesis.

Also, I thank my friends Ayçin İplikçi, Eda Kırımlı, Elif Uğur Üsküplü and Ege Şirin for supporting me spiritually.

Finally, I would express my very profound gratitude to my parents for supporting me and continuous encouragement throughout my years of study. This thesis would not have been possible without them. Thank you.

Contents

Introduction

Concatenation and the matrix-product (MP) constructions are well-known coding theory techniques to construct new codes from a given set of other codes. In concatenation, one can have one (simple concatenation) or several (generalized or multi-level concatenation) ”outer” codes over extensions of the finite field $\mathbb{F}_q$. The inner code, defined over $\mathbb{F}_q$, is then used to construct a long code over $\mathbb{F}_q$ ([3]). In the MP construction, codes defined over $\mathbb{F}_q$, which are called constituent codes, are used together with the so-called defining matrix of full-rank to produce again a long code over $\mathbb{F}_q$ ([1], [9]). Both of these methods have been widely used in the literature for various purposes.

In both constructions, the resulting codes' length and dimension can be explicitly written in terms of the length and dimension of the codes used in the construction. Moreover, there is a minimum distance lower bound for both the concatenated code and the MP code, in terms of the minimum distances of codes utilized in the constructions. In fact, the minimum distance bounds for the two constructions are identical. The reason for this is that an MP code can be viewed as a concatenated code. The converse, however, is not known to the best of our knowledge.

On the other hand, the Schur product operation can be used to construct a new code out of two given codes. Besides coding theoretic interest, the Schur product of linear codes is of interest for post-quantum cryptography. One of the schemes proposed in post-quantum cryptography is based on linear codes and it dates back to the work of McEliece ([8]). The name is hence McEliece cryptosystem, where a linear code is ”permuted” for the purpose of secrecy and is used as public key. The security of the system relies on the hardness of decoding linear codes. It has been observed that codes whose Schur product has large dimension is desirable against certain attacks to the McEliece cryptosystem ([2], [12]).

In this thesis, we introduce basic properties of concatenated codes, MP codes and investigate the relation between them. We show how an MP code can be viewed as a concatenated code. Moreover, we present an MP representation for a specific concatenated code (namely, Turyn's construction). Finally, we present results obtained by Cascudo et al. on the Schur product of some families of MP codes.

Chapter 1

Preliminaries

1.1 Linear Codes

We recall very briefly some of the basic notations and facts about linear codes. Throughout the thesis $\mathbb{F}_q$ denotes the finite field with q elements.

Definition 1.1.1. A k-dimensional subspace C of $\mathbb{F}_q^n$ is called a **linear code** of length n and dimension k.

We denote such a code as $[n,k]_q$ code, or just as $[n,k]$ code, if there is no need to emphasize the finite field. Elements of a code are referred to as codewords.

Definition 1.1.2. Let $x, y \in \mathbb{F}_q^n$. The **Hamming distance** between x and y, denoted by $d(x,y)$, is defined to be

$$d(x,y) = |\{i \in \{1,...,n\} : x_i \neq y_i\}|.$$

The **Hamming weight** of x is defined as

$$wt(x) = d(x,0),$$

where 0 denotes the zero vector.

Definition 1.1.3. The **minimum distance** of C is defined as

$$d(C) = \min\{d(x,y) : x, y \in C, x \neq y\}.$$

It's very easy to see that the minimum distance of a linear code C is equal to the minimum weight among all nonzero codewords in C. An $[n, k]$ linear code with minimum distance d is denoted as $[n, k, d]$ code. So, there are three main parameters of a linear code.

Definition 1.1.4. A **generator matrix** for a linear code C is a matrix G whose rows form a basis for C.

Hence, a generator matrix G for an $[n, k]$ code is a $k \times n$ matrix of rank k. In general, there are many generator matrices for a linear code. Note that an $[n, k]$ code can be described by a generator matrix G as

$$C = \{uG : u \in \mathbb{F}_q^k\}.$$

Definition 1.1.5. For an $[n, k]$-code C over $\mathbb{F}_q$, the **(Euclidean) dual** of C is defined as

$$C^{\perp} = \{x \in \mathbb{F}_q^n : x.c = 0, \forall c \in C\},$$

where . denotes the Euclidean inner product on $\mathbb{F}_q^n$.

In other words, the dual code $C^{\perp}$ is the orthogonal complement of C. It is clear that $C^{\perp}$ is an $[n, n-k]$ linear code over $\mathbb{F}_q$.

Definition 1.1.6. A generator matrix H of the dual code $C^{\perp}$ of an $[n, k]$ linear code C is called a **parity-check matrix** of C.

It is clear that H is an $(n-k) \times n$ matrix of rank $(n-k)$. Moreover, we clearly see $GH^T = 0$, where G is a generator matrix of C.

