Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas - Programa de Magister en Matemática

Construcciones de Códigos Cíclicos de Tipo Generalizado
(Constructions of Cyclic Codes of Generalized Type)

LUIS FELIPE TAPIA CUITIÑO
CONCEPCIÓN-CHILE
2013

Profesor Guía: Andrea Luigi Tironi
Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Contents

Introducción

La teoría de códigos, desarrollada a partir de los años 50, siendo uno de sus fundadores Richard Hamming quien propuso el Código Hamming (ver [16], § 5.3.1), trata de resolver el problema de cómo poder transmitir información de manera **segura y fiable**, a través de un canal que sea **poco seguro y poco fiable**. Un canal es **poco seguro** si terceras personas, distintas al emisor o de aquella a quien el mensaje estaba dirigido, pueden enterarse de lo que dice un mensaje, o bien alterarlo. Por otro lado, un canal es **poco fiable** si en el canal hay *ruido*, es decir que el mensaje puede llegar alterado a su destino.

La Criptografía sirve para mejorar la seguridad y los Códigos detectores y correctores sirven para mejorar la fiabilidad. Nuestro estudio se centrará en estos últimos tipos de códigos.

En particular, la transmisión de un mensaje puede ser representada por el siguiente esquema:

$$\begin{array}{ccccccc}
 & & & \text{ruido } (=r) & & & \\
 & & & \downarrow & & & \\
\text{EMISOR} & \rightarrow & \text{CODIFICADOR} & \Rightarrow & \text{DESCODIFICADOR} & \rightarrow & \text{RECEPTOR} \\
m & \rightarrow & u & \rightarrow & v{=}u{+}r & \rightarrow & m
\end{array}$$

En base a este proceso, antes de enviar un mensaje m, el emisor lo codifica como u. Esto se hace añadiendo a m informaciones redundantes, de manera que si en el canal de transmisión se produce un ruido r y se recibe un mensaje alterado v, el receptor sea capaz de recuperar el mensaje enviado u y decodificarlo en el mensaje original m.

Un ejemplo sencillo de codificación es el siguiente: 0 representa un **no** y 1 representa un **si**. En este caso, si se quiere transmitir un 1 y se recibe un 0 en vez de 1, el receptor del mensaje no sabrá que hubo un error. Pero si en cambio se conviene que 00 sea **no** y 11 sea **si**, entonces si por ejemplo se recibe un 01, el receptor detectará que hubo un error, aunque no sabrá cual es el mensaje enviado. Estas dos situaciones pueden ser mejoradas sencillamente. Si la convención es que 000 es **no** y 111 es un **si**, y se supiese que al transmitir un mensaje solo es posible cometer a lo más un error de dígito, entonces al recibir un 001, el receptor sabrá que se trata de un **no**, detectando y corrigiendo el error.

En esta tesis, nos enfocaremos en la construcción de algunos tipos de códigos que permitan una buena codificación y decodificación de mensajes y una eficaz detección y corrección de eventuales errores. En literatura se define un alfabeto como un conjunto finito de símbolos, una palabra como una sucesión finita de estos símbolos y un código como un conjunto de palabras. Para nosotros el alfabeto será un campo finito $\mathbb{F}_q$ con q elementos, una palabra será un vector del espacio vectorial

$$\mathbb{F}_q^n = \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{n-\text{veces}}$$

y un código $\mathscr{C} \subseteq \mathbb{F}_q^n$ será un subespacio vectorial de $\mathbb{F}_q^n$, es decir $\mathscr{C}$ es tal que $a\vec{x} + b\vec{y} \in \mathscr{C}$ para todo $a, b \in \mathbb{F}_q$ y para todo $\vec{x}, \vec{y} \in \mathscr{C}$. Tales códigos serán llamados *Códigos lineales* (ver Ch. 1, Definition 1.1.1). A partir de los años 60, se comenzó a estudiar de forma sistemática un tipo de códigos lineales llamados *Códigos Cíclicos* (ver Ch. 2, Definition 2.1.1) que gozan de la propiedad de ser invariantes por la matriz de permutación

$$P := \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline 1 & 0 & \dots & 0 \end{array}\right).$$

Mediante un isomorfismo de espacios vectoriales

$$\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[X]/(X^n - 1),$$

descrito en la §2.1 del Capítulo 2, podemos identificar un código cíclico $\mathscr{C} \subseteq \mathbb{F}_q^n$ con un ideal $I \subseteq \mathbb{F}_q[X]/(X^n - 1)$ y viceversa, para aprovechar todas las propiedades de los ideales y del anillo cociente que permiten un mejor manejo de los códigos desde un punto de vista computacional. Ya en los años 70 se comenzó a generalizar estos códigos y se llegó a un tipo de código lineal llamado

λ-*constacyclic code* (ver [21], Definition 2), invariante por la siguiente matriz

$$\overline{P} := \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline \lambda & 0 & \dots & 0 \end{array}\right),$$

donde $\lambda \in \mathbb{F}_q$. En este caso el isomorfismo π se convierte en el siguiente

$$\pi_\lambda : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[X]/(X^n - \lambda),$$

otra vez con la propiedad que cada código lineal invariante por $\overline{P}$ se corresponde a un ideal $I' \subseteq \mathbb{F}_q[X]/(X^n - \lambda)$ y viceversa. En los años posteriores surgieron más generalizaciones de los códigos cíclicos en un contexto conmutativo, como por ejemplo los *Quasi Cyclic Codes* (ver [15], § III) que son códigos invariantes por la matriz $(P)^s$ para algún $s \in \mathbb{N}$, y los *Quasi-Twisted Cyclic Codes* (ver [1], Definnition 1.1) que son códigos invariantes por la matriz $(\overline{P})^r$ para algún $r \in \mathbb{N}$. Luego de estos, en un contexto no conmutativo, aparecieron otras generalizaciones, como por ejemplo los *Skew Cyclic Codes* (ver [7], Definition 1) que son códigos invariantes por las composición de una potencia de un automorfismo de Frobenius (ver Ch. 4, §4.1) con la matriz P, y los *Skew Quasi Cyclic Codes* (ver [2], Definition 3) que son invariantes por las composición de una potencia de un automorfismo de Frobenius con la matriz $(P)^s$ para algún $s \in \mathbb{N}$. Cabe mencionar que todos los códigos anteriores heredan de forma natural la gran mayoría de las ventajas y propiedades de los códigos cíclicos.

En este trabajo, generalizaremos los códigos cíclicos en ambos contextos, conmutativo y no conmutativo. La primera generalización, descrita en el Capítulo 3, será dada por códigos lineales invariantes por una matriz

$$A := \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline f_0 & f_1 & \cdots & f_{n-1} \end{array}\right),$$

donde $f_i \in \mathbb{F}_q$ y $f_0 \neq 0$. Al igual que en los códigos cíclicos, en este caso podemos establecer un isomorfismo de espacios vectoriales

$$\pi_f : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[X]/(f)$$

donde f es el polinomio $X^n - f_{n-1}X^{n-1} - \ldots - f_1X + f_0$. Esto nos permitirá identificar un ideal $I \subseteq \mathbb{F}_q[X]/(f)$ con un código invariante por A y viceversa (ver Ch. 3, Proposition 3.2.7). A estos tipos de códigos les llamaremos *A-Generalized Cyclic Codes*. Notar que el cociente lo hacemos por cualquier polinomio, por lo que el anillo cociente resulta ser el más general posible respecto a los *λ-constacyclic codes*. Por otro lado, este tipo de código es invariante por una matriz A de forma particular. De aquí nace la siguiente pregunta:

Dada una matriz M con $\det M \neq 0$, ¿Cuáles son los códigos lineales $\mathscr{C}_M$ invariantes por M?

Una respuesta se puede encontrar en la forma racional canónica de una matriz (ver Ch. 3, §3.1). Toda matriz M con $\det M \neq 0$ es similar a una matriz R de tipo especial, es decir existe una matriz invertible S tal que $M = SRS^{-1}$, con R una matriz a bloques y cada bloque tiene una forma semejante a la de la matriz A descrita anteriormente. Gracias a esta propiedad se obtiene una correspondencia uno a uno entre códigos $\mathscr{C}_M$ invariantes por M y códigos $\mathscr{C}_R$ invariantes por R (ver Ch. 3, §3.2). Para construir códigos $\mathscr{C}_M$ será entonces suficiente construir códigos $\mathscr{C}_R$. Además se mostrará que cada $\mathscr{C}_R$ es isomorfo como espacio vectorial a un producto $\mathscr{C}_1 \times \cdots \times \mathscr{C}_s$, donde cada $\mathscr{C}_i$ es un A_i-Generalized Cyclic Code para alguna matriz A_i (ver Ch. 4, Theorem 4.1.10). De aquí nace la definición de *Product M-codes*. Estos tipos de códigos generalizan a los A-Generalized Cyclic Codes, a los Quasi Cyclic Codes y a los Quasi-Twisted Cyclic Codes. Finalmente, en el caso no conmutativo, se definen y estudian los *Product T-Codes* (ver Ch. 4, Definition 4.2.2), los cuales son códigos lineales invariantes por cualquier transformación semilineal T (ver Ch. 4, §4.1). Bajo una biyección parecida a la anterior, nos enfocaremos en productos de códigos invariantes por una particular transformación semilineal (ver Ch. 4, Hypothesis $(*)$) como primeros ejemplos no triviales de códigos invariantes bajo la acción de una transformación semilineal de tipo general.

En el **Capítulo 1**, basado en [16], se definirá el concepto de *Linear Codes* (Definition 1.6.3) y se estudiarán algunas de sus propiedades: el código dual (ver §1.1), la distancia Hamming y el peso Hamming (ver §1.2), una matriz generadora y una parity-check matrix (ver §1.4). Además, en la §1.5 se introducirá la codificación clásica con un código lineal y en la §1.6 dos tipos de decodificación: la “Nearest neighbour decoding” y la “Syndrome decoding”.

En el **Capítulo 2**, tambien basado en [16], estudiaremos los *Cyclic Codes* (ver §2.1). En los preliminares de este capítulo se definirá un isomorfismo (ver §2.1) que permite conectar la estructura gométrica de estos códigos con una estructura algebraica y hacer uso de ambas. Además, se definirá el polinomio generador asociado a un código cíclico (ver §2.2) que resultará ser una herramienta importante en el contexto de estos tipos de códigos. El polinomio anterior describe completamente un código cíclico, su dimensión, matriz generadora, etc. Por último, en la §2.4 se mostrarán tres nuevas formas de codificar que resultarán ser más eficaces que la de un código lineal, y un tipo de decodificación, detección y corrección de errores, llamado *Meggitt Decoding* (ver [12], Ch. 4, §4.6).

En el **Capítulo 3**, se estudiará un nuevo tipo de código lineal, llamado *Generalized Cyclic Code* (ver §3.2) que resulta ser una generalización de los *Cyclic Codes.* En §3.2 y en §3.3 se observará que muchas de las propiedades de los códigos cíclicos se heredan naturalmente (3.2.7, 3.2.10, 3.3.1, 3.3.3). Sin embargo el dual de un *Generalized Cyclic Code* no resulta ser uno de estos códigos (3.2.4). Además, en la §3.4 se analizarán estos códigos como subespacios invariantes bajo la acción de una *companion matrix* (ver Definition 3.1.4), entregando otro método para encontrar propiedades algebraicas de estos códigos (3.4.8), una matriz generadora (3.4.9) y una parity-check matrix (3.4.10), todo esto inspirado en el trabajo [21]. En la §3.5, definiremos un algoritmo para construir estos tipos de códigos a travez de los espacios proyectivos. En la §3.6 mostraremos una aplicación inyectiva (3.6.1, 3.6.2) que nos permitirá estudiar nuevos tipos de códigos duales, los *Quasi-Euclidean dual codes* (3.7.3, 3.7.7) y los *Hermitian dual codes* (3.8.1, 3.8.3, 3.8.4, 3.8.8). Finalizaremos este capítulo con una generalización de tipo *Meggitt decoding* como en la §2.4.2 del Capítulo 2.

Para concluir, en el **Capítulo 4** introduciremos la noción de *Product Semi-Linear T-codes* (ver §4.2), una generalización de los *Generalized Cyclic Codes* en el contexto no conmutativo, de los *Skew Cyclic Codes*, *Module Skew Codes* y *Skew Quasi Cyclic Codes*, y un caso especial de códigos lineales invariantes bajo una transformación semilineal (4.1.1, 4.1.5, 4.2.5), todo esto inspirado en los recientes trabajos [4], [5] y [6]. Cabe mencionar que estos códigos se definen en un anillo no conmutativo de polinomios, llamado *skew polynomial ring* (ver §4.1). En fín, se revisarán propiedades asociadas a estos códigos (4.1.6, 4.1.11, 4.1.12, 4.2.8), se estudiarán tres tipos de códigos duales, como los *Euclidean duals* (4.3.3), los *Quasi-Euclidean duals* (4.3.11, 4.3.22, 4.3.28, 4.3.37, 4.3.38) y los *Hermitian duals* (4.3.35, 4.3.36), y en las §§4.4, 4.5 se entregarán métodos de codificación y decodificación y una generalización natural de la construcción de códigos dada en la §3.6 del Capítulo 3.

Chapter 1

Linear Codes

In this first chapter, we give some basic definitions and notation in coding theory, we introduce a kind of classical codes, the so-called linear codes, and we discuss some of their elementary properties, as the dual code, the weight and the Hamming distance, the concept of a generator matrix and of a parity-check matrix of a linear code. Finally, we introduce a classical encoding algorithm with a linear code and two types of decoding methods.

1.1 Linear Codes

Let us give the background material and some basic definitions about linear codes.

Definition 1.1.1. *A* ***linear code*** $\mathscr{C}$ *over* $\mathbb{F}_q$ *is a vector subspace of* $\mathbb{F}_q^n$.

Definition 1.1.2. *Let* $\mathscr{C} \subseteq \mathbb{F}_q^n$ *be a linear code.*

(i) The ***dual code*** $\mathscr{C}^\perp$ *of* $\mathscr{C}$ *is the orthogonal complement of the* $\mathscr{C}$ *in* $\mathbb{F}_q^n$.

(ii) The ***dimension*** $\dim(\mathscr{C})$ *of* $\mathscr{C}$ *is the dimension of* $\mathscr{C}$ *as a vector space over* $\mathbb{F}_q$, *i.e.* $dim(\mathscr{C}) := \dim_{\mathbb{F}_q} \mathscr{C}$.

The following is a known result in linear algebra.

Theorem 1.1.3 ([16],Theorem 4.2.4)**.** *Let* $\mathscr{C} \subseteq \mathbb{F}_q^n$ *be a linear code. Then,* (*i*) $|\mathscr{C}| = q^{dim(\mathscr{C})}$, *i.e.* $dim(\mathscr{C}) = \log_q |\mathscr{C}|$, *where* $|\mathscr{C}|$ *is the cardinality of* $\mathscr{C} \subseteq \mathbb{F}_q^n$;

(*ii*) $\mathscr{C}^\perp$ *is a linear code and* $dim(\mathscr{C}) + dim(\mathscr{C}^\perp) = n$;

(*iii*) $(\mathscr{C}^\perp)^\perp = \mathscr{C}$.

Definition 1.1.4. *Let* $\mathscr{C} \subseteq \mathbb{F}_q^n$ *be a linear code.*

(*i*) $\mathscr{C}$ *is* ***self-orthogonal*** *if* $\mathscr{C} \subseteq \mathscr{C}^\perp$.

(*ii*) $\mathscr{C}$ *is* ***self-dual*** *if* $\mathscr{C} = \mathscr{C}^\perp$.

Proposition 1.1.5. *Let* $\mathscr{C} \subseteq \mathbb{F}_q^n$ *be a linear code.*

(*a*) *If* $\mathscr{C}$ *is a self-orthogonal code, then* $\dim \mathscr{C} \leq \frac{n}{2}$;

(*b*) *If* $\mathscr{C}$ *is a self-dual code, then* $\dim \mathscr{C} = \frac{n}{2}$.

Proof. The statement are consequence of Theorem 1.1.3 (*ii*) and Definitions 1.1.4. □

Example 1.1.6. (*a*) *Consider* $\mathscr{C} = \{(0,0,0,0),(1,0,1,0),(0,1,0,1),(1,1,1,1)\} \subset \mathbb{F}_2^4$, *then by* Theorem 1.1.3 (*i*) and (*ii*), *we have* $dim(\mathscr{C}) = \log_2 |\mathscr{C}| = \log_2 4 = 2$ *and* $dim(\mathscr{C}^\perp) = 2$. *It is easy to see that* $\mathscr{C}^\perp = \{(0,0,0,0),(1,0,1,0),(0,1,0,1),(1,1,1,1)\} = \mathscr{C}$. *Note that in this case* $\mathscr{C}$ *is self-dual code.*

(*b*) *Consider the linear code*

$$\mathscr{C} = \{(0,0,0),(0,0,1),(0,0,2),(0,1,0),(0,2,0),(0,1,1),(0,1,2),(0,2,1),(0,2,2)\} \subset \mathbb{F}_3^3.$$

Then by Theorem 1.1.3 (*i*) and (*ii*), *we have* $dim(\mathscr{C}) = \log_3 |\mathscr{C}| = \log_3 9 = 2$ *and* $dim(\mathscr{C}^\perp) = 1$. *Moreover one checks readily that* $\mathscr{C}^\perp = \{(0,0,0),(1,0,0),(2,0,0)\}$.

1.2 Hamming distance and Hamming weight

In this section we give the definitions of Hamming distance and Hamming weight.

Definition 1.2.1. *If $\vec{x}, \vec{y} \in \mathbb{F}_q^n$, then the **distance** $d(\vec{x}, \vec{y})$ of $\vec{x}$ and $\vec{y}$ is defined by*

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

*The **weight** $w(\vec{x})$ of $\vec{x} \in \mathbb{F}_q^n$ is defined by*

$$w(\vec{x}) := d(\vec{x}, \vec{0})$$

*where $\vec{0} := (0, \ldots, 0) \in \mathbb{F}_q^n$. This distance is called **Hamming distance** and is indeed a metric on $\mathbb{F}_q^n$.*

Remark 1.2.2. *For every $c \in \mathbb{F}_q$, define the Hamming weight as follows:*

$$w_h(c) := \begin{cases} 1 & si\ c \neq 0 \\ 0 & si\ c = 0. \end{cases}$$

Then, by writing $\vec{x} \in \mathbb{F}_q^n$ as $\vec{x} = (x_1, \ldots, x_n)$, the Hamming weight of $\vec{x}$ can be also defined as

$$w(\vec{x}) := w_h(x_1) + \ldots + w_h(x_n)$$

Then by [[16], Lemma 4.3.3] for every $\vec{x}, \vec{y} \in \mathbb{F}_q^n$, we have $d(\vec{x}, \vec{y}) = w(\vec{x} - \vec{y}) = w(\vec{y} - \vec{x})$. In particular if $q = 2$ then we get $d(\vec{x}, \vec{y}) = w(\vec{x} + \vec{y})$ for every $\vec{x} \in \mathbb{F}_q^n$.

Definition 1.2.3. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code such that $\mathscr{C} \neq \{\vec{0}\}$. The **minimum distance** of $\mathscr{C}$ is defined as*

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

*and, equivalently, the **minimum weight** of $\mathscr{C}$ can be defined as*

$$w(\mathscr{C}) := min\{w(\vec{x}) : \vec{x} \in \mathscr{C},\ \vec{x} \neq \vec{0}\}.$$

Theorem 1.2.4 ([16], Theorem 4.3.8)**.** *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. Then $d(\mathscr{C}) = w(\mathscr{C})$.*

Example 1.2.5. *Consider the linear code $\mathscr{C} = \{(0,0,0,0), (1,0,0,0), (0,1,0,0), (1,1,0,0)\} \subset \mathbb{F}_2^4$. By* Definition 1.2.1 *we see that $w((1,0,0,0)) = 1,\ w((0,1,0,0)) = 1,\ w((1,1,0,0)) = 2$. Hence, by* Theorem 1.2.4 *we easily obtain that $d(\mathscr{C}) = w(\mathscr{C}) = 1$*

1.3 Bases for linear codes

Since a linear code is a vector space, all its elements can be described in terms of a basis. In this section, we discuss three algorithms that yield either a basis for a given linear code or its dual. We first recall some facts from linear algebra. (see [16], Ch 4, §4).

Definition 1.3.1. *Let A be a matrix over $\mathbb{F}_q$. An* ***elementary row operation*** *performed on A is any one of the following three operations:*

(i) interchanging two rows (columns);

(ii) multiplying a row (column) by a non-zero scalar;

(iii) replacing a row (column) by its sum with the scalar multiple of another row (column).

Definition 1.3.2. *Two matrices are* ***row (column) equivalent*** *if one can be obtained from the other by a sequence of elementary row (column) operations.*

We are now ready to describe the two useful algorithms in coding theory.

Algorithm 1.3.3. *Input: A non-empty subset S of $\mathbb{F}_q^n$.*
Output: A basis for the linear code $\mathscr{C} = \langle S \rangle$ generated by S.
Description: Form the matrix A whose rows are the vectors of S. By using elementary row operations, find a row echelon form (REF) A' of A. Then the non-zero rows of A' form a basis for $\mathscr{C}$.

Example 1.3.4. *Let $S = \{(1,2,1,0,1),(2,0,1,1,0),(0,1,1,2,2),(1,1,0,1,0)\}$ a subset of $\mathbb{F}_3^5$ and write*

$$A = \begin{pmatrix} 1 & 2 & 1 & 0 & 1 \\ 2 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

by elementary row operations we obtain

$$A \to \begin{pmatrix} 1 & 2 & 1 & 0 & 1 \\ 0 & 2 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 & 2 \\ 0 & 2 & 2 & 1 & 2 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 0 & 1 \\ 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} := A'.$$

By Algorithm 1.3.3*,* $\{(1,2,1,0,1),(0,1,1,2,2),(0,0,0,0,1)\}$ *is a basis for* $\mathscr{C} = \langle S \rangle$*.*

Remark 1.3.5. *There exists an other algorithm similar to Algorithm 1.3.3 which operates columns instead of rows (see* [16], Ch 4, §4*). We observe that in general the bases obtained by this algorithms are different.*

Algorithm 1.3.6. *Input: A nonempty subset S of $\mathbb{F}_q^n$.*
Output: A basis for the dual code $\mathscr{C}^{\perp}$, where $\mathscr{C} = \langle S \rangle$.
Description: Form the matrix A whose rows are the vectors of S. Use elementary row operations to put A in reduced row echelon form (RREF) A' and let G be the $k \times n$ submatrix of A' consisting of all the non-zero rows of A':

$$A \to \begin{pmatrix} G \\ O \end{pmatrix} := A',$$

where O denotes the zero matrix. The matrix G contains k leading columns. Permute the columns of G to form

$$G' = (X|I_k)\,,$$

where I_k denotes the $k \times k$ identity matrix. Then write the matrix H' as follows:

$$H' = (I_{n-k}| - X_t)\,,$$

where X_t denotes the transpose matrix of X. Apply the inverse of the permutation applied to the columns of G to the columns of H' to form the matrix H. Then the rows of H form a basis for $\mathscr{C}^{\perp}$.

Example 1.3.7. *Let S be a non-empty subset of $\mathbb{F}_3^{10}$ such that the matrix G of the* Algorithm 1.3.6

is as follows

$$G = \begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 2 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

Note that the leading columns of G are columns $1,\ 4,\ 5,\ 7$ and 9. We permute the columns of G into the order $2,\ 3,\ 6,\ 8,\ 10,\ 1,\ 4,\ 5,\ 7,\ 9$ to form the matrix

$$G' = (X|I_5) = \begin{pmatrix} 0 & 2 & 2 & 1 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Form the matrix

$$H' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 & 0 & 2 & 1 \end{pmatrix},$$

and finally rearrange its columns of H' by using the inverse permutation to obtain

$$H = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 1 & 1 \end{pmatrix}$$

By Algorithm 1.3.6*, the rows of H form a basis for $\mathscr{C}^{\perp}$.*

1.4 Generator matrix and parity-check matrix

Knowing a basis for a linear code enables us to describe all vectors explicitly. For this reason from now on we can consider two kind of matrices which will play an important role in coding theory.

Definition 1.4.1. (*i*) *A* ***generator matrix*** *G of a linear code $\mathscr{C}$ is a matrix whose rows form a basis for $\mathscr{C}$.*

(*ii*) *A* ***parity-check matrix*** *H of a linear code $\mathscr{C}$ is a generator matrix for the dual code $\mathscr{C}^{\perp}$.*

Remark 1.4.2. (*i*) *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. Then a generator matrix of $\mathscr{C}$ is a $k \times n$ matrix and its parity-check matrix of $\mathscr{C}$ is an $(n-k) \times n$ matrix.*

(*ii*) *In fact* Algorithm 1.3.6 *includes* Algorithm 1.3.3 *and that it can be used to find both generator and parity-check matrices for a linear code.*

(*iii*) *A generator matrix for a linear code not is unique, since in general the vector space admit many bases for the same linear code.*

Definition 1.4.3. (*i*) *A generator matrix of the form $(X|I_k)$ is said to be in* ***standard form****.*

(*ii*) *A parity-check matrix in the form $(I_{n-k}|Y)$ is said to be in* ***standard form****.*

Lemma 1.4.4 ([16], Lemma 4.5.4)**.** *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code of dimension k with generator matrix G. Then $\vec{x} \in \mathbb{F}_q^n$ belongs to $\mathscr{C}^{\perp}$ if and only if $\vec{x}$ is orthogonal to every row of G, i.e. $\vec{x} \in \mathscr{C}^{\perp} \Leftrightarrow \vec{x}G_t = \vec{0}$. In particular, given an $(n-k) \times n$ matrix H, then H is a parity-check matrix for $\mathscr{C}$ if and only if the rows of H are linearly independent and $HG_t = O$.*

Remark 1.4.5. *An equivalent but alternative formulation of the previous result can be obtained by substituting in* Lemma 1.4.4 *the generator matrix G with the parity-check matrix H and $\mathscr{C}$ with $\mathscr{C}^{\perp}$ (see* [16], Remark 4.5.5*).*

One of the main consequences of Lemma 1.4.4 is the following theorem wich relates the distance of a linear code $\mathscr{C}$ to some properties of its parity-check matrix.

Theorem 1.4.6. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. Denote by H be a parity-check matrix of $\mathscr{C}$. Then*

(*i*) *$d(\mathscr{C}) \geq d$ if and only if any $d-1$ columns of H are linearly independent;*

(*ii*) *$d(\mathscr{C}) \leq d$ if and only if H has d columns that are linearly dependent.*

Proof. Let $\vec{x} = (x_1, \dots, x_n) \in \mathscr{C}$ be a vector of weight $e > 0$. Suppose the non-zero coordinates are in the positions $i_1, \dots, i_e$, so that $\vec{x}_j = 0$ if $j \notin \{i_1, \dots, i_e\}$. Let $\underline{c}^i$ $(1 \leq i \leq n)$ be the ith column of H. By Lemma 1.4.4 (or its equivalent formulation in Remark 1.4.5), $\mathscr{C}$ contains a non-zero word $\vec{x} = (x_1, \dots, x_n)$ of weight e (whose non-zero coordinates are $x_{i_1}, \dots, x_{i_e}$) if and only if

$$\vec{0} = \vec{x}H_t = x_{i_1}\underline{c^{i_1}}_t + \cdots + x_{i_e}\underline{c^{i_e}}_t,$$

which is true if and only if there are e columns of H (namely, $\underline{c_{i_1}}, \dots, \underline{c_{i_e}}$) that are linearly dependent. To say that the distance $d(\mathscr{C})$ of $\mathscr{C}$ is $\geq d$ is equivalent to saying that $\mathscr{C}$ does not contain any non-zero word of weight $\leq d-1$, which is in turn equivalent to saying that any $\leq d-1$ columns of H are linearly independent. This proves (i). Similarly, to say that the $(\mathscr{C}) \leq d$ is equivalent to saying that $\mathscr{C}$ contains a non-zero word of weight $\leq d$, which is equivalent to saying that H has $\leq d$ columns linearly dependent (and hence d columns). This proves (ii). □

An immediate consequence of Theorem 1.4.6 is the following result.

Corollary 1.4.7. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. Denote by H be a parity-check matrix of $\mathscr{C}$. Then the following statements are equivalent:*

(*i*) *$d(\mathscr{C}) = d$*

(*ii*) *any $d-1$ columns of H are linearly independent and H has d columns that are linearly dependent.*

Example 1.4.8. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code with parity-check matrix*

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Observe that there are no zero columns and no two columns of H are linearly dependent, i.e. any two columns of H are linearly independent. However, columns 1, 3 *and* 4 *are linearly dependent. Hence, by* Corollary 1.4.7 *the distance of $\mathscr{C}$ is equal to* 3.

Theorem 1.4.9. *If $G = (X|I_k)$ is a generator matrix of a linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ of dimension k then a parity-check matrix for $\mathscr{C}$ is give by $H = (I_{n-k}| - X_t)$.*

Proof. Obviously, the equation $HG_t = O$ is satisfied. Moreover it is clear that the rows of H are linearly independent. Therefore, the conclusion follows from Lemma 1.4.4. □

Remark 1.4.10. Theorem 1.4.9 *show that* Algorithm 1.3.6 *actually gives what it claims to yield.*

1.5 Encoding with linear codes

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. Each vector of $\mathscr{C}$ can represent one piece of information, so $\mathscr{C}$ can represent exactly q^k distinct pieces of information. Once a basis $\{\vec{c}_1, \dots, \vec{c}_k\}$ is fixed for $\mathscr{C}$, any its vector can be uniquely written as a linear combination

$$\vec{x} = u_1\vec{c}_1 + \cdots + u_k\vec{c}_k,$$

where $u_1, \dots, u_k \in \mathbb{F}_q$. Equivalently, set G to be the generator matrix of $\mathscr{C}$ whose ith row is the vector c_i in the chosen basis. Given a vector $\vec{u} = (u_1, \dots, u_k) \in \mathbb{F}_q^k$, it is clear that

$$\vec{x} = \vec{u}G = u_1\vec{c}_1 + \cdots + u_k\vec{c}_k \in \mathscr{C}.$$

Conversely, any $\vec{x} \in \mathscr{C}$ can be written uniquely as $\vec{u}G$, for some $\vec{u} = (u_1, \dots, u_k) \in \mathbb{F}_q^k$. Hence, every vector $\vec{u} \in \mathbb{F}_q^k$ can be encoded as $\vec{x} = \vec{u}G$.

The encoding process with the linear code is nothing else that representing the elements $\vec{u} \in \mathbb{F}_q^k$ as vectors $\vec{x} = \vec{u}G \in \mathscr{C}$.

Example 1.5.1. *Let $\mathscr{C} \subset \mathbb{F}_2^5$ be a linear code with generator matrix*

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

Then the vector $\vec{u} = (1,0,1) \in \mathbb{F}_2^3$ can be encoded as

$$\vec{x} = \vec{u}G = (1,0,1)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix} = (1,0,0,1,1).$$

Remark 1.5.2. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code $\mathscr{C}$ of dimension k. If its generator matrix G is in standard form, $G = (X|I_k)$, then it is trivial to recover the original vector $\vec{u}$ from $\vec{u}G$, since*

$$\vec{x} = \vec{u}G = \vec{u}(X|I_k) = (\vec{u}X|\vec{u});$$

*i.e. the last k coordinates $\vec{x} = \vec{u}G$ give the vector $\vec{u}$. The remaining $n-k$ coordinates of $\vec{x} \in \mathscr{C}$ represent the **redundancy** which has been added to the vector $\vec{u}$ for protection against transmission error.*

1.6 Decoding with linear codes

A code is of practical use only if an efficient decoding scheme can be applied to it. In this section, we discuss a rather simple but elegant decoding algorithm for linear codes, called the "nearest neighbour decoding" as well as a modification of it, called "syndrome decoding", that improves its performance when the length of the code is large.

1.6.1 Cosets

We begin with the notion of a coset. Cosets play a crucial role in the decoding schemes to be discussed in this section.

Definition 1.6.1. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code, and let $\vec{u} \in \mathbb{F}_q^n$. We define the **coset of $\mathscr{C}$ determined by** $\vec{u}$ to be the set*

$$\vec{u} + \mathscr{C} := \{\vec{u} + \vec{x} : \vec{x} \in \mathscr{C}\}.$$

Let us give here some properties of coset.

Theorem 1.6.2 ([16], Theorem 4.8.4)**.** *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code of dimension k. Then,* (*i*) *every vector of* $\mathbb{F}_q^n$ *is contained in some coset of* $\mathscr{C}$*;*

(*ii*) *for all* $\vec{u} \in \mathbb{F}_q^n$, $|\vec{u} + \mathscr{C}| = |\mathscr{C}| = q^k$ *;*

(*iii*) *for all* $\vec{u}, \vec{v} \in \mathbb{F}_q^n$, $\vec{u} \in \vec{v} + \mathscr{C}$ *implies that* $\vec{u} + \mathscr{C} = \vec{v} + \mathscr{C}$*;*

(*iv*) *two cosets are either identical or they have empty intersection;*

(*v*) *there are* q^{n-k} *different cosets of* $\mathscr{C}$*;*

(*vi*) *for all* $\vec{u}, \vec{v} \in \mathbb{F}_q^n$, $\vec{u} - \vec{v} \in \mathscr{C}$ *if and only if* $\vec{u}$ *and* $\vec{v}$ *are in the same coset.*

Example 1.6.3. *Let* $\mathscr{C} = \{(0,0,0,0), (1,0,1,1), (0,1,0,1), (1,1,1,0)\} \in \mathbb{F}_2^4$ *be a linear code. The cosets of* $\mathscr{C}$ *are as follows:*

$$\begin{array}{rcccc}
(0,0,0,0) + \mathscr{C}: & (0,0,0,0) & (1,0,1,1) & (0,1,0,1) & (1,1,1,0) \\
(0,0,0,1) + \mathscr{C}: & (0,0,0,1) & (1,0,1,0) & (0,1,0,0) & (1,1,1,1) \\
(0,0,1,0) + \mathscr{C}: & (0,0,1,0) & (1,0,0,1) & (0,1,1,1) & (1,1,0,0) \\
(1,0,0,0) + \mathscr{C}: & (1,0,0,0) & (0,0,1,1) & (1,1,0,1) & (0,1,1,0)
\end{array}$$

The above array is called a ***(Slepian) standard array****.*

Definition 1.6.4. *A vector of the least (Hamming) weight in a coset is called a* ***coset leader****.*

Example 1.6.5. *In* Example 1.6.3*, the vectors of the first column of standard array are coset leaders for the respective cosets. Note* $(0,0,0,1) + \mathscr{C}$ *have* $(0,1,0,0)$ *as coset leader.*

Proposition 1.6.6. *Let* $\mathscr{C} \subseteq \mathbb{F}_q^n$ *be a linear code such that* $d(\mathscr{C}) = d$*. Then a vector* $\vec{x} \in \mathbb{F}_q^n$ *is the unique coset leader of* $\vec{x} + \mathscr{C}$ *if* $w(\vec{x}) \leq \lfloor (d-1)/2 \rfloor$*, where* $\lfloor a \rfloor$ *is integer part of* a*.*

Proof. Let $\vec{x} + \vec{c}$ be any vector of $\vec{x} + \mathscr{C}$, where $\vec{c} \in \mathscr{C} \setminus \{\vec{0}\}$. Then we have that

$$w(\vec{x} + \vec{c}) = d(\vec{x}, -\vec{c}) \geq d(\vec{0}, -\vec{c}) - d(\vec{x}, \vec{0}) \geq d - (d-1)/2 > (d-1)/2 \geq w(\vec{x}).$$

Hence, $\vec{x}$ is the unique coset leader of $\vec{x} + \mathscr{C}$. □

1.6.2 Nearest neighbour decoding for linear codes

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. Assume the vector $\vec{v}$ is transmitted and the vector $\vec{w}$ is received, with an **error pattern**.

$$\vec{e} = \vec{w} - \vec{v} \in \vec{w} + \mathscr{C}.$$

It is clear that both $\vec{e}$ and $\vec{w}$ are in $\vec{w} + \mathscr{C}$.