Theorem 1.1.7. *Let C be a linear code and let H be a parity-check matrix for C. Then, C has distance $\leq d$ if and only if H has d columns that are linearly dependent.*

Proposition 1.1.8. *(Singleton Bound) The minimum distance d of an $[n, k]$ linear code C over $\mathbb{F}_q$ satisfies*

$$d \leq n - k + 1.$$

Proof. Suppose that H is a parity-check matrix for C. Then, by definition, the rank of H is $n-k$. Therefore, any $n-k+1$ columns of H form a linearly dependent set. By Theorem 1.1.7, $d \leq n-k+1$. □

Definition 1.1.9. Let m and l be two positive integers. A linear code C of length lm over $\mathbb{F}_q$ is called a **quasi-cyclic code** (QC) of index l if it is invariant under shift of codewords by l units, where l is the smallest positive integer with this property.

1.2 Concatenated Codes

Concatenation is a well-known technique in coding theory to construct new codes from a given set of other codes. We introduce the basic notions on concatenated codes in this section. Our presentation closely follows that in [3] and [11].

Definition 1.2.1. Let $\mathcal{C}$ be a linear code with the parameters $[N, K, d(\mathcal{C})]$ over $\mathbb{F}_{q^k}$ $(k \geq 1)$. For $k \leq n$, let

$$\pi : \mathbb{F}_{q^k} \to \mathbb{F}_q^n$$

be an $\mathbb{F}_q$-linear injection and set $\mathcal{A} := im(\pi)$. The set

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

is called a **concatenated code**.

Remark 1.2.2. Note that $\mathcal{A}$ is an $[n, k]$ linear code over $\mathbb{F}_q$. It is easy to see that the concatenated code $\pi(\mathcal{C})$ is an $\mathbb{F}_q$-linear code with parameters $[nN, kK]$. Moreover,

$$d(\pi(\mathcal{C})) \geq d(\mathcal{C})d(\mathcal{A}).$$

The distance bound above can be observed as follows. If $c = (c_1, ..., c_N)$ is a nonzero codeword in $\mathcal{C}$, then it has at least $d(\mathcal{C})$ nonzero coordinates. Since π is an $\mathbb{F}_q$-linear injection, each nonzero coordinate $c_j \in \mathcal{C}$ is mapped to a nonzero codeword $\pi(c_j) \in \mathcal{A}$ and hence $wt(\pi(c_j)) \geq d(\mathcal{A})$. Therefore,

$$wt(\pi(\mathcal{C})) \geq d(\mathcal{C})d(\mathcal{A}).$$

In this construction, $\mathcal{C}$ is called the **outer code** and $\mathcal{A}$ is called the **inner code**. The concatenated code $\pi(\mathcal{C})$ is also denoted by $\mathcal{A}\square\mathcal{C}$.

Next, we introduce concatenated codes with more than one outer code. Such codes are also known as **generalized concatenated codes** or **multilevel concatenated codes** ([3]).

Definition 1.2.3. Let $\mathcal{C}_i$ be an $[N, K_i]$ linear code over $\mathbb{F}_{q^{k_i}}$, for $1 \leq i \leq s$. Consider the set

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

Denote the columns of an element $c \in \mathcal{C}$ by $c_1, ..., c_N$ and the rows by $c^1, ..., c^s$. Note that $c_i \in \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_s}}$ for all $i \in \{1, ..., N\}$. Let,

$$\pi : \mathbb{F}_{q^{k_1}} \times \cdots \times \mathbb{F}_{q^{k_s}} \to \mathbb{F}_q^n,$$

be an $\mathbb{F}_q$-linear injection and denote its image, which is an $\mathbb{F}_q$-linear $[n, k_1 + ... + k_s]$ code, by $\mathcal{A}$. The set

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

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

Remark 1.2.4. In this construction, $\mathcal{C}_1, ..., \mathcal{C}_s$ are called **outer codes** and $\mathcal{A}$ is called the **inner code**. Note that the simple concatenation (Definition 1.2.1) is a special case with $s = 1$. A GCC as in Definition 1.2.3 is also denoted by $\mathcal{A}\square\mathcal{C}$.

The next result provides information on the parameters of a GCC. The proof of the first part is clear. We give a proof for the second part following ideas similar to those in the proof of [3, Theorem 2.14].

Proposition 1.2.5. *Let $\pi(\mathcal{C})$ be a GCC as described in Definition 1.2.3. Then*

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

(ii)

$$d(\pi(\mathcal{C})) \geq \min_{1\leq i\leq s}\{d(\mathcal{C}_i)d(\mathcal{A}_1\bigoplus\cdots\bigoplus\mathcal{A}_i)\}, \tag{1.2.2}$$

where

$$\mathcal{A}_i = \pi(\{0\}\times\cdots\times\{0\}\times\mathbb{F}_{q^{k_i}}\times\{0\}\times\cdots\times\{0\})$$

for $i = 1, ..., s$.