Since error patterns of small weight are the most likely to occur, nearest neighbour decoding works for a linear code $\mathscr{C}$ in the following manner. Upon receiving the vector $\vec{w}$, we choose a vector $\vec{e}$ of least weight in the coset $\vec{w} + \mathscr{C}$ and conclude that $\vec{v} = \vec{w} - \vec{e}$ was the vector transmitted.

Example 1.6.7. *Let $\mathscr{C}$ be as* Example 1.6.3 *and assume that the following words are received: (i) $\vec{w} = (1,1,0,1)$; (ii) $\vec{w} = (1,1,1,1)$.*

For the convenience of the reader, we recall here the (Slepian)standard array of $\mathscr{C}$ (exactly the one in Example 1.6.3):

$$\begin{array}{lllll}
(0,0,0,0)+\mathscr{C}: & (0,0,0,0) & (1,0,1,1) & (0,1,0,1) & (1,1,1,0) \\
(0,0,0,1)+\mathscr{C}: & (0,0,0,1) & (1,0,1,0) & (0,1,0,0) & (1,1,1,1) \\
(0,0,1,0)+\mathscr{C}: & (0,0,1,0) & (1,0,0,1) & (0,1,1,1) & (1,1,0,0) \\
(1,0,0,0)+\mathscr{C}: & (1,0,0,0) & (0,0,1,1) & (1,1,0,1) & (0,1,1,0)
\end{array}$$

(*i*) *Note that $\vec{w} + \mathscr{C}$ is the fourth coset which has $(1,0,0,0)$ as a unique coset leader. Hence $(1,1,0,1) - (1,0,0,0) = (0,1,0,1)$ was the most likely vector transmitted.*

(*ii*) *In this case $\vec{w} + \mathscr{C}$ is the second coset. Note that there are two coset leader, $(0,0,0,1)$ and $(0,1,0,0)$, in this coset. When a coset of a received vector has more than one possible coset leader, the approach we take for decoding depends on the decoding scheme (i.e., incomplete or complete) used. If we are doing incomplete decoding, we ask for a retransmission. If we are doing complete decoding, we arbitrarily choose one of the coset leaders and than we decode with this. Back to the example, if for instance we choose $(0,0,0,1)$ as the coset leader of $\vec{w} + \mathscr{C}$, than we can conclude that $(1,1,1,1) - (0,0,0,1) = (1,1,1,0)$ was the most likely codeword sent.*

1.6.3 Syndrome decoding

The decoding scheme based on the standard array works reasonably well when the length n of the linear code is small, but it may take a considerable amount of time when n is large. Some this time can be saved by making use of the concept of syndrome to identify the coset to which the received vector belongs.

Definition 1.6.8. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code of dimension k and let H be a parity-check matrix of $\mathscr{C}$ in standard form. For any $\vec{w} \in \mathbb{F}_q^n$, the* ***syndrome*** *of $\vec{w}$ is the vector $S_H(\vec{w}) = \vec{w}H_t \in \mathbb{F}_q^{n-k}$.*

Theorem 1.6.9. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code of dimension k and let H be a parity-check matrix of $\mathscr{C}$ in standard form. For any $\vec{u}, \vec{v} \in \mathbb{F}_q^n$, we have*

(i) $S_H(\vec{u} + \vec{v}) = S_H(\vec{u}) + S_H(\vec{v})$*;*

(ii) $S_H(\vec{u}) = \vec{0}$ *if and only if $\vec{u}$ is a codeword in $\mathscr{C}$;*

(iii) $S_H(\vec{u}) = S_H(\vec{v})$ *if and only if $\vec{u}$ and $\vec{v}$ are in the same coset of $\mathscr{C}$.*

Proof. (i) It is an immediate consequence of Definition 1.6.8.

(ii) From Definition 1.6.8 it follows, $S_H(\vec{u}) = \vec{0}$ if and only if $\vec{u}H_t = \vec{0}$. By Remark 1.4.5, is equivalent to $\vec{u} \in \mathscr{C}$.

(iii) It follows from (i), (ii) and Theorem 1.6.2 (vi). □

Remark 1.6.10. *Part (iii) of* Theorem 1.6.9 *says that we can identify a coset by its syndrome. Conversely, all the vectors in a given coset yield the same syndrome, so the syndrome of a coset is the syndrome of any vector in it. In other words, there is a one-to-one correspondence between the cosets and the syndromes. In particular by* Theorem 1.6.2 (v) *we know that there are q^{n-k} distinct syndromes, that is all the vectors in $\mathbb{F}_q^{n-k}$ appear as syndromes.*

Definition 1.6.11. *A table which matches each coset leader with its syndrome is called a* ***syndrome look-up table****. Sometimes such a table is called a* ***standard decoding array (SDA).***

To construct a syndrome look-up table by assuming complete nearest neighbour decoding

One can follows the following to steps are needed. *Step 1*: List all the cosets of the code and choose from each coset a vector $\vec{u}$ with least weight as coset leader $\vec{u}$.

Step 2: Find a parity-check matrix H for the code and for each coset leader $\vec{u}$ calculate its syndrome $S_H(\vec{u}) = \vec{u}H_t$.

Example 1.6.12. *By assuming complete nearest neighbour decoding, we construct the a syndrome look-up table*

N°	*Coset leader* $\vec{u}$	*Syndrome* $S(\vec{u})$
1	$(0,0,0,0,0,0)$	$(0,0,0)$
2	$(1,0,0,0,0,0)$	$(1,1,0)$
3	$(0,1,0,0,0,0)$	$(0,1,1)$
4	$(0,0,1,0,0,0)$	$(1,1,1)$
5	$(0,0,0,1,0,0)$	$(1,0,0)$
6	$(0,0,0,0,1,0)$	$(0,1,0)$
7	$(0,0,0,0,0,1)$	$(0,0,1)$
8	$(0,0,0,1,0,1)$	$(1,0,1)\star$

for the linear code $\mathscr{C} \subset \mathbb{F}_2^6$ *with parity-check matrix*

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

By Corollary 1.4.7 *the distance* d *of* $\mathscr{C}$ *is equal to* 3.

As $\lfloor (d-1)/2 \rfloor = 1$, *by* Proposition 1.6.6, *all the error patterns with weight* 0 *or* 1 *will be coset leaders. Then it is sufficient to compute the syndrome for each of them to obtain only the first seven rows of the syndrome look-up table. Since by* Remark 1.6.10 *every vector of length* 3 *must be a syndrome, the remaining coset leader* $\vec{u}$ *has syndrome* $\vec{u}H_t = (1,0,1)$. *Moreover,* $\vec{u}$ *must have weight* ≥ 2 *since all the vectors of weight* 0 *or* 1 *have already been included in the syndrome look-up table. Since we are looking for a coset leader, it is reasonable to start looking among the remaining vectors of the smallest available weight, i.e.* 2. *Doing so, we find three possible coset leaders:*

$(1,0,1,0,0,0)$, $(0,1,0,0,0,1)$ *and* $(0,0,0,1,1,0)$. *Since we are using complete nearest neighbour decoding, we can arbitrarily choose* $(1,0,1,0,0,0)$ *as a coset leader and to complete the syndrome look-up table.*

Syndrome decoding

Step1: Compute the syndrome $S_H(\vec{w})$ where $\vec{w}$ is the received vector.

Step 2: Find the coset leader $\vec{u}$ such that the syndrome $S_H(\vec{u}) = S_H(\vec{w})$ in the syndrome look-up table.

Step 3: Decode $\vec{w}$ as $\vec{v} = \vec{w} - \vec{u}$.

Example 1.6.13. *Let* $\mathscr{C} = \{(0,0,0,0),(1,0,1,1),(0,1,0,1),(1,1,1,0)\} \subset \mathbb{F}_2^4$ *be a linear code. Use the following syndrome look-up table to decode (i)* $\vec{w} = (1,1,0,1)$*; (ii)* $\vec{w} = (1,1,1,1)$.

Coset Leader $\vec{u}$	*Syndrome* $S(\vec{u})$
$(0,0,0,0)$	$(0,0)$
$(0,0,0,1)$	$(0,1)$
$(0,0,1,0)$	$(1,0)$
$(1,0,0,0)$	$(1,1)$

Since a generator matrix of $\mathscr{C}$ *in standard form is* $G = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, *by* Theorem 1.4.9 $H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ *is the parity-check matrix of* $\mathscr{C}$ *in standard form.*

(i) *Since* $S_H(\vec{w}) = \vec{w}H_t = (1,0)$. *From the above table, we deduce that the coset leader is* $(0,0,1,0)$. *Hence* $(1,1,0,1) - (0,0,1,0) = (1,1,1,1)$ *was a most likely vector sent.*

(ii) *Since* $S_H(\vec{w}) = \vec{w}H_t = (0,1)$. *From the above table, it follows that the coset leader is* $(0,0,0,1)$. *Then* $(1,1,1,1) + (0,0,0,1) = (1,1,1,0)$ *was a most likely vector sent.*

Chapter 2

Cyclic Codes

In the previous chapter, we concentrated mostly on linear codes because they have algebraic structures. These structures simplify the study of linear codes. For example, a linear code can be described by its generator or parity-check matrix; the minimum distance is determined by the Hamming weight, etc. However, we have to introduce more structures besides linearity in order for codes to be implemented easily. For the sake of easy encoding and decoding, one naturally requires a cyclic shift of a codeword in a code $\mathscr{C}$ to be still a codeword of $\mathscr{C}$. This requirement looks like a combinatorial structure and fortunately this structure can be converted into an algebraic one.

In this second chapter, we introduce the cyclic codes, a special case of linear codes, and we discuss some of their algebraic structures and main properties. In the last two sections, some further decoding algorithms are considered and studied.

2.1 Preliminaries

First of all let us give here the following

Definition 2.1.1. *A linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ is called* ***cyclic code*** *if it is invariant by the linear transformation*

$$\phi : (a_0, \ldots, a_{n-1}) \longmapsto (a_{n-1}, a_0, \ldots, a_{n-2}).$$

Say that a linear code $\mathscr{C}$ is invariant under ϕ is equivalent to saying that $\mathscr{C}$ it is invariant under the action of the permutation matrix

$$P = \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline 1 & 0 & \cdots & 0 \end{array}\right) \tag{2.1.1}$$

i.e. $\{\vec{c}P : \vec{c} \in \mathscr{C}\} = \mathscr{C}$.

Theorem 2.1.2. *If $\mathscr{C} \subseteq \mathbb{F}_q^n$ is a cyclic code then the dual code $\mathscr{C}^\perp \subseteq \mathbb{F}_q^n$ is also a cyclic code.*

Proof. If $\vec{h} = (h_0, \ldots, h_{n-1}) \in \mathscr{C}^\perp$ then $\vec{h} \cdot \vec{c} = 0$ for all $\vec{c} = (c_0, \ldots, c_{n-1}) \in \mathscr{C}$. Thus we have

$$\begin{aligned} \phi(\vec{h}) \cdot \vec{c} &= (h_{n-1}, h_0, \ldots, h_{n-2}) \cdot (c_0, c_1, \ldots, c_{n-1}) \\ &= h_{n-1}c_0 + h_0c_1 + \ldots h_{n_2}c_{n-1} \\ &= \vec{h} \cdot \phi^{n-1}(\vec{c}) = 0, \end{aligned}$$

since $\phi^{n-1}(\vec{c}) \in \mathscr{C}$ where $\phi^k = \underbrace{\phi \circ \cdots \circ \phi}_{\text{k}-\text{times}}$ $\forall k \in \mathbb{N}$. Hence, $\mathscr{C}^\perp$ is a cyclic code. □

In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider the following correspondence:

$$\pi_n : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[X]/(X^n - 1), \quad (a_0, a_1, \ldots, a_{n-1}) \longmapsto a_0 + a_1X + \cdots + a_{n-1}X^{n-1}. \tag{2.1.2}$$

Observe that π_n is a linear $\mathbb{F}_q$-isomorphism of vector spaces over $\mathbb{F}_q$. So, we will sometimes identify $\mathbb{F}_q^n$ with $\mathbb{F}_q[X]/(X^n - 1)$ and a vector $\vec{a} = (a_0, \ldots, a_{n-1})$ with the polynomial $\pi_n(\vec{a}) : a = \sum_{i=0}^{n-1} a_iX^i$. Since $\mathbb{F}_q[X]/(X^n - 1)$ is a ring, we have a multiplicative operation on $\mathbb{F}_q[X]/(X^n - 1)$ besides the addition inherited by the one on $\mathbb{F}_q^n$ via π_n.

2.2 Generator polynomials

The reason for defining π_n in the previous section is the following result which connects ideal with cyclic codes.

Theorem 2.2.1. *Let π_n be as in (2.1.2). Then a non-empty subset $\mathscr{C}$ of $\mathbb{F}_q^n$ is a cyclic code if and only if $\pi_n(\mathscr{C})$ is an ideal of $\mathbb{F}_q[X]/(X^n-1)$.*

Proof. Suppose that $\pi_n(\mathscr{C})$ is an ideal of $\mathbb{F}_q[X]/(X^n-1)$. Then, for any $\alpha, \beta \in \mathbb{F}_q \subset \mathbb{F}_q[X]/(X^n-1)$ and $\vec{a}, \vec{b} \in \mathscr{C}$, we have $\alpha\pi_n(\vec{a}), \beta\pi_n(\vec{b}) \in \pi_n(\mathscr{C})$. Thus $\pi_n(\alpha\vec{a}+\beta\vec{b}) = \alpha\pi_n(\vec{a}) + \beta\pi_n(\vec{b}) \in \pi_n(\mathscr{C})$, i.e. $\alpha\vec{a}+\beta\vec{b} \in \mathscr{C}$. This shows that $\mathscr{C}$ is a linear code.

Now let $\vec{c} = (c_0, \dots, c_{n-1}) \in \mathscr{C}$ and $\pi_n(\vec{c}) = c_0 + c_1X + \cdots + c_{n-2}X^{n-2} + c_{n-1}X^{n-1} \in \pi_n(\mathscr{C})$. Since $\pi_n(\mathscr{C})$ is an ideal, the polynomial

$$\begin{aligned} X \cdot \pi_n(\vec{c}) &= c_0X + c_1X^2 + \cdots + c_{n-2}X^{n-1} + c_{n-1}X^n \\ &= c_{n-1} + c_0X + c_1X^2 + \cdots + c_{n-2}X^{n-1} \in \pi_n(\mathscr{C}) \\ &\quad (\text{since } X^n - 1 = 0 \text{ in } \mathbb{F}_q[X]/(X^n-1)) \end{aligned}$$

i.e. $(c_{n-1}, c_0, \dots, c_{n-2}) \in \mathscr{C}$.

Conversely, suppose that $\mathscr{C} \subseteq \mathbb{F}_q^n$ is a cyclic code. For any polynomial

$$f := f_0 + f_1X + \cdots + f_{n-2}X^{n-2} + f_{n-1}X^{n-1} = \pi_n(f_0, f_1, \dots, f_{n-1})$$

of $\pi_n(\mathscr{C})$ with $(f_0, f_1, \dots, f_{n-1}) \in \mathscr{C}$, the polynomial

$$X \cdot f = f_{n-1} + f_0X + f_1X^2 + \cdots + f_{n-2}X^{n-1}$$

is also an element of $\pi_n(\mathscr{C})$ since $\mathscr{C}$ is cyclic. Thus $X^2 \cdot f = X(X \cdot f) \in \pi_n(\mathscr{C})$ and by inductive argument we see that $X^i \cdot f \in \pi_n(\mathscr{C})$ for all integer $i \geq 0$. Since $\mathscr{C}$ is a linear code and π_n is a linear transformation, $\pi_n(\mathscr{C}) \subseteq \mathbb{F}_q[X]/(X^n-1)$ is a group with respect to the sum and for any $g = g_0 + g_1X + \cdots + g_{n-1}X^{n-1} \in \mathbb{F}_q[X]/(X^n-1)$, the polynomial

$$gf = \sum_{i=0}^{n-1} g_i(X^i f)$$

is an element of $\pi_n(\mathscr{C})$. Therefore, $\pi_n(\mathscr{C})$ is an ideal of $\mathbb{F}_q[X]/(X^n-1)$. □

Example 2.2.2. *The set $I = \{0, 1+X^2, X+X^3, 1+X+X^2+X^3\}$ is an ideal in $\mathbb{F}_2[X]/(X^4-1)$. The corresponding cyclic code is $\pi_n^{-1}(I) = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$.*

Remark 2.2.3. *The trivial cyclic codes* $\{\vec{0}\}$ *and* $\mathbb{F}_q^n$ *correspond to the trivial ideals* (0) *and* $\mathbb{F}_q[X]/(X^n-1)$*, respectively.*

The proof of the following results is easy and it makes use principally of the division algorithm

Theorem 2.2.4 ([16], Theorem 7.2.3)**.** *Let* I *be a non-zero ideal in* $\mathbb{F}_q[X]/(X^n-1)$ *and let* g *be a non-zero monic polynomial of the least degree in* I*. Then* g *is a generator of* I *and it divides* X^n-1*.*

Since $\mathbb{F}_q[X]/(X^n-1)$ is a principal ideal domain (PID), we deduce that any of its ideal is principal. Therefore any cyclic code $\mathscr{C}$ is uniquely determined by the monic generator of $\pi_n(\mathscr{C})$, as the following result shows

Proposition 2.2.5. *There is a unique monic polynomial of the least degree in every non-zero ideal* I *of* $\mathbb{F}_q[X]/(X^n-1)$ *and by* Theorem 2.2.4*, it is a generator of* I*.*

Proof. Let g_1, g_2, be two distinct monic generators of the least degree of the ideal I. Then a suitable scalar multiple of $g_1 - g_2$ is a non-zero monic polynomial of smaller degree in I. But this give a contradiction. □

From the above result, the following definition makes sense.

Definition 2.2.6. *For a cyclic code* $\mathscr{C} \subseteq \mathbb{F}_q^n$*, the unique monic polynomial of the least degree of* $\pi_n(\mathscr{C})$ *is called the* ***generator polynomial*** *of* $\mathscr{C}$*.*

From the above results we obtain the following

Corollary 2.2.7. *There is a one-to-one correspondence between the cyclic codes* $\mathscr{C} \subseteq \mathbb{F}_q^n$ *and the monic divisors of* $X^n - 1 \in \mathbb{F}_q[X]$*.*

Proof. Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a cyclic code. Then by Theorem 2.2.1 $\pi_n(\mathscr{C})$ is an ideal of $\mathbb{F}_q[X]/(X^n-1)$. Since $\mathbb{F}_q[X]/(X^n-1)$ is a PID, from Proposition 2.2.5 it follows that $\pi_n(\mathscr{C}) = (g)$ for a unique monic polynomial $g \in \mathbb{F}_q[X]$. Moreover, by Theorem 2.2.4 we know that g divides X^n-1. Conversely, let $g \in \mathbb{F}_q[X]$ be a monic divisor of X^n-1 and consider the unique ideal $(g) \subseteq \mathbb{F}_q[X]/(X^n-1)$. By Theorem 2.2.1 we conclude that $\pi_n^{-1}((g))$ is a cyclic code via the isomorphism π_n. □

Example 2.2.8. *In order to find all cyclic codes $\mathscr{C} \subset \mathbb{F}_2^6$ we factorize the polynomial $X^6 - 1 \in \mathbb{F}_2[X]$:*

$$X^6 - 1 = (1+X)^2(1+X+X^2)^2.$$

List all monic divisor of $X^6 - 1$:

$$\begin{array}{ccc} 1, & 1+X, & 1+X+X^2 \\ (1+X)^2, & (1+X)(1+X+X^2), & (1+X)^2(1+X+X^2) \\ (1+X+X^2)^2, & (1+X)(1+X+X^2)^2, & (1+X^6). \end{array}$$

By Corollary 2.2.7 *there are nine cyclic codes $\mathscr{C} \subset \mathbb{F}_2^6$. By the map π_6^{-1}, we can easily write down all these cyclic codes. For instance, the cyclic code which corresponds to the polynomial $(1+X+X^2)^2$ is*

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

From the above example, we deduce the number of cyclic codes $\mathscr{C} \subseteq \mathbb{F}_q^n$ can be determined if we know the factorization of $X^n - 1$. We have the following

Theorem 2.2.9. *If $X^n - 1 = \displaystyle\prod_{i=1}^{r} p_i^{e_i}$ is the factorization of $X^n - 1 \in \mathbb{F}_q[X]$ where $p_1, \ldots, p_r$ are distinct monic irreducible polynomials and $e_i \in \mathbb{N} \setminus \{0\}$ for all $i = 1, \ldots, r$, then there are $\prod_{i=1}^{r}(e_i + 1)$ cyclic codes $\mathscr{C} \subseteq \mathbb{F}_q^n$.*

Proof. The statement follows from Corollary 2.2.7 by counting the number of all monic divisors of $X^n - 1$. □

Since a cyclic code $\mathscr{C} \subseteq \mathbb{F}_q^n$ is totally determined by its generator polynomial g, all the parameters of $\mathscr{C}$ are also determined by the g. For example, the following result gives the dimension of $\mathscr{C}$ in terms of g.

Theorem 2.2.10. *Let g be the generator polynomial of an ideal $I \in \mathbb{F}_q[X]/(X^n - 1)$. Then the corresponding cyclic code $\pi_n^{-1}(\mathscr{C})$ has dimension k if and only if the degree of g is equal to $n - k$.*

Proof. Note that for two distinct polynomials c_1, c_2 with $\deg(c_i) \leq k - 1$ $(i = 1, 2)$, we have that $c_1 g \neq c_2 g \pmod{X^n - 1}$. Hence, the set

$$A := \{cg : c \in \mathbb{F}_q[X]/(X^n - 1),\ \deg(c) \leq k - 1\}$$

has q^k elements and it is a subset of the ideal (g). On the other hand, for any polynomial ag with $a \in \mathbb{F}_q[X]/(X^n - 1)$, write

$$ag = u(X^n - 1) + r \tag{2.2.1}$$

with $\deg(r) < n$. By (2.2.1), we get that $r = ag - u \cdot (X^n - 1)$. Hence, g divides r. Write $r = bg$ for some polynomial b. Then $\deg(b) \leq k - 1$, so $r \in A$. This shows that A is equal to (g). Hence, by Theorem 1.1.3 (i), the dimension of the code $\pi_n^{-1}((g))$ is $\log_q |A| = k$. □

Example 2.2.11. *Based on the factorization: $X^7 - 1 = (1+X)(1+X^2+X^3)(1+X+X^3) \in \mathbb{F}_2[X]$, we know that there are only two cyclic codes $\mathscr{C}_1$ and $\mathscr{C}_2$ in $\mathbb{F}_2^7$ with dimendion 3:*

$$\begin{aligned}\mathscr{C}_1 = \pi_7^{-1}((1+X)(1+X^2+X^3)) =& \{(0,0,0,0,0,0,0),(1,1,1,0,1,0,0),(0,1,1,1,,0,1,0),\\ &(0,0,1,1,1,0,1),(1,0,0,1,1,1,0),(0,1,0,0,1,1,1),\\ &(1,0,1,0,0,1,1),(1,1,0,1,0,0,1)\}\end{aligned}$$

and

$$\begin{aligned}\mathscr{C}_2 = \pi_7^{-1}((1+X)(1+X+X^3)) =& \{(0,0,0,0,0,0,0),(1,0,1,1,1,0,0),(0,1,0,1,1,1,0),\\ &(0,0,1,0,1,1,1),(1,0,0,1,0,1,1),(1,1,0,0,1,0,1),\\ &(1,1,1,0,0,1,0),(0,1,1,1,0,0,1)\}.\end{aligned}$$

2.3 Generator and parity-check matrices

In the previous section, we showed that a cyclic code is totally determined by its generator polynomial. Hence, such a code should also have generator matrices related to this polynomial. More precisely, we have the following

Theorem 2.3.1. *Let $g = g_0 + g_1 X + \cdots + g_{n-k} X^{n-k}$ be the generator polynomial of a cyclic code $\mathscr{C} \subseteq \mathbb{F}_q^n$ in $\mathbb{F}_q^n$ with $\deg(g) = n - k$. Then the matrix*

$$G = \begin{pmatrix} \pi_n^{-1}(g) \\ \pi_n^{-1}(X \cdot g) \\ \vdots \\ \pi_n^{-1}(X^{k-1} \cdot g) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \dots & \dots & g_{n-k} & 0 & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & \dots & \dots & g_0 & g_1 & \dots & \dots & \dots & g_{n-k} \end{pmatrix}$$

is a generator matrix of $\mathscr{C}$.

Proof. Consider the polynomials $g,\ X \cdot g, \dots,\ X^{k-1} \cdot g$ of $\pi_n(\mathscr{C})$. It is clear are linearly independent over $\mathbb{F}_q$. Moreover, by Theorem 2.2.10, we know that $\dim(\mathscr{C}) = k$. Then $\pi_n^{-1}(g),\ \pi_n^{-1}(X \cdot g), \dots,\ \pi_n^{-1}(X^{k-1} \cdot g)$ form a basis of $\mathscr{C}$. □

Example 2.3.2. *Consider the cyclic code $\mathscr{C} \subset \mathbb{F}_2^7$ with dimension 4 and generator polynomial $g = 1 + X^2 + X^3$. Then this code has a generator matrix given by*

$$G = \begin{pmatrix} \pi_7^{-1}(g) \\ \pi_7^{-1}(X \cdot g) \\ \pi_7^{-1}(X^2 \cdot g) \\ \pi_7^{-1}(X^3 \cdot g) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

This generator matrix is not in standard form. By elementary row operations on the rows of G we can obtain the following

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

Remark 2.3.3. *By knowing the generator matrix of a cyclic code, its parity-check matrix in standard form can be easily obtained by* Theorem 2.3.1 *row elementary operations and* Theorem 1.4.9.

However, since the dual code of a cyclic code $\mathscr{C}$ is also cyclic, we should be able to find a parity-check matrix from the generator polynomial of the dual code. The next problem will be to find the generator polynomial of the dual code $\mathscr{C}^\perp$. To do this we need the following

Definition 2.3.4. *Let $h = \sum_{i=0}^{k} h_i X^i$ be a polynomial of degree k over $\mathbb{F}_q$. Define the **reciprocal polynomial** h_R of h by*

$$h_R := X^k \cdot h(1/X) = \sum_{i=0}^{k} a_{k-i} X^i.$$

Theorem 2.3.5 ([16], Theorem 7.3.7)**.** *Let g be the generator polynomial cyclic code $\mathscr{C} \subseteq \mathbb{F}_q^n$ with dimension k. Put $h = (X^n - 1)/g$. Then $h_0^{-1} h_R$ is the generator polynomial of $\mathscr{C}^\perp$, where h_0 is the constant term of h.*

Definition 2.3.6. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a cyclic code. The polynomial $h_0^{-1}h_R$ of* Theorem 2.3.5 *is called the **parity-check polynomial** of the cyclic code.*

Corollary 2.3.7. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a cyclic code with generator polynomial g. Put $h = (X^n - 1)/g = h_0 + h_1X + \cdots + h_kX^k$. Then the matrix*

$$H = \begin{pmatrix} \pi_n^{-1}(h_R) \\ \pi_n^{-1}(X \cdot h_R) \\ \vdots \\ \pi_n^{-1}(X^{n-k-1} \cdot h_R) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & \dots & \dots & h_0 & 0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & \dots & h_0 & 0 & 0 & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & \dots & \dots & h_k & h_{k-1} & \dots & \dots & \dots & h_0 \end{pmatrix}$$

is a parity-check matrix of $\mathscr{C}$.

Proof. The result immediately follows from Theorem 2.3.5 and 2.3.1. □

Example 2.3.8. *Let $\mathscr{C} \subset \mathbb{F}_2^7$ be the cyclic code with generator polynomial $g = 1 + X^2 + X^3$. Write $h = (X^7 - 1)/g = 1 + X^2 + X^3 + X^4$. Then by* Theorem 2.3.5 *$h_R = 1 + X + X^2 + X^4$ is the parity-check polynomial of $\mathscr{C}$. and by* Corollary 2.3.7

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

is a parity.check matrix of $\mathscr{C}$.

2.4 Encoding and Decoding methods with cyclic codes

Given a cyclic code $\mathscr{C} \subset \mathbb{F}_q^n$ of dimension $k < n$, a classical codification of a message $\vec{M} \in \mathbb{F}_q^k$ is given by $\vec{M}G$, where G is a generator matrix of $\mathscr{C}$. However, this encoding method is not systematic, i.e. it is not strictly related with an easy decoding algorithm.

So, let us give here a non-trivial and systematic encoding method for cyclic codes. Let $\vec{M} \in \mathbb{F}_q^k$ be the original message. Let $\mathscr{C}$ be a cyclic code such that $\dim(\mathscr{C}) = k$. Therefore, consider the natural injective map $i : \mathbb{F}_q^k \to \mathbb{F}_q^n$ such that $i(a_1, ..., a_k) := (a_1, ..., a_k, 0, ..., 0)$.

Define $\vec{m} := i(\vec{M}) = (\vec{M}, \vec{0}) \in \mathbb{F}_q^n$ and denote by $m \in R_n$ the representation of the message $\vec{m} = i(\vec{M}) \in \mathbb{F}_q^n$, via the vector isomorphism

$$\pi : \mathbb{F}_q^n \to \mathbb{F}_q[X]/(X^n - 1) \ .$$

At this point, we can encode the original message $\vec{m} := i(\vec{M})$ by working equivalently on either (i) $\mathbb{F}_q[X]/(X^n - 1)$, or (ii) $\mathbb{F}_q^n$.

(i) Multiply the original messages m by X^{n-k}, where $m = m_{,0} + m_1X + ... + m_{k-1}X^{k-1}$ and $k = \dim(\mathscr{C})$. The result is $X^{n-k} \cdot m = m_0)X^{n-k} + m_1X^{n-k+1} + ... + m_{k-1}X^{n-1}$. Write $X^{n-k} \cdot m = qg + r$, where $\deg r < n - k$. Since $qg \in \mathscr{C}$, we can encode the original message $\vec{m} \in \mathbb{F}_q^n$ by

$$\vec{m}' := \pi^{-1}(X^{n-k} \cdot m - r) \in \mathscr{C}$$

Since $\deg r < n - k$, observe that all the information about the original messages m is contained in the last powers $X^{n-k}, ..., X^{n-1}$ of $X^{n-k} \cdot m - r \in \pi(\mathscr{C})$.

(ii) Define the map

$$\overline{P} : \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ \vec{x} & \longmapsto & \vec{x}_1 P^{n-k} \end{array} ,$$

where the P is the permutation matrix as (2.1.1). By applying $\overline{P}$ to $\vec{m}$ we have

$$\begin{aligned} \vec{m}\overline{P} &= (\vec{M}, \vec{0})P^{n-k}) \\ &= (\vec{0}, \vec{M}) \end{aligned}$$

If $\vec{m}' := (\vec{c}, \vec{M})$ is such that $\vec{m}'H_t = \vec{0}$, where H is the parity check matrix of $\mathscr{C}$ in standar form, i.e. $H = (I_{n-k} \mid (T)_t)$ is given by Proposition 3.3.3. Then $\vec{m}' \in \mathscr{C}$ is the encoded message of $\vec{m} \in \mathbb{F}_q^n$.

Now, let $\vec{m}''$ be the received message. If during the transmission of the encoded message $\vec{m}'$ there were not errors, i.e. $\vec{m}'' \in \mathscr{C}_1 \times \cdots \times \mathscr{C}_r$, then in both cases (i) and (ii) we can decode $\vec{m}'' = (\vec{m}_1'', ..., \vec{m}_r'')$ by applying $\Theta^{-n_i+k_i}$ to each component $\vec{m}_i''$ of $\vec{m}''$. The original components $\vec{m}_i$ of $\vec{m} = (\vec{m}_1, ..., \vec{m}_r)$ will be given by the last k_i coordinates of $(\vec{m}_i'')\Theta^{-n_i+k_i}$ for every $i = 1, ..., r$.

2.4.1 Syndrome decoding of cyclic codes

The syndrome decoding of cyclic codes consists of the same three steps as the decoding of linear codes: computing the syndrome, finding the syndrome corresponding to the error pattern; and correcting the errors. Cyclic codes have considerable algebraic and geometric properties. If these properties are properly used, simplicity in the decoding can be easily achieved. For this all reasons,we will see that the above three steps for cyclic codes are usually simpler.

From Corollary 2.3.7, by performing elementary row operations, we can easily produce for a cyclic code the unique parity-check matrix of the form

$$H = (I_{n-k}|A). \tag{2.4.1}$$

Recall that all syndromes considered in this section will be computed with respect to the parity-check matrix of the form as in (2.4.1).