Proof. We only prove part (ii). Let $c \in \mathcal{C}$ be such that

$$c^i \neq 0,\ c^{i+1} = \cdots = c^s = 0.$$

Note that for a nonzero element $c \in \mathcal{C}$, the number i described in this way is at least 1. In other words, let the i^{th} row be the last nonzero row in c. Hence, each column $c_1, ..., c_N$ of c belongs to

$$\mathbb{F}_{q^{k_1}}\times\cdots\times\mathbb{F}_{q^{k_i}}\times\{0\}\times\cdots\times\{0\}.$$

Note that the i^{th} row c^i has at least $d(\mathcal{C}_i)$ nonzero coordinates. Therefore, at least $d(\mathcal{C}_i)$ columns of $c = (c_1, ..., c_N)$ is a nonzero s-tuple. Each of these nonzero columns is mapped to

$$\pi(\mathbb{F}_{q^{k_1}}\times\cdots\times\mathbb{F}_{q^{k_i}}\times\{0\}\times\cdots\times\{0\}) = \mathcal{A}_1\bigoplus\cdots\bigoplus\mathcal{A}_i \subseteq \mathcal{A}$$

and therefore has weight at least $d(\mathcal{A}_1\bigoplus\cdots\bigoplus\mathcal{A}_i)$. Since there are $d(\mathcal{C}_i)$ nonzero columns, we conclude

$$wt(\pi(c)) \geq d(\mathcal{C}_i)d(\mathcal{A}_1\bigoplus\cdots\bigoplus\mathcal{A}_i).$$

Letting i take any value between 1 and s, we reach the conclusion. □

Remark 1.2.6. The following inclusions are clear.

$$\mathcal{A}_1 \subseteq \mathcal{A}_1\bigoplus\mathcal{A}_2 \subseteq \cdots \subseteq \bigoplus_{i=1}^{s-1}\mathcal{A}_i \subseteq \bigoplus_{i=1}^{s}\mathcal{A}_i = \mathcal{A}.$$

Hence,

$$d(\mathcal{A}_1) \geq d(\mathcal{A}_1\bigoplus\mathcal{A}_2) \geq \cdots \geq d(\bigoplus_{i=1}^{s-1}\mathcal{A}_i) \geq d(\mathcal{A}).$$

Therefore, if the outer codes are arranged in a way that

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

the bound in (1.2.2) will yield the optimal value.

1.3 Matrix-Product Codes

Matrix-product (MP) codes were first introduced in [1] as a generalization of some well-known code constructions such as the $(u, u+v)$ construction. The MP construction, like concatenated codes, is a method to construct new and longer codes from a given set of codes.

Definition 1.3.1. Let C_i be an $[n, k_i]$ linear code over $\mathbb{F}_q$ for $1 \leq i \leq s$. Let A be an $s \times l$ matrix (with $s \leq l$) of full rank s. The **matrix-product code** is defined as

$$C = [C_1, ..., C_s]A = \{[c_1, ..., c_s]A; c_i \in C_i\}.$$

Remark 1.3.2. Since A is of full rank, it represents an injective $\mathbb{F}_q$-linear transformation. Hence, it is easy to observe that the MP code $[C_1, ..., C_s]A$ is an $[nl, \sum\limits_{i=1}^{s} k_i]$ linear code over $\mathbb{F}_q$. The matrix A is called the **defining matrix** of the MP code. Codes $C_1, ..., C_s$ are called **constituent codes**.

Proposition 1.3.3. *([2, Proposition 2.2]) Consider the MP code $C = [C_1, ..., C_s]A$ as described in Definition 1.3.1. Let G_i be a generator matrix for C_i $(1 \leq i \leq s)$ of size $k_i \times n$ and rank k_i. If $A = (a_{ij})$, then a generator matrix of C is given by*

$$G = \begin{bmatrix} a_{11}G_1 & \cdots & a_{1l}G_1 \\ \vdots & \ddots & \vdots \\ a_{s1}G_s & \cdots & a_{sl}G_s \end{bmatrix}.$$

Let A_i be the matrix consisting of the first i rows of A, for each $i \in \{1, ..., s\}$. Hence, A_i is an $i \times l$ matrix. Denote the minimum distance of the code $<A_i>$, whose generator matrix is A_i, by D_i. The following bound is well-known for MP codes ([2, Proposition 2.3])

Proposition 1.3.4. *With the notation so far, we have*

$$d([C_1, ..., C_s]A) \geq \min\{D_1 d_1, D_2 d_2, ..., D_s d_s\}.$$

where $d_i = d(C_i)$ and $D_j = d(<A_i>)$ for all i and j.

It has been proved in [6] that if the constituent codes are nested $C_1 \supset C_2 \supset \ldots \supset C_s$, then the lower bound in Proposition 1.3.4 is reached.

Remark 1.3.5. We note the analogy between the bound in Proposition 1.3.4 with the minimum distance bound for concatenated codes (1.2.2). In the next chapter we will present how to view an MP code as a GCC code. This observation will imply the proof of Proposition 1.3.4 as well.

1.4 The Schur Product of Codes

Definition 1.4.1. Let $x, y \in \mathbb{F}_q^n$. The **Schur product** of x and y is their component-wise product

$$x \star y = (x_1 y_1, ..., x_n y_n).$$

Definition 1.4.2. Let C, C' be two linear codes of length n. Then we define their **Schur product** as

$$C \star C' = \langle \{c \star c' | c \in C, c' \in C'\} \rangle.$$

The Schur square of a code C is $C^{\star 2} = C \star C$.