Theorem 2.4.1. *Let $H = (I_{n-k}|A)$ be the parity-check matrix of a cyclic code $\mathscr{C} \subseteq \mathbb{F}_q^n$. Let g be the generator polynomial of $\mathscr{C}$. Then the syndrome of a vector $\vec{v} \in \mathbb{F}_q^n$ correspond to the principal remainder of* $v\mathrm{mod}\ g$ *via π_{n-k}, where $\pi_n(\vec{v}) = v$.*

Proof. Denote by a_i the polynomial of degree at most $n-k-1$ which correspond to the i-th column vector of A by π_{n-k}. By Theorem 1.4.9 , we know that $G = (-A^T|I_k)$ is a generator matrix for $\mathscr{C}$. Therefore, $[X^{n-k+i} - a_i]$ is a polynomial class of $\pi_n(\mathscr{C})$. Put $X^{n-k+i} - a_i = q_i g$ for some $q_i \in \mathbb{F}_q[X]$, that is

$$[a_i] = [X^{n-k+i} - q_i g]$$

where $\deg(a_i) \leq n-k-1$ for every $i = 0, \ldots, k-1$. Write $v = v_0 + v_1 X + \ldots + v_{n-1}X^{n-1}$. For the syndrome $\vec{v}H_t$ of $\vec{v}$, the corresponding polynomial is

$$\begin{aligned}
s &= v_0 + v_1 X + \ldots + v_{n-k-1}X^{n-k-1} + v_{n-k}a_0 + \ldots + v_{n-1}a_{k-1} \\
&= \sum_{i=0}^{n-k-1} v_i X^i + \sum_{j=0}^{k-1} v_{n-k+j}(X^{n-k+j} - q_j g) \\
&= \sum_{i=0}^{n-1} v_i X^i - \left(\sum_{j=0}^{k-1} v_{n-k+j} q_j \right) \cdot g,
\end{aligned}$$

i.e. $v = \left(\sum_{j=0}^{k-1} v_{n-k+j} q_j\right) \cdot g + s$. As the polynomial s has degree at most $n-k-1$, by the unicity of the Division Algorithm we conclude that $s = v (\text{mod } g)$. □

The three steps of the syndrome decoding (see Ch 1, § 1.6) for cyclic codes can be resumed in the following result

Corollary 2.4.2. *Let g be the generator polynomial of a cyclic code $\mathscr{C} \subseteq \mathbb{F}_q^n$. For a received polynomial v, if the remainder s of v divided by g correspond to a vector with weight less than or equal to $\lfloor (d(\mathscr{C})-1)/2 \rfloor$, then s is the error pattern of v and v can be decoded by $v-s$. Otherwise, we ask for a retransmission of v.*

Proof. From Theorem 2.4.1, we know that v and s are in the same coset $v + (g)$. Furthermore, by Proposition 1.6.6 s is the unique coset leader since $w(\pi_n^{-1}(s)) \leq \lfloor (d(\mathscr{C})-1)/2 \rfloor$. So the desired result follows. □

Example 2.4.3. *Consider the cyclic code $\mathscr{C} \subseteq \mathbb{F}_q^n$ with generator polynomial $g = 1 + X^2 + X^3$ such that $d(\mathscr{C}) = 3$. Then, by performing elementary row operations on the matrix of* Example 2.3.8*, we obtain a parity-check matrix $H = (I_3|A)$, where A is the matrix*

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

For $\vec{v} = (0,1,1,0,1,1,0)$, the syndrome is $\vec{v}H_t = (0,1,0)$. On the other hand, $v = X + X^2 + X^4 + X^5 = X + X^2 \cdot g$. Thus, the remainder v $(\text{mod } g)$ is X, which corresponds to $(0,1,0,0,0,0,0,) \in \mathbb{F}_2^7$. Therefore, v is decoded as $v - X = X^2 + X^4 + X^5$ which corresponds to the word $(0,0,1,0,1,1,0) \in \mathbb{F}_2^7$. If the polynomial $v_1 = 1 + X^2 + X^3 + X^4$ is received, then the remainder v_1 $(\text{mod } g)$ is $1 + X + X^2$. In this case, we can use syndrome decoding to obtain the codeword $v_1 - X^4 = 1 + X^2 + X^3 = (1,0,1,1,0,0,0)$ as the word $(0,0,0,0,1,0,0)$ is the coset leader for the coset in which v_1 lies.

2.4.2 Meggitt decoding of cyclic codes

In this subsection we present a technique for decoding of cyclic codes called **Meggitt decoding**. This decoding is performing in quotient $\mathbb{F}_q[X]/(X^n - 1)$.

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a cyclic code with $d(\mathscr{C}) = d$ and generator polynomial g of degree $n - k$. By working with polynomials instead of vectors, suppose that $c \in \pi_n(\mathscr{C})$ is transmitted and $y = c + e$ is received, where e is the error vector with $w(\pi_n^{-1}(e)) \leq \lfloor (d-1)/2 \rfloor$. The Meggitt decoder stores syndromes of error patterns (see § 1.6.2) with n coordinate. By shifting y at most n times, the decoder finds the error polynomials e from a list and then corrects this error e we will see that Meggitt decoding takes advantages of the nature of the cyclic codes.

Define the **shift syndrome polynomial** $\overline{s}([v])$ of any $[v] \in \mathbb{F}_q[X]/(X^n - 1)$ to be:

$$\overline{s}([v]) := [X^{n-k} v] \pmod{g},$$

where g is the monic polynomial such that $\pi_n(\mathscr{C}) = (g)$.

Lemma 2.4.4. *If $[v] \in \mathbb{F}_q[X]/(X^n - 1)$, then $\overline{s}([v]) = 0$ if and only if $[v] \in \pi_n(\mathscr{C})$.*

Proof. Let $[v] \in \mathbb{F}_q[X]/(X^n - 1)$ such that $\overline{s}([v]) = 0$, i.e. $(X^{n-k} \cdot v) = 0 \pmod{g}$. Hence we can deduce that $[X^{n-k} \cdot v] \in \pi_n(\mathscr{C})$, that is $X^{n-k} \cdot v = h \cdot g$ for some $h \in \mathbb{F}_q[X]/(X^n - 1)$. Since $X^n = 1$, we get

$$[X^k \cdot h \cdot g] = [X^k \cdot (X^{n-k} \cdot v)] = [(X^n \cdot v] = [v],$$

that is, $[v] \in \pi_n(\mathscr{C})$. On the other hand, if $[v] \in \pi_n(\mathscr{C})$, then $v = q \cdot g$ for some $q \in \mathbb{F}_q[X]$. Thus by definition we can conclude that $\overline{s}([v]) = 0$. □

Lemma 2.4.5 ([12], Theorem 4.6.2)**.** *Let g be a monic divisor of $X^n - 1$ of degree $n - k$. If $s = [X^{n-k} v] (\bmod\ g)$, then*

$$\overline{s}([X \cdot s]) = [X \cdot s + s_{n-k-1} g]$$

where s_{n-k-1} is the coefficient of X^{n-k-1} in s.

We now describe **Meggitt Decoding Algorithm** and we use an example to illustrate each of its steps.

Step I:

Find all the shift syndrome polynomials $\overline{s}([e])$ of error patterns $e = \sum_{i=0}^{n-1} e_i X^i$ such that $w(\vec{e}) \leq \lfloor (d-1)/2 \rfloor$ and $e_{n-1} \neq 0$, where $\vec{e} = (e_0, \ldots, e_{n-1})$ is the vector corresponding to e.

Example 2.4.6. *Let $\mathscr{C} \subseteq \mathbb{F}_2^{15}$ be a cyclic code with $d(\mathscr{C}) = 5$ and generator polynomial $g = 1 + X^4 + X^6 + X^7 + X^8$. Then, with an abuse of notation, the shift syndrome polynomial $\overline{s}([e])$ of an error pattern e is equal to $X^8 e \pmod g$. The Step I produces the following shift syndrome polynomials:*

e	$\overline{s}([e])$
X^{14}	X^7
$X^{13} + X^{14}$	$X^6 + X^7$
$X^{12} + X^{14}$	$X^5 + X^7$
$X^{11} + X^{14}$	$X^4 + X^7$
$X^{10} + X^{14}$	$X^3 + X^7$
$X^9 + X^{14}$	$X^2 + X^7$
$X^8 + X^{14}$	$X + X^7$
$X^7 + X^{14}$	$1 + X^7$

e	$\overline{s}([e])$
$X^5 + X^{14}$	$X^2 + X^4 + X^5 + X^6 + X^7$
$X^6 + X^{14}$	$X^3 + X^5 + X^6$
$X^4 + X^{14}$	$X + X^3 + X^4 + X^5 + X^7$
$X^3 + X^{14}$	$1 + X^2 + X^3 + X^4 + X^7$
$X^2 + X^{14}$	$X + X^2 + X^5 + X^6$
$X + X^{14}$	$1 + X + X^4 + X^5 + X^6 + X^7$
$1 + X^{14}$	$1 + X^4 + X^6$

Setp II:

Suppose that y is the received polynomial. Compute the syndrome polynomial $\overline{s}([y]) = [X^{n-k}y] \pmod g$. Since $y = c + e$, where $c \in \pi_n(\mathscr{C})$, then by *Lemma 2.4.4* we see that $\overline{s}([y]) = \overline{s}([e])$.

Example 2.4.7. *Continuing with* Example 2.4.6, *suppose that $y = 1 + X^4 + X^7 + X^9 + X^{10} + X^{12}$ is received. Then*

$$\overline{s}([y]) = [X^8 \cdot y] (\bmod\ g) = X + X^2 + X^6 + X^7$$

.

Step III:

If $\overline{s}([y])$ belongs to the list computed in Step I, then we have the error polynomial e and we $c = y - e$. If $\overline{s}([y])$ does not appear in the list, go on to Step IV.

Example 2.4.8. *We see that $\overline{s}([y])$ does not appear in the list of shift syndrome polynomial.*

Step IV:

Since $\overline{s}([y])$ is not appear in the list we can write $y = c + e'$ with $c \in \pi_n(\mathscr{C})$, where e' is the error pattern such that $w(\pi_n^{-1}(e')) \leq \lfloor \frac{d-1}{2} \rfloor$ and $\deg(e') < n - 1$. By Lemma 2.4.5 compute the shift syndrome polynomial of $X \cdot y = X \cdot c + X \cdot e'$, $X^2 y = X^2 \cdot c + X^2 \cdot e', \ldots, X^{n-1-\deg(e')} \cdot y = X^{n-1-\deg(e')} \cdot c + X^{n-1-\deg(e')} \cdot e'$. Observe that $\deg(X^{n-1-\deg(e')} \cdot e') = n-1$ and $w(\pi_n^{-1}(X^{n-1-\deg(e')} \cdot e')) \leq \lfloor \frac{d-1}{2} \rfloor$. Then $\overline{s}([X^{n-1-\deg(e')} \cdot y])$ belongs to the list and it is associated with the error polynomial $e'' := X^{n-1-\deg(e')} \cdot e'$. Then the received vector can be decoded as $y - X^{\deg(e')+1} \cdot e''$.

Remark 2.4.9. *The definition of the shift syndrome polynomial is typical of the Meggitt decoding algorithm. Moreover it allows us to construct a table of shift syndrome polynomial smaller than the classical one we have to consider in syndrome decoding of* §1.6.2.

Example 2.4.10. *Continuing with* Example 2.4.7*, we have* $\overline{s}([X \cdot y]) = X(X + X^2 + X^6 + X^7) - 1 \cdot g = 1 + X^2 + X^3 + X^4 + X^6$ *which is not in the list of* Example 2.4.6*. Thus consider* $\overline{s}(X^2 y) = X(1 + X^2 + X^3 + X^4 + X^6) - 0 \cdot g = X + X^3 + X^4 + X^5 + X^7$*. Since* $\overline{s}([X^2 \cdot y])$ *corresponds to the error* $X^4 + X^{14}$*, we can decoded* y *as* $y - X^{13}(X^4 + X^{14}) = y - (X^2 + X^{12}) = 1 + X^2 + X^4 + X^7 + X^9 + X^{10}$*. Note that this is equal to* $(1 + X^2)g \in \pi_n(\mathscr{C})$*.*

Chapter 3

Generalized Cyclic Codes

In this third chapter, we study a new type of linear code, called Generalized Cyclic Code, which happens to be a generalization of cyclic codes. Furthermore, we show that in this case many of the main properties of cyclic codes are naturally inherited and that these codes can be analyzed as subspaces invariant under the action of a companion matrix, providing a method to find other algebraic properties of these codes, a generator matrix and a parity-check matrix. In the last part of this chapter, we give an algorithm to construct these kind of codes via projective spaces and by an immersion map we explore two further dual codes, the Quasi-Euclidean and the Hermitian dual codes, by ending with a generalization of a Meggitt type algorithm as in Chapter 2.

3.1 Preliminaries and Background Material

In this section we study the main tools to construct a class of generalized cyclic codes. Each matrix M of order $n \times n$, with coefficients in a finite field $\mathbb{F}_q$, can be associated to an $n \times n$ matrix R called the rational canonical form of M. The matrix R is a block matrix whose blocks are matrices of special type called companion matrices.

From now on, denote by A an $n \times n$ matrix with coefficients in $\mathbb{F}_q$.

Definition 3.1.1. *A monic polynomial of minimum degree that annihilates the matrix A is called* ***minimal polynomial*** *of A.*

Remark 3.1.2. *The minimal polynomial of A is unique.*

We have the following

Lemma 3.1.3 ([9], Lemma 6.7.1)**.** *Suppose that $f(X) = X^n - f_{n-1}X^{n-1} \ldots - f_1X - f_0$ is the minimal polynomial of A. Then there is a basis $\{\vec{r}_1, \ldots, \vec{r}_n\}$ of $\mathbb{F}_q^n$ such that*

$$A = S \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline f_0 & f_1 & \cdots & f_{n-1} \end{array} \right) S^{-1}$$

where $S = \left(\begin{array}{c|c|c} \vec{r}_{1t} & \cdots & \vec{r}_{nt} \end{array} \right)$.

Definition 3.1.4. *If $f = X^n - f_{n-1}X^{n-1} - \ldots - f_1X - f_0 \in \mathbb{F}_q[X]$ then the matrix*

$$A_{c,f} := \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline f_0 & f_1 & \cdots & f_{n-1} \end{array} \right)$$

is called the ***companion matrix*** *of f. When f is known we simply write A_c.*

Remark 3.1.5. Lemma 3.1.3 *says that if f is the minimal polynomial of A in $\mathbb{F}_q[X]$ then for some basis of $\mathbb{F}_q^n$ the matrix A is similar to $A_{c,f}$. Thus f is also the minimal polynomial of $A_{c,f}$.*

Let $f \in \mathbb{F}_q[X]$ be the minimal polynomial of A. Since $\mathbb{F}_q[X]$ is an Euclidean Domain, up to permutation we can write

$$f = q_1^{e_1} \cdot \ldots \cdot q_k^{e_k} \tag{3.1.1}$$

for some $e_i \in \mathbb{N}_{>0}$ and distinct monic irreducible polynomials q_i for every $i = 1, \ldots, k$.

Theorem 3.1.6 ([9], Theorem 6.7.1)**.** *If $f = q^e$ is the minimal polynomial of A where q is a monic irreducible polynomial in $\mathbb{F}_q[X]$, then there exists a basis $\{\vec{r}_1, \ldots, \vec{r}_n\}$ of $\mathbb{F}_q^n$ such that*

$$A = S \begin{pmatrix} A_{c,q^{e_1}} & & \\ & \ddots & \\ & & A_{c,q^{e_k}} \end{pmatrix} S^{-1},$$

where $A_{c,q^{e_i}}$ denotes the companion matrix of q^{e_i}, $S = \left(\vec{r}_{1t} \middle| \cdots \middle| \vec{r}_{nt} \right)$ and $e = e_1 \geq \ldots \geq e_k$.

The following Corollary is an immediate consequence of the above result.

Corollary 3.1.7. *If $f = q_1^{e_1} \cdot \ldots \cdot q_k^{e_k}$ is the minimal polynomial of A, where q_i are as in (3.1.1), then there exists a basis $\{\vec{r}_1, \ldots, \vec{r}_n\}$ of $\mathbb{F}_q^n$ such that*

$$A = SRS^{-1} = S \begin{pmatrix} R_1 & & \\ & \ddots & \\ & & R_k \end{pmatrix} S^{-1}$$

with each

$$R_i = \begin{pmatrix} A_{c,q_i^{e_{i1}}} & & \\ & \ddots & \\ & & A_{c,q_i^{e_{is_i}}} \end{pmatrix},$$

where $A_{c,q_i^{e_{ij}}}$ denote the companion matrix of $q_i^{e_{ij}}$ for all $1 \leq j \leq s_i$ and $1 \leq i \leq k$, $S = \left(\vec{r}_{1t} \middle| \cdots \middle| \vec{r}_{nt} \right)$ and $e_i = e_{i1} \geq \ldots \geq e_{is_i}$.

Definition 3.1.8. *The matrix R of* Corollary 3.1.7 *is called the* ***rational canonical form*** *of A.*

Example 3.1.9. *Consider the following matrix with coefficients in $\mathbb{F}_{11}$*

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

By the following Magma *Program*

```
A:=Matrix(GF(11),6,6,[0,0,0,0,1,0,0,0,0,0,0,1,1,0,0,0,0,0,0,1,0,0,0,0,0,0,
1,0,0,0,0,0,0,1,0,0]);
R,T:=RationalForm(A);
R,T^(-1);
```

the rational canonical form of A is

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

$$\textit{that is, } A = SRS^{-1} \textit{ where } S = \begin{pmatrix} 4 & 4 & 4 & 8 & 7 & 7 \\ 3 & 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 7 & 7 & 8 \\ 4 & 4 & 3 & 4 & 4 & 4 \\ 4 & 4 & 4 & 7 & 8 & 7 \\ 4 & 3 & 4 & 4 & 4 & 4 \end{pmatrix}.$$

3.2 Generalized Cyclic Codes

The main results of the previous section says that an $n \times n$ matrix A is similar to its rational canonical form R, i.e. there exists a non-singular matrix S such that

$$A = SRS^{-1}. \tag{3.2.1}$$

Let $\mathscr{C}_A \subseteq \mathbb{F}_q^n$ be a linear code invariant by the matrix A. Define $\mathscr{C}_A \star S := \{\vec{c}S : \vec{c} \in \mathscr{C}_A\}$ and $\mathscr{C}_R := \mathscr{C}_A \star S$. Then by (3.2.1) we obtain

$$\mathscr{C}_R \star R = \mathscr{C}_A \star (SR) = \mathscr{C}_A \star (S(S^{-1}AS)) = (\mathscr{C}_A \star A) \star S \subseteq \mathscr{C}_A \star S = \mathscr{C}_R,$$

i.e. $\mathscr{C}_R$ is invariant by R. Since S is an invertible matrix, this shows that we can construct a *one-to-one* correspondence between the set of linear codes invariant by A and the set of linear codes invariant by R.

By using this argument, we first reduce the study of linear codes invariant by a matrix to that of linear codes invariant by companion matrices. The general case will be consider in Chapter 4.

Definition 3.2.1. *A linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ is called φ-**generalized cyclic code**, or simply φ-**GC code**, if it is invariant by the linear transformation*

$$\varphi : \ (c_0, c_1, \ldots, c_{n-1}) \mapsto (f_0 c_{n-1}, c_0 + f_1 c_{n-1}, \ldots, c_{n-2} + f_{n-1} c_{n-1})$$

where $f_0, \ldots, f_{n-1} \in \mathbb{F}_q$ and $f_0 \neq 0$.

Remark 3.2.2. *The linear transformation φ can be represented by the right multiplication of the following matrix*

$$A_c := \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline f_0 & f_1 & \cdots & f_{n-1} \end{array}\right), \tag{3.2.2}$$

where $det(A_c) = f_0 \neq 0$. Then a linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$ is a φ-GC code if only if $\mathscr{C} \star A_c = \mathscr{C}$.

From now on, by Remark 3.2.2 we simply refer to a φ-GC code as an A_c-**GC code** and viceversa, where φ and A_c are as in Definition 3.2.1 and the equation (3.2.2) respectively.

Remark 3.2.3. *If $\mathscr{C} \subseteq \mathbb{F}_q^n$ is an A_c-GC code with $f_1 = \ldots = f_{n-1} = 0$, then $\mathscr{C}$ is an f_0-constacyclic code, i.e. $\mathscr{C}$ is invariant by the matrix*

$$\overline{P} := \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline f_0 & 0 & \ldots & 0 \end{array}\right),$$

. In particular, if furthermore $f_0 = 1$, then $\mathscr{C}$ is a cyclic code.

Proposition 3.2.4. *If $\mathscr{C} \subseteq \mathbb{F}_q^n$ is an A_c-GC code, then $\mathscr{C}^\perp \star (A_c)_t = \mathscr{C}^\perp$, where $\mathscr{C}^\perp$ is the dual code of $\mathscr{C}$.*

Proof. If $\vec{a} \in \mathscr{C}^\perp$, then we have

$$\vec{a}(A_c)_t \cdot \vec{c} = \vec{a}(A_c)_t \vec{c}_t = \vec{a}(\vec{c}A_c)_t = \vec{a} \cdot (\vec{c}A_c) = 0, \quad \forall \vec{c} \in \mathscr{C}.$$

Since $\dim(\mathscr{C}^\perp) = \dim(\mathscr{C}^\perp \star (A_c)_t)$, we conclude that $\mathscr{C}^\perp \star (A_c)_t = \mathscr{C}^\perp$. □

The following consequence of Proposition 3.2.4 is well-know (see [21], Proposition 4).

Corollary 3.2.5. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be an f_0-constacyclic code, then $\mathscr{C}^{\perp}$ is an f_0^{-1}-constacyclic code.*

Proof. Note that $A_c = \left(\begin{array}{c|c} \vec{0}_t & I \\ \hline f_0 & \vec{0} \end{array}\right)$ and $f_0^{-1}A_c^{n-1} = \left(\begin{array}{c|c} \vec{0}_t & I \\ \hline f_0^{-1} & \vec{0} \end{array}\right)$. By Proposition 3.2.4, it follows that $\mathscr{C}$ is invariant under $\left(\begin{array}{c|c} \vec{0}_t & I \\ \hline f_0^{-1} & \vec{0} \end{array}\right)$. □

Remark 3.2.6. Theorem 2.1.2 *is a consequence of* Corollary 3.2.5 *when* $f_0 = 1$.

Consider now the polynomial ring $R := \mathbb{F}_q[X]$ with the usual addition and multiplication.

Denote by

$$f = X^n - \sum_{i=0}^{n-1} f_i X^i \in R$$

a polynomial of degree n. Define $\pi_f : \mathbb{F}_q^n \to R/Rf$ as the linear transformation defined by

$$\pi_f((c_0, ..., c_{n-1})) := \left[\sum_{i=0}^{n-1} c_i X^i\right] \in R/Rf \qquad \forall\ (c_0, ..., c_{n-1}) \in R.$$

Consider the companion matrix of f given by

$$A_c = \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline f_0 & f_1 & \cdots & f_{n-1} \end{array}\right).$$

Proposition 3.2.7. *A non-empty subset $\mathscr{C}$ of $\mathbb{F}_q^n$ is an A_c-GC code if and only if $\pi_f(\mathscr{C})$ is an ideal of R/Rf.*

Proof. Observe that for any $\vec{c} = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n$ we have

$$\begin{aligned} X \cdot \pi_f(\vec{c}) &= [c_0 X + \cdots + c_{n-2}X^{n-1} + c_{n-1}X^n] \\ &= [f_0 c_{n-1} + (c_0 + f_1 c_{n-1})X + \cdots + (c_{n-2} + f_{n-1}c_{n-1})X^{n-1}] = \pi_f(\vec{c}A_c). \end{aligned}$$

The rest of the proof is similar to that of Theorem 2.2.1. □

Remark 3.2.8. *From* Proposition 3.2.7, *we can deduce that* $X^k \cdot \pi_f(\vec{v}) = \pi_f((\vec{v})(A_c^k))$ *for all* $\vec{v} \in \mathbb{F}_q^n$ *and* $k \in \mathbb{N}$.

As in §2 of Chapter 2, the following definition makes sense.

Definition 3.2.9. *For an* A_c*-GC code* $\mathscr{C} \subseteq \mathbb{F}_q^n$*, the generator polynomial of* $\pi_f(\mathscr{C})$ *is called the* ***generator polynomial*** *of* $\mathscr{C}$*.*

Remark 3.2.10. Theorems 2.2.9, 2.2.10 *and* Corollary 2.2.7 *hold with* f *instead of* $X^n - 1$.

If $\mathscr{C} \subseteq \mathbb{F}_q^n$ is an A_c-GC code with generator polynomial $g = g_0 + \cdots + g_{n-k}X^{n-k} \in R/Rf$, we simply write $\mathscr{C} = (g)_{n,q}^k$.

By Remark 3.2.10 we can focus on finding divisors of f to construct A_c-GC codes.

Example 3.2.11. *Let* $f = \alpha^2 + \alpha X + X^3 + X^4 \in \mathbb{F}_4[X]$*, where* $\mathbb{F}_4 := \mathbb{F}_2[\alpha] \cong \mathbb{F}_2[X]/(X^2+X+1)$ *and* $\alpha \in \mathbb{F}_q$ *is such that* $\alpha^2 + \alpha + 1 = 0$*. Since* $f = (\alpha + X^2) \cdot (\alpha + X + X^2)$*, the linear codes* $\mathscr{C}_1 = (\alpha + X^2)_{4,4}^2$ *and* $\mathscr{C}_2 = (\alpha + X + X^2)_{4,4}^2$ *are* A_c*-GC codes, where*

$$A_c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \alpha^2 & \alpha & 0 & 1 \end{pmatrix}.$$

Remark 3.2.12. *Let* $\mathscr{C} = (g)_{n,q}^k$ *be an* A_c*-GC code and take* $[h] \in ([g])$ *such that* $[h] = [p \cdot g]$ *for some* $p \in R$*, where* $[a]$ *is the class of the polynomial* a *in* R/Rf*. Observe that* $[h] = [h']$ *for some* $h' \in R$ *with* $\deg(h') \leq n-1$*. Since* $[h'] = [p \cdot g]$ *we deduce that* $h' = p \cdot g + q \cdot f$ *for some* $q \in R$*. By the Division Algorithm write* $p \cdot g = q' \cdot f + r'$ *for some* $q', r' \in R$ *such that* $\deg(r') \leq \deg(f) - 1 = n-1$*. This gives* $r' = p' \cdot g$ *for some* $p' \in R$*. Note that* $\deg(p') \leq \deg(r') - \deg(g) - 1 \leq \deg(f') - \deg(g) - 1$*. Then we have*

$$[h] = [h'] = [p \cdot g] = [r'] = [p'][g],$$

i.e. for any $[h] \in ([g])$ *we can write* $[h] = [p'][g]$ *with*

$$p' = \sum_{i=0}^{deg(f)-deg(g)-1} p'_i X^i.$$

3.3 Generator and parity-check matrices

As in §3 of Chapter 2, the generator polynomial characterizes an A_c-GC code.

Theorem 3.3.1. *If $\mathscr{C} = (g)_{n,q}^k$ is an A_c-GC code with $g = g_0 + \cdots + g_{n-k}X^{n-k}$, then*

$$G = \begin{pmatrix} \pi_f^{-1}(g) \\ \pi_f^{-1}(g)A_c \\ \vdots \\ \pi_f^{-1}(g)A_c^{k-1} \end{pmatrix}$$

is a generator matrix of $\mathscr{C}$.

Proof. The proof is similar to that of Theorem 2.3.1. □

Example 3.3.2. *Let f and A_c be as in* Example 3.2.11. *Consider $\mathscr{C} = (\alpha + X + X^2)_{4,4}^2$. Then a generator matrix for $\mathscr{C}$ is*

$$G = \begin{pmatrix} (\alpha, 1, 1, 0) \\ (\alpha, 1, 1, 0)A_c \end{pmatrix} = \begin{pmatrix} \alpha & 1 & 1 & 0 \\ 0 & \alpha & 1 & 1 \end{pmatrix}.$$

The following result provides a matrix in standard form for the dual code of an A_c-GC code. This allows us to encode and decode easily. Moreover, by Corollary 1.4.7 the distance of the code can be calculated immediately.

Proposition 3.3.3. *Let $\mathscr{C} = (g)_{n,q}^k$ be an A_c-GC code. For any integer i such that $0 \leq i \leq k-1$, write in R*

$$X^{n-k+i} = q_i \cdot g + r_i, \text{ with } 0 \leq \deg r_i < n-k.$$

Denote by T the following matrix

$$T := \begin{pmatrix} \rho_{n-k}(\pi_f^{-1}(r_0)) \\ \rho_{n-k}(\pi_f^{-1}(r_1)) \\ \vdots \\ \rho_{n-k}(\pi_f^{-1}(r_{k-1})) \end{pmatrix},$$

where ρ_{n-k} is the projection map onto the first $n-k$ coordinates, i.e.

$$\rho_{n-k}(v_1, ..., v_{n-k}, v_{n-k+1}, ..., v_n) := (v_1, ..., v_{n-k}).$$

Then a parity check matrix H of $\mathscr{C}$ is given by $H := \left(\begin{array}{c|c} I_{n-k} & T_t \end{array}\right)$, where I_{n-k} is the $(n-k)\times(n-k)$ identity matrix and T_t is the transpose matrix of T.

Proof. Since $\deg r_i < n-k$, note that

$$\pi_f^{-1}(X^{n-k+i} - r_i) \in \mathscr{C}$$

are linearly independent for $0 \le i \le k-1$. Thus $\left(\begin{array}{c|c} -T & I_k \end{array}\right)$ is a generator matrix for $\mathscr{C}$. Since $(\mathscr{C}^{\perp})^{\perp} = \mathscr{C}$, this implies that the matrix H as in the statement is a parity check matrix for the code $\mathscr{C}$. □

The MAGMA Program 0 (Ch. 5) gives the list of all the reminders r_i of Proposition 3.3.3 which we need to construct the parity check matrix H as in the above result.

Remark 3.3.4. Proposition 3.3.3 *gives immediately the generator matrix and the parity-check matrix of $\mathscr{C}$ in standard form. Moreover in the cyclic case, this result is useful in the syndrome decoding (see* Ch. 2, §2.4.1*).*

Example 3.3.5. *Write $f = \alpha^2 + \alpha X + X^3 + \alpha X^4 + \alpha X^6 + X^7 + X^8 \in \mathbb{F}_4[X]$ and let $\mathscr{C} = (\alpha^2 + X^2 + \alpha^2 X^3 + X^4)_8^4$ be an A_c-GC code, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$ and*

$$A_c = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ \alpha^2 & \alpha & 0 & 1 & \alpha & 0 & \alpha & 1 \end{pmatrix}.$$

Divide X^{4+i} *by* $\alpha^2 + X^2 + \alpha^2 X^3 + X^4$ *for* $i = 1, \dots, 4$. *By MAGMA* Program 0 *(Ch. 5) we obtain*

$$r_1 = \alpha^2 + X^2\alpha^2X^3, \qquad r_2 = \alpha + \alpha^2 X + \alpha^2 X^2 + \alpha^2 X^3,$$

$$r_3 = \alpha + \alpha X + X^3, \qquad r_4 = \alpha^2 + \alpha X + \alpha^2 X^2 + \alpha^2 X^3.$$

Then by Proposition 3.3.3 *we have*

$$T = \begin{pmatrix} \alpha^2 & 0 & 1 & \alpha^2 \\ \alpha & \alpha^2 & \alpha^2 & \alpha^2 \\ \alpha & \alpha & 0 & 1 \\ \alpha^2 & \alpha & \alpha^2 & \alpha^2 \end{pmatrix}.$$

Hence

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & \alpha^2 & \alpha & \alpha & \alpha^2 \\ 0 & 1 & 0 & 0 & 0 & \alpha^2 & \alpha & \alpha \\ 0 & 0 & 1 & 0 & 1 & \alpha^2 & 0 & \alpha^2 \\ 0 & 0 & 0 & 1 & \alpha^2 & \alpha^2 & 1 & \alpha^2 \end{pmatrix}$$

is the parity-check matrix of $\mathscr{C} \subseteq \mathbb{F}_4^8$ *in standard form.*

3.4 Generalized cyclic codes as invariants subspaces

Since linear codes are linear subspaces of $\mathbb{F}_q^n$, the description of generalized cyclic codes in terms of linear algebra becomes natural. Observe that the linear transformation φ as in Definition 3.2.1 is a linear operator on $\mathbb{F}_q^n$. Our approach is to consider generalized cyclic codes as invariant subspaces of $\mathbb{F}_q^n$ with respect to this operator and then to obtain a description of them.

Let φ and

$$A_c = \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline a_0 & a_1 & \cdots & a_{n-1} \end{array}\right)$$

be as in Definition 3.2.1.

The characteristic polynomial χ_{A_c} of A_c is

$$\chi_\varphi := \chi_{A_c} = \det \begin{pmatrix} -X & 1 & & \\ \vdots & -X & \ddots & \\ 0 & & -X & 1 \\ a_0 & a_1 & \cdots & a_{n-1}-X \end{pmatrix} = (-1)^n(X^n - a_{n-1}X^{n-1} - \ldots - a_1X - a_0).$$

For simplicity, we will write χ instead of χ_{A_c} or χ_φ.

Definition 3.4.1. *A subspace U of $\mathbb{F}_q^n$ is said φ-invariant if $\varphi(\vec{u}) \in U$ for all $\vec{u} \in U$.*

For our purposes we need the following well known fact.

Proposition 3.4.2 ([9], Lemma 6.6.1.)**.** *Let U be a φ-invariant subspace of $\mathbb{F}_q^n$. Then $\chi_{\varphi_{|U}}$ divides χ_φ, where $\chi_{\varphi_{|U}}$ is the characteristic polynomial of $\varphi_{|U}$. In particular, if $\mathbb{F}_q^n = U \oplus W$ and W is a φ-invariant subspace of $\mathbb{F}_q^n$, then $\chi_\varphi = \chi_{\varphi_{|U}}\chi_{\varphi_{|W}}$.*

Lemma 3.4.3. *Let K be a finite field and let A be a square matrix with coefficients in K. Then*

$$K[X]/(m_A) \cong K[A],$$

where m_A is the minimal polynomial of A.

Proof. Consider the module homomorphism $\sigma : K[X] \to K[A]$, defined by $p \mapsto p(A)$. By construction, σ is an onto homomorphism and $\ker(\sigma) = (m_A)$. Then there exists an isomorphism $\overline{\sigma}$ between $K[X]/(m_A)$ and $K[A]$. Moreover, $\overline{\sigma}$ is defined by $[p] \mapsto p(A)$, where $[p]$ is the class of a polynomial p. □

Remark 3.4.4. *If $p = q$ in $K[X]$, then $[p] = [q]$ in $K[X]/(m_A)$. Thus $p(A) = q(A)$ via $\overline{\sigma}$.*

Let $\chi = (-1)^n \chi_1 \cdot \ldots \cdot \chi_t$ be the factorization of χ into irreducible factors over $\mathbb{F}_q[X]$. According to Cayley-Hamilton Theorem, the matrix A_c satisfies

$$\chi(A_c) = O, \text{ where } O \text{ is the null matrix.}$$

Moreover, A_c is a companion matrix and the polynomial χ is equal to the minimal polynomial of A_c.