Definition 1.4.3. Let G be a $k \times n$ matrix with rows g_i for $1 \leq i \leq k$. The **Schur matrix** of G consists of the rows $g_i \star g_j$ for $1 \leq i \leq j \leq k$ which we denote by $S(G)$.

Note that $S(G)$ is of the size $\frac{1}{2}(k^2 + k) \times n$.

Let C_1 and C_2 be two linear codes in $\mathbb{F}_q^n$. Suppose that their generator matrices are G_1 and G_2, respectively, which are defined as

$$G_1 = \begin{bmatrix} g_1 \\ \vdots \\ g_s \end{bmatrix},$$

$$G_2 = \begin{bmatrix} g_1 \\ \vdots \\ g_l \end{bmatrix}.$$

If we take Schur product of the rows of G_1 with the rows of G_2, we obtain a generating set for $C_1 \star C_2$. Some of the resulting rows can of course be linearly dependent.

Example 1.4.4. Let C_1, C_2 be two linear codes in $\mathbb{F}_2^4$ of dimensions $k_1 = 2$ and $k_2 = 3$, respectively, defined by the following generator matrices:

$$G_1 = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix},$$

$$G_2 = \begin{bmatrix} 0001 \\ 0010 \\ 1110 \end{bmatrix}.$$

Then,

$$G_1 \star G_2 = \begin{bmatrix} 1000 \\ 0010 \\ 1010 \\ 0001 \\ 0000 \\ 0100 \end{bmatrix}.$$

If we remove linearly dependent rows, we obtain

$$G_1 \star G_2 = \begin{bmatrix} 1000 \\ 0010 \\ 0001 \\ 0100 \end{bmatrix}.$$

Note that if we take $C_2 = C_1$, then the Schur matrix of the generator matrix of a code is the generator matrix of the square code.

Proposition 1.4.5. *Let C, C' be two linear codes of length n. Then*

$$dim(C \star C') \leq dim(C)dim(C').$$

Proof. Suppose that G, G' are generator matrix of C and C', respectively, in the form

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_k \end{bmatrix},$$

$$G' = \begin{bmatrix} g'_1 \\ \vdots \\ g'_{k'} \end{bmatrix}.$$

Then, a generator matrix of $C \star C'$ can be obtained from $G \star G'$, which is a $kk' \times n$ matrix. By the definition of rank,

$$rank(G \star G') \leq \min\{kk', n\} \leq kk'.$$

This completes the proof. □

The following is also known for the dimension of the Schur square of a code.

Proposition 1.4.6. *Let C be a linear code of length n and dimension k. Then*

$$k \leq dim(C^{\star 2}) \leq \min\{n, \tbinom{k+1}{2}\}.$$

Proof. After Example 1.4.4, we have infered the generator matrix of the square code, which is the Schur matrix. Since the Schur matrix has $\binom{k+1}{2}$ rows and n columns, we have

$$rank(C^{\star 2}) \leq \min\{\tbinom{k+1}{2}, n\}.$$

□

The following Singleton-like bound is known for the Schur square.

Proposition 1.4.7. *([10]) Let C be a linear code of length n and dimension k. Then $C^{\star 2}$ has minimum distance*

$$d(C^{\star 2}) \leq \max\{1, n - 2k + 2\}.$$

Chapter 2

Relation Between Concatenated Codes and Matrix-Product Codes

It is known that one can view an MP code as a concatenated code. In Section 2.1, we present a proof of this. The converse, that is whether any concatenated code can be viewed as an MP code, is unknown to the best of our knowledge. In Section 2.2, we present an approach to view a particular concatenated code as an MP code.

2.1 The Concatenated Representation of an MP Code

Consider an MP code $[C_1, ..., C_s]A$ as described in Section 1.3. Define

$$\begin{array}{rcl} \pi : \mathbb{F}_q^s = \mathbb{F}_q \times \cdots \times \mathbb{F}_q & \longrightarrow & \mathbb{F}_q^l \\ (x_1, \ldots, x_s) & \longmapsto & (x_1, \ldots, x_s)A \end{array}, \tag{2.1.1}$$

which is an injective $\mathbb{F}_q$-linear map, since A is an $s \times l$ matrix of full rank s. If we denote a codeword in $c^i \in C_i$ by

$$c^i = (c^i_1, \ldots, c^i_n),$$

for all $1 \leq i \leq s$, as in Section 1.2, then observe that

$$(c^1, c^2, \ldots, c^s)A = (\pi(c_1), \ldots, \pi(c_n))^T,$$

where $c_1, \ldots, c_n$ represent the columns of $c \in C$ in (1.2.1). hence, we have the following.

Proposition 2.1.1. *Let C_i be an $\mathbb{F}_q$-linear $[n, k_i, d_i]$ code over $\mathbb{F}_q$ for $1 \leq i \leq s$, and A be an $s \times l$ matrix of rank s. Let C be defined as in (1.2.1), where the rows come from the codes $C_1, ..., C_s$. For π defined as in (2.1.1), we have*

$$[C_1, ..., C_s]A = \pi(C)^T.$$

Remark 2.1.2. Recall from Sections 1.2 and 1.3 the following definitions, which are adapted to the setting in this section:

$$\mathcal{A}_i = \pi(\{0\} \times \cdots \times \{0\} \times \mathbb{F}_q \times \{0\} \times \cdots \times \{0\})$$
$$A_i = i \times l \text{ matrix formed by the first } i \text{ rows of } A.$$

Observe that for each $i \in \{1, \ldots, s\}$, the code $<A_i>$ generated by A_i satisfies

$$<A_i>= \mathcal{A}_1 \bigoplus \cdots \bigoplus \mathcal{A}_i.$$

Hence, if we apply the minimum distance bound for concatenated codes (Proposition 1.2.5) to the MP code $[C_1, ..., C_s]A$, we obtain the proof of Proposition 1.3.4 immediately as a consequence.

2.2 MP View of a Concatenated Code: Turyn's Construction

We observed that the constituents of an MP code play the role of outer codes in the concatenated representation of the code. For a GCC, however, the outer codes may be defined over extensions of $\mathbb{F}_q$, whereas the constituents of an MP code, according to the definition (Definition 1.3.1), are defined over $\mathbb{F}_q$. Hence, if we want to view a GCC as an MP code, this is an obstacle to overcome. The following example from [7] gives us an idea to resolve this problem for a special concatenated code.

Example 2.2.1 (Turyn's Construction, [7])**.** For $q \equiv 2 \mod 3$, a quasi-cyclic code C over $\mathbb{F}_q$ of length $3l$ and index l decompose via Chinese Remainder Theorem into the direct sum of two linear codes C_1 and C_2, where C_1 is defined over $\mathbb{F}_q$ and C_2 is defined over $\mathbb{F}_{q^2}$. These codes are the outer codes of C in its GCC representation, where the concatenation map, as described in [7], is

$$\begin{array}{rcc} \pi : \mathbb{F}_q \times \mathbb{F}_{q^2} & \longrightarrow & \mathbb{F}_q^3 \\ (u, v + \zeta w) & \longmapsto & (u + 2v - w, u - v + 2w, u - v - w) \end{array} . \tag{2.2.1}$$

See also [5] for concatenated view of quasi-cyclic codes. Here, $\{1, \zeta\}$ is a basis for $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Hence,

$$C = \{(x + 2a - b|x - a + 2b|x - a - b); x \in C_1, a + \zeta b \in C_2\}, \tag{2.2.2}$$

and C is a GCC with outer codes C_1 and C_2 via the concatenation map π. In characteristic 2, (2.2.2) amounts to the so called **Turyn's construction**.

Observe that the map π in (2.2.1) can also be viewed as follows:

$$\begin{array}{rcc} \pi : \mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q & \longrightarrow & \mathbb{F}_q^3 \\ (u, v, w) & \longmapsto & (u + 2v - w, u - v + 2w, u - v - w) \end{array} . \tag{2.2.3}$$

Define **component codes** of C_2 as

$$C_2{}^1 = \{a \in \mathbb{F}_q^l; a + \zeta b \in C_2 \text{ for some } b \in \mathbb{F}_q^l\}$$

$$C_2{}^2 = \{b \in \mathbb{F}_q^l; a + \zeta b \in C_2 \text{ for some } a \in \mathbb{F}_q^l\},$$

and note that both $C_2{}^1$ and $C_2{}^2$ are linear codes over $\mathbb{F}_q$. Hence, C can also be viewed as a GCC with three linear codes $C_1, C_2{}^1, C_2{}^2$ over $\mathbb{F}_q$ as its outer codes and π in (2.2.3) as the concatenation map. Assume that,

$$C_2 = C_2{}^1 \bigoplus \zeta C_2{}^2$$

$$= \{a + \zeta b : a \in C_2{}^1, b \in C_2{}^2\}.$$

Then, C can be viewed as an MP code easily

$$C = [C_1, C_2{}^1, C_2{}^2]A,$$

where

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix} = \begin{bmatrix} \pi(1,0,0) \\ \pi(0,1,0) \\ \pi(0,0,1) \end{bmatrix}.$$

Indeed, for $x \in C_1$, $a \in {C_2}^1$, $b \in {C_2}^2$, we have

$$\begin{bmatrix} x_1 & a_1 & b_1 \\ \vdots & \vdots & \vdots \\ x_l & a_l & b_l \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \\ 2 & -1 & -1 \\ -1 & 2 & -1 \end{bmatrix} = \begin{bmatrix} x_1 + 2a_1 - b_1 & x_1 - a_1 + 2b_1 & x_1 - a_1 - b_1 \\ \vdots & \vdots & \vdots \\ x_l + 2a_l - b_l & x_l - a_l + 2b_l & x_l - a_l - b_l \end{bmatrix}$$

$$= (x + 2a - b | x - a + 2b | x - a - b).$$

Remark 2.2.2. The MP view of Turyn's construction in the previous example gives a hint for viewing any GCC as an MP code. This problem and related consequences on MP codes will be the subject of a future study.