Lemma 3.4.5. *Let $f = b_0 + b_1X + \ldots + b_nX^n$ be a polynomial of degree n in $\mathbb{F}_q[X]$. Denote by $f_1 \cdot \ldots \cdot f_t$ the factorization of f into irreducible factors over $\mathbb{F}_q[X]$. Then, $f_i \neq f_j$ for all $i \neq j$, if and only if $\gcd(f, \partial f) = 1$, where $\partial f := nX^{n-1} - \sum_{i=1}^{n-1} ia_iX^{i-1}$ is the usual first derivative of f.*

Proof. Write $q = p^s$ for some prime number $p = \mathrm{Char}(\mathbb{F}_q)$ and $s \in \mathbb{N}_{>0}$. Assume that $f = g^2 \cdot h$ with $g, h \in \mathbb{F}_q[X]$ and $\deg g \geq 1$. Then $\partial f = 2g \cdot \partial g \cdot h + g^2 \cdot \partial h = g(2\partial g \cdot h + g \cdot \partial h)$, so $\gcd(f, \partial f) \neq 1$. This proves the "if" part of the statement. Suppose now that $\gcd(f, \partial f) = d$ with $\deg(d) \geq 1$. If d is not irreducible, take an irreducible factor of d and write $f = d' \cdot h$, where $h \in \mathbb{F}_q[X]$ and $\deg(d') \geq 1$. Hence $\partial f = \partial d' \cdot h + d' \cdot \partial h$. Since d' divides also ∂f, we see that d' divides $\partial d' \cdot h$. Because of the irreducibility of d', it follows that either d' divides $\partial d'$ or d' divides h. If d' divides h, we have $f = d'^2 \cdot h'$ for some $h' \in \mathbb{F}_q[X]$. On the other hand, if d' divides $\partial d'$, then $\partial d' = 0$, since $0 \leq \deg(\partial d') < \deg(d')$.

Claim. $d' = \sum d_iX^{ph_i}$. Write $d' = \sum d_iX^{m_i} = d_0X^{m_0} + d_1X^{m_1} + \ldots + d_sX^{m_s}$, with $d_i \neq 0$ and $m_0 < m_1 < \ldots < m_s$. Since $0 = \partial d' = d_0m_0X^{m_0-1} + d_1m_1X^{m_1-1} + \ldots + d_sm_sX^{m_s-1} = X^{m_0-1}(d_0m_0 + d_1m_1X^{m_1-m_0} + \ldots + d_sm_sX^{m_s-m_0})$ and since $\mathbb{F}_q[X]$ is an integer domain, we obtain that $d_0m_0 + d_1m_1X^{m_1-m_0} + \ldots + +d_sm_sX^{m_s-m_0}$ is the zero polynomial. Thus when $X = 0$, since $d_0 \neq 0$, we deduce $m_0 = 0$, i.e. $m_0 = ph_0$ for some $h_0 \in \mathbb{F}_q$. By an inductive argument, we can conclude that $m_s = ph_s$ for some $h_s \in \mathbb{F}_q$ and for any $s = 0, \ldots, \deg(d')$. Q.E.D.

Since the Frobenius map $a \mapsto a^p$ is an automorphism of $\mathbb{F}_q$, we can write

$$d' = \sum d_iX^{ph_i} = \sum e_i^pX^{ph_i} = \left(\sum e_iX^{h_i}\right)^p \text{ for some } e_i,$$

but this gives a contradiction. □

Remark 3.4.6. *When $f = X^n - a$ with $a \in \mathbb{F}_q \backslash \{0\}$, the condition $\gcd(f, \partial f) = 1$ is also equivalent to $\gcd(n, p) = 1$, where p is the characteristic of $\mathbb{F}_q$.*

From now on, assume that $\gcd(\chi, \partial\chi) = 1$, where χ is the characteristic polynomial of A_c. In this case χ has distinct factors $\chi_i \in \mathbb{F}_q[X]$ such that their leader coefficients are ±1 for every $i = 1, \ldots, t$. Furthermore, consider the set of homogeneous equations

$$\vec{x}\chi_i(A_c) = \vec{0}, \ \vec{x} \in \mathbb{F}_q^n \tag{3.4.1}$$

for $i = 1, \ldots, t$. If U_i is the solution space of equation (3.4.1), then we write $U_i = \mathrm{Ker}\chi_i(A_c)$.

Theorem 3.4.7. *The subspaces U_i of $\mathbb{F}_q^n$ satisfy the following conditions:*

(a) *U_i is a φ-invariant subspace of $\mathbb{F}_q^n$;*

(b) *if W is a φ-invariant subspace of $\mathbb{F}_q^n$ and $W_i := W \cap U_i$ for $i = 1, \dots, t$, then W_i is a φ-invariant subspace of $\mathbb{F}_q$ and $W = W_1 \oplus \cdots \oplus W_t$;*

(c) *$\mathbb{F}_q^n = U_1 \oplus \cdots \oplus U_t$;*

(d) *$\dim U_i = \deg(\chi_i)$;*

(e) *$\chi_{\varphi_{|U_i}} = (-1)^{k_i}\chi_i$;*

(f) *U_i is a minimal φ-invariant subspace of $\mathbb{F}_q^n$.*

Proof. (a) Let $\vec{u} \in U_i$. Then we have $\vec{u}\chi_i(A_c) = \vec{0}$. Hence $\varphi(\vec{u})\chi_i(A_c) = \vec{u}A_c\chi_i(A_c) = \vec{u}\chi_i(A_c)A_c = \vec{0}A_c = \vec{0}$, i.e. $\varphi(\vec{u}) \in U_i$.

(b) Denote by $\widehat{\chi}_i := \frac{\chi}{\chi_i}$ for every $i = 1 \dots, t$. Since the χ_i's are all distinct irreducible polynomial, we get $\gcd(\widehat{\chi}_1, \dots, \widehat{\chi}_t) = 1$. Then, by Bézout's identity there exist polynomials $a_1, \dots, a_t \in \mathbb{F}_q[X]$ such that

$$a_1 \cdot \widehat{\chi}_1 + \cdots + a_t \cdot \widehat{\chi}_t = 1.$$

By Remark 3.4.4, for every vector $\vec{w} \in W$ the equality $\vec{w} = \vec{w}a_1(A_c)\widehat{\chi}_1(A_c) + \cdots + \vec{w}a_t(A_c)\widehat{\chi}_t(A_c)$ holds. Define $\vec{w}_i = \vec{w}a_i(A_c)\widehat{\chi}_i(A_c) \in W$. Then $\vec{w}_i\chi_i(A_c) = \vec{w}a_i(A_c)\widehat{\chi}_i(A_c)\chi_i(A_c) = \vec{w}a_i(A_c)\chi(A_c) = \vec{w}a_i(A_c)O = \vec{0}$, and so $\vec{w}_i \in U_i \cap W = W_i$. Hence we can write

$$W = W_1 + \cdots + W_t.$$

Assume now that $\vec{w} \in W_i \cap \sum_{i \neq j} W_j$. If $\vec{w} \in \sum_{i \neq j} W_j$ then $\vec{w} = \sum_{i \neq j} \vec{w}_j$ and so $\vec{w}\widehat{\chi}_i(A_c) = (\sum_{i \neq j} \vec{w}_j)\widehat{\chi}_i(A_c) = \sum_{i \neq j} \vec{w}_j\widehat{\chi}_i(A_c) = \vec{0}$. Since $\vec{w} \in W_i \subset U_i$, by definition we have $\vec{w}\chi_i(A_c) = \vec{0}$. Since $\gcd(\chi_i, \widehat{\chi}_i) = 1$, we know that there exist polynomials $a, b \in \mathbb{F}_q[X]$ such that $\chi_i \cdot a + \widehat{\chi}_i \cdot b = 1$. Hence

$$\vec{w} = \vec{w}a(A_c)\chi_i(A_c) + \vec{w}b(A_c)\widehat{\chi}_i(A_c) = \vec{0},$$

and this give $W_i \cap \sum_{i \neq j} W_j = \{\vec{0}\}$ for every $i =, \dots, t$. Then $W = W_1 \oplus \cdots \oplus W_t$.

(c) This follows from $b)$ with $W = \mathbb{F}_q^n$.

(d) Take $\vec{g} \in U_i$ with $\vec{g} \neq \vec{0}$. Let $k_i \geq 1$ be the smallest positive integer such that $\vec{g}I, \vec{g}A_c, \ldots, \vec{g}A_c^{k_i}$ are linearly dependent. Then there exist $c_0, \ldots, c_{k_i-1} \in \mathbb{F}_q$ such that

$$\vec{g}A_c^k = c_0\vec{g}I + \cdots + c_{k-1}\vec{g}A_c^{k_i-1}.$$

Define $t := X^{k_i} - c_{k_i-1}X^{k_i-1} - \ldots - c_0$. Since $\vec{g}t(A_c) = \vec{g}\chi_i(A_c) = \vec{0}$ and $\gcd(t, \chi_i) = t \cdot a + \chi_i \cdot b$ for some $a, b \in \mathbb{F}_q[X]$, we see that $\vec{g}[\gcd(t, \chi_i)(A_c)] = \vec{0}$. Since χ_i is irreducible, $\gcd(t, \chi_i)$ is either 1 or χ_i. Suppose that $\gcd(t, \chi_i) = 1$. Then

$$\vec{0} = \vec{g}t(A_c)a(A_c) + \vec{g}\chi_i(A_c)b(A_c) = \vec{g},$$

but this give a contradiction. So $\gcd(t, \chi_i) = \chi_i$ and $\deg(\chi_i) \leq \deg(t) = k_i$.

On the other hand, the vectors $\vec{g}, \vec{g}A_c, \ldots, \vec{g}A_c^{\deg(\chi_i)}$ are linearly dependent, since $\vec{g}\chi_i(A_c) = \vec{0}$. From the minimality of k_i, we get $k_i = \deg(\chi_i)$. Then $\dim(U_i) \geq \deg(\chi_i)$ because $\vec{g}, \vec{g}A_c, \ldots, \vec{g}A_c^{\deg(\chi_i)-1}$ are linearly independent. Therefore by (c) we obtain that

$$n = \dim(\mathbb{F}_q^n) = \sum_{i=1}^{t} \dim(U_i) \geq \sum_{i=1}^{t} deg\chi_i = deg(\chi) = n,$$

i.e. $\dim(U_i) = \deg(\chi_i)$.

(e) Let $g^{(i)} = \{\vec{g}_1^{(i)}, \ldots, \vec{g}_{\deg(\chi_i)}^{(i)}\}$ be a basis of U_i over $\mathbb{F}_q$, for $i = 1, \ldots, t$ and let A_i be the matrix of $\varphi_{|U_i}$ with respect to $g^{(i)}$. Let $\chi_{\varphi_{|U_i}}$ be as Proposition 3.4.2. Suppose that $\gcd(\chi_{\varphi_{|U_i}}, \chi_i) = 1$. Hence there are polynomials $a, b \in \mathbb{F}_q[X]$ such that $a(A_i)\chi_{\varphi_{|U_i}}(A_i) + b(A_i)\chi_i(A_i) = I$. Since $\chi_{\varphi_{|U_i}}(A_i) = O$, we obtain that $b(A_i)\chi_i(A_i) = I$.

By Property (c) we see that $\mathfrak{G} = \{\vec{g}_1^{(1)}, \ldots, \vec{g}_{k_1}^{(1)}, \ldots, \vec{g}_1^{(t)}, \ldots, \vec{g}_{k_t}^{(t)}\}$ is a basis of $\mathbb{F}_q^n$ and φ can be represented by

$$A' = \begin{pmatrix} A_1 & & \\ & \ddots & \\ & & A_t \end{pmatrix}$$

with respect to $\mathfrak{G}$. Furthermore, $A' = TAT^{-1}$, where T is the transformation matrix from the standard basis of $\mathbb{F}_q^n$ to the basis g. Let T_i be the matrix which represents the change of basis between $g^{(i)}$ and the corresponding vector of the standard basis of $\mathbb{F}_q^n$. Then $T_iA_iT_i^{-1}$ represents $\varphi_{|U_i}$. Hence

$$\chi_i(A') = \begin{pmatrix} \chi_i(A_1) & & \\ & \ddots & \\ & & \chi_i(A_t) \end{pmatrix} = \chi_i(TA_cT^{-1}) = T\chi_i(A_c)T^{-1}.$$

Put $\vec{g}_j^{(i)} = \lambda_{j1}^{(i)}\vec{e}_1 + \ldots + \lambda_{jn}^{(i)}\vec{e}_n$ for $j = 1, \ldots, \deg(\chi_i)$. Since $\vec{g}_j^{(i)} \in U_i$, we obtain that

$$\vec{e}_\alpha = \chi_i(A') = \vec{e}_\alpha T\chi_i(A_c)T^{-1} = \vec{g}_j^{(i)}\chi_i(A_c)T^{-1} = \vec{0}$$

with $\alpha = k_1 + \ldots k_{i-1} + j$. Thus we have $\chi_i(A_i) = O$ but this contradicts $b(A_i)\chi(A_i) = I$. Therefore $\gcd(\chi_{\varphi_{|U_i}}, \chi_i) \neq 1$. Since χ_i and $\chi_{\varphi_{|U_i}}$ are polynomials of the same degree and χ_i is monic and irreducible, for the Proposition 3.4.2, we can conclude that $\chi_{\varphi_{|U_i}} = (-1)^{k_i}\chi_i$.

(f) Assume that $U \subset U_i$ with $U \neq \{\vec{0}\}$ a $\varphi_{|U_i}$-invariant subspace. Then by Proposition 3.4.2 we know that $\chi_{\varphi_{|U}}$ divides χ_i. Since χ_i is irreducible, we have $\dim(U) = \dim(U_i)$, i.e. $U = U_i$. □

Theorem 3.4.8. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be an A_c-GC code. Then the following facts hold.*

(i) *$\mathscr{C} = U_{i_1} \oplus \cdots \oplus U_{i_s}$ for some minimal φ-invariant subspaces U_{i_r} of $\mathbb{F}_q^n$, where $k := \dim(\mathscr{C}) = k_{i_1} + \cdots + k_{i_s}$, with $k_{i_r} = \dim(U_{i_r})$.*

(ii) *$\chi_{\varphi_{|\mathscr{C}}} = (-1)^k\chi_{i_1} \cdot \ldots \cdot \chi_{i_s}$, where $\chi_{i_j} = \chi_{\varphi_{|U_{i_j}}}$.*

(iii) *$\vec{c} \in \mathscr{C}$ if and only if $\vec{c}\chi_{\varphi_{|\mathscr{C}}}(A_c) = \vec{0}$.*

(iv) *The polynomial $\chi_{\varphi_{|\mathscr{C}}}$ is the minimal polynomial which satisfies the equivalence (iii).*

(v) *$\mathrm{rk}(\chi_{\varphi_{|\mathscr{C}}}(A_c)) = n - k$, where $\mathrm{rk}(\chi_{\varphi_{|\mathscr{C}}}(A_c))$ is the rank of the matrix $\chi_{\varphi_{|\mathscr{C}}}(A_c)$.*

Proof. (i) This follows from Theorem 3.4.7 (b) and (f).

(ii) This is a consequence of Theorem 3.4.7 (e) and its proof.

(iii) Let $\vec{c} \in \mathscr{C}$. Then by (i) we can write $\vec{c} = \vec{u}_{i_1} + \cdots + \vec{u}_{i_s}$ for some $\vec{u}_{i_r} \in U_{i_r}$, $r = 1, \ldots, s$. By commutativity in $\mathbb{F}_q[X]$, we obtain that

$$\vec{c}\chi_{\varphi_{|\mathscr{C}}}(A_c) = (-1)^k[\vec{u}_{i_1}(\chi_{i_1} \cdot \ldots \cdot \chi_{i_s})(A_c) + \cdots + \vec{u}_{i_s}(\chi_{i_1} \cdot \ldots \cdot \chi_{i_s})(A_c)] = \vec{0}.$$

Conversely, suppose that $\vec{c}\chi_{\varphi|_{\mathscr{C}}}(A_c) = \vec{0}$ for some $\vec{c} \in \mathbb{F}_q^n$. According to Theorem 3.4.7 (*c*), we have $\vec{c} = \vec{u}_1 + \cdots + \vec{u}_t$, with $\vec{u}_i \in U_i$. Then

$$\vec{c}\chi_{\varphi|_{\mathscr{C}}}(A_c) = (-1)^k[\vec{u}_1(\chi_{i_1} \cdot \ldots \cdot \chi_{i_s})(A_c) + \cdots + \vec{u}_t(\chi_{i_1} \cdot \ldots \cdot \chi_{i_s})(A_c)] = \vec{0},$$

i.e. $[\vec{u}_{j_1} + \cdots + \vec{u}_{j_l}]\chi_{\varphi|_{\mathscr{C}}}(A_c) = \vec{0}$, where $\{j_1, \ldots, j_l\} = \{1, \ldots, t\} \setminus \{i_1, \ldots, i_s\}$. Denote by $\vec{v} := \vec{u}_{j_1} + \cdots + \vec{u}_{j_l}$ and $h = \chi/\chi_{\varphi|_{\mathscr{C}}} = (-1)^{n-k}\chi_{j_1} \cdot \ldots \cdot \chi_{j_l}$. Since $\gcd(h, \chi_{\varphi|_{\mathscr{C}}}) = 1$, there are two polynomials $a, b \in \mathbb{F}_q[X]$ such that $h \cdot a + \chi_{\varphi|_{\mathscr{C}}} \cdot b = 1$. Hence

$$\vec{v} = \vec{v}h(A_c)a(A_c) + \vec{v}\chi_{\varphi|_{\mathscr{C}}}(A_c)b(A_c) = \vec{0},$$

that is $\vec{c} = \vec{u}_{i_1} + \cdots + \vec{u}_{i_s} \in \mathscr{C}$.

(*iv*) Suppose that $b \in \mathbb{F}_q[X]$ is a non-zero polynomial of smallest degree such that $\vec{c}b(A_c) = \vec{0}$ for all $\vec{c} \in \mathscr{C}$. By division algorithm there are polynomials $q, r \in \mathbb{F}_q[X]$ such that $\chi_{\varphi|_{\mathscr{C}}} = b \cdot q + r$, where $\deg r < \deg b$. Then for each vector $\vec{c} \in \mathscr{C}$ we have $\vec{c}\chi_{\varphi|_{\mathscr{C}}}(A_c) = \vec{c}b(A_c)q(A_c) + \vec{c}r(A_c)$ and hence $\vec{c}r(A_c) = \vec{0}$. But this contradicts the choice of b unless r is identically zero. Thus, b divides $\chi_{\varphi|_{\mathscr{C}}}$. If $\deg b < \deg(\chi_{\varphi|_{\mathscr{C}}})$ then b is a product of some of the irreducible factors of $\chi_{\varphi|_{\mathscr{C}}}$. Up to renaming we can suppose that $b = (-1)^{k_{i_1} + \cdots + k_{i_m}}\chi_{i_1} \cdot \ldots \cdot \chi_{i_m}$ with $m < s$. Let us consider the code $\mathscr{C}' = U_{i_1} \oplus \cdots \oplus U_{i_m} \subset \mathscr{C}$. Take $\vec{c} = \vec{c}_{i_1} + \cdots + \vec{c}_{i_m} + \vec{c}_{i_{m+1}} + \cdots + \vec{c}_{i_s} \in \mathscr{C}$. Write $\vec{a} = \vec{c}_{i_1} + \cdots + \vec{c}_{i_m}$ and $\vec{b} = \vec{c}_{i_{m+1}} + \cdots + \vec{c}_{i_s}$ and note that $\vec{b}b(A_c) = \vec{0}$. Since $\gcd((\chi_{i_1} \cdot \ldots \cdot \chi_{i_m}), (\chi_{i_{m+1}} \cdot \cdots \cdot \chi_{i_s})) = 1$, there exist two polynomials $\alpha, \beta \in \mathbb{F}_q[X]$ such that $\alpha \cdot (\chi_{i_1} \cdot \cdots \cdot \chi_{i_m}) + \beta \cdot (\chi_{i_{m+1}} \cdot \cdots \cdot \chi_{i_s}) = 1$. Thus

$$\begin{aligned}
\vec{b} &= \vec{b}\alpha(A_c) \cdot (\chi_{i_1} \cdot \cdots \cdot \chi_{i_m})(A_c) + \vec{b}\beta(A_c) \cdot (\chi_{i_{m+1}} \cdot \cdots \cdot \chi_{i_s})(A_c) \\
&= \vec{b}b(A_c) \cdot \alpha(A_c) + \vec{b}(\chi_{i_1} \cdot \cdots \cdot \chi_{i_m})(A_c) \cdot \beta(A_c) \\
&= \vec{0}.
\end{aligned}$$

So that $\vec{c} \in \mathscr{C}'$. This contradiction proves the statement.

(*v*) By property (*iii*) $\mathscr{C}$ is the kernel of the linear transformation $\chi_{\varphi|_{\mathscr{C}}}(A_c)$. Then

$$n = \mathrm{rk}(\chi_{\varphi|_{\mathscr{C}}}(A_c)) + \ker \chi_{\varphi|_{\mathscr{C}}}(A_c) = \mathrm{rk}(\chi_{\varphi|_{\mathscr{C}}}(A_c)) + \dim(\mathscr{C}) = \mathrm{rk}(\chi_{\varphi|_{\mathscr{C}}}(A_c)) + k,$$

i.e. $\mathrm{rk}(\chi_{\varphi|_{\mathscr{C}}}(A_c)) = n - k$. □

Corollary 3.4.9. *The matrix whose rows are a set of $n-k$ linearly independent columns of $\chi_{\varphi|_{\mathscr{C}}}(A_c)$ is a parity-check matrix for the code $\mathscr{C} = U_{i_1} \oplus \cdots \oplus U_{i_s} \subseteq \mathbb{F}_q^n$.*

Proof. The statement follows from Theorem 3.4.8 (iii) and (v). □

Corollary 3.4.10. *The matrix G, the rows of which are a set of k linearly independent rows of $(h(A_c))_t$, is a generator matrix of the code $\mathscr{C}$.*

Proof. Since $h(A_c)\chi_{\varphi|_{\mathscr{C}}}(A_c) = \chi(A_c) = O$, note that all the rows h_i of $h(A_c)$ are vectors of $\mathscr{C}$.

We show now that $\mathrm{rk}(h(A_c)) = k$. By Sylvester's rank inequality, we obtain that

$$0 = \mathrm{rk}(O) \geq \mathrm{rk}(\chi_{\varphi|_{\mathscr{C}}}(A_c)) + \mathrm{rk}(h(A_c)) - n,$$

i.e. $\mathrm{rk}(h(A_c)) \leq k$. On the other hand, Sylvester's rank inequality applied to the product $h(A_c) = (-1)^{n-k}\chi_{j_1}(A_c)\cdots\chi_{j_l}(A_c)$ gives us that $\mathrm{rk}(h(A_c)) \geq \mathrm{rk}(\chi_{j_1}(A_c)) + \cdots + \mathrm{rk}(\chi_{j_l}(A_c)) - n(l-1) = \mathrm{rk}(\chi_{\varphi|_{U_{j_1}}}(A_c)) + \cdots + \mathrm{rk}(\chi_{\varphi|_{U_{j_l}}}(A_c)) - nl + n = n - \dim(\ker(\chi_{\varphi|_{U_{j_1}}}(A_c))) - \ldots - \dim(\ker(\chi_{\varphi|_{U_{j_l}}}(A_c))) = n - (\dim(U_{j_1}) + \cdots + \dim(U_{j_l})) = n - (k_{j_1} + \cdots + k_{j_l}) = n - (n - k_{i_1} - \ldots - k_{i_s}) = n - (n-k) = k$. Therefore $\mathrm{rk}(h(A_c)) = k$. □

Example 3.4.11. *Consider the finite field $\mathbb{F}_4 = \mathbb{F}[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$ and the matrix*

$$A_c = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & \alpha & 1 & \alpha^2 & \alpha^2 & \alpha \end{pmatrix}.$$

Thus we have

$$\chi_\varphi = \chi_{A_c} = 1 + X + \alpha X^2 + X^3 + \alpha^2 X^4 + \alpha^2 X^5 + \alpha X^6 + X^7.$$

By the Magma command `Factorization` *we obtain*

$$\chi_\varphi = \chi_1 \cdot \chi_2 \cdot \chi_3 \cdot \chi_4 = (1+X)\cdot(\alpha+X)\cdot(\alpha^2+X+X^2)\cdot(1+X+X^3).$$

The factors χ_i *define minimal* φ*-invariant subspaces* U_i*, for* $i = 1, 2, 3, 4$*. Define the* A_c*-GC code*

$$\mathscr{C} := U_2 \oplus U_3.$$

According to Theorem 3.4.8(a)*, we have* $\dim(\mathscr{C}) = 3$ *and*

$$g := \chi_{\varphi_{|\mathscr{C}}} = (\alpha + X) \cdot (\alpha^2 + X + X^2) = 1 + X + \alpha^2 X^2 + X^3.$$

So the by Magma Program

```
A:=Matrix(F,7,7,[0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1,0,0,
0,0,0,0,0,1,0,0,0,0,0,0,0,1,1,1,w,1,w^2,w^2,w]);
g:=X^3+w^2*X^2+X+1;
gA:=A^3+w^2*A^2+A+E;
```

it follows that

$$g(A_c) = \begin{pmatrix} 1 & 1 & \alpha^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & \alpha^2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & \alpha^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & \alpha^2 & 1 \\ 1 & 1 & \alpha & 1 & \alpha & \alpha & 1 \\ 1 & 0 & \alpha^2 & \alpha^2 & \alpha & 1 & 0 \\ 0 & 1 & 0 & \alpha^2 & \alpha^2 & \alpha & 1 \end{pmatrix}.$$

By Theorem 3.4.8 (v) *the rank of this matrix is* $\operatorname{rk}(g(A_c)) = 7 - 3 = 4$*. If we take the last 4 linearly independent columns of* $g(A_c)$*, then by* Proposition 3.4.9 *we have the following parity check matrix for the code* $\mathscr{C}$

$$H = \begin{pmatrix} 1 & \alpha^2 & 1 & 1 & 1 & \alpha^2 & \alpha^2 \\ 0 & 1 & \alpha^2 & 1 & \alpha & \alpha & \alpha^2 \\ 0 & 0 & 1 & \alpha^2 & \alpha & 1 & \alpha \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Furthermore, since $h = \chi/g = (1+X) \cdot (1+X+X^3) = 1+X^2+X^3+X^4$*, by the Magma command s*

```
h:=1+X^2+X^3+X^4;
```

```
hA:=E+A^2+A^3+A^4;
```

we get

$$h(A_c)=\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & \alpha & 0 & \alpha^2 & \alpha & \alpha^2 \\ \alpha^2 & \alpha & 0 & 1 & \alpha & 1 & \alpha^2 \\ \alpha^2 & 0 & \alpha^2 & \alpha^2 & \alpha^2 & 0 & 0 \\ 0 & \alpha^2 & 0 & \alpha^2 & \alpha^2 & \alpha^2 & 0 \end{pmatrix}.$$

From the Magma command

```
gA*hA;
```

it follows $h(A_c)g(A_c) = O$ *and* $\mathrm{rk}(h(A_c)) = 3$. *By* Proposition 3.4.10, *if we take* 3 *linearly independent rows of* $h(A_c)$, *then we obtain the following generator matrix of* $\mathscr{C}$

$$G=\begin{pmatrix} 1 & 0 & 0 & 1 & \alpha^2 & \alpha^2 & \alpha^2 \\ 0 & 1 & 0 & 1 & \alpha & 0 & \alpha^2 \\ 0 & 0 & 1 & \alpha^2 & \alpha^2 & 0 & 0 \end{pmatrix}.$$

3.5 A construction of an A_c-GC code

First of all, inspired by [14], let us give here the following definitions.

Definition 3.5.1. *An* A_c*-GC code* $\mathscr{C}$ *is a code of type* $[n,k,d]_q$ *if* $\mathscr{C} \subseteq \mathbb{F}_q^n$, $\dim(\mathscr{C}) = k$ *and* $d(\mathscr{C}) = d$.

Definition 3.5.2.

$$D_q^{A_c}(n,k) := \max\{d \mid \exists \text{ an } A_c\text{−GC code of type } [n,k,d]_q\}$$

Similarly to [14, Proposition 3.1], we have the following

Proposition 3.5.3.

$$D_q^{A_c}(n,k) \geq D_q^{A_c}(n+1,k+1).$$

Proof. Let $g = g_0 + g_1X + ... + g_{n-k}X^{n-k}$ be the generator polynomial of an A_c-GC code $\mathscr{C}_{n+1,k+1}$ with parameters $[n+1, k+1, D_q^{A_c}(n+1,k+1)]$. Observe that g_0 and g_{n-k} are distinct to zero and that the generator matrix $G_{n+1,k+1}$ of $\mathscr{C}_{n+1,k+1}$ has the form

$$\left(\begin{array}{c|cccccc} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ \hline 0 & & & & & & \\ \vdots & & & G_{n,k} & & & \\ 0 & & & & & & \end{array}\right),$$

where $G_{n,k}$ is the following matrix

$$\begin{pmatrix} g_0 & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{n-k} & \dots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \dots & 0 & g_0 & \dots & g_{n-k} \end{pmatrix}.$$

Note that the minimum (Hamming) distance obtained from $G_{n,k}$ is at least $D_q^{A_c}(n+1,k+1)$. Since g can be considered as also a generator polynomial of an A_c-GC code $\mathscr{C}_{n,k}$ of type $[n,k,d]_q$ with $d \geq D_q^{A_c}(n+1,k+1)$, we get $D_q^{A_c}(n,k) \geq d \geq D_q^{A_c}(n+1,k+1)$. □

Remark 3.5.4. *If $\mathscr{C}$ is an A_c-GC code of type $[n,k,\Delta]_q$ with distance $\Delta \geq 1$, then we have $D_q^{A_c}(n,k) \geq \Delta$. Therefore by* Proposition 3.5.3 *we see that for any integer δ such that $0 \leq \delta < k$ there exists at least an A_c-GC code $\mathscr{C}'$ of type $[n-\delta, k-\delta, d]_q$ with $d \geq \Delta \geq 1$. Thus the above result can be useful to ensure the existence and the construction of A_c-GC code's of type $[n,k,d]_q$ with distance d greater than or equal to some fixed value Δ and small values for n and k.*

In what follows we try to construct vectors $\vec{v} \in \mathbb{F}_q^n$ such that $1 \leq \dim[\vec{v}] \leq k$ for some integer $k < n$, where $[\vec{v}] \subset \mathbb{F}_q^n$ is the vector subspace generated by $\{\vec{v}, \vec{v}A_c, \vec{v}A_c^2, ...\}$.

For any integer h such that $1 \leq h \leq n-1$, consider the equation

$$\vec{v}A_c^h x_h + ... + \vec{v}A_c^1 x_1 + \vec{v}x_0 = \vec{0}. \tag{3.5.1}$$

If there exist a non-trivial vector $\vec{v}$ and non-zero $x_h \in \mathbb{F}_q$ which satisfy the above equation (3.5.1), we can deduce that $\vec{v}A_c^h$ can be written as a linear combination of vectors in $\{\vec{v}, \vec{v}A_c, ..., \vec{v}A_c^{h-1}\}$, i.e. $1 \leq \dim[\vec{v}] \leq h$.

Thus the existence of a non-trivial vector $\vec{v} \in \mathbb{F}_q^n$ which satisfies equation (3.5.1) is ensured by the existence of non-trivial solutions $x_h, ..., x_1, x_0$ of the equation

$$\det(A_c^h x_h + ... + A_c x_1 + I x_0) = 0. \tag{3.5.2}$$

So we have reduced the problem of finding a vector $\vec{v} \neq \vec{0}$ in $\mathbb{F}_q^n$ which is a solution of (3.5.1) to the problem of finding non-trivial solutions $x_h, ..., x_1, x_0$ in $\mathbb{F}_q$ of (3.5.2). Define

$$F_h(x_0, x_1, ..., x_h) := \det(A_c^h x_h + ... + A_c x_1 + I x_0).$$

We have the following

Lemma 3.5.5. *The polynomial $F_h(x_0, x_1, ..., x_h)$ is a homogeneous polynomial of degree n in the variables $x_0, x_1, ..., x_h$.*

Proof. For any $\lambda \in \mathbb{F}_q$, we get

$$\begin{aligned} F_h(\lambda x_0, \lambda x_1, ..., \lambda x_h) &= \det(A_c^h(\lambda x_h) + ... + A_c(\lambda x_1) + I(\lambda x_0)) \\ &= \det(\lambda I \cdot (A_c^h x_h + ... + A_c x_1 + I x_0)) \\ &= \det(\lambda I) \cdot \det(A_c^h x_h + ... + A_c x_1 + I x_0) \\ &= \lambda^n \cdot F_h(x_0, x_1, ..., x_h), \end{aligned}$$

and this gives the statement. □

From Lemma 3.5.5 it follows that the zero locus $Z(F_h(x_0, x_1, ..., x_h))$ of $F_h(x_0, x_1, ..., x_h)$ on the projective space $\mathbb{P}^h(\mathbb{F}_q)$ is well defined. Put

$$Z_{h,n} := Z(F_h(x_0, x_1, ..., x_h)) \subset \mathbb{P}^h(\mathbb{F}_q).$$

Then $Z_{h,n}$ is a hypersurface of $\mathbb{P}^h(\mathbb{F}_q)$, i.e. $\dim Z_h = h - 1$, of degree $n \geq h + 1$. Moreover, all the points of $Z_{h,n}$ represent non-trivial solutions of (3.5.2). This gives a relation between the construction of an A_c-GC code $\mathscr{C} = [\vec{v}]$, with $\vec{v} \in \mathbb{F}_q^n$, of dimension less or equal to h with the existence of (rational) points on the hypersurface $Z_{h,n} \subseteq \mathbb{P}^h(\mathbb{F}_q)$.

Remark 3.5.6. *We know from* [10] *that the number N_q of $\mathbb{F}_q$-points of the hypersurface $Z_{h,n}$ is bounded for the following inequalities: (i) $N_q \leq (n-1)q+1$ if $h=2$, except for a curve $Z_{2,4}$ over $\mathbb{F}_4$; (ii) $N_q \leq (n-1)q^{h-1} + nq^{h-2} + \frac{q^{h-2}-1}{q-1}$ if $h \geq 3$.*

Example 3.5.7. *Consider the vector space $\mathbb{F}_3^5$ and the matrix*

$$A_c = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 2 & 2 & 1 & 2 & 1 \end{pmatrix}.$$

Consider now the following equation

$$\vec{v}A_c^4x_4 + \vec{v}A_c^3x_3 + \vec{v}A_c^2x_2 + \vec{v}A_cx_1 + \vec{v}Ix_0 = \vec{0},$$

where $\vec{v} \neq \vec{0}$ and $x_i \in \mathbb{F}_3$ for $i = 0, \dots, 4$. Hence

$$\det(A_c^4x_4 + A_c^3x_3 + A_c^2x_2 + A_cx_1 + Ix_0) = 0.$$

Define

$$F_4(x_0, x_1, x_2, x_3, x_4) := \det(A_c^4x_4 + A_c^3x_3 + A_c^2x_2 + A_cx_1 + Ix_0).$$

By Lemma 3.5.5, *we see that F_4 is a homogeneous polynomial of degree 5. So $Z_{4,5} := Z(F_4(x_0, x_1, x_2, x_3, x_4) \subset \mathbb{P}^4(\mathbb{F}_3)$ is a hypersurface with $\dim Z_4 = 3$ and degree 5. By* Remark 3.5.6 *we have $N_4 \leq 341$. Moreover, the following Magma Program*

```
A:=Matrix(GF(3),5,5,[0,1,0,0,0,0,0,1,0,0,0,0,0,1,0,0,0,0,0,1,2,2,1,2,1]);
PointsCode := function(M);
 k:=Parent(M[1,1]);
 n:=Nrows(M);
 P<[x]>:=ProjectiveSpace(k,n);
 X:=Scheme(P,Determinant(&+[x[i+1]*A^i : i in [0..n]]));
 pts:=Points(X);
 ll:=[];
 for pp in pts do
  p:=Eltseq(pp);
  ll := ll cat [NullSpace(&+[p[i+1]*A^i : i in [0..n]])];
 end for;
 return ll;
end function;
```

we can find all the solutions of $F_4(x_0, x_1, x_2, x_3, x_4) = 0$. *The two rational points* $p_1 = [2:0:1:2:1]$ *and* $p_2 = [0:2:1:1:1]$ *of* $Z_{4,5} \subset \mathbb{P}^4(\mathbb{F}_3)$ *give the matrices*

$$A_1 = \begin{pmatrix} 2 & 0 & 1 & 2 & 1 \\ 2 & 1 & 1 & 0 & 0 \\ 0 & 2 & 1 & 1 & 0 \\ 0 & 0 & 2 & 1 & 1 \\ 2 & 2 & 1 & 1 & 2 \end{pmatrix}, \; A_2 = \begin{pmatrix} 0 & 2 & 1 & 1 & 1 \\ 2 & 2 & 0 & 0 & 2 \\ 1 & 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 2 & 0 \\ 0 & 1 & 2 & 2 & 2 \end{pmatrix},$$

and the vector $\vec{v}_1 = (1,0,1,1,2)$ *and* $\vec{v}_2 = (1,0,0,0,1)$ *of the null spaces of* A_1 *and* A_2 *respectively. By the following Magma Command*

```
[Basis(PointsCode(A)[1])[1]*A^i : i in [0..Nrows(A)-1]];
```

we obtain the codes

$$\mathscr{C}_1 = \langle \vec{v}_1, \vec{v}_1 A_c, \vec{v}_1 A_c^2, \vec{v}_1 A_c^3 \rangle = \langle (1,0,1,1,2), (1,2,2,2,0), (0,1,2,2,2), (1,1,0,0,1) \rangle \quad \textit{and}$$

$$\mathscr{C}_2 = \langle \vec{v}_2, \vec{v}_2 A_c, \vec{v}_2 A_c^2, \vec{v}_2 A_c^3 \rangle = \langle (1,0,0,0,1), (2,0,1,2,1), (2,1,1,0,0), (0,2,1,1,0) \rangle,$$

i.e.

$$\mathscr{C}_1 = \langle (1,0,1,1,2), (1,2,2,2,0) \rangle \quad \textit{and} \quad \mathscr{C}_2 = \langle (1,0,0,0,1), (2,0,1,2,1), (2,1,1,0,0) \rangle.$$

3.6 An immersion map for an A_c-GC code

In this section we will construct an immersion map of $\mathbb{F}_q^n$ into $\mathbb{F}_q^m$ which will be useful for finding duals codes of A_c-GC codes.

Define $f := X^n - \sum_{i=0}^{n-1} f_i X^i \in R := \mathbb{F}_q[X]$ and put $m := \min\{i \in \mathbb{N} \mid A_c^i = I\}$, where A_c is as in (3.2.2). Note that the polynomial $X^m - 1$ is satisfied by A_c and $n \leq m$. Then by the Division Algorithm there are $q, r \in R$ such that $X^m - 1 = (-1)^n f \cdot q + r$, where $\deg r < \deg f$. Suppose that $r \neq 0$. By replacing the matrix A_c in the last equation, we get

$$O = A_c^m - I = (-1)^n f(A_c) q(A_c) + r(A_c) = r(A_c)$$

which contradicts the minimality of $(-1)^n f$. Hence $r = 0$, that is $X^m - 1 = (-1)^n f \cdot q$. This tells us that we can always find a natural number m such that

$$X^m - 1 = f \cdot q_f \quad \text{for some } q_f \in R. \tag{3.6.1}$$

Note that q_f can be written as $q_f = X^{m-n} + \displaystyle\sum_{i=0}^{m-n-1} q_i X^i$ with $q_0 \neq 0$.

It is easy to see from (3.6.1) that $(X^m - 1) \subseteq (f)$, i.e. $R/Rf \subseteq R/(X^m - 1)$.

This is the motivation for the following

Lemma 3.6.1. *Let m be as in* (3.6.1) *and let P be the $m \times m$ matrix*

$$\left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline 1 & 0 & \dots & 0 \end{array}\right).$$

Denote by $\vec{q_f} := (q_0, ..., q_{m-n}, 0, ..., 0) \in \mathbb{F}_q^m$, where the q_i's are the coefficients of $q_f \in R$ as in (3.6.1)*. Then there exists a commutative diagram*

$$\begin{tikzcd} \mathbb{F}_q^n \arrow[r, "i"] \arrow[d, "\pi_f"'] & \mathbb{F}_q^m \arrow[d, "\pi_m"] \\ R/Rf \arrow[r, "j"'] & R_m \end{tikzcd}$$

such that $\pi_m \circ i = j \circ \pi_f$, where $R_m := R/(X^m - 1)$ and $i(\vec{v}) := \vec{v}Q$ with Q the matrix

$$\begin{pmatrix} \vec{q_f} \\ \vec{q_f}P \\ \vdots \\ \vec{q_f}P^{n-1} \end{pmatrix}$$

and $j(a+f) := (a \cdot q_f) + (X^m - 1)$ *for any* $a \in R$*.*

Proof. This follows from the linearity of the maps i, j, π_f and π_m by considering the canonical basis of $\mathbb{F}_q^n$. □

Proposition 3.6.2. *With the same notation as in* Lemma 3.6.1*, we have*

$$i(\vec{c}A_c^k) = i(\vec{c})P^k$$

for any $\vec{c} \in \mathbb{F}_q^n$ *and* $k \in \mathbb{N}$*.*

Proof. Let $\vec{c} \in \mathbb{F}_q^n$. By Lemma 3.6.1 and Remark 3.2.8, we have the following two commutative diagrams:

$$\begin{tikzcd}
\vec{c} \arrow[r, "i"] \arrow[d, "\pi_f"'] & i(\vec{c}) \arrow[d, "\pi_m"] \\
\pi_f(\vec{c}) \arrow[r, "j"'] & j(\pi_f(\vec{c}))
\end{tikzcd}$$

where $j(\pi_f(\vec{c})) = \pi_m(i(\vec{c}))$, and

$$\begin{tikzcd}
\vec{c}A_c^k \arrow[r, "i"] \arrow[d, "\pi_f"'] & i(\vec{c}A_c^k) \arrow[d, "\pi_m"] \\
X^k \cdot \pi_f(\vec{c}) \arrow[r, "j"'] & j(X^k \cdot \pi_f(\vec{c}))
\end{tikzcd}$$

where $j(X^k \cdot \pi_f(\vec{c})) = \pi_m(i(\vec{c}A_c^k))$. Since π_m is an isomorphism, by the commutative diagram of Lemma 3.6.1, we obtain

$$i(\vec{c}A_c^k) = (\pi_m)^{-1}(j(X^k \cdot \pi_f(\vec{c}))) =$$

$$= (\pi_m)^{-1}(X^k \cdot \pi_f(\vec{c}) \cdot q_f) = (\pi_m)^{-1}(X^k \cdot j(\pi_f(\vec{c}))) =$$

$$= (\pi_m)^{-1}(X^k \cdot \pi_m(i(\vec{c}))) = \pi_m)^{-1} \circ \pi_m(i(\vec{c})P^k,$$

that is, $i(\vec{c}A_c^k) = i(\vec{c})P^k$ for any $k \in \mathbb{N}$. □

Remark 3.6.3. *The maps* i *and* j *in* Lemma 3.6.1 *are injective. Moreover,* Proposition 3.6.2 *shows that the image via* i *of an* A_c*-GC code in* $\mathbb{F}_q^n$ *is a cyclic code in* $\mathbb{F}_q^m$*, where* m *is defined as in* (3.6.1)*.*

Finally, let us give also some upper bounds and estimations about the integer m of (3.6.1). Let GL_n be the linear group of matrices $n \times n$ with coefficients in $\mathbb{F}_q$. From [20, p. 3] we know that

$$|\mathrm{Stab}_{GL_n}(U)| = \frac{|GL_n|}{|\mathbb{G}_q(k,n)|},$$

where $\mathbb{G}_q(k,n)$ is the grassmannian variety over $\mathbb{F}_q$ and $\mathrm{Stab}_{GL_n}(U)$ is the stabilizer of any $U \in \mathbb{G}_q(k,n)$. Since

$$|GL_n| = \prod_{i=0}^{n-1}(q^n - q^i)$$

and

$$|\mathbb{G}_q(k,n)| = \frac{(q^n-1)(q^n-q)...(q^n-q^{k-1})}{(q^k-1)(q^k-q)...(q^k-q^{k-1})},$$

we obtain that

$$|\mathrm{Stab}_{GL_n}(U)| = \frac{(q^k-1)(q^k-q)...(q^k-q^{k-1})\prod_{i=0}^{n-1}(q^n-q^i)}{(q^n-1)(q^n-q)...(q^n-q^{k-1})} =$$

$$= \prod_{i=k}^{n-1}(q^n-q^i)\cdot\prod_{j=0}^{k-1}(q^k-q^j). \tag{3.6.2}$$

This allows us to prove the following upper bound for m.

Lemma 3.6.4.

$$m \leq \min_{g|f}\left\{\prod_{i=k}^{n-1}(q^n-q^i)\cdot\prod_{j=0}^{k-1}(q^k-q^j) \mid k = n-\deg g\right\}.$$

Proof. Let g be any divisor of f in R. By Proposition 3.2.7 we deduce that the A_c-GC code $\pi_f^{-1}((g)_{n,q}^k)$ is invariant with respect to A_c. Thus $\langle A_c\rangle \subseteq \mathrm{Stab}_{GL_n}(\pi_f^{-1}((g)_{n,q}^k))$ and since $m := |\langle A_c\rangle|$, the statement follows from (3.6.2). □

Remark 3.6.5. *Let $\mathbb{F}_q \subseteq \mathbb{K}$ be a finite extension of $\mathbb{F}_q$ such that $f = \prod_{i=1}^n (X - a_i)$ with $a_i \in \mathbb{K}$ and A_c is diagonalizable over $\mathbb{K}$. If $m_i := \min\left\{h_i \mid a_i^{h_i} = 1\right\}$, then $m = lcm(m_1, ..., m_n)$.*

Remark 3.6.6. *Let $p := \mathrm{Char}(\mathbb{F}_q)$. If f has a root of multiplicity ≥ 2, then $X^m - 1$ has a root of multiplicity ≥ 2. By* Remark 3.4.6 *we have $gcd(m,p) \neq 1$ and since p is a prime number, we get $m \equiv 0 \mod p$.*

The next result gives a more simple computation for m.

Proposition 3.6.7. *Denote by* $\vec{f} := \pi_f^{-1}(X^n - f)$ *and let*

$$k := \min\left\{h \in \mathbb{N} \cup \{0\} \mid \vec{f} A_c^h = \vec{e}_1\right\}.$$

Then $m = n + k$*. In particular, we have* $\deg q_f := m - n = k$*.*

Proof. For every $h = 1, ..., n$, we have

$$\vec{e}_h\ A_c^{n+k} = ((\vec{e}_h A_c^{n-h+1})A_c^k)A_c^{h-1} = ((\vec{e}_n A_c)A_c^k)A_c^{h-1} =$$

$$= (\vec{f} A_c^k)A_c^{h-1} = \vec{e}_1 A_c^{h-1} = \vec{e}_h.$$

Hence $A_c^{n+k} = I$ and for the minimality of m we deduce that $m \leq n + k$. Furthermore, since $A_c^m = I$ we get

$$\vec{e}_1 = ((\vec{e}_1 A_c^{n-1})A_c)A_c^{m-n} = (\vec{e}_n A_c)A_c^{m-n} = \vec{f} A_c^{m-n},$$

that is, $\vec{f} A_c^{m-n} = \vec{e}_1$. So, by definition of k we can conclude that $k \leq m - n$, i.e. $m \geq n + k$. □

Let p_0 be the order of $\det(A_c)$. Since $A_c^m = I$, it follows that $(\det A_c)^m = 1$, i.e. $m \equiv 0 \mod p_0$ with p_0 the order of $\det A_c$. This gives immediately also the following

Proposition 3.6.8. *Denote by* $B := A_c^{p_0}$*. Let* m' *be the minimum integer such that* $B^{m'} = I$*. Then* $m = p_0 m'$*. In particular, we have* $\deg q_f = p_0 m' - n$*.*

All the above results produce the following

Algorithm 1:

Input: f

- *Define* $a_0 := \det A_c$*;*

- *Compute the order* p_0 *of* a_0*;*

- *Define* $B := A_c^{p_0}$*;*

- *Find the rational canonical form* B' *of* B*;*

- *For any diagonal block B_i, $i = 1, ..., s$, of B' compute $m'_i = \min\left\{h \mid B_i^h = I\right\}$.*

Output: $m = lcm(m'_1, ..., m'_s) \cdot p_0$.

By using the computer algebra system Magma [3], the MAGMA Program 1 (Ch. 5) allows us to find the integer m as in (3.6.1) for any polynomial $f \in R$.

3.7 Quasi-Euclidean dual Codes

In what follows we study another kind of dual codes, the Quasi-Euclidean dual codes, and we investigate some of their properties and connections between them and the Euclidean dual codes.

Let

$$f = X^n - \sum_{i=0}^{n-1} f_i X^i \in R$$

be a monic polynomial of degree n. By Lemma 3.6.1, we know that there exists an injective map $i : \mathbb{F}_q^n \to \mathbb{F}_q^m$ with $m \geq n$. Denote by $\mathscr{I}$ the image of i and by P the $m \times m$ permutation matrix of Lemma 3.6.1. Define $B := QQ_t$ with Q as in Lemma 3.6.1, where Q_t is the transpose of Q. Note that B is a symmetric matrix.

Let r be the rank of the matrix B and observe that

$$r := \text{rk}B = n - \dim(\text{Ker } Q_t \cap \mathscr{I})$$

with $0 \leq r \leq n$.

Remark 3.7.1. *When $r = 0$, we see that B is the null matrix and in this case Q represents the generator matrix of a self-orthogonal cyclic code of dimension n in $\mathbb{F}_q^m$.*

Definition 3.7.2. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. We denote by $\cdot_*$ the **quasi-euclidean scalar product** on $\mathbb{F}_q^n$ defined by $\vec{a} \cdot_* \vec{b} := \vec{a}B\vec{b}_t$ for any $\vec{a}, \vec{b} \in \mathbb{F}_q^n$ and by $\mathscr{C}^*$ the linear **quasi-euclidean dual code** of $\mathscr{C}$ with respect to $\cdot_*$, i.e.*

$$\mathscr{C}^* := \left\{\vec{x} \in \mathbb{F}_q^n \mid \vec{x} \cdot_* \vec{c} = 0 \text{ for every } \vec{c} \in \mathscr{C}\right\}.$$

Proposition 3.7.3. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. Then we have* *(i)* $\mathscr{C}^* = (\mathscr{C} \star B)^\perp$.

(ii) $\dim \mathscr{C}^* = \dim \mathscr{C}^\perp + \dim(\mathscr{C} \cap \operatorname{Ker}\ B) \geq \dim \mathscr{C}^\perp$;

(iii) $\mathscr{C}^* \star B = \mathscr{C}^\perp \cap (Im\ B)$;

(iv) $(\mathscr{C}^*)^* = \mathscr{C} + \operatorname{Ker}\ B$;

(v) $i(\mathscr{C}^*) = i(\mathscr{C})^\perp \cap \mathscr{I} = i(\mathscr{C} + \operatorname{Ker}\ B)^\perp \cap \mathscr{I}$;

(vi) $(\mathbb{F}_q^n)^* = \operatorname{Ker}\ B = (Im\ B)^\perp,\ (\operatorname{Ker}\ B)^* = \mathbb{F}_q^n,\ (\operatorname{Ker}\ B)^{**} = \operatorname{Ker}\ B.$

Proof. *(i)* To prove $\mathscr{C}^* = (\mathscr{C} \star B)^\perp$, we observe that

$$\begin{aligned}
\vec{w} \in (\mathscr{C} \star B)^\perp &\iff \vec{w} \cdot (\vec{c}B) = 0, \quad \forall \vec{c} \in \mathscr{C} \\
&\iff \vec{w}B_t\vec{c}_t = 0, \quad \forall \vec{c} \in \mathscr{C} \\
&\iff \vec{w}B\vec{c}_t = 0, \quad \forall \vec{c} \in \mathscr{C} \\
&\iff \vec{w} \cdot_* \vec{c} = 0, \quad \forall \vec{c} \in \mathscr{C} \\
&\iff \vec{w} \in \mathscr{C}^* \ .
\end{aligned}$$

(ii) This follows from

$$\dim(\mathscr{C} \star B) = \dim \mathscr{C} - \dim(\mathscr{C} \cap \operatorname{Ker}\ B)$$

and $\dim \mathscr{C}^* = n - \dim(\mathscr{C} \star B)$.

(iii) If $\vec{x} \in \mathscr{C}^* \star B$, then $\vec{x} \in Im\ B$ and $\vec{x} = \vec{c^*}B$ with $\vec{c^*} \in \mathscr{C}^*$. Hence for every $\vec{c} \in \mathscr{C}$ we get

$$\vec{x} \cdot \vec{c} = \vec{c^*}B \cdot \vec{c} = \vec{c^*} \cdot_* \vec{c} = 0,$$

i.e. $\mathscr{C}^* \star B \subseteq C^\perp \cap (Im\ B)$.

On the other hand, let $\vec{y} \in \mathscr{C}^\perp \cap (Im\ B)$. Then $\vec{y} = \vec{v}B \in \mathscr{C}^\perp$ for some $\vec{v} \in \mathbb{F}_q^n$. Thus for every $\vec{c} \in \mathscr{C}$ we have

$$\vec{v} \cdot_* \vec{c} = \vec{v}B\vec{c}_t = \vec{y} \cdot \vec{c} = 0,$$

that is, $\mathscr{C}^\perp \cap (Im\ B) \subseteq \mathscr{C}^* \star B$.

(iv) If $\vec{c}+\vec{b}\in\mathscr{C}+\text{Ker } B$ where $\vec{c}\in\mathscr{C}$ and $\vec{b}\in\text{Ker } B$, then for every $\vec{x}_t\in\mathscr{C}^*$ we get

$$(\vec{c}+\vec{b})\cdot_*\vec{x}=(\vec{c}+\vec{b})B\vec{x}_t=\vec{c}B\vec{x}_t+\vec{b}B\vec{x}_t=\vec{c}B\vec{x}_t=\vec{c}\cdot_*\vec{x}=0,$$

that is, $\mathscr{C}+\ker(B)\subseteq(\mathscr{C}^*)^*$.

Conversely, to prove $(\mathscr{C}^*)^*\subseteq\mathscr{C}+\text{Ker } B$ it is sufficient to observe that

$$\begin{aligned}
\vec{x}\in(\mathscr{C}^*)^* &\Rightarrow \vec{v}\cdot_*\vec{x}=0, \quad \forall\vec{x}\in\mathscr{C}^*\\
&\Rightarrow \vec{v}B\vec{x}_t=0, \quad \forall\vec{x}\in\mathscr{C}^*\\
&\Rightarrow \vec{v}B\in(\mathscr{C}^*)^\perp=\mathscr{C}\star B\\
&\Rightarrow \vec{v}B=\vec{c}B, \quad \text{for some } \vec{c}\in\mathscr{C}\\
&\Rightarrow (\vec{v}-\vec{c})B=\vec{0}, \quad \text{for some } \vec{c}\in\mathscr{C}\\
&\Rightarrow \vec{v}-\vec{c}\in\text{Ker } B, \quad \text{for some } \vec{c}\in\mathscr{C}\\
&\Rightarrow \vec{v}\in\mathscr{C}+\text{Ker } B.
\end{aligned}$$

(v) If $\vec{x}\in i(\mathscr{C}^*)$, then $\vec{x}=i(\vec{v})=\vec{v}Q\in\mathscr{I}$ for some $\vec{v}\in\mathscr{C}^*$. Hence for every $\vec{c}\in\mathscr{C}$ and $\vec{b}\in\text{Ker } B$, we have

$$\vec{x}\cdot i(\vec{c}+\vec{b})=\vec{x}\cdot i(\vec{c})+\vec{x}\cdot i(\vec{b})=\vec{v}\cdot_*\vec{c}+\vec{v}\cdot(\vec{b}B)=0,$$

that is, $(\mathscr{C}^*)\subseteq i(\mathscr{C}+\text{Ker } B)^\perp\cap\mathscr{I}$. Now, let $\vec{x}\in(\mathscr{C}+\text{Ker } B)^\perp\cap\mathscr{I}$, i.e. $\vec{x}=(\vec{v})=\vec{v}Q\in i(\mathscr{C}+\text{Ker } B)^\perp\subseteq i(\mathscr{C})^\perp$ for some $\vec{v}\in\mathbb{F}_q^n$. Thus for every $\vec{y}\in\mathscr{C}$ we have

$$\vec{v}\cdot_*\vec{y}=\vec{v}B\vec{y}_t=(\vec{v}Q)(\vec{y}Q)_t=\vec{x}\cdot i(\vec{y})=0,$$

i.e. $\vec{v}\in\mathscr{C}^*$. Hence we get $\vec{x}=i(\vec{v})\in i(\mathscr{C}^*)$, that is, $i(\mathscr{C}+\text{Ker } B)^\perp\cap\mathscr{I}\subseteq i(\mathscr{C}^*)$.

Let us prove now that $i(\mathscr{C}^*)$ is also equal to $i(\mathscr{C})^\perp\cap\mathscr{I}$. Let $\vec{x}\in i(\mathscr{C}^*)$. Then $\vec{x}=i(\vec{c^*})\in\mathscr{I}$ for some vector $\vec{c^*}\in\mathscr{C}^*$. Therefore for every $\vec{c}\in\mathscr{C}$ we have

$$\vec{x}\cdot i(\vec{c})=i(\vec{c^*})\cdot i(\vec{c})=\vec{c^*}\cdot_*\vec{c}=0,$$

i.e. $\vec{x}\in i(\mathscr{C})^\perp\cap\mathscr{I}$. On the other hand, let $\vec{y}\in i(\mathscr{C})^\perp\cap\mathscr{I}$. Then $\vec{y}=\vec{i}(\vec{z})\in\mathscr{I}$ for some $\vec{z}\in\mathbb{F}_q^n$ and for every $\vec{c}\in\mathscr{C}$ we get

$$0=i(c)\cdot\vec{y}=i(c)\cdot i(z)=\vec{c}\cdot_*\vec{z}.$$

Hence $\vec{z} \in \mathscr{C}^*$, i.e. $\vec{y} \in i(\mathscr{C}^*)$.

(vi) Since $(\{\vec{0}\})^* = \mathbb{F}_q^n$, the equalities $(\mathbb{F}_q^n)^* = (Im\ B)^\perp$ and $(\mathbb{F}_q^n)^* = \text{Ker } B$ follow easily from (i) with $\mathscr{C} = \mathbb{F}_q^n$ and from (iv) with $\mathscr{C} = \{\vec{0}\}$ respectively. Finally, by taking $\mathscr{C} = \text{Ker } B$, the equalities $(\text{Ker } B)^* = \mathbb{F}_q^n$ and $(\text{Ker } B)^{**} = \text{Ker } B$ are immediate consequences of (i) and (iv), respectively. □

Remark 3.7.4. *From* Theorem 3.7.4 (iv) *it follows that* $\mathscr{C} \subseteq (\mathscr{C}^*)^*$.

Corollary 3.7.5. *Let* $\mathscr{C} \subseteq \mathbb{F}_q^n$ *be a linear code. If* $r = n$*, then we have*

(j) $\mathscr{C}^* = \mathscr{C}^\perp \star B^{-1}$;

(jj) $\dim \mathscr{C}^* = \dim \mathscr{C}^\perp$;

(jjj) $(\mathscr{C}^*)^* = \mathscr{C}$.

(jv) $i(\mathscr{C}^*) = i(\mathscr{C})^\perp \cap \mathscr{I}$;

(v) $(\mathbb{F}_q^n)^* = \{\vec{0}\}$, $(\{\vec{0}\})^* = \mathbb{F}_q^n$.

Proof. Parts (j) and (jj) follow from Proposition 3.7.3(ii) and (iii). As to (jjj), it is sufficient to note that $r = n$ implies that $\text{Ker } B = \{\vec{0}\}$. □

Remark 3.7.6. *When* $r = n$*, from* Corollary 3.7.5 *we know that* $\mathscr{C}^* = \mathscr{C}^\perp \star B^{-1}$. *Thus* Proposition 3.3.3 *allows us to find easily a generator matrix of* $\mathscr{C}^*$ *by multiplying on the right the parity check matrix of* $\mathscr{C}$ *in* Proposition 3.3.3 *by* B^{-1}.

Corollary 3.7.7. *Let* $\mathscr{C} \subseteq \mathbb{F}_q^n$ *be a linear code. Then*

$$\mathscr{C} \subseteq \mathscr{C}^* \iff i(\mathscr{C}) \subseteq i(\mathscr{C})^\perp,$$

i.e. $\mathscr{C}$ *is self-ortogonal with respect to* $\cdot_*$ *if and only if* $i(\mathscr{C})$ *is self-ortogonal with respect to* $\cdot$.

Proof. Since i is injective, the statement is an immediate consequence of Proposition 3.7.3 (v) and the following equivalence: $i(\mathscr{C}) \subseteq i(\mathscr{C})^\perp \cap \mathscr{I} \iff i(\mathscr{C}) \subseteq i(\mathscr{C})^\perp$. □

Remark 3.7.8. *If $\mathscr{C} \subseteq \mathbb{F}_q^n$ is an A_c-GC code and* $\operatorname{Ker} B \subseteq \mathscr{C}$*, then the code* $\mathscr{C} + \operatorname{Ker} B$ *is an A_c-GC code. In particular, when $r = n$, it follows that*

$$\mathscr{C} = \mathscr{C}^{\perp} \iff \mathscr{C} \star B^{-1} \text{ is the dual code } \mathscr{C}^{*} \text{ of } \mathscr{C}.$$

Example 3.7.9. *In $\mathbb{F}_4^3$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$, consider the following four polynomials:*

(a) $f_0 = X^3 + X^2 + 1$;

(b) $f_1 = X^3 + \alpha^2 X^2 + \alpha^2 X + 1$;

(c) $f_2 = X^3 + \alpha X^2 + \alpha X + 1$;

(d) $f_3 = X^3 + \alpha^2$.

By applying Program 2 *(Ch. 5), we obtain $m = 7$ for the first case, $m = 9$ for the fourth case and $m = 5$ for the other cases. Then*

$$X^7 - 1 = f_0 \cdot q_{f_0}, \;\; X^5 - 1 = f_1 \cdot q_{f_1} = f_2 \cdot q_{f_2}, \;\; X^9 - 1 = f_3 \cdot q_{f_3}$$

where

$$q_{f_0} = X^4 + X^3 + X^2 + 1, \quad q_{f_1} = X^2 + \alpha^2 X + 1,$$
$$q_{f_2} = X^2 + \alpha X + 1, \quad q_{f_3} = X^6 + \alpha^2 X^3 + \alpha.$$

Therefore this gives

$$Q_0 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad Q_1 = \begin{pmatrix} 1 & \alpha^2 & 1 & 0 & 0 \\ 0 & 1 & \alpha^2 & 1 & 0 \\ 0 & 0 & 1 & \alpha^2 & 1 \end{pmatrix},$$

$$Q_2 = \begin{pmatrix} 1 & \alpha & 1 & 0 & 0 \\ 0 & 1 & \alpha & 1 & 0 \\ 0 & 0 & 1 & \alpha & 1 \end{pmatrix}, \quad Q_3 = \begin{pmatrix} \alpha & 0 & 0 & \alpha^2 & 0 & 0 & 1 & 0 & 0 \\ 0 & \alpha & 0 & 0 & \alpha^2 & 0 & 0 & 1 & 0 \\ 0 & 0 & \alpha & 0 & 0 & \alpha^2 & 0 & 0 & 1 \end{pmatrix},$$

and

$$B_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},\ B_1 = \begin{pmatrix} \alpha & 0 & 1 \\ 0 & \alpha & 0 \\ 1 & 0 & \alpha \end{pmatrix},$$

$$B_2 = \begin{pmatrix} \alpha^2 & 0 & 1 \\ 0 & \alpha^2 & 0 \\ 1 & 0 & \alpha^2 \end{pmatrix},\ B_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

with rk $B_0 = B_3 = 0$ *and* rk $B_1 =$ rk $B_2 = 3$. *Note that from* Remark 3.7.1 *it follows that* Q_0 *and* Q_3 *are the generator matrices of self-orthogonal cyclic codes of* $\mathbb{F}_4^7$ *and* $\mathbb{F}_4^9$ *respectively.*

By Magma Program 5 *(Ch. 5) we see that* f_0 *and* f_3 *are irreducible polynomial in* $\mathbb{F}_4[X]$ *and*

$$f_1 = (X+1)\cdot(X^2+\alpha X+1), \qquad f_2 = (X+1)(X^2+\alpha^2 X+1)$$

Therefore, we have the following non-trivial codes

$$\mathscr{C}_1 = (X+1)^2_{3,4},\ (X^2+\alpha X+1)^1_{3,4}\ , \qquad \mathscr{C}_2 = (X+1)^2_{3,4},\ (X^2+\alpha^2 X+1)^1_{3,4}\ ,$$

with generator matrices

$$G_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & \alpha & 1 \end{pmatrix} \quad \textit{and} \quad G_2 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & \alpha^2 & 1 \end{pmatrix};$$

respectively. From Proposition 3.3.3 *we deduce that the parity check matrices of the* $\mathscr{C}_i$*'s for* $i = 1, 2$ *are*

$$H_1 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & \alpha \end{pmatrix} \quad \textit{and} \quad H_2 = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix},\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & \alpha^2 \end{pmatrix};$$

Therefore we have

$$\mathscr{C}_1^* = (X^2+\alpha X+1)^1_{3,4},\ (X+1)^2_{3,4};$$

$$\mathscr{C}_2^* = (X^2+\alpha^2+1)^1_{3,4},\ (X+1)^2_{3,4}.$$

3.8 Hermitian dual Codes

We can introduce also the notion of dual Hermitian codes and give some of their properties.

We define a “conjugation” map Φ on R/RF for some $F \in R$ such that

$$\Phi(aX^i) := aX^{\deg F - i},$$

where $0 \leq i \leq \deg F - 1$, which is extended to all elements of R/RF by linearity. We then define a Hermitian product of two elements $p(X) = p_0 + p_1X + ... + p_{m-1}X^{m-1}$ and $t(X) = t_0 + t_1X + ... + t_{m-1}X^{m-1}$ of $R/(X^m - 1)$ by

$$p(X) *_P t(X) := p(X)\Phi(t(X)).$$

By Lemma 3.6.1 we can also define the Hermitian product of two elements $a(X) = a_0 + a_1X + ... + a_{n-1}X^{n-1}$ and $b(X) = b_0 + b_1X + ... + b_{n-1}X^{n-1}$ of R/Rf by

$$< a(X), b(X) >:= j(a(X)) *_P j(b(X)).$$

The following two results are now an immediate generalization of [15, Proposition 3.2 and Corollary 3.3].

Theorem 3.8.1. *If $\vec{a}, \vec{b} \in \mathbb{F}_q^n$ and let $a(X)$ and $b(X)$ be their polynomial representation in R/Rf via π_f, respectively. Then*

$$\vec{a} \cdot_* \vec{b}A_c^h = 0 \quad \text{for all } 0 \leq h \leq m-1 \quad \Longleftrightarrow \quad < a(X), b(X) >= 0.$$

Proof. The condition $< a(X), b(X) >= 0$ is equivalent to

$$\begin{aligned} j(a(X)) *_P j(b(X)) = 0 &\Longleftrightarrow a(X)q_f\Phi(b(X)q_f) = 0 \\ &\Longleftrightarrow \left(\sum_{i=0}^{m-1} a'_iX^i\right) \cdot \Phi\left(\sum_{k=0}^{m-1} b'_kX^k\right) = 0 \\ &\Longleftrightarrow \left(\sum_{i=0}^{m-1} a'_iX^i\right) \cdot \left(\sum_{k=0}^{m-1} b'_kX^{m-k}\right) = 0 \\ &\Longleftrightarrow \sum_{h=0}^{m-1}\left(\sum_{i=0}^{m-1} a'_{i+h}b'_i\right)X^h = 0, \end{aligned}$$

where the subscript $i+h$ is taken modulo m. Comparing the coefficients of X^h on both sides of the last equation, we get

$$\sum_{i=0}^{m-1} a'_{i+h}b'_i = 0, \text{ for all } 0 \leq h \leq m-1.$$

By Proposition 3.6.2 the above equation is equivalent for all $0 \leq h \leq m-1$ to

$$\begin{aligned} \vec{a'} \cdot \vec{b'}(\Theta^h \circ P^h) = 0 &\iff i(\vec{a}) \cdot i(\vec{b})P^h = 0 \\ &\iff i(\vec{a}) \cdot i(\vec{b}A_c^h) = 0 \\ &\iff \vec{a}Q \cdot (\vec{b}A_c^h)Q = 0 \end{aligned}$$

i.e. $\vec{a} \cdot_* \vec{b}A_c^h = 0$ for all $0 \leq h \leq m-1$. □

Let I be a left ideal of R/Rf.

We define I^ν to be the dual of I in R/Rf taken with respect to the Hermitian scalar product $<,>$, as

$$I^\nu := \{a(X) \in R/Rf \mid \ < a(X), t(X) >= 0 \ , \ \forall t(X) \in I \ \}.$$

Remark 3.8.2. *Note that I^ν is an ideal of R/Rf with respect to the addition in R/Rf.*

From Theorem 3.8.1, we deduce the following

Theorem 3.8.3. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a A_c-GC code. We have*

$$\pi_f(\mathscr{C}^*) = \pi_f(\mathscr{C})^\nu \ .$$

Proof. Let $\pi_f(\vec{b}) \in \pi_f(\mathscr{C}^*)$ for some $\vec{b} \in \mathscr{C}^*$. Then we have for any $\vec{a} \in \mathscr{C}$ and $h \in \mathbb{Z}_{\geq 0}$

$$\vec{b} \cdot_* \vec{a}A_c^h = 0.$$

Thus by Theorem 3.8.1 we get

$$< \pi_f(\vec{b}), \pi_f(\vec{a}) >= 0 \ \forall \ \vec{a} \in \mathscr{C},$$

i.e. $\pi_f(\vec{b}) \in \pi_f(\mathscr{C})^\nu$. Hence $\pi_f(\mathscr{C}^*) \subseteq \pi_f(\mathscr{C})^\nu$. Finally, let $b(X) \in \pi_f(\mathscr{C})^\nu$. Then we see that

$$< b(X), \pi_f(\vec{a}) >= 0, \ \forall \vec{a} \in \mathscr{C}.$$

By Theorem 3.8.1 with $h = 0$, this implies that

$$\pi_f^{-1}(b(X)) \cdot_* \vec{a} = 0, \ \forall \vec{a} \in \mathscr{C},$$

i.e. $\pi_f^{-1}(b(X)) \in \mathscr{C}^*$. This shows that

$$b(X) = \pi_f(\pi_f^{-1}(b(X)) \in \pi_f(\mathscr{C}^*),$$

i.e. $\pi_f(\mathscr{C})^\nu \subseteq \pi_f(\mathscr{C}^*)$. □

Corollary 3.8.4. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. We have*

(i) If $\mathscr{C}$ is a A_c-GC code then $\mathscr{C}^*$ is also a A_c-GC code.

(ii) $\mathscr{C}^*$ is an A_c-GC code if and only if $\mathscr{C} + \mathrm{Ker}\ B$ is an A_c-GC code.

Proof. (i) If $\mathscr{C}$ is an A_c-GC code then $\pi_f(\mathscr{C})$ is an ideal of R/Rf. By Remark 3.8.2 and Corollary 3.8.3 we have that $\pi_f(\mathscr{C}^*) = \pi_f(\mathscr{C})^\nu$ is an ideal of R/Rf, so that $\mathscr{C}^*$ is an A_c-GC code.

(ii) By Part (i), if $\mathscr{C}^*$ is an A_c-GC code, then $(\mathscr{C}^*)^* = \mathscr{C} + \mathrm{Ker}\ B$ is an A_c-GC code.

Conversely we note that if $\mathscr{C} + \mathrm{Ker}\ B$ is an A_c-GC code, then $i(\mathscr{C} + \mathrm{Ker}\ B)$ is a cyclic code, thus $i(\mathscr{C} + \mathrm{Ker}\ B)^\perp$ is a cyclic code. Since $\mathscr{I}$ is a cyclic code, by Proposition 3.7.3 (v) we obtain that $i(\mathscr{C}^*) = i(\mathscr{C} + \mathrm{Ker}\ B)^\perp \cap \mathscr{I}$ is a cyclic code, so that $\mathscr{C}^*$ is an A_c-GC code. □

Let us note here that the converse of Corollary 3.8.4 is not true in general, as the following example shows.

Example 3.8.5. *In $\mathbb{F}_4^3$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$, consider the polynomial $f_2 = X^3 + \alpha^2 X^2 + \alpha^2 X + \alpha$. Then by Magma* Program 2 *(Ch. 5), we obtain $m = 6$ and*

$$B_2 = \begin{pmatrix} 0 & \alpha^2 & \alpha^2 \\ \alpha^2 & 0 & \alpha^2 \\ \alpha^2 & \alpha^2 & 0 \end{pmatrix},$$

with $\mathrm{rk}\ B_2 = 2$. *Consider the linear code $\mathscr{C} \subset \mathbb{F}_4^3$ generated by the vectors $\vec{e}_1 = (1, 0, 0)$ and $\vec{e}_3 = (0, 0, 1)$. Since*

$$(\vec{e}_3 A_c = (\vec{e}_3) \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha & \alpha^2 & \alpha^2 \end{pmatrix} = (\alpha, \alpha^2, \alpha^2) \notin \mathscr{C},$$

we see that $\mathscr{C}$ is not an A_c-GC code. On the other hand, since Ker B_2 *is generated by the vector* $(1,1,1)$ *and* $\mathscr{C} \cap \text{Ker } B_2 = \{\vec{0}\}$*, we obtain that*

$$\mathscr{C} + \text{Ker } B_2 = \mathscr{C} \oplus \text{Ker } B_2 = \mathbb{F}_4^3$$

is an A_c-GC code. By Corollary 3.8.4 *we get that $\mathscr{C}^*$ is an A_c-GC code.*

Example 3.8.6. *Consider the vector space $\mathbb{F}_4^3$ where $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ with $\alpha^2+\alpha+1=0$. Let $f = X^3 + \alpha^2 X + \alpha X + 1$ and write $A_c = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}$. By applying the Magma* Program 2 *(Ch. 5), we obtain $m = 12$, i.e. $A_c^{12} = I$. Then by* Lemma 3.6.1 *there exist a commutative diagram*

$$\begin{tikzcd}
\mathbb{F}_4^3 \arrow[r, "i"] \arrow[d, "\pi_f"'] & \mathbb{F}_4^{12} \arrow[d, "\pi_m"] \\
R/Rf \arrow[r, "j"'] & R_{12}
\end{tikzcd}$$

such that $\pi' \circ i = j \circ \pi_f$, where $R_{12} := R/R(X^{12}-1)$, $R = \mathbb{F}_4[X]$, $i(\vec{v}) := \vec{v}Q$ with

$$Q = \begin{pmatrix} 1 & \alpha & 0 & 0 & \alpha & \alpha^2 & 0 & 0 & \alpha^2 & 1 & 0 & 0 \\ 0 & 1 & \alpha & 0 & 0 & \alpha & \alpha^2 & 0 & 0 & \alpha^2 & 1 & 0 \\ 0 & 0 & 1 & \alpha & 0 & 0 & \alpha & \alpha^2 & 0 & 0 & \alpha^2 & 1 \end{pmatrix}.$$

Since $f = (X+\alpha^2)^3 = (X+\alpha^2)(X^2+\alpha)$, we considering the A_c-GC code's $\mathscr{C}_1 = (X+\alpha^2)_3^2$ and $\mathscr{C}_2 = (X^2+\alpha)_3^1$. Is easy to see that $B := QQ_t = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, then $\mathscr{C}_1^* = \mathscr{C}_2^* = \mathbb{F}_4^3$. By Theorem 3.8.3 $\pi(\mathscr{C}_1)^\nu = \pi(\mathscr{C}_1^*) = \pi(\mathscr{C}_2^*) = R/Rf$.

By Corollary 3.7.5, the following proposition is immediate.

Corollary 3.8.7. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code and $r = n$, then*

$$\mathscr{C} \textit{ is an } A_c\textit{-GC code} \Leftrightarrow \mathscr{C}^* \textit{ is an } A_c\textit{-GC code.}$$

Corollary 3.8.8. *If $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a A_c-GC code, then*

$$\mathscr{C} = \mathscr{C}^* \iff \pi_f(\mathscr{C}) = \pi_f(\mathscr{C})^\nu \ ,$$

i.e. $\mathscr{C}$ is self-dual with respect to $\cdot_*$ if and only if $\pi_f(\mathscr{C})$ is self-dual with respect to $<,>$.

Proof. Since π_f is an isomorphism, this follows immediately from Corollary 3.8.3. □

3.9 A Meggitt type decoding

In this section, we give here a generalization of Meggitt Decoding of Chapter 2, §2.6.

Let $\mathscr{C} = (g)_{n,q}^k$ an A_c-GC code. Denote by $R_g(v)$ the rest of the division of $v \in R$ by g and define the syndrome $S(v)$ of v as $S(v) := R_g(X^{n-k} \cdot v)$, where $\deg g = n - k$.

Lemma 3.9.1. *Under the same hypothesis as above, we have*

$$S(v) = 0 \in R \quad \textit{if and only if} \quad v \in \pi_f(\mathscr{C}).$$

Proof. Let $v \in R$ such that $S(v) = 0 \in R$. Then $R_g(X^{n-k} \cdot v) = 0$ and so we can deduce that $X^{n-k} \cdot v \in \pi_f(\mathscr{C})$, i.e. $X^{n-k} \cdot v = h \cdot g$ for some $h \in R$.

Put $t := f_0^{-1}X^{n-1} - ... - f_0^{-1}f_1$ and note that $t \cdot X = 1$ in R. Hence

$$t^{n-k} \cdot h \cdot g = t^{n-k} \cdot (X^{n-k} \cdot v) = (t^{n-k} \cdot (X^{n-k})) \cdot v = v,$$

that is, $v \in \pi_f(\mathscr{C})$. On the other hand, if $v \in \pi(\mathscr{C})$, then $v = q \cdot g$ for some $q \in R$. Thus by definition we can conclude that $S(v) = 0 \in R$. □

Let $\vec{m} \in \mathbb{F}_q^k$ be the original message and code $\vec{m}$ as

$$\vec{m}' := \vec{m} \cdot G \in \mathscr{C},$$

where G is the above generator matrix of $\mathscr{C} = (g)_n^k$. Note that

$$\pi_f(\vec{m}') = \pi_f(\vec{m} \cdot G) = \pi_f(\vec{m}) \cdot g \in (g) \subset R.$$

We now give here a Meggitt algorithm for an A_c-GC code. For any $c \in R$, denote by $wt(c)$ the Hamming weight of $\pi^{-1}(c) \in \mathbb{F}_q^n$. Let us recall that in this situation the main hypothesis is that the error $\vec{e}$ defined by

$$\vec{e} := \vec{m}'' - \vec{m}' \in \vec{m}'' + \mathscr{C}$$

has weight $\leq \frac{d-1}{2}$, where d is the distance of $\mathscr{C}$ and $\vec{m}''$ is the received message. Moreover, by Lemma 3.9.1 we have

$$S(\pi_f(\vec{m}'')) = S(\pi_f(\vec{e}))$$

and recall that

$$(f_0^{-1}X^{n-1} - ... - f_0^{-1}f_1) \cdot X = 1 \in R/Rf.$$

Algorithm 2 **(An** A_c**-Meggitt type algorithm):**

Input: $\vec{m}''$

- **Step 1**: Compute all the syndromes $S(e')$, where $e' = \sum_{i=0}^{n-1} e'_i X^i$ is such that $wt(e') \leq \frac{d-1}{2}$ and $e'_{n-1} \neq 0$;
- **Step 2**: Compute $S(\pi(\vec{m}''))$ and define $s := S(\pi(\vec{m}''))$;
- **Step 3**: If $s = 0 \in R$ then write $\vec{e} = \vec{0}$;
- **Step 4**: If s is equal to some of the syndromes $S(e')$ of Step 1, then write $\vec{e} = \pi^{-1}(e')$;
- **Step 5**: If s is not in the list of Step 1, then

$$\vec{m}'' = \vec{m}' + \pi^{-1}(\overline{e})$$

for some error $\overline{e} \in R$ such that $wt(\overline{e}) \leq \frac{d-1}{2}$ and $\overline{e} = \sum_{j=0}^{h} \overline{e}_j X^j$ with $\overline{e}_h \neq 0$ and $h < n-1$. Always there exists an integer $k := n-h-1$ such that

$$e'' := X^k \cdot \overline{e}$$

is an error as in Step 1, that is, $e'' = \sum_{i=0}^{n-1} e''_i X^i$ with $wt(e'') \leq \frac{d-1}{2}$ and $e''_{n-1} \neq 0$. Thus by Lemma 3.9.1 the syndrome $S(X^k \pi(\vec{m}''))$ is equal to $S(e'')$ with e'' as in Step 1 and we write

$$\vec{e} = \pi_f^{-1}((f_0^{-1}X^{n-1} - ... - f_0^{-1}f_1)^k e'');$$

Output: $\vec{m}' = \vec{m}'' - \vec{e}$.

Example 3.9.2. *This decoding is analogous to Meggitt Decoding of* Chapter 3. *However, in step 5, the decoding is different. Let* $\mathscr{C} = (1+X^4+X^6+X^7+X^8)^7_{15}$ *be a binary* A_c*-GC code with* $d(\mathscr{C})$*,such that* $\pi_f(\mathscr{C})$ *is an ideal of* R/Rf *where* $f = 1+X+X^4+X^5+X^6+2X^8+X^9+X^{11}+X^{13}+X^{14}+X^{15}$. *As in* Example 2.4.10, *the polynomial* $e' := 1 + X^2 + X^3 + X^4 + X^6$ *is not in the list in* Example 2.4.6. *In this case* $k = 1$ *and*

$$e'' := X \cdot e' = X + X^3 + X^4 + X^5 + X^7$$

is an error as in Step 1. *We write*

$$\vec{e} = \pi_f^{-1}((1 + X^3 + X^4 + X^5 + 2X^7 + X^8 + X^{10} + X^{12} + X^{13} + X^{14}) \cdot e'')$$

and decoding $\vec{m}' = \vec{m}'' - \vec{e}$.

Chapter 4

Product Semi-Linear Codes

Recently there has been a lot of interest in algebraic codes in the setting of skew polynomial rings which form an important family of non-commutative rings. Skew polynomials rings have found applications in the construction of algebraic codes, where codes are defined as ideals (submodules) in the quotient rings (modules) of skew polynomials rings. The main motivation for considering these codes is that polynomials in skew polynomial rings exhibit many factorizations and hence there are many more ideals in a skew polynomial ring than in the commutative case. Furthermore, the research on codes in this setting has resulted in the discovery of many new codes with better Hamming distance than any previously known linear code with same parameters.

In this chapter, we introduce the notion of product semi-linear T-codes, a generalization of module skew codes and a subcase of linear codes invariant under a semi-linear transformation T of $\mathbb{F}_q^n$ with $n \geq 2$. In particular, we study from a theoretical point of view some properties of the Euclidean, Quasi-Euclidean and Hermitian dual codes of products semi-linear T-codes and the main relations among them. Finally, we show a method for encoding, decoding and detecting errors by the above code and we give an algorithm to construct a code invariant under any given semi-linear transformation.

4.1 Notation and background material

Denote by $\theta : \mathbb{F}_q \to \mathbb{F}_q$ an automorphism of the finite field $\mathbb{F}_q$. Let us recall here that if $q = p^s$ for some prime number p, then the map $\tilde{\theta} : \mathbb{F}_q \to \mathbb{F}_q$ defined by $\tilde{\theta}(a) = a^p$ is an automorphism on the field $\mathbb{F}_q$ which fixes the subfield with p elements. This automorphism $\tilde{\theta}$ is called the *Frobenius automorphism* and it has order s. Moreover, it is known that the cyclic group it generates is the full group of automorphisms of $\mathbb{F}_q$, i.e. $\mathrm{Aut}(\mathbb{F}_q) =< \tilde{\theta} >$. Therefore, any $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ is defined as $\theta(a) := \tilde{\theta}^t(a) = a^{p^t}$, where $a \in \mathbb{F}_q$ and t is an integer such that $0 \leq t \leq s$. Furthermore, when θ will be the identity automorphism $id : \mathbb{F}_q \to \mathbb{F}_q$, we will write simply $\theta = id$.

From [8], a semi-linear map $T : \mathbb{F}_q^n \to \mathbb{F}_q^n$ is the composition of an automorphism θ of $\mathbb{F}_q$ with an $\mathbb{F}_q$-linear transformation M, i.e. $(\vec{v})T := (\vec{v})\Theta \circ M$, where $(v_1, ..., v_n)\Theta := (\theta(v_1), ..., \theta(v_n))$ and M is an $n \times n$ matrix with coordinates in $\mathbb{F}_q$. In this case we call T a *θ-semi-linear map*, or a *θ-semi-linear transformation.*

For any $\vec{v} \in \mathbb{F}_q^n$ and any T as above, let $[\vec{v}]$ denote the T-cyclic subspace of $\mathbb{F}_q^n$ spanned by $\{\vec{v}, (\vec{v})T, (\vec{v})T^2, ...\}$.

Vector subspaces $\mathscr{C}_T \subset \mathbb{F}_q^n$ invariant by a θ-semi-linear transformation T will be called here *semi-linear T-codes*, or *T-codes* for simplicity.

Remark 4.1.1. *If $\theta = id$, then $\mathscr{C}_T$ is invariant by M. If $\theta \neq id$ and $M = A_c$, where A_c is as in* Definition 3.2.1*, then $\mathscr{C}_T$ is invariant by $\Theta \circ A_c$ and we can observe that this code is a generalization of an A_c-GC code.*

The main result of [13] allows us to decompose the vector space $\mathbb{F}_q^n$ into a direct sum of very special vector subspaces and to find a normal canonical form for any θ-semi-linear transformation.

Definition 4.1.2. *Let A and B be two matrices. We say that A* ***is θ-similar to*** *B, and we write $A \sim_\theta B$, if there exists an invertible matrix C such that $A = (C_\theta)^{-1}BC$, where C_θ is the matrix obtained by applying the automorphism θ to each entry of C. Moreover, we say that two θ-semi-linear maps $T = \Theta \circ M$ and $T' = \Theta \circ M'$ of $\mathbb{F}_q^n$ are θ-similar if $M \sim_\theta M'$ and in this case we simply write $T \sim_\theta T'$.*

By choosing the basis of $\mathbb{F}_q^n$ to be the union of appropriate bases

$$\{\vec{u}_i, T(\vec{u}_i), T^2(\vec{u}_i), ..., T^{\dim[\vec{u}_i]-1}(\vec{u}_i)\}$$

of T-cyclic subspaces $[\vec{u}_i]$, $i = 1, ..., r$, it follows immediately the existence of a normal canonical form for any θ-semi-linear map T.

Theorem 4.1.3 ([13], Theorem 5)**.** *Let θ and T be an automorphism of $\mathbb{F}_q$ and a θ-semi-linear transformation on $\mathbb{F}_q^n$, respectively. Then*

$$\mathbb{F}_q^n = [\vec{u}_1] \oplus ... \oplus [\vec{u}_r],$$

for T-cyclic subspaces $[\vec{u}_i]$ satisfying $\dim[\vec{u}_1] \geq \dim[\vec{u}_2] \geq ... \geq \dim[\vec{u}_r]$. Moreover, if $T = \Theta \circ M$ then

$$T \sim_\theta \Theta \circ \operatorname{diag}(M_1, ..., M_r),$$

where $M \sim_\theta \operatorname{diag}(M_1, ..., M_r)$ and each M_i is a $n_i \times n_i$ matrix of the following form

$$\left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline a_{i,0} & a_{i,1} & \dots & a_{i,n_i-1} \end{array}\right)$$

with $n_i \geq 1$ and such that $\sum_{i=1}^r n_i = n$.

Construction: We recall here the construction of the vectors $\vec{u}_i$, $i = 1, ..., r$, which appear in the above result (see [13, §6]). Let $\{\vec{e}_1, ..., \vec{e}_n\}$ be a basis for $\mathbb{F}_q^n$ and suppose that the θ-semi-linear map T sends $\vec{e}_k$ into

$$\vec{e}_k T = \vec{e}_1 \tau_{1k} + ... + \vec{e}_n \tau_{nk},$$

for $k = 1, ..., n$, or using the usual rule of matrix multiplication

$$(\vec{e}_1 T, ..., \vec{e}_n T) = (\vec{e}_1, ..., \vec{e}_n)\mathscr{T},$$

where $\mathscr{T} = [\tau_{ij}]$.

Let $\mathbb{F}_q^n[t]$ be the extension of $\mathbb{F}_q^n$ obtained by allowing the coefficients to range in $\mathbb{F}_q[t,\theta]$, i.e. $\mathbb{F}_q^n[t]$ is the totally of forms $\vec{x}(t) := \sum_{i=1}^n \vec{e}_i\xi_i(t)$, where $\xi_i(t) \in \mathbb{F}_q[t,\theta]$. Note that this definition is independent of the choice of basis of $\mathbb{F}_q^n$ and that $\mathbb{F}_q^n[t]$ is an abelian group under addition. The correspondence $\vec{x}(t) \to \vec{x}(t)a(t)$ with $a(t) \in \mathbb{F}_q[t,\theta]$ is an automorphism of this group. Thus $\mathbb{F}_q^n[t]$ may be looked upon as an abelian group $(\mathbb{F}_q^n[t], \mathbb{F}_q[t,\theta])$ with operators $\mathbb{F}_q[t,\theta]$. With $\vec{x}(t) := \sum_{i=1}^n \vec{e}_i\xi_i(t)$ we associate the vector $\vec{x} := \sum_{i=1}^n \vec{e}_i\xi_i(T)$ and with the automorphism $\vec{x}(t) \to \vec{x}(t)a(t)$ we associate the automorphism $\vec{x} \to \vec{x}a(T)$. These correspondences define a surjective operator homomorphism Φ of $(\mathbb{F}_q^n[t], \mathbb{F}_q[t,\theta])$ onto $(\mathbb{F}_q^n, \mathbb{F}_q[T,\theta])$. Define $f_1(t), ..., f_n(t)$ by

$$(f_1(t), ..., f_n(t)) = (\vec{e}_1, ..., \vec{e}_n)(\mathscr{T} - tI),$$

where $\mathscr{T} = [\tau_{ij}]$ and I denotes the unit matrix. From [13, Lemma 4] we know that $\{f_1(t), ..., f_n(t)\}$ is a basis for Ker Φ, the kernel of Φ. We may replace the bases $\{\vec{e}_1, ..., \vec{e}_n\}$ and $\{f_1(t), ..., f_n(t)\}$ of $\mathbb{F}_q^n[t]$ and Ker Φ respectively by

$$(\vec{e^*}_1(t), ..., \vec{e^*}_n(t)) = (\vec{e}_1, ..., \vec{e}_n)U(t)^{-1}$$

and

$$(f_1^*(t), ..., f_n^*(t)) = (f_1(t), ..., f_n(t))V(t),$$

where $U(t)$ and $V(t)$ are invertible matrices in the ring of matrices of n rows and columns with coordinates in $\mathbb{F}_q[t,\theta]$. Then we have

$$(f_1^*(t), ..., f_n^*(t)) = (\vec{e^*}_1(t), ..., \vec{e^*}_n(t))U(t)(\mathscr{T} - tI)V(t),$$

and in view of [13, §5] we may choose $U(t)$ and $V(t)$ so that $V(t)(\mathscr{T} - tI)U(t)$ has the form

$$\begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \mu_1(t) & & \\ & & & & \ddots & \\ & & & & & \mu_r(t) \end{pmatrix}$$

where the invariant factors $\mu_i(t)$ are bounded with bounds $\mu_i^*(t) = \mu_i(t)h_i(t)$ dividing $\mu_i(t)$ if $i < r$ and $i < j$ (e.g., see the Appendix 5.1).

Define $\vec{e^*}_i := \Phi(\vec{e^*}_i(t))$ for $i = 1, ..., r$. Since $\vec{e^*}_j(t) \in \text{Ker } \Phi$ for $j = 1, ..., n-r$, we have $\vec{e^*}_1 = \vec{0}, ..., \vec{e^*}_{n-r} = \vec{0}$. Thus denote by

$$\vec{u}_i := \vec{e^*}_{n-r+i} = \Phi(\vec{e^*}_{n-r+i}(t)),$$

for $i = 1, ..., r$. From [13, p. 496] it follows that if

$$\mu_i(t) = t^{m_i} - a_{i,m_i-1}t^{m_i-1} - ... - a_{i,2}t^2 - a_{i,1}t - a_{i,0},$$

then

$$(\vec{u}_1, \vec{u}_1T, ..., \vec{u}_1T^{m_1-1}, ..., ..., \vec{u}_r, \vec{u}_rT, ..., \vec{u}_rT^{m_r-1})$$

is a basis for $\mathbb{F}_q^n$.

This gives a construction method to find the vectors $\vec{u}_i$ of Theorem 4.1.3.

Remark 4.1.4. *By* Theorem 4.1.3*, we know that any θ-semi-linear transformation $T = \Theta \circ M$ is θ-similar to*

$$D := \Theta \circ \text{diag}(M_1, ..., M_r) = (\Theta \circ M_1, ..., \Theta \circ M_r),$$

i.e. there exists an invertible matrix

$$C := \begin{pmatrix} C_1 \\ \vdots \\ C_r \end{pmatrix}, \quad \text{where } C_i := \begin{pmatrix} \vec{u}_i \\ (\vec{u}_i)T \\ \vdots \\ (\vec{u}_i)T^{n_i-1} \end{pmatrix} \text{ for every } i = 1, ..., r,$$

such that

$$T = C^{-1}DC = C^{-1}(\Theta \circ \text{diag}(M_1, ..., M_r))C = C^{-1}(\Theta \circ M_1, ..., \Theta \circ M_r)C,$$

where $n_i := \dim[\vec{u}_i]$ for $i = 1, ..., r$ and each $\Theta \circ M_i$ is the θ-semi-linear transformation on $\mathbb{F}_q^{n_i}$ such that $\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ with $\sum_{i=1}^r n_i = n$. This gives a one -to-one correspondence between linear codes invariant under T and linear codes invariant under D. Therefore we can construct any semi-linear D-code $\mathscr{C}_D := \mathscr{C}_T \star C^{-1}$ from a semi-linear T-code $\mathscr{C}_T$, and vice versa.

Remark 4.1.5. *Let $T = \Theta \circ M$ be a θ-semi-linear transformation. If M is an $n \times n$ matrix with coordinates in $\mathbb{F}_q^\theta \subseteq \mathbb{F}_q$, the subfields of $\mathbb{F}_q$ fixed by θ, then M admits a rational normal form (by Magma command* `RationalForm(M)`*, i.e. there exists an invertible matrix C with coordinates in $\mathbb{F}_q^\theta$ such that $M = C^{-1}M'C$, where $M' := \operatorname{diag}(M_1, ..., M_k)$ and each M_i is a $n_i \times n_i$ matrix as in* Theorem 4.1.3 *defined over $\mathbb{F}_q^\theta$ (see* Example 3.1.9*) . Thus we have*

$$CTC^{-1} = C(\Theta \circ M)C^{-1} = \Theta \circ CMC^{-1} = \Theta \circ M' = D$$

and in this case it is easy to find a matrix C which transforms a T-code into a D-code, and vice versa. Typical examples of this situation are the skew quasi-cyclic codes, where the matrix M is a permutation matrix P such that $P = P_\theta = P_{\theta^{-1}}$.

Consider the ring structure defined on the following set:

$$R := \mathbb{F}_q[X;\theta] = \{a_sX^s + ... + a_1X + a_0 \mid a_i \in \mathbb{F}_q \text{ and } s \in \mathbb{N}\}.$$

The addition in R is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $X \cdot a = \theta(a)X$ for any $a \in \mathbb{F}_q$ and extended to all elements of R by associativity and distributivity. The ring R is known as skew polynomial ring and its elements are skew polynomials. Moreover, it is right Euclidean ring whose left ideals are principals.

From now on, together with the same notation as above, we will always assume the following

Hypothesis $(*)$ **:** *$T = \Theta \circ M$ is a fixed θ-semi-linear transformation of $\mathbb{F}_q^n$ which is θ-similar to $D := \Theta \circ \operatorname{diag}(M_1, ..., M_r)$ by a matrix C and $f_j := (-1)^{n_j}(X^{n_j} - \sum_{i=0}^{n_j-1} a_{j,i}X^i) \in R$ is the characteristic polynomial of M_j with $a_{j,0} \neq 0$, where the coefficients $a_{j,i}$ are given by* Theorem 4.1.3 *for every $j = 1, ..., r$ and $i = 0, ..., n_j - 1$.*

Denote by $\pi_j : \mathbb{F}_q^{n_j} \to R/Rf_j$ the linear transformation which sends a vector $\vec{c_j} = (c_0, ..., c_{n_j-1}) \in \mathbb{F}_q^{n_j}$ to the polynomial class $c_j(X) = \sum_{i=0}^{n_j-1} c_iX^i$ of R/Rf_j.

Moreover, consider the linear map

$$\pi : \ \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r} \to R_n := R/Rf_1 \times ... \times R/Rf_r,$$

where $\pi = (\pi_1, ..., \pi_r)$ and the linear transformation $\pi_j : \mathbb{F}_q^{n_j} \to R/Rf_j$ is defined as above for each $j = 1, ..., r$.

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code and define the linear code

$$\mathscr{C} \star C^{-1} := \{ \vec{c}\, C^{-1} \in \mathbb{F}_q^n \mid \vec{c} \in \mathscr{C} \}.$$

We can obtain now the following characterization of any T-code in $\mathbb{F}_q^n$.

Theorem 4.1.6. *With the same notation as in $(*)$, let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code and put $\mathscr{C}' := \mathscr{C} \star C^{-1}$. Then*

$\mathscr{C}$ is a T-code $\iff$ $\mathscr{C}'$ is a linear code invariant under D $\iff$ $\pi(\mathscr{C}')$ is a left R-submodule of R_n.

Proof. . From Remark 4.1.4, we know that any T-code can be written as $\mathscr{C}' \star C$, where $\mathscr{C}'$ is a linear code invariant by D, and vice versa. So it is sufficient to show that a linear code $\mathscr{C}'$ is invariant under D if and only if $\pi(\mathscr{C}')$ is a left R-submodule of R_n. Let $\mathscr{C}'$ be a linear code invariant by D. Note that $\pi(\mathscr{C}')$ is an abelian group with respect to the sum. Moreover, observe that $X \cdot \pi(\vec{v}) = \pi(\vec{v}D) \in \pi(\mathscr{C}')$ for any $\vec{v} \in \mathscr{C}'$. By an inductive argument and linearity, this implies that $g \cdot \pi(\vec{v}) \in \pi(\mathscr{C}')$ for any $g \in R$, that is, $\pi(\mathscr{C}')$ is an R-submodule of R_n. On the other hand, let $\pi(\mathscr{C}')$ be an R-submodule of R_n. Then $\mathscr{C}' = \pi^{-1}(\pi(\mathscr{C}'))$ is a vector subspace of $\mathbb{F}_q^n$ and for every $\vec{c} \in \mathscr{C}'$ we have $\vec{c}D = \pi^{-1}(X \cdot \pi(\vec{c})) \in \pi^{-1}(\pi(\mathscr{C}')) = \mathscr{C}'$, since $X \cdot \pi(\vec{c}) \in \pi(\mathscr{C}')$. □

Remark 4.1.7. *If $T = \Theta \circ M_1$, where M_1 is a matrix as in* Theorem 4.1.3 *with $a_{1,0} \neq 0$, then C in $(*)$ is the identity matrix and the above result becomes a geometric characterization of the module θ-codes (see* [4, Definition 1 and Proposition 1]*) associated to the polynomial $f_1 := (-1)^{n_1}(X^{n_1} - a_{1,n_1-1}X^{n_1-1} - ... - a_{1,0})$. Moreover, if $\theta = id$, then* Theorem 4.1.6 *generalizes* [14, (2.1)].

Example 4.1.8. *In $\mathbb{F}_4^6$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$, consider the matrix*

$$D = \left(\begin{array}{c|c} E & O \\ \hline O & E \end{array}\right), \quad \text{where } E = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ and } O = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

and the semi-linear transformation $\Theta \circ D$*. The code* $\mathscr{C} = \langle\ (1,1,1,1,1,1)\ \rangle$ *is invariant by* $\Theta \circ D$*,* $\mathscr{C} \cong \langle\ (1,1,1,0,0,0)\ \rangle = \langle\ (1,1,1)\ \rangle \times \langle\ (0,0,0)\ \rangle$*, but* $\mathscr{C} \neq \mathscr{C}_1 \times \mathscr{C}_2$ *for any* θ*-code* $\mathscr{C}_i \subseteq \mathbb{F}_4^3$ *invariant by* $\Theta \circ E$ *for* $i = 1, 2$*.*

Remark 4.1.9. *In the commutative case, i.e.* $\theta = id$*, the Chinese Remainder Theorem says that if* $(f_1), ..., (f_k)$ *are ideals of* R *which are pairwise coprime, that is* $(f_i) + (f_j) = R$ *for all* $i \neq j$*, then* $I := (f_1) \cap ... \cap (f_k) = (f_1) \cdot ... \cdot (f_k)$ *and the quotient ring* R/I *is isomorphic to the product ring* $R/(f_1) \times ... \times R/(f_k)$ *via the isomorphism* $\psi : R/I \to R/(f_1) \times ... \times R/(f_k)$ *such that* $\psi(a + I) := (a + (f_1), ..., a + (f_k))$*.*

In the non-commutative case there exists an analogous of the above result. When $\theta \neq id$*, if* $Rf_1, ..., Rf_k$ *are pairwise coprime two-sided ideals of* R*, then*

$$R/(Rf_1 \cap ... \cap Rf_k) \cong R/Rf_1 \times ... \times R/Rf_k$$

as R*-modules and* $I := Rf_1 \cap ... \cap Rf_k$ *can be replaced by a sum over all orderings of* $Rf_1, ..., Rf_k$ *of their product (or just a sum over enough orderings, using inductively that* $J \cap K = JK + KJ$ *for coprimes ideals* J, K*). In both situations, we have a method to find all the* R*-submodules of* $R/Rf_1 \times ... \times R/Rf_k$ *via* R/I*.*

Example 4.1.10. *In the case* $\theta = id$*, consider the finite field* $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ *with* $\alpha^2 + \alpha + 1 = 0$ *and the polynomials* $f_1 = X + \alpha^2$*,* $f_2 = X^2 + \alpha^2 X + \alpha$ *in* $R := \mathbb{F}_4[X]$*. By the Magma command* `Factorization`*, we can see that* $\gcd(f_1, f_2) = 1$*. Then we can consider the ideal* $I := (f_1) \cap (f_2) = (\operatorname{lcm}(f_1, f_2)) = (X^3 + 1)$ *and the isomorphism*

$$\begin{array}{rccc} \psi : & R/I & \longrightarrow & R/(f_1) \times R/(f_2) \\ & p + I & \longmapsto & (p + (f_1), p + (f_2)) \end{array}.$$

By the Magma command `Factorization` *we obtain* $X^3 + 1 = (X+1)(X+\alpha)(X+\alpha^2)$*. Thus* R/I *has* 6 *non-trivials* R*-submodules which correspond to* 6 *non-trivials* R*-submodules of* $R/(f_1) \times R/(f_2)$ *via* f*. For instance, since* $((X + \alpha)(X + \alpha^2)) = (X^2 + X + 1)$ *is an* R*-submodule of* R/I *and* $\psi(X^2 + X + 1) = (0, \alpha X + \alpha^2 + (f_2))$*, the ideal* $(0) \times (X + \alpha)$ *is an* R*-submodule of* $R/(f_1) \times R/(f_2)$*.*

Finally, we have the following two results.