Chapter 3

On the Schur Product of Some Matrix-Product Codes

We present the work of Cascudo et al. [2] in this section. Namely, the Schur product of two special MP codes will be presented. The main aim is to represent the Schur product as an MP code again. In the last section, we present the Schur square of an MP code, which is not addressed in [2].

3.1 $(u|u+v)$ Codes

Let U and V be linear codes in $\mathbb{F}_q^n$. The $(u|u+v)$ construction produces a longer code out of U and V as follows:

$$\{(u|u+v); u \in U, v \in V\}. \tag{3.1.1}$$

Note that this is a linear code over $\mathbb{F}_q$ of length $2n$. If we let

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \tag{3.1.2}$$

be the defining matrix, then it is clear that the code (3.1.1) can be represented as an MP code (up to equivalence):

$$[U, V]A.$$

Theorem 3.1.1. *([2]) Let $C_1, C_2, C_1', C_2' \subseteq \mathbb{F}_q^n$ be linear codes and let A be the* *matrix in (3.1.2). For $C = [C_1, C_2]A$ and $C' = [C_1', C_2']A$, we have*

$$C \star C' = [C_1 \star C_1', C_1 \star C_2' + C_2 \star C_1' + C_2 \star C_2']A.$$

Proof. By Proposition 1.3.2, we know that

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix},$$

$$G' = \begin{bmatrix} G_1' & G_1' \\ 0 & G_2' \end{bmatrix}.$$

are generator matrices for C and C' respectively, where G_1, G_2, G_1', G_2' as generator matrices for C_1, C_2, C_1', C_2' respectively. Also, if we take the componentwise products of all the rows in G with all the rows in G', we have $G \star G'$ as

$$G \star G' = \begin{bmatrix} G_1 \star G_1' & G_1 \star G_1' \\ 0 & G_1 \star G_2' \\ 0 & G_2 \star G_1' \\ 0 & G_2 \star G_2' \end{bmatrix}.$$

After that, if we remove all linearly dependent rows, we obtain a generator matrix for $C \star C'$ by Proposition 1.3.2, in this form

$$\bar{G} = \begin{bmatrix} \bar{G_1} & \bar{G_1} \\ 0 & \bar{G_2} \end{bmatrix}.$$

Here, $\bar{G_1}$ is a generator matrix for $C_1 \star C_1'$ and $\bar{G_2}$ is a generator matrix for $C_1 \star C_2' + C_2 \star C_1' + C_2 \star C_2'$. By Proposition 1.3.2, we have that $\bar{G}$ is a generator matrix for the code $[C_1 \star C_1', C_1 \star C_2' + C_2 \star C_1' + C_2 \star C_2']A$. □

Corollary 3.1.2. *([2]) Let $C_1, C_2 \subseteq \mathbb{F}_q^n$ be linear codes and let A be a matrix as in the above assumption and denote by $C = [C_1, C_2]A$. Then*

$$C^{\star 2} = [C_1^{\star 2}, (C_1 + C_2) \star C_2]A,$$

and we have that

$$d(C^{\star 2}) \geq \min\{2d(C_1^{\star 2}), d((C_1 + C_2) \star C_2)\}.$$

Additionally, if $C_2 \subseteq C_1$ *we obtain*

$$C^{\star 2} = [C_1^{\star 2}, C_1 \star C_2]A.$$

Proof. In Theorem 3.1.1, if we take $C_1' = C_1$ and $C_2' = C_2$ we have that $C' = C$. Then

$$C^{\star 2} = [C_1 \star C_1, C_1 \star C_2 + C_2 \star C_1 + C_2 \star C_2]A = [C_1^{\star 2}, (C_1 + C_2) \star C_2]A.$$

Then, we can obtain the minimum distance bound for $C^{\star 2}$ by Proposition 1.3.4. Also, assume $C_2 \subseteq C_1$. Then $C_1 + C_2 = C_1$. □

3.2 Vandermonde Matrix

We describe the Schur square of an MP code which is defined by the Vandermonde matrix.

Theorem 3.2.1. *([2]) Let* $C_0, C_1, ..., C_{s-1} \subseteq \mathbb{F}_q^n$ *be linear codes. Consider the Vandermonde matrix defined as*

$$V = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_{q-1}^1 \\ \vdots & \vdots & \vdots & \\ \alpha_1^{s-1} & \alpha_2^{s-1} & \cdots & \alpha_{q-1}^{s-1} \end{bmatrix},$$

where $\alpha_1, ..., \alpha_{q-1}$ *are the nonzero elements of* $\mathbb{F}_q$. *Let* $C = [C_0, C_1, ..., C_{s-1}]V$. *Then,*

$$C^{\star 2} = [\sum_{i+j=0} C_i \star C_j, \sum_{i+j=1} C_i \star C_j, ..., \sum_{i+j=\tilde{s}-1} C_i \star C_j]\tilde{V},$$

where $\tilde{V}$ *depends on* $\tilde{s}$ *which is the minimum of* $2s - 1$ *and* $q - 1$ *also the sums* $i + j$ *modulo* $q - 1$.