Theorem 4.1.11. *Suppose that $\theta = id$. Then any R-submodule S of $R_n = R/Rf_1 \times ... \times R/Rf_r$ is R-isomorphic to a product $S_1 \times ... \times S_r$, where each S_j is an R-submodule of R/Rf_j for every $j = 1, ..., r$. In particular, any D-code $\mathscr{C}_D \subseteq \mathbb{F}_q^n$ with $D = \mathrm{diag}(M_1, ..., M_r)$ is isomorphic to a product code $\mathscr{C}_1 \times \cdots \times \mathscr{C}_r \subseteq \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ as a vector subspace of $\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$, i.e. $\mathscr{C}_D = (\mathscr{C}_1 \times \cdots \times \mathscr{C}_r) \star \widehat{C}$ for some invertible matrix $\widehat{C}$, where each $\mathscr{C}_i \subseteq \mathbb{F}_q^{n_i}$ is a linear code invariant by M_i, M_i being the $n_i \times n_i$ matrix of* Theorem 4.1.3.

Proof. It is sufficient to prove the first part of the statement for $r \geq 2$, since the second one follows immediately from this by putting $n_i := \deg f_i$ for $i = 1, ..., r$.

If each polynomial $f_j \in R$ is written as a product $F_{j1}^{a_{j1}} \cdots F_{jt_j}^{a_{jt_j}}$ of distinct irreducible polynomials F_{jk} for some integers $a_{ji} \geq 1$, then by the Chinese Reminder Theorem we can obtain via isomorphisms a decomposition A of $R_n = R/Rf_1 \times ... \times R/Rf_r$ such that

$$A := (R/RF_{11}^{a_{11}} \times ... \times R/RF_{1t_1}^{a_{1t_1}}) \times ... \times (R/RF_{r1}^{a_{r1}} \times ... \times R/RF_{rt_r}^{a_{rt_r}}) \cong R_n.$$

Let S be an R-submodule of R_n. Then, up to isomorphisms, S corresponds to an R-submodule S' of A. Thus we have to prove only that every R-submodule S' of A is isomorphic to a product $S_{11} \times ... \times S_{rt_r} \subseteq A$ of R-submodules $S_{ij_i} \subseteq R/RF_{ij_i}^{a_{ij_i}}$ for every $i = 1, ..., r$ and $j_i = 1, ..., t_i$.

So, let W be an R-submodule of A. Then W is R-isomorphic to a direct sum $Rg_1 \oplus \cdots \oplus Rg_k$ of non-zero distinct cyclic R-submodules Rg_i of A with $g_i \in A$ for $i = 1, ..., k$. Consider the surjective R-homomorphism $\pi_i : R \to Rg_i$ and note that $Rg_i \cong R/(\mathrm{Ker}\ \pi_i)$ for any $i = 1, ..., k$. Since R is a principal ideal domain, we see that $\mathrm{Ker}\ \pi_i = (p_i)$ for some $p_i \in R$. Let F be the product $F_{11}^{a_{11}} \cdot ... \cdot F_{st_s}^{a_{st_s}}$ of all distinct polynomials with the respective maximum powers which appear in the decompositions $F_{j1}^{a_{j1}} \cdots F_{jt_j}^{a_{jt_j}}$ of the polynomials f_j. Then we deduce that $F \in \mathrm{Ker}\ \pi_i = (p_i)$, i.e. for every $i = 1, ..., k$ there exists a polynomial q_i such that $F = q_i p_i$. This implies that $p_i = F_{11}^{c_{11}} \cdot ... \cdot F_{st_s}^{c_{st_s}}$ for some integers c_{jt_j} such that $0 \leq c_{jt_j} \leq a_{jt_j}$ for every $i = 1, ..., k$ and $j = 1, ..., s$. So we conclude that

$$Rg_i \cong R/(p_i) = R/(F_{11}^{c_{11}} \cdot ... \cdot F_{st_s}^{c_{st_s}}) \cong R/F_{11}^{c_{11}} \times ... \times R/F_{st_s}^{c_{st_s}} \subseteq A,$$

i.e. $Rg_i \cong RF_{11}^{a_{11}-c_{11}}/F_{11}^{a_{11}} \times ... \times RF_{st_s}^{a_{st_s}-c_{st_s}}/F_{st_s}^{a_{st_s}} \cong S_{11} \times ... \times S_{rt_r} \subseteq A$, where $\{0\} \subseteq S_{ij_i} \subseteq R/RF_{ij_i}^{a_{ij_i}}$ is an R-submodule for every $i = 1, ..., r$ and $j_i = 1, ..., t_i$. □

Proposition 4.1.12. *Suppose that $\theta \neq id$. If $R_n = R/Rf_1 \times ... \times R/Rf_r$ with $Rf_1, ..., Rf_r$ pairwise coprime two-sided ideals of R, then any R-submodule S of $R_n = R/Rf_1 \times ... \times R/Rf_r$ is R-isomorphic to a product $S_1 \times ... \times S_r$, where each S_j is an R-submodule of R/Rf_j for every $j = 1, ..., r$. In particular, any D-code $\mathscr{C}_D \subseteq \mathbb{F}_q^n$ is isomorphic to a product code $\mathscr{C}_1 \times \cdots \times \mathscr{C}_r \subseteq \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ as a vector subspace of $\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$, i.e. $\mathscr{C}_D = (\mathscr{C}_1 \times \cdots \times \mathscr{C}_r) \star \widehat{C}$ for some invertible matrix $\widehat{C}$, where each $\mathscr{C}_i \subseteq \mathbb{F}_q^{n_i}$ is a linear code invariant by $\Theta \circ M_i$, M_i being the $n_i \times n_i$ matrix of* Theorem 4.1.3.

Proof. Let S be an R-submodule of R_n. Then S is R-isomorphic to a direct sum $Rg_1 \oplus \cdots \oplus Rg_k$ of non-zero distinct cyclic R-submodules Rg_i of R_n with $g_i \in R_n$ for $i = 1, ..., k$. Write $g_i = (g_{i1}, ..., g_{ir})$ and consider the polynomial $F := f_1 \cdot ... \cdot f_r$. Denote by F_h the product F without the factor f_h. Then we get

$$F_h g_i = (0, ..., 0, F_h g_{ih}, 0, ..., 0).$$

Since the (right) $g.c.m.(f_h, F_h) = 1$, we know that there exist two polynomials $a, b \in R$ such that $af_h + bF_h = 1$. Hence $bF_h g_i = (0, ..., 0, g_{ih}, 0, ..., 0)$ for every $i = 1, ..., k$ and $h = 1, ..., r$. Therefore we have

$$Rg_i = R(g_{i1}, 0, ..., 0) \oplus ... \oplus R(0, ..., 0, g_{ir}) \cong (Rg_{i1}, ..., Rg_{ir})$$

for every $i = 1, ..., k$, i.e. $S \cong Rg_1 \oplus \cdots \oplus Rg_k \cong (S_1, ..., S_r)$ for some R-submodules $S_j \subset R/Rf_j$, where $j = 1, ..., r$. □

4.2 Product semi-linear codes

Let us recall here the following

Definition 4.2.1 (see [4])**.** *An f_j-**module θ-code** (or simply a **module θ-code**) $\mathscr{C}_j$ is a linear code in $\mathbb{F}_q^{n_j}$ which corresponds via $\pi_j : \mathbb{F}_q^{n_j} \to R/Rf_j$ to a left R-submodule $Rg_j/Rf_j \subset R/Rf_j$ in the basis $1, X, ..., X^{n_j - 1}$, where g_j is a right divisor of f_j in R. The length of the code $\mathscr{C}_j$ is $n_j = \deg(f_j)$ and its dimension is $k_j = \deg(f_j) - \deg(g_j)$. For simplicity, we will denote this code $\mathscr{C}_j = (g_j)_{n_j,q}^{k_j,\theta}$ and when there will not be any confusion, we will call an f_j-module θ-code simply a module θ-code.*

Remark 4.2.2. *When $\theta = id$, by* Proposition 3.2.7 *the above* Definition 4.2.1 *coincides with the definition of an A_c-GC code (see* Definition 3.2.1*).*

From Theorem 4.1.11, Proposition 4.1.12 and Definition 4.2.1, it follows naturally the below

Definition 4.2.3. *Let $\mathscr{C}_T \subseteq \mathbb{F}_q^n$ be a semi-linear T-code invariant by a θ-semi-linear map T as in $(*)$. We say that $\mathscr{C}_T$ is a **product semi-linear T-code**, or **a product T-code**, if $\mathscr{C}_T = (\mathscr{C}_1 \times \ldots \times \mathscr{C}_r) \star C \subseteq \mathbb{F}_q^{n_1} \times \ldots \times \mathbb{F}_q^{n_r}$, where any $\mathscr{C}_j \subseteq \mathbb{F}_q^{n_j}$ is an f_j-module θ-codes with respect to $\Theta \circ M_j$ and $f_j = (-1)^{n_j}(X^{n_j} - \sum_{k=0}^{n_j-1} a_{j,k}X^k)$ is as in $(*)$ for every $j = 1, \ldots, r$ and $n = \sum_{j=1}^{r} n_j$.*

Remark 4.2.4. *When C is the identity matrix and $r = 1$, then* Definition 4.2.3 *is nothing else that the definition of an f_1-module θ-code.*

Remark 4.2.5. *When either $\theta = id$, or $\theta \neq id$ and $R_n = R/Rf_1 \times \ldots \times R/Rf_r$ with $Rf_1, \ldots, Rf_r$ pairwise coprime two-sided ideals of R,* Theorem 4.1.11 *and* Proposition 4.1.12 *show that any T-code $\mathscr{C}_T$ is isomorphic to a product T-code as vector spaces, i.e. for any T-code $\mathscr{C}_T \subseteq \mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times \ldots \times \mathbb{F}_q^{n_r}$ there exists an invertible matrix C' such that $\mathscr{C}_T = (\mathscr{C}_1 \times \ldots \times \mathscr{C}_r) \star CC'$ for some T-product code $(\mathscr{C}_1 \times \ldots \times \mathscr{C}_r) \star C \subseteq \mathbb{F}_q^{n_1} \times \ldots \times \mathbb{F}_q^{n_r}$.*

From Definition 4.2.3 we deduce that a generator matrix of a product semi-linear code $\mathscr{C}_T = (\mathscr{C}_1 \times \ldots \times \mathscr{C}_r) \star C$ is given by

$$\begin{pmatrix} G_1 & & & \\ & G_2 & & \\ & & \ddots & \\ & & & G_r \end{pmatrix} \cdot C,$$

where $k_i := \dim \mathscr{C}_i$, $\sum_{i=1}^{r} k_i = \dim \mathscr{C}_T$ and each block

$$G_i := \begin{pmatrix} \vec{g}_i \\ (\vec{g}_i)(\Theta \circ M_i) \\ \vdots \\ (\vec{g}_i)(\Theta \circ M_i)^{k_i - 1} \end{pmatrix}$$

is a $k_i \times n_i$ generator matrix of the module θ-code $\mathscr{C}_i = (g_i)^{k_i}_{n_i,\theta}$, where $\vec{g}_i = \pi_i^{-1}(g_i)$ and $\pi_i : \mathbb{F}_q^{n_i} \to R/Rf_i$ for every $i = 1, ..., r$.

Example 4.2.6. *Consider the vector space $\mathbb{F}_4^6$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$, and $\theta \in Aut(\mathbb{F}_4)$ such that $\theta(x) = x^2$. Let $T = \Theta \circ M$ be a semi-linear transformation where*

$$M = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Then T is θ-similar to $\Theta \circ diag(M_1, M_2)$, where $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $M_2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$, i.e. $T = C^{-1}(\Theta \circ diag(M_1, M_2))C$ with

$$C = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Let $\mathscr{C}_1 = (X + \alpha^2)^{1,\theta}_{2,4}$ be an f_1-module θ-code with $f_1 = X^2 + 1$ and let $\mathscr{C}_2 = (X^2 + \alpha X + 1)^{2,\theta}_{4,4}$ be an f_2-module θ-code with $f_2 = X^4 + X^2 + 1$. Since both $\pi_1(\mathscr{C}_1)$ and $\pi_2(\mathscr{C}_2)$ are R-submodules of R/Rf_1 and R/Rf_2 respectively, $\pi(\mathscr{C}_1 \times \mathscr{C}_2)$ is a R-submodules of $R/Rf_1 \times R/Rf_2$. Furthermore, by the Magma Program

```
F<w>:=GF(4);

E:=[x : x in F | x ne 0];
```

```
RightDivisors := function(qq,g)
R<x>:=TwistedPolynomials(F:q:=qq);
f:=R!g;
n:=Degree(f);
S:=CartesianProduct(E,CartesianPower(F,n-1));
dd:=[];
for ss in S do
ll:=[ss[1]] cat [p : p in ss[2]];
q,r:=Quotrem(f,R!ll);
if r eq R![0] then dd := dd cat [[q,R!ll]]; end if;
end for;
return dd;
end function;
```

we see that the polynomials X^2+1 and X^4+X^2+1 are coprimes. Since $R(X^2+1)$ and $R(X^4+X^2+1)$ are two-sided ideal of R, by Proposition 4.1.12 *we conclude that $\mathscr{C}_T := (\mathscr{C}_1 \times \mathscr{C}_2) \star C$ is a product T-code. Note that $\mathscr{C}$ is a code of type $[6,3]_4$. Furthermore, the following matrix*

$$G = \left(\begin{array}{cc|cccc} \alpha^2 & 1 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & \alpha & 1 & 0 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 \end{array}\right) \cdot C = \begin{pmatrix} \alpha & \alpha^2 & 1 & \alpha^2 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ \alpha & 1 & \alpha^2 & \alpha^2 & 1 & \alpha^2 \end{pmatrix}$$

is a generator matrix of $\mathscr{C}_T$.

Definition 4.2.7. *A linear code $\mathscr{C}$ is a code of type $[n,k]_q$ if $\mathscr{C} \subseteq \mathbb{F}_q^n$ and $\dim \mathscr{C} = k$.*

The following result gives in the commutative case a necessary and sufficient condition for the existence of T-codes $\mathscr{C}_T$ of type $[n,k]_q$.

Theorem 4.2.8. *Suppose that $\theta = id$ and let $T = M$ be a linear transformation over $\mathbb{F}_q^n$ as in $(*)$. Let $\mathbb{F}_q^n = \mathbb{F}_q^{N_1} \times ... \times \mathbb{F}_q^{N_s}$ be a decomposition of $\mathbb{F}_q^n$ as in the proof of* Theorem 4.1.11 *and denote by π the corresponding isomorphism*

$$\pi : \mathbb{F}_q^n = \mathbb{F}_q^{N_1} \times ... \times \mathbb{F}_q^{N_s} \to R/RF_1^{\alpha_1} \times ... \times R/RF_s^{\alpha_s},$$

where $\pi = (\pi_1, ..., \pi_s)$ *and* $\pi_j : \mathbb{F}_q^{N_j} \to R/RF_j$ *are the usual isomorphisms and the* F_j*'s are irreducible (not necessarily distinct) polynomials on* R *such that* $N_j = \alpha_j \deg F_j \geq 1$ *for* $j = 1, ..., s$*. Then*

$\exists$ *a* T*-code of type* $[n,k]_q \iff k = \sum_{i=1}^{s} a_i \deg F_i$*, where* $0 \leq a_i \leq \alpha_i$*.*

Proof. . Note that for every $i = 1, ..., s$ an R-submodule of $R/RF_i^{\alpha_i}$ is of type $RF_i^{h}/RF_i^{\alpha_i} \cong R/RF_i^{\alpha_i - h}$ for some integer h such that $0 \leq h \leq \alpha_i$. Moreover, observe that by Remark 4.1.4 the set of the T-codes $\mathscr{C}_T$ is in one-to-one correspondence with the set of linear codes $\mathscr{C}_D$ invariant by the linear transformation $D := \text{diag}(M_1, ..., M_r)$ of type $[n,k]_q$. Let $\mathscr{C}_T \subset \mathbb{F}_q^n$ be a T-code of type $[n,k]_q$. Then $\mathscr{C}_T \star C^{-1}$ is a linear code $\mathscr{C}_D$ invariant by the linear transformation $D := \text{diag}(M_1, ..., M_r)$. With the same notation as in the statement, $\pi(\mathscr{C}_D)$ is an R-submodule of $R/RF_1^{\alpha_1} \times ... \times R/RF_s^{\alpha_s}$. Since by Theorem 4.1.11 every R-submodule of $R/RF_1^{\alpha_1} \times ... \times R/RF_s^{\alpha_s}$ is isomorphic to $I_1 \times ... \times I_s$ with I_j an R-submdule of $R/RF_j^{\alpha_j}$ for every $j = 1, ..., s$, we conclude that $k := \dim \mathscr{C}_T = \dim \mathscr{C}_D = \sum_{i=1}^{s} a_i \deg F_i$, where $0 \leq a_i \leq \alpha_i$. On the other hand, assume that $k = \sum_{i=1}^{s} a_i \deg F_i$ with $0 \leq a_i \leq \alpha_i$. Then the product code

$$\pi_1^{-1}(RF_1^{\alpha_1 - a_1}/RF_1^{\alpha_1}) \times ... \times \pi_s^{-1}(RF_s^{\alpha_s - a_s}/RF_1^{\alpha_s}) =$$

$$= \pi^{-1}(RF_1^{\alpha_1 - a_1}/RF_1^{\alpha_1} \times ... \times RF_s^{\alpha_s - a_s}/RF_1^{\alpha_s})$$

is a T-code of type $[n,k]_q$. □

4.3 Dual codes of product T-codes

In this section we study three kind of dual codes of product semi-linear T-codes and some main relations between them.

4.3.1 Euclidean duals

In [4] the authors prove that the Euclidean dual code of a module θ-code is a module θ-code if and only if it is a θ-constacyclic code. Moreover, they establish that a module θ-code which is not θ-constacyclic code is a shortened θ-constacyclic code and that its Euclidean dual is a punctured

θ-constacyclic code. This enables them to give a form of the parity-check matrix for module θ-codes.

Let us only observe here that there exists an alternative method to find a parity-check matrix for any module θ-code.

Proposition 4.3.1. *Let $\mathscr{C}_j = (g_j)_{n_j,\theta}^{k_j} \subseteq \mathbb{F}_q^{n_j}$ be a module θ-code. For any integer i such that $0 \leq i \leq k_j - 1$, write in R*

$$X^{n_j-k_j+i} = q_i g_j + r_i, \text{ with } 0 \leq \deg r_i < n_j - k_j.$$

Denote by S the following matrix

$$S := \begin{pmatrix} \rho_{n_j-k_j}(\pi_j^{-1}(r_0)) \\ \rho_{n_j-k_j}(\pi_j^{-1}(r_1)) \\ \vdots \\ \rho_{n_j-k_j}(\pi_j^{-1}(r_{k_j-1})) \end{pmatrix},$$

where $\pi_j : \mathbb{F}_q^{n_j} \to R/Rf_j$ and $\rho_{n_j-k_j}$ is the projection map onto the first $n_j - k_j$ coordinates, i.e.

$$\rho_{n_j-k_j}(v_1, ..., v_{n_j-k_j}, v_{n_j-k_j+1}, ..., v_{n_j}) := (v_1, ..., v_{n_j-k_j}).$$

Then a generator matrix G_j of $\mathscr{C}_j$ is

$$G_j := \left(\begin{array}{c|c} -S & I_{k_j} \end{array} \right)$$

and a parity check matrix H_j is given by

$$H_j := \left(\begin{array}{c|c} I_{n_j-k_j} & S_t \end{array} \right),$$

where $I_{n_j-k_j}$ is the $(n_j - k_j) \times (n_j - k_j)$ identity matrix and S_t is the transpose matrix of S.

Proof. Since $\deg r_i < n_j - k_j$, note that $\pi_j^{-1}(X^{n_j-k_j+i} - r_i) \in \mathscr{C}_j$ are linearly independent for $0 \leq i \leq k_j - 1$. Thus $\left(\begin{array}{c|c} -S & I_{k_j} \end{array} \right)$ is a generator matrix G_j for the code $\mathscr{C}_j$. Moreover, since $(\mathscr{C}_j^{\perp})^{\perp} = \mathscr{C}_j$, we see that the matrix $H_j := \left(\begin{array}{c|c} I_{n_j-k_j} & S_t \end{array} \right)$ as in the statement is a parity check matrix for $\mathscr{C}_j$. $\square$

By the Magma program

```
F<w>:=GF(4);
PcMatrix:=function(qq,g,n)
R<x>:=TwistedPolynomials(F:q:=qq);
g:=R!g;
d:=Degree(g);
ll:=[];
for i in [0.. n-d-1] do
a,b:=Quotrem(R![1]*R![0,1]^(d+i),g);
ll:=ll cat [b];
end for;
return ll;
end function;
```

we can find the parity-check matrix of Proposition 4.3.1

Remark 4.3.2. Proposition 4.3.1 *works also for any module* (θ, δ)*-code (see* [5, Definition 1]*), where* $\delta : \mathbb{F}_q \to \mathbb{F}_q$ *is a derivation, and it allows us to obtain directly a generator and a parity-check matrix in standard form for any module* (θ, δ)*-code.*

Theorem 4.3.3. *Let* $\mathscr{C}_T = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star \widehat{C} \subseteq \mathbb{F}_q^n$ *be a linear code,* $\mathscr{C}_i \subseteq \mathbb{F}_q^{n_i}$ *being a linear code and* $\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$*. If* $\widehat{C}$ *is an invertible matrix, then*

$${\mathscr{C}_T}^{\perp} = (\mathscr{C}_1^{\perp} \times ... \times \mathscr{C}_r^{\perp}) \star \widehat{C}_t^{-1},$$

where $\widehat{C}_t$ *is the transpose matrix of* $\widehat{C}$ *and* $\mathscr{C}_i^{\perp} \subseteq \mathbb{F}_q^{n_i}$ *is the Euclidean dual code of* $\mathscr{C}_i$ *for every* $i = 1, ..., r$*. Furthermore, a parity check matrix of* $\mathscr{C}_T$ *is*

$$\begin{pmatrix} H_1 & & \\ & \ddots & \\ & & H_r \end{pmatrix} \cdot \widehat{C}_t^{-1}$$

where $h_i := \dim \mathscr{C}_i^{\perp}$*,* $\sum_{i=1}^{r} h_i = \dim \mathscr{C}_T^{\perp}$ *and* H_i *is the* $h_i \times n_i$ *parity check matrix of* $\mathscr{C}_i$ *given by* Proposition 4.3.1 *for every* $i = 1, ..., r$.

Proof. Put $\mathscr{C} := (\mathscr{C}_1^\perp \times ... \times \mathscr{C}_r^\perp) \star \widehat{C}_t^{-1}$ and note that

$$\dim \mathscr{C} = \dim(\mathscr{C}_1^\perp \times ... \times \mathscr{C}_r^\perp) = \sum_{i=1}^{r} \dim \mathscr{C}_i^\perp = \sum_{i=1}^{r}(m_i - \dim \mathscr{C}_i) =$$

$$= \sum_{i=1}^{r} m_i - \sum_{i=1}^{r} \dim(\mathscr{C}_i) = n - \dim \mathscr{C}_T = \dim {\mathscr{C}_T}^\perp.$$

Let $\vec{v} \in \mathscr{C}$. Since $\mathscr{C} = (\mathscr{C}_1^\perp \times ... \times \mathscr{C}_r^\perp) \star \widehat{C}_t^{-1}$, we deduce that $\vec{v} = \vec{w}\widehat{C}_t^{-1}$ for some vector $\vec{w} = (\vec{c_1}^\perp, ..., \vec{c_r}^\perp) \in (\mathscr{C}_1^\perp \times ... \times \mathscr{C}_r^\perp)$. Thus for every $\vec{c} = (\vec{c_1}, ..., \vec{c_r})\widehat{C} \in \mathscr{C}_T$, we see that

$$\vec{v} \cdot \vec{c} = \vec{w} C_t^{-1} \vec{c}_t = (\vec{c_1}^\perp, ..., \vec{c_r}^\perp)\widehat{C}_t^{-1}((\vec{c_1}, ..., \vec{c_r})\widehat{C})_t =$$

$$= (\vec{c_1}^\perp, ..., \vec{c_r}^\perp)(\vec{c_1}, ..., \vec{c_r})_t = \vec{c_1}^\perp \cdot \vec{c_1} + ... + \vec{c_r}^\perp \cdot \vec{c_r} = 0,$$

i.e. $\mathscr{C} \subseteq {\mathscr{C}_T}^\perp$. Since $\dim \mathscr{C} = \dim {\mathscr{C}_T}^\perp$, we conclude $\mathscr{C} = {\mathscr{C}_T}^\perp$.

Finally, the second part of the statement follows easily from the first one. □

Example 4.3.4. *Continuing with* Example 4.2.6*, by the Magma Program*

```
F<w>:=GF(4);

PcMatrix:=function(qq,g,n)

R<x>:=TwistedPolynomials(F:q:=qq);

g:=R!g;

d:=Degree(g);

ll:=[];

for i in [0.. n-d-1] do

a,b:=Quotrem(R![1]*R![0,1]^(d+i),g);

ll:=ll cat [b];

end for;

return ll;

end function;
```

and Proposition 4.3.1*, we deduce that the matrix*

$$H = \left(\begin{array}{cc|cccc} 1 & \alpha^2 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 & \alpha^2 \\ 0 & 0 & 0 & 1 & \alpha & 0 \end{array}\right) \cdot C_t^{-1}$$

is a parity-check matrix of $\mathscr{C}_T$, where $H_1 = (1\ \alpha^2)$ and $H_2 = \begin{pmatrix} 1 & 0 & 1 & \alpha^2 \\ 0 & 1 & \alpha & 0 \end{pmatrix}$ are the parity-check matrices of $\mathscr{C}_1$ and $\mathscr{C}_2$ respectively. Furthermore, by Theorem 4.3.3 *we can conclude that*

$$\mathscr{C}_T^{\perp} = (\mathscr{C}_1^{\perp} \times \mathscr{C}_2^{\perp}) \star C_t^{-1}$$

is the dual code of $\mathscr{C}_T$, where $\mathscr{C}_1^{\perp} = \langle(1, \alpha^2)\rangle$ and $\mathscr{C}_2^{\perp} = \langle(1, 0, 1, \alpha^2), (0, 1, \alpha, 0)\rangle$.

Remark 4.3.5. *The above result is useful to construct the Euclidean dual code and to calculate the minimum Hamming distance of any product T-code. In particular, when either $\theta = id$, or $\theta \neq id$ and $R_n = R/Rf_1 \times \ldots \times R/Rf_r$ with $Rf_1, \ldots, Rf_r$ pairwise coprime two-sided ideals of R,* Theorem 4.3.3 *together with* Theorem 4.1.11 and Proposition 4.1.12 *allow us to find the Euclidean dual code of every T-code.*

The proof of the below result is immediate.

Lemma 4.3.6. *We have the following two properties:*

(a) $\Theta \circ \overline{M}_\theta = \overline{M} \circ \Theta$, *for any matrix* $\overline{M} = [m_{ij}]$, *where* $\overline{M}_\theta := [\theta(m_{ij})]$;

(b) $(\vec{a}\ \Theta^{-1}) \cdot \vec{b} = 0 \iff \vec{a} \cdot (\vec{b}\ \Theta) = 0, \ \forall\ \vec{a}, \vec{b} \in \mathbb{F}_q^n$.

Finally, we obtain the following characterization of Euclidean dual codes of T-codes.

Proposition 4.3.7. *Let $\mathscr{C}_T \subseteq \mathbb{F}_q^n$ be a T-code invariant under a θ-semi-linear transformation $T = \Theta \circ \overline{M}$. Then the Euclidean dual code $\mathscr{C}_T^{\perp}$ is a T'-code, where $T' = \Theta^{-1} \circ (\overline{M}_t)_{\theta^{-1}}$.*

Proof. If $\vec{a} \in \mathscr{C}_T^{\perp}$, then for every $\vec{c} \in \mathscr{C}_T$ we have

$$(\vec{a}\overline{M}_t) \cdot (\vec{c}\ \Theta) = \vec{a}(\vec{c}\ \Theta \circ \overline{M})_t = \vec{a} \cdot (\vec{c}\ T) = 0.$$

Thus by Lemma 4.3.6 we deduce that

$$(\vec{a}\ T') \cdot \vec{c} = (\vec{a}\Theta^{-1} \circ (\overline{M}_t)_{\theta^{-1}}) \cdot \vec{c} = (\vec{a}\overline{M}_t \circ \Theta^{-1}) \cdot \vec{c} = 0,$$

for every $\vec{c} \in \mathscr{C}_T$, i.e. $\mathscr{C}_T^{\perp}$ is invariant under the semi-linear transformation T'. □

4.3.2 Quasi-Euclidean duals

In this subsection we introduce the new concept of quasi-Euclidean dual codes and some of their properties related to the Euclidean dual codes. Before to do this, we have to define a special injective map for module θ-codes.

An injective map for an f-module θ-code.

Given a polynomial $f \in R$ of degree $n \geq 2$, we present here an algorithm to show that there exists always a suitable integer $m \geq n$ such that $X^m - 1$ is a right multiple of f. This will allow us to construct an immersion map of the code space $\mathbb{F}_q^n$ into an $\mathbb{F}_q^m$ which will be useful for the definition of quasi-Euclidean dual codes of a product T-code.

Let $f = (-1)^n(X^n - \sum_{i=0}^{n-1} f_i X^i) \in R$ and consider the right division

$$X^n - 1 = f \cdot q_n + r_n,$$

where $q_n, r_n \in R$ and $0 \leq \deg r_n < \deg f$. Assume that r_n is not equal to zero, otherwise we are done.

Let k be an integer such that $k > n$ and consider again the right divisions

$$X^k - 1 = f \cdot q_k + r_k,$$

where $q_k, r_k \in R$ and $0 \leq \deg r_k < \deg f$. Since there are at most $q^{\deg r_k + 1}$ distinct polynomials r_k, we see that for some $k_2 > k_1 \geq n$ we get $r_{k_1} = r_{k_2}$. Thus we obtain that

$$X^{k_1} \cdot (X^{k_2 - k_1} - 1) = (X^{k_2 - k_1} - 1) \cdot X^{k_1} = f \cdot (q_{k_2} - q_{k_1}).$$

Put $q' := q_{k_2} - q_{k_1}$ and note that $q' \neq 0 \in R$. This shows that $X = 0$ is a root of $f \cdot q'$. Since $f(0) \neq 0$, we deduce that $q'(0) = 0$. Hence $q' = q_1 \cdot X$ for some $q_1 \in R$.

Thus we have

$$(X^{k_2 - k_1} - 1) \cdot X^{k_1} = f \cdot q_1 \cdot X$$

and since R has not non-zero zero divisors, we can deduce that

$$(X^{k_2 - k_1} - 1) \cdot X^{k_1 - 1} = f \cdot q_1$$

where $q_1 \in R$. By an inductive argument, we can conclude that

$$X^{k_2-k_1} - 1 = f \cdot q''$$

for some $q'' \in R$. This shows that there exists always an integer $t \geq n$ such that $X^t - 1 = f \cdot q_f$ for some non-zero $q_f = \sum_{i=0}^{m-n} q_i X^i \in R$.

From now on, we denote by m the minimum integer such that $m \geq n$ and $X^m - 1$ is a right multiple of f, i.e.

$$m := \min\left\{ i \in \mathbb{N} \mid X^i - 1 = f \cdot p \text{ for some } p \in R \right\} \ . \tag{**}$$

In this case, we write

$$X^m - 1 = f \cdot q_f \ .$$

Moreover, by the above construction, we have

$$n \leq m \leq q^n + n - 2.$$

By the Magma program

```
F<w>:=GF(4);
PeriodNc:=function(qq,g)
R<x>:=TwistedPolynomials(F:q:=qq);
f:=R!g;
n:=Degree(f)-1;
repeat
n:=n+1;
_,r:=Quotrem(X^n-1,f);
until r eq R![0];
return n;
end function;
```

we can calculate m in (**).

Let us introduce the following isomorphism of rings $\Theta : \; R \to R$ defined as

$$(\sum_{i=0}^{t} a_i X^i)\Theta := \sum_{i=0}^{t} \theta(a_i) X^i \ .$$

Lemma 4.3.8. *Put*

$$m^* := \min\left\{ j \in \mathbb{N} \mid X^j - 1 = p \cdot f^* \text{ for some } p \in R \right\} \ ,$$

where $f^* := 1 - \sum_{i=1}^{n} \theta^i(f_{n-i}) X^i \in R$*. Then* $m^* = m$*.*

Proof. Let $X^m - 1 = f \cdot q_f$. By [4, Lemma 1(1)] we know that $X^m - 1 = (1 - X^m)^* = (f \cdot (-q_f))^* = q' \cdot f^*$ for some $q' \in R$. This implies that $m \geq m^*$. On the other hand, let $X^{m^*} - 1 = q_{f^*} \cdot f^*$. By [4, Lemma 1] we see that

$$X^{m^*} - 1 = (1 - X^{m^*})^* = ((-q_{f^*}) \cdot f^*)^* =$$

$$= ((f^*)^*)\Theta^{m^*-n} \cdot q'' = ((f)\Theta^n)\Theta^{m^*-n} \cdot q'' = (f)\Theta^{m^*} \cdot q''$$

for some $q'' \in R$. Hence we get

$$X^{m^*} - 1 = (X^{m^*} - 1)\Theta^{-m^*} = ((f)\Theta^{m^*} \cdot q'')\Theta^{-m^*} = f \cdot (q'')\Theta^{-m^*},$$

i.e. $m^* \geq m$. This gives $m^* = m$. □

Remark 4.3.9. *If $\theta = id$, then the characteristic and minimal polynomial of*

$$A_c := \left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline f_0 & f_1 & \dots & f_{n-1} \end{array} \right)$$

are both equal to $f = (-1)^n (X^n - \sum_{i=0}^{n-1} f_i X^i) \in R$*. Let* $m' := \min\{i \in \mathbb{N} \mid A_c^i = I\}$ *and note that the polynomial* $X^{m'} - 1$ *is satisfied by* A_c*. Therefore, it follows that there exists a polynomial* $q_f = \sum_{i=0}^{m-n} q_i X^i \in R$ *such that* $X^{m'} - 1 = f \cdot q_f$*. This gives* $m = m'$*, that is,* $m = \min\{i \in \mathbb{N} \mid A_c^i = I\}$*.*

By the Magma Command `Order` we can calculate m in the commutative context.