Proof. If $C = [C_0, C_1, ..., C_{s-1}]V$, then generator matrix for C is

$$G = \begin{bmatrix} G_0 & G_0 & \cdots & G_0 \\ \alpha_1^1 G_1 & \alpha_2^1 G_1 & \cdots & \alpha_{q-1}^1 G_1 \\ \vdots & \vdots & \vdots & \\ \alpha_1^{s-1} G_{s-1} & \alpha_2^{s-1} G_{s-1} & \cdots & \alpha_{q-1}^{s-1} G_{s-1} \end{bmatrix},$$

where $G_0, G_1, ...G_{s-1}$ are generator matrices for $C_0, C_1, ..., C_{s-1}$, respectively by Proposition 1.3.3. Then,

$$G \star G = \begin{bmatrix} G_0 \star G_0 & G_0 \star G_0 & \cdots & G_0 \star G_0 \\ \alpha_1^1 G_0 \star G_1 & \alpha_2^1 G_0 \star G_1 & \cdots & \alpha_{q-1}^1 G_0 \star G_1 \\ \vdots & \vdots & \vdots & \\ \alpha_1^{s-1} G_0 \star G_{s-1} & \alpha_2^{s-1} G_0 \star G_{s-1} & \cdots & \alpha_{q-1}^{s-1} G_0 \star G_{s-1} \\ \alpha_1^1 G_1 \star G_0 & \alpha_2^1 G_1 \star G_0 & \cdots & \alpha_{q-1}^1 G_1 \star G_0 \\ \alpha_1^1 \alpha_1^1 G_1 \star G_1 & \alpha_2^1 \alpha_2^1 G_1 \star G_1 & \cdots & \alpha_{q-1}^1 \alpha_{q-1}^1 G_1 \star G_1 \\ \vdots & \vdots & \vdots & \\ \alpha_1^1 \alpha_1^{s-1} G_1 \star G_{s-1} & \alpha_2^1 \alpha_2^{s-1} G_1 \star G_{s-1} & \cdots & \alpha_{q-1}^1 \alpha_{q-1}^{s-1} G_1 \star G_{s-1} \\ \vdots & \vdots & \vdots & \\ \alpha_1^{s-1} G_{s-1} \star G_0 & \alpha_2^{s-1} G_{s-1} \star G_0 & \cdots & \alpha_{q-1}^{s-1} G_{s-1} \star G_0 \\ \alpha_1^{s-1} \alpha_1^1 G_{s-1} \star G_1 & \alpha_2^{s-1} \alpha_2^1 G_{s-1} \star G_1 & \cdots & \alpha_{q-1}^{s-1} \alpha_{q-1}^1 G_{s-1} \star G_1 \\ \vdots & \vdots & \vdots & \\ \alpha_1^{s-1} \alpha_1^{s-1} G_{s-1} \star G_{s-1} & \alpha_2^{s-1} \alpha_2^{s-1} G_{s-1} \star G_{s-1} & \cdots & \alpha_{q-1}^{s-1} \alpha_{q-1}^{s-1} G_{s-1} \star G_{s-1} \end{bmatrix}.$$

After removing linearly dependent rows of $G^{\star 2}$, we have $(G_0 \star G_0, G_0 \star G_0, ...G_0 \star G_0)$ as the first row of $G \star G$, $(\alpha_1^1 G_0 \star G_1, \alpha_2^1 G_0 \star G_1, ..., \alpha_{q-1}^1 G_0 \star G_1)$ as the second row of $G \star G$, $(\alpha_1^2(G_0 \star G_2 + G_1 \star G_1), \alpha_2^2(G_0 \star G_2 + G_1 \star G_1), ..., \alpha_{q-1}^1(G_0 \star G_2 + G_1 \star G_1)$ as the third row of $G \star G$. We continue this until power of α_i's reach $2s-2$ where $i = 1, ..., q-1$. Then, we obtain

$$C^{\star 2} = [\sum_{i+j=0} C_i \star C_j, \sum_{i+j=1} C_i \star C_j, ..., \sum_{i+j=\tilde{s}-1} C_i \star C_j]\tilde{V}.$$

□

3.3 $(a+x|b+x|a+b+x)$ Codes

In this section, we consider $(a+x|b+x|a+b+x)$-construction as described in [4]. Note that this code looks similar to the binary Turyn's construction in Example 2.2.1 but they are not identical to each other.