The following example shows that Remark 4.3.9 does not hold in general when θ is not equal to the identity of $\mathbb{F}_q$.

Example 4.3.10. *In $\mathbb{F}_4^3$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$, consider the polynomial $f = X^3 + \alpha X + 1$ associated to the matrix*

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 0 \end{pmatrix}$$

and define $\theta(x) = x^2$ for any $x \in \mathbb{F}_4$. It follows that $\min\{i \in \mathbb{N} \mid A_c^i = I\} = 21$. Moreover, we have $X^{21} - 1 = f \cdot q + r$, where

$$q = X^{18} + \alpha^2 X^{16} + X^{15} + \alpha X^{14} + X^{13} + X^{10} + \alpha^2 X^8 + X^7 + \alpha X^6 + X^5 + X^2 + \alpha^2$$

and $r = X^2 + \alpha^2 X + \alpha \neq 0$. This shows that $m \neq \min\{i \in \mathbb{N} \mid A_c^i = I\}$. Moreover, we get $m = 8(< 21)$. Hence $X^8 - 1 = (X^3 + \alpha X + 1) \cdot q_f$ with $q_f = X^5 + \alpha^2 X^3 + X^2 + \alpha X + 1$.

In connection with the above arguments, we have the following results.

Proposition 4.3.11. *Let m be an integer as in $(**)$ and let P be the $m \times m$ matrix*

$$\left(\begin{array}{c|ccc} 0 & 1 & & \\ \vdots & & \ddots & \\ 0 & & & 1 \\ \hline 1 & 0 & \dots & 0 \end{array}\right).$$

Denote by $\vec{q_f} := (q_0, ..., q_{m-n}, 0, ..., 0) \in \mathbb{F}_q^m$, where the q_i's are the coefficients of $q_f \in R$ as in $(**)$. Then there exists a commutative diagram

$$\begin{tikzcd} \mathbb{F}_q^n \arrow[r, "i"] \arrow[d, "\pi"'] & \mathbb{F}_q^m \arrow[d, "\pi'"] \\ R_n \arrow[r, "j"'] & R_m \end{tikzcd}$$

such that $\pi' \circ i = j \circ \pi$*, where* $R_n := R/Rf$*,* $R_m := R/R(X^m - 1)$*,* $i(\vec{v}) := \vec{v}Q$ *with* Q *the matrix*

$$\begin{pmatrix} \vec{q_f} \\ (\vec{q_f})(\Theta \circ P) \\ (\vec{q_f})(\Theta \circ P)^2 \\ \dots \\ (\vec{q_f})(\Theta \circ P)^{n-1} \end{pmatrix}$$

and $j(a + Rf) := (a \cdot q_f) + R(X^m - 1)$ *for any* $a \in R$*.*

Proof. By using the canonical basis of $\mathbb{F}_q^n$, the statement follows easily from the linearity of the maps i, j, π and π'. □

Proposition 4.3.12. *With the same notation as in* Proposition 4.3.11*, for any* $\vec{c} \in \mathbb{F}_q^n$ *and* $k \in \mathbb{N}$ *we have*

$$i((\vec{c})(\Theta \circ A_c)^k) = (i(\vec{c}))(\Theta \circ P)^k,$$

where A_c *is the matrix defined in* Remark 4.3.9*.*

Proof. Let $\vec{c} \in \mathbb{F}_q^n$. By Proposition 4.3.11, we have the following two commutative diagrams:

$$\begin{tikzcd}
\vec{c} \arrow[r, "i"] \arrow[d, "\pi"'] & i(\vec{c}) \arrow[d, "\pi'"] \\
\pi(\vec{c}) \arrow[r, "j"'] & j(\pi(\vec{c}))
\end{tikzcd}$$

where $j(\pi(\vec{c})) = \pi'(i(\vec{c}))$, and

$$\begin{tikzcd}
(\vec{c})(\Theta \circ A_c)^k \arrow[r, "i"] \arrow[d, "\pi"'] & i((\vec{c})(\Theta \circ A_c)^k) \arrow[d, "\pi'"] \\
X^k \cdot \pi(\vec{c}) \arrow[r, "j"'] & j(X^k \cdot \pi(\vec{c}))
\end{tikzcd}$$

where $j(X^k \cdot \pi(\vec{c})) = \pi'(i((\vec{c})(\Theta \circ A_c)^k))$. Since π' is an isomorphism, by the commutative diagram of Proposition 4.3.11, we obtain

$$i((\vec{c})(\Theta \circ A_c)^k) = (\pi')^{-1}(j(X^k \cdot \pi(\vec{c}))) = (\pi')^{-1}(X^k \cdot \pi(\vec{c}) \cdot q_f) =$$

$$= (\pi')^{-1}(X^k \cdot j(\pi(\vec{c}))) = (\pi')^{-1}(X^k \cdot \pi'(i(\vec{c}))) = (\pi')^{-1} \circ \pi'((i(\vec{c}))(\Theta \circ P)^k),$$

that is, $i((\vec{c})(\Theta \circ A_c)^k) = (i(\vec{c}))(\Theta \circ P)^k$ for any $k \in \mathbb{N}$. □

Remark 4.3.13. *The maps i and j in* Proposition 4.3.11 *are injective. Moreover, em* Proposition 4.3.12 *shows that the image via i of an f-module θ-code in $\mathbb{F}_q^n$ is a module θ-cyclic code in $\mathbb{F}_q^m$, where m is defined as in $(**)$ (or as in* Remark 4.3.9*).*

Let s be the order of θ. From the above results, we can deduce the following two consequences.

Corollary 4.3.14. *Let m be as in $(**)$. If $m = as + r$, $0 \leq r < s$, then $(\vec{q_f})\Theta^r = \vec{q_f}$.*

Proof. Since $X^m - 1 = f \cdot q_f$ and f, q_f are monic polynomials, by [4, Lemma 2(2)] we see that $X^m = 1 + (q_f)\Theta^m \cdot f$. Since $(\Theta \circ P)^m = \Theta^m \circ P^m = \Theta^m$ and Θ^s is the identity, from the following commutative diagram

$$\begin{tikzcd}
\vec{e}_1(\Theta \circ A_c)^m \arrow[r, "i"] \arrow[d, "\pi"'] & i(\vec{e}_1)(\Theta \circ P)^m \arrow[d, "\pi'"] \\
X^m = 1 \arrow[r, "j"'] & j(1) = q_f
\end{tikzcd}$$

we conclude that $\vec{q_f} = (\pi')^{-1}(q_f) = i(\vec{e}_1)(\Theta \circ P)^m = (\vec{q_f})\Theta^m = (\vec{q_f})\Theta^r$. □

Corollary 4.3.15. *Let $f = (-1)^n(X^n - \sum_{i=0}^{n-1} f_i X^i) \in R$. If*

$$(f_0, f_1, ..., f_{n-1})\Theta^t \neq (f_0, f_1, ..., f_{n-1})$$

for every integer t such that $0 < t < s$, then the order s of Θ divides m.

Proof. Since $X^m - 1 = f \cdot q_f$, from Corollary 4.3.14 it follows that

$$f \cdot q_f = X^m - 1 = (X^m - 1)\Theta^m = (f)\Theta^m \cdot (q_f)\Theta^m = (f)\Theta^m \cdot q_f,$$

i.e. $f = (f)\Theta^m$. Let $m = as + r$ with $0 \leq r < s$.

Assume now that $r \neq 0$. Then we get $f = (f)\Theta^m = (f)\Theta^r$, that is,

$$(f_0, f_1, ..., f_{n-1})\Theta^r = (f_0, f_1, ..., f_{n-1})$$

for some $0 < r < s$, but this is a contradiction. Thus $r = 0$ and s divides m. □

Example 4.3.16. *In $\mathbb{F}_4^5$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$ and θ is the Frobenius map, consider the following two polynomials:*

(1) $f = X^5 + X^3 + X^2 + 1$; (2) $g = X^5 + X^2 + 1$.

Note that in both cases the hypothesis of Corollary 4.3.15 *is not satisfied. Moreover, we have* $m = 12$ *in case* (1) *and* $m = 31$ *in case* (2).

Finally, let us give here also some results about the integer m in $(**)$ when $\theta = id$.

Remark 4.3.17. *Let $\mathbb{F}_q \subseteq \mathbb{K}$ be a finite extension of $\mathbb{F}_q$ such that $f = \prod_{i=1}^{n}(X - a_i)$ with $a_i \in \mathbb{K}$ and A_c is diagonalizable over $\mathbb{K}$. If $m_i := \min\left\{h_i \mid a_i^{h_i} = 1\right\}$, then $m = lcm(m_1, ..., m_n)$.*

Remark 4.3.18. *Let* $p := \mathrm{Char}(\mathbb{F}_q)$. *If the polynomial f has a root of multiplicity ≥ 2, then $X^m - 1$ has a root of multiplicity ≥ 2. This shows that $gcd(m, p) \neq 1$ and since p is a prime number, we get* $m \equiv 0 \mod p$.

The next two results give a more simple computation of m.

Proposition 4.3.19. *Denote by* $\vec{f} := (f_0, ..., f_{n-1})$ *and let*

$$k := \min\left\{h \in \mathbb{N} \cup \{0\} \mid \vec{f} A_c^h = \vec{e}_1\right\}.$$

Then $m = n + k$. In particular, we have $\deg q_f = k$.

Proof. For any $h = 1, ..., n$, we have

$$\vec{e}_h\ A_c^{n+k} = ((\vec{e}_h A_c^{n-h+1}) A_c^k) A_c^{h-1} = ((\vec{e}_n A_c) A_c^k) A_c^{h-1} =$$

$$= (\vec{f} A_c^k) A_c^{h-1} = \vec{e}_1 A_c^{h-1} = \vec{e}_h.$$

Hence $A_c^{n+k} = I$ and for the minimality of m we deduce that $m \leq n+k$. Furthermore, since $A_c^m = I$ we get $\vec{e}_1 = ((\vec{e}_1 A_c^{n-1}) A_c) A_c^{m-n} = (\vec{e}_n A_c) A_c^{m-n} = \vec{f} A_c^{m-n}$, that is, $\vec{f} A_c^{m-n} = \vec{e}_1$. So, by definition of k we can conclude that $k \leq m - n$, i.e. $m \geq n + k$. Finally, observe that $\deg q_f = m - n := k$. □

Let p_0 be the order of $\det A_c$. Since $A_c^m = I$, it follows that $(\det A_c)^m = 1$, i.e. $m \equiv 0 \mod p_0$ with p_0 the order of $\det A_c$. Denote by $B := A_c^{p_0}$. From this it follows immediately also the following

Proposition 4.3.20. *Let m' be the minimum integer such that $B^{m'}$ is the identity matrix. Then $m = p_0 m'$. In particular, we have $\deg q_f = p_0 m' - n$.*

When $\theta = id$, all the above results give the following

Algorithm 3:

Input: f

- Define $a_0 := \det A_c$;
- Compute the order p_0 of a_0;
- Define $B := A_c^{p_0}$;
- Find the rational canonical form B' of B;
- For any diagonal block B_i, $i = 1, ..., s$, of B' compute $m_i' = \min\left\{h \mid B_i^h = I\right\}$.

Output: $m = lcm(m_1', ..., m_s') \cdot p_0$.

Definition and basic properties of quasi-Euclidean dual codes

Under the hypothesis $(*)$, write $\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ with $r \geq 1$ and $n = \sum_{k=1}^r n_k$. From Proposition 4.3.11, we know that for every $k = 1, ..., r$ there exists a commutative diagram

$$\begin{tikzcd}
\mathbb{F}_q^{n_k} \arrow[r, "i_k"] \arrow[d, "\pi_k"'] & \mathbb{F}_q^{m_k} \arrow[d, "\pi_k'"] \\
R/Rf_k \arrow[r, "j_k"'] & R/R(X^{m_k} - 1)
\end{tikzcd} .$$

Consider the further commutative diagram:

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[d, "\varphi := C^{-1}"'] \arrow[dr, "\bar{i}"] & \\
\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r} \arrow[r, "i"'] \arrow[d, "\pi"'] & \mathbb{F}_q^{m_1} \times ... \times \mathbb{F}_q^{m_r} = \mathbb{F}_q^m \arrow[d, "\pi'"'] \\
R_n \arrow[r, "j"'] & R_m
\end{tikzcd}$$

where $n = \sum_{i=1}^{r} n_i$, $m = \sum_{i=1}^{r} m_i$ with the m_i's as in $(*)$, $f_i = (-1)^{n_i}(X^{n_i} - \sum_{j=0}^{n_i-1} f_{i,j}X^j) \in R$,

$$R_n := R/Rf_1 \times ... \times R/Rf_r,$$

$$R_m := R/R(X^{m_1} - 1) \times ... \times R/R(X^{m_r} - 1),$$

$i(\vec{v}) := \vec{v}\widehat{Q}$ with

$$\widehat{Q} := \begin{pmatrix} Q_1 & & & \\ & Q_2 & & \\ & & \ddots & \\ & & & Q_r \end{pmatrix}$$

and all the Q_i's are matrices $n_i \times m_i$ as in Proposition 4.3.11, $\pi = (\pi_1, ..., \pi_r)$ with $\pi_i : \mathbb{F}_q^{n_i} \to R/Rf_i$, $\pi' = (\pi'_1, ..., \pi'_r)$ with $\pi'_i : \mathbb{F}_q^{m_i} \to R/R(X^{m_i} - 1)$ and

$$j(p_1, ..., p_r) := (p_1 \cdot q_{f_1}, ..., p_r \cdot q_{f_r})$$

with all the q_{f_i}'s polynomials in R as in Proposition 4.3.11.

Denote by $\mathscr{I}$ the image of $\bar{i} = i \circ \varphi$ and define

$$B := C^{-1}\widehat{Q}\ \widehat{Q}_t(C^{-1})_t,$$

where M_t is the transpose of a matrix M. Note that B is a symmetric matrix.

Let r be the rank of B and observe that

$$r := \mathrm{rk}B = \mathrm{rk}(\widehat{Q} \cdot \widehat{Q}_t) = n - \dim(\mathrm{Ker}\ \widehat{Q}_t \cap \mathscr{I})$$

with $0 \leq r \leq n$.

Definition 4.3.21. *Let T be a semi-linear transformation of $\mathbb{F}_q^n$ as in $(*)$. We define the quasi-Euclidean scalar product $\cdot_*$ on $\mathbb{F}_q^n$ as $\vec{a} \cdot_* \vec{b} := \vec{a}B\vec{b}_t$ for any $\vec{a}, \vec{b} \in \mathbb{F}_q^n$, and we denote by $\mathscr{C}^*$ the linear **quasi-Euclidean dual code** of a linear code C with respect to $\cdot_*$, i.e.*

$$\mathscr{C}^* := \left\{ \vec{x} \in \mathbb{F}_q^n \mid \vec{x} \cdot_* \vec{c} = 0 \text{ for every } \vec{c} \in \mathscr{C} \right\}.$$

Proposition 4.3.22. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. Then we have the following properties:*

(i) $\mathscr{C}^* = (\mathscr{C} \star B)^\perp$;

(ii) $\dim \mathscr{C}^* = \dim \mathscr{C}^\perp + \dim(\mathscr{C} \cap \text{Ker } B)$;

(iii) $\mathscr{C}^* \star B = \mathscr{C}^\perp \cap (Im\ B)$;

(iv) $(\mathscr{C}^*)^* = \mathscr{C} + \text{Ker } B$;

(v) $\bar{i}(\mathscr{C}^*) = \bar{i}(\mathscr{C})^\perp \cap \mathscr{I} = \bar{i}(\mathscr{C} + \text{Ker } B)^\perp \cap \mathscr{I}$;

(vi) $(\mathbb{F}_q^n)^* = \text{Ker } B = (Im\ B)^\perp,\ (\text{Ker } B)^* = \mathbb{F}_q^n,\ (\text{Ker } B)^{**} = \text{Ker } B.$

Proof. (i) To prove $\mathscr{C}^* = (\mathscr{C} \star B)^\perp$, we observe that

$$\begin{aligned} \vec{w} \in (\mathscr{C} \star B)^\perp &\iff \vec{w} \cdot (\vec{c}B) = 0, \quad \forall \vec{c} \in \mathscr{C} \\ &\iff \vec{w}B_t\vec{c}_t = 0, \quad \forall \vec{c} \in \mathscr{C} \\ &\iff \vec{w}B\vec{c}_t = 0, \quad \forall \vec{c} \in \mathscr{C} \\ &\iff \vec{w} \cdot_* \vec{c} = 0, \quad \forall \vec{c} \in \mathscr{C} \\ &\iff \vec{w} \in \mathscr{C}^* \ . \end{aligned}$$

(ii) This follows easily from

$$\dim(\mathscr{C} \star B) = \dim \mathscr{C} - \dim(\mathscr{C} \cap \text{Ker } B)$$

and $\dim \mathscr{C}^* = n - \dim(\mathscr{C} \cdot B)$.

(iii) If $\vec{x} \in \mathscr{C}^* \star B$, then $\vec{x} \in Im\ B$ and $\vec{x} = \vec{c^*}B$ for some $\vec{c^*} \in \mathscr{C}^*$. Hence for every $\vec{c} \in \mathscr{C}$ we get

$$\vec{x} \cdot \vec{c} = \vec{c^*}B \cdot \vec{c} = \vec{c^*} \cdot_* \vec{c} = 0,$$

i.e. $\mathscr{C}^* \star B \subseteq \mathscr{C}^\perp \cap (Im\ B)$. On the other hand, let $\vec{y} \in \mathscr{C}^\perp \cap (Im\ B)$. Then $\vec{y} = \vec{v}B \in \mathscr{C}^\perp$ for some $\vec{v} \in \mathbb{F}_q^n$. Thus for any $\vec{c} \in \mathscr{C}$ we have

$$\vec{v} \cdot_* \vec{c} = \vec{v}B\vec{c}_t = \vec{y} \cdot \vec{c} = 0,$$

that is, $\mathscr{C}^\perp \cap (Im\ B) \subseteq \mathscr{C}^* \star B$.

(iv) Let $\vec{x} = \vec{c} + \vec{b} \in \mathscr{C} + \text{Ker } B$. Then for every $\vec{c^*} \in \mathscr{C}^*$ by (i) we have

$$\vec{x} \cdot_* \vec{c^*} = \vec{x} B \vec{c^*}_t = (\vec{c}B + \vec{b}B) \cdot \vec{c^*} = (\vec{c}B) \cdot \vec{c^*} = 0,$$

i.e. $\mathscr{C} + \text{Ker } B \subseteq (\mathscr{C}^*)^*$. Let $\vec{v} \in (\mathscr{C}^*)^*$. Then for any $\vec{x} \in \mathscr{C}^*$ we get

$$\vec{v}B \cdot \vec{x} = \vec{v} B \vec{x}_t = \vec{v} \cdot_* \vec{x} = 0,$$

i.e. $\vec{v}B \in (\mathscr{C}^*)^\perp = \mathscr{C} \star B$. Thus there exists a $\vec{c} \in \mathscr{C}$ such that $\vec{v}B = \vec{c}B$. This implies that $(\vec{v} - \vec{c})B = \vec{0}$, that is, $\vec{v} - \vec{c} \in \text{Ker } B$ and $\vec{v} = \vec{c} + \vec{b}$ for some $\vec{b} \in \text{Ker } B$.

(v) If $\vec{x} \in \bar{i}(\mathscr{C}^*)$, then $\vec{x} = \bar{i}(\vec{v}) = \vec{v}C^{-1}\widehat{Q} \in \mathscr{I}$ for some $\vec{v} \in \mathscr{C}^*$. Hence for every $\vec{c} \in \mathscr{C}$ and $\vec{b} \in \text{Ker } B$, we have

$$\vec{x} \cdot \bar{i}(\vec{c} + \vec{b}) = \vec{x} \cdot \bar{i}(\vec{c}) + \vec{x} \cdot \bar{i}(\vec{b}) = \vec{v} \cdot_* \vec{c} + \vec{v} \cdot (\vec{b}B) = 0,$$

that is, $\bar{i}(\mathscr{C}^*) \subseteq \bar{i}(\mathscr{C} + \text{Ker } B)^\perp \cap \mathscr{I}$. Now, let $\vec{x} \in \bar{i}(\mathscr{C} + \text{Ker } B)^\perp \cap \mathscr{I}$, i.e. $\vec{x} = \bar{i}(\vec{v}) = \vec{v}C^{-1}\widehat{Q} \in \bar{i}(\mathscr{C} + \text{Ker } B)^\perp \subseteq \bar{i}(\mathscr{C})^\perp$ for some $\vec{v} \in \mathbb{F}_q^n$. Thus for every $\vec{y} \in \mathscr{C}$ we have

$$\vec{v} \cdot_* \vec{y} = \vec{v} B \vec{y}_t = (\vec{v}C^{-1}\widehat{Q})(\vec{y}C^{-1}\widehat{Q})_t = \vec{x} \cdot \bar{i}(\vec{y}) = 0,$$

i.e. $\vec{v} \in \mathscr{C}^*$. Hence we get $\vec{x} = \bar{i}(\vec{v}) \in \bar{i}(\mathscr{C}^*)$, that is, $\bar{i}(\mathscr{C} + \text{Ker } B)^\perp \cap \mathscr{I} \subseteq \bar{i}(\mathscr{C}^*)$.

Let us prove now that $\bar{i}(\mathscr{C}^*)$ is also equal to $\bar{i}(\mathscr{C})^\perp \cap \mathscr{I}$. Let $\vec{x} \in \bar{i}(\mathscr{C}^*)$. Then $\vec{x} = \bar{i}(\vec{c^*}) \in \mathscr{I}$ for some vector $\vec{c^*} \in \mathscr{C}^*$. Therefore for every $\vec{c} \in \mathscr{C}$ we have

$$\vec{x} \cdot \bar{i}(\vec{c}) = \bar{i}(\vec{c^*}) \cdot \bar{i}(\vec{c}) = \vec{c^*} \cdot_* \vec{c} = 0,$$

i.e. $\vec{x} \in \bar{i}(\mathscr{C})^\perp \cap \mathscr{I}$. On the other hand, let $\vec{y} \in \bar{i}(\mathscr{C})^\perp \cap \mathscr{I}$. Then $\vec{y} = \bar{i}(\vec{z}) \in \mathscr{I}$ for some $\vec{z} \in \mathbb{F}_q^n$ and for every $\vec{c} \in \mathscr{C}$ we get

$$0 = \bar{i}(c) \cdot \vec{y} = \bar{i}(c) \cdot \bar{i}(z) = \vec{c} \cdot_* \vec{z}.$$

Hence $\vec{z} \in \mathscr{C}^*$, i.e. $\vec{y} \in \bar{i}(\mathscr{C}^*)$.

(vi) Since $(\{\vec{0}\})^* = \mathbb{F}_q^n$, the equalities $(\mathbb{F}_q^n)^* = (Im\ B)^\perp$ and $(\mathbb{F}_q^n)^* = \text{Ker } B$ follow easily from (i) with $\mathscr{C} = \mathbb{F}_q^n$ and from (iv) with $\mathscr{C} = \{\vec{0}\}$ respectively. Finally, by taking $\mathscr{C} = \text{Ker } B$, the equalities $(\text{Ker } B)^* = \mathbb{F}_q^n$ and $(\text{Ker } B)^{**} = \text{Ker } B$ are immediate consequences of (i) and (iv), respectively. □

Corollary 4.3.23. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. If $r = n$, then we have*

(*j*) $\mathscr{C}^* = \mathscr{C}^\perp \star B^{-1}$;

(*jj*) $\dim \mathscr{C}^* = \dim \mathscr{C}^\perp$;

(*jjj*) $(\mathscr{C}^*)^* = \mathscr{C}$;

(*jv*) $\bar{i}(\mathscr{C}^*) = \bar{i}(\mathscr{C})^\perp \cap \mathscr{I}$;

(*v*) $(\mathbb{F}_q^n)^* = \{\vec{0}\}, \ (\{\vec{0}\})^* = \mathbb{F}_q^n$.

Remark 4.3.24. *When $r = n$, by* Corollary 4.3.23 (*j*) *we can easily obtain a generator matrix of $\mathscr{C}^*$ by multiplying the parity check matrix of $\mathscr{C}$ with the matrix B^{-1}. Moreover, when $r = 0$, we see that B is the null matrix and in this case $\widehat{Q}$ represents a generator matrix of an euclidean self-orthogonal code $\mathscr{C}$ (i.e. $\mathscr{C} \subseteq \mathscr{C}^\perp$) of dimension n in $\mathbb{F}_q^m$.*

Remark 4.3.25. *From* Proposition 4.3.22 (*vi*), *it follows that* Ker $B \subseteq \{\vec{v}\}^*$ *for any $\vec{v} \in \mathbb{F}_q^n$. In particular, we deduce that* Ker $B \subseteq \mathscr{C}^*$ *for any linear code $\mathscr{C} \subseteq \mathbb{F}_q^n$.*

Example 4.3.26. *In $\mathbb{F}_4^3$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$, consider the following four polynomials:*

(1) $f_0 = X^3 + X^2 + 1$; (2) $f_1 = X^3 + \alpha^2 X^2 + \alpha^2 X + \alpha$;

(3) $f_2 = X^3 + X^2 + \alpha X + \alpha^2$; (4) $f_3 = X^3 + \alpha^2$.

Note that $m = 7$ for the first case, while $m = 6$ for the other cases. Then

$$X^6 - 1 = f_1 \cdot q_{f_1} = f_2 \cdot q_{f_2} = f_3 \cdot q_{f_3}, \ X^7 - 1 = f_0 \cdot q_{f_0}$$

where

$$q_{f_0} = X^4 + X^3 + X^2 + 1, \quad q_{f_1} = X^3 + \alpha X^2 + \alpha^2 X + \alpha^2,$$
$$q_{f_2} = X^3 + X^2 + \alpha X + \alpha, \quad q_{f_3} = X^3 + \alpha.$$

Therefore this gives

$$Q_0 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}, \quad Q_1 = \begin{pmatrix} \alpha^2 & \alpha^2 & \alpha & 1 & 0 & 0 \\ 0 & \alpha & \alpha & \alpha^2 & 1 & 0 \\ 0 & 0 & \alpha^2 & \alpha^2 & \alpha & 1 \end{pmatrix},$$

$$Q_2 = \begin{pmatrix} \alpha & \alpha & 1 & 1 & 0 & 0 \\ 0 & \alpha^2 & \alpha^2 & 1 & 1 & 0 \\ 0 & 0 & \alpha & \alpha & 1 & 1 \end{pmatrix}, \quad Q_3 = \begin{pmatrix} \alpha & 0 & 0 & 1 & 0 & 0 \\ 0 & \alpha^2 & 0 & 0 & 1 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 1 \end{pmatrix},$$

and

$$B_0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; B_1 = \begin{pmatrix} \alpha & 1 & \alpha \\ 1 & \alpha^2 & 1 \\ \alpha & 1 & \alpha \end{pmatrix},$$

$$B_2 = \begin{pmatrix} 0 & \alpha^2 & 0 \\ \alpha^2 & 0 & \alpha \\ 0 & \alpha & 0 \end{pmatrix}, \; B_3 = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \alpha^2 & 0 \\ 0 & 0 & \alpha \end{pmatrix},$$

with rk $B_i = i$ *for* $i = 0, ..., 3$. *Observe that from* Remark 4.3.24 *it follows that* Q_0 *is the generator matrix of an euclidean self-orthogonal code (in fact, an euclidean self-orthogonal cyclic code) of type* $[7,3]_4$ *with minimum Hamming distance equal to three.*

Corollary 4.3.27. *Let* $\mathscr{C}$ *be a linear code in* $\mathbb{F}_q^n$. *Then*

$$\mathscr{C} \subseteq \mathscr{C}^* \iff \bar{\imath}(\mathscr{C}) \subseteq \bar{\imath}(\mathscr{C})^\perp,$$

i.e. $\mathscr{C}$ *is self-ortogonal with respect to* $\cdot_*$ *if and only if* $\bar{\imath}(\mathscr{C})$ *is self-ortogonal with respect to* $\cdot$.

Proof. Since $\bar{\imath}$ is injective, the statement is an immediate consequence of Proposition 4.3.22 (v) and the following equivalence: $\bar{\imath}(\mathscr{C}) \subseteq \bar{\imath}(\mathscr{C})^\perp \cap \mathscr{I} \iff \bar{\imath}(\mathscr{C}) \subseteq \bar{\imath}(\mathscr{C})^\perp$. □

Lemma 4.3.28. *For any* $\vec{c} \in \mathbb{F}_q^n$ *and* $k \in \mathbb{N}$, *we have*

$$\bar{\imath}(\vec{c}\, T^k) = \bar{\imath}(\vec{c})(\Theta \circ \widehat{P})^k,$$

where

$$\widehat{P} := \begin{pmatrix} P_1 & & & \\ & P_2 & & \\ & & \ddots & \\ & & & P_r \end{pmatrix}$$

and the P_i's are the $m_i \times m_i$ matrices as in Proposition 4.3.11 *for every $i = 1, ..., r$.*

Proof. It is sufficient to prove the statement for $k = 1$. Thus, for every $\vec{c} \in \mathbb{F}_q^n$, let $\vec{v} = (\vec{v}_1, ..., \vec{v}_r) \in \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ be the vector such that $\vec{c} = \vec{v}C$. By definition and Proposition 4.3.12 we have

$$\bar{i}(\vec{c}\,T) = i(\vec{c}\,TC^{-1}) = i(\vec{c}\,C^{-1}(\Theta \circ D)CC^{-1}) = i((\vec{v})(\Theta \circ D)) =$$

$$= i((\vec{v}_1\Theta \circ M_1, ..., \vec{v}_r\Theta \circ M_r)) = ((\vec{v}_1)(\Theta \circ M_1)Q_1, ..., (\vec{v}_r)(\Theta \circ M_r)Q_r) =$$

$$= (i_1(\vec{v}_1\Theta \circ M_1), ..., i_r(\vec{v}_r\Theta \circ M_r)) = (i_1(\vec{v}_1)(\Theta \circ P_1), ..., i_r(\vec{v}_r)(\Theta \circ P_r)) =$$

$$= (i_1(\vec{v}_1), ..., i_r(\vec{v}_r))(\Theta \circ \widehat{P}) = (\vec{v}_1Q_1, ..., \vec{v}_rQ_r)(\Theta \circ \widehat{P}) =$$

$$= (\vec{v}_1, ..., \vec{v}_r)\widehat{Q}(\Theta \circ \widehat{P}) = (\vec{v})\widehat{Q}(\Theta \circ \widehat{P}) = i(\vec{v})(\Theta \circ \widehat{P}),$$

that is, $\bar{i}(\vec{c}\,T) = i(\vec{v})(\Theta \circ \widehat{P}) = \bar{i}(\vec{c})(\Theta \circ \widehat{P})$. □

Corollary 4.3.29. *Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a linear code. Then*

$\mathscr{C}$ is a T-code $\iff$ $\bar{i}(\mathscr{C})$ is a linear code invariant under $\Theta \circ \widehat{P}$.

Proof. From Lemma 4.3.28 it follows that

$\mathscr{C}$ is a product T-code $\iff$ $\varphi(\mathscr{C})$ is a linear code invariant by $\Theta \circ D$ $\iff$ $i(\varphi(\mathscr{C})) = \bar{i}(\mathscr{C})$ is a linear code invariant by $\Theta \circ \widehat{P}$. □

Corollary 4.3.30. *Let $\mathscr{C} = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star \widehat{C}C$ be a linear code in $\mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$, where $\widehat{C}$ is an invertible matrix and $\mathscr{C}_i \subseteq \mathbb{F}_q^{n_i}$ is a linear code for every $i = 1, ..., r$. If there exists an invertible matrix $\overline{C}$ such that $\widehat{C}(\widehat{Q}\widehat{Q}_t) = (\widehat{Q}\widehat{Q}_t)\overline{C}$, then $\mathscr{C}^* = (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star \overline{C}_t^{-1}C$, where $\mathscr{C}_i^* \subseteq \mathbb{F}_q^{n_i}$ is the quasi-Euclidean dual code of $\mathscr{C}_i$ for every $i = 1, ..., r$. In particular, if $\mathscr{C} = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$ is a product T-code, then $\mathscr{C}^* = (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star C$.*

Proof. By Proposition 4.3.22(i) and Theorem 4.3.3, we have

$$\mathscr{C}^* = (\mathscr{C} \star B)^{\perp} = ((\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star \widehat{C}CB)^{\perp} = ((\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star \widehat{C}\widehat{Q}\ \widehat{Q}_t C_t^{-1})^{\perp} =$$

$$= ((\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star \widehat{Q}\ \widehat{Q}_t \overline{C} C_t^{-1})^{\perp} = ((\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star CBC_t \overline{C} C_t^{-1})^{\perp} =$$

$$= ((\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star CB)^{\perp} \star C^{-1} \overline{C}_t^{-1} C = ((\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C)^{*} \star C^{-1} \overline{C}_t^{-1} C =$$

$$= (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star CC^{-1} \overline{C}_t^{-1} C = (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star \overline{C}_t^{-1} C,$$

i.e. $\mathscr{C}^* = (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star \overline{C}_t^{-1} C$. □

Finally, we have the following

Proposition 4.3.31. *Let $\mathscr{C}_T \subseteq \mathbb{F}_q^n$ be a semi-linear T-code invariant under a θ-semi-linear transformation $T = \Theta \circ \overline{M}$. If there exists a matrix $\widehat{M}$ such that $B_\theta \widehat{M} = \overline{M} B$, then the quasi-Euclidean dual code $\mathscr{C}_T^*$ is a T'-code, where $T' = \Theta^{-1} \circ (\widehat{M_t})_{\theta^{-1}}$.*

Proof. Note that the linear code $\mathscr{C}_T \star B$ is invariant under the θ-semi-linear transformation $\Theta \circ \widehat{M}$. Thus we can conclude by Propositions 4.3.22 (i) and 4.3.7. □

4.3.3 Hermitian duals

Assume that the order s of $\theta \in Aut(\mathbb{F}_q)$ divides m_i for every $i = 1, ..., r$, i.e.

$$m_i = m_i' \cdot s \ , \ m_i' \in \mathbb{N} \ . \qquad (\diamond\diamond)$$

Note that assumption ($\diamond\diamond$) is always satisfied when $\theta = id$.

Define a "conjugation" map Φ on $R_m := R/R(X^{m_1} - 1) \times ... \times R/R(X^{m_r} - 1)$ such that

$$\Phi((a_{i_1} X^{i_1}, ..., a_{i_r} X^{i_r})) := (\Phi_1(a_{i_1} X^{i_1}), ..., \Phi_r(a_{i_r} X^{i_r})),$$

where

$$\Phi_k(a_{i_k} X^{i_k}) := \theta^{-i_k}(a_{i_k}) X^{m_k - i_k} \in R/R(X^{m_k} - 