Let C_1 and C_2 be linear codes in $\mathbb{F}_q^n$. The $(a+x|b+x|a+b+x)$ construction is defined as follows:

$$\{(a+x|b+x|a+b+x); a \in C_1, b \in C_1, x \in C_2\}. \tag{3.3.1}$$

If we let

$$A = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \tag{3.3.2}$$

be the defining matrix, then it is clear that the code (3.3.1) can be represented as follows as an MP code (up to equivalence):

$$C = [C_1, C_1, C_2]A.$$

Theorem 3.3.1. *Let $C_1, C_2 \subseteq \mathbb{F}_q^n$ be linear codes, let A be the matrix in (3.3.2) and $C = [C_1, C_1, C_2]A$. Then*

$$C^{\star 2} = [C_1 \star (C_1 + C_2), C_1 \star (C_1 + C_2), C_2^{\star 2}, C_1^{\star 2}]B.$$

where B is defined as

$$B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Proof. Let G_1, G_2 be generator matrices for C_1, C_2 respectively. By Proposition 1.3.2, we have that

$$G = \begin{bmatrix} G_1 & 0 & G_1 \\ 0 & G_1 & G_1 \\ G_2 & G_2 & G_2 \end{bmatrix}$$

is a generator matrix for C. Now, if we take the componentwise products of all the rows in G with all the rows in G, we have $G \star G$ as

$$G \star G = \begin{bmatrix} G_1^{\star 2} & 0 & G_1^{\star 2} \\ 0 & 0 & G_1^{\star 2} \\ G_1 \star G_2 & 0 & G_1 \star G_2 \\ 0 & 0 & G_1^{\star 2} \\ 0 & G_1^{\star 2} & G_1^{\star 2} \\ 0 & G_1 \star G_2 & G_1 \star G_2 \\ G_2 \star G_1 & 0 & G_2 \star G_1 \\ 0 & G_2 \star G_1 & G_2 \star G_1 \\ G_2^{\star 2} & G_2^{\star 2} & G_2^{\star 2} \end{bmatrix}.$$

After that, if we remove all linearly dependent rows, the following matrix generates $C \star C$,

$$G \star G = \begin{bmatrix} G_1^{\star 2} & 0 & G_1^{\star 2} \\ 0 & 0 & G_1^{\star 2} \\ G_1 \star G_2 & 0 & G_1 \star G_2 \\ 0 & G_1^{\star 2} & G_1^{\star 2} \\ 0 & G_1 \star G_2 & G_1 \star G_2 \\ G_2^{\star 2} & G_2^{\star 2} & G_2^{\star 2} \end{bmatrix}.$$

Since we have linearly independent rows, we can combine the similar rows. Since the rows $(G_1^{\star 2}, 0, G_1^{\star 2})$ and $(G_1 \star G_2, 0, G_1 \star G_2)$ are similar, by combining them, we have obtained the row $(G_1 \star (G_1 + G_2), 0, G_1 \star (G_1 + G_2))$. Also, we applied the same argumnet for the fourth and fifth rows. The rows second and sixth remain the same. Hence, we have

$$= \begin{bmatrix} G_1 \star (G_1 + G_2) & 0 & G_1 \star (G_1 + G_2) \\ 0 & G_1 \star (G_1 + G_2) & G_1 \star (G_1 + G_2) \\ G_2^{\star 2} & G_2^{\star 2} & G_2^{\star 2} \\ 0 & 0 & G_1^{\star 2} \end{bmatrix}.$$

Then,

$$C^{\star 2} = [C_1 \star (C_1 + C_2), C_1 \star (C_1 + C_2), C_2^{\star 2}, C_1^{\star 2}]B.$$

□

Bibliography

[1] Tim Blackmore, Graham H. Norton, “Matrix-product codes over $\mathbb{F}_q$”, *Applicable Algebra in Engineering, Communication and Computing*, vol. 12, 477-500, 2001.

[2] Ignacio Cascudo, Jaron Skovsted Gundersen, Diego Ruano, “Squares of matrix-product codes”, *Finite Fields and Their Applications*, vol. 62, 101606, 21 pp., 2020.

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

[4] Marc P. C. Fossorier, Shu Lin, “Some decomposable codes: The $|a+x|b+x|a+b+x|$ construction”, *IEEE Trans. Inform. Theory*, vol. 43, no.5, 1997.

[5] Cem Güneri, Ferruh Özbudak, “The concatenated structure of quasi-cyclic codes and an improvement of Jensen’s bound”, *IEEE Trans. Inform. Theory*, vol. 59, no.2, 2013.

[6] Fernando Hernando, Kristine Lally, “Construction and decoding of matrix-product codes from nested codes”, *Applicable Algebra in Engineering, Communication and Computing*, vol. 20, 497-507, 2009.

[7] San Ling, Patrick Solé, “On the algebraic structure of quasi-cyclic codes I: Finite Fields”, *IEEE Trans. Inform. Theory*, vol. 47, no.7, 2001.

[8] R. McEliece, “A public-key cryptosystem based on algebraic coding theory”, *DSN Progress Report*, vol. 42, Pages: 114-116, 1978.

[9] Ferruh Özbudak, Henning Stichtenoth, “Note on Niederreiter-Xing’s propagation rule for linear codes”, *Applicable Algebra in Engineering, Communication and Computing*, vol. 13, 53-56, 2002.

[10] Hugues Randriambololona, "An upper bound of singleton type for componentwise products of linear codes". arXiv:1305.4840v3, 2013.

[11] Elif Saçıkara, "Concatenated structure and construction of certain code families", PhD thesis, Sabancı University, Istanbul, 2018.

[12] Violetta Weger, "A code-based cryptosystem using GRS codes", Master thesis, University of Zurich, 2016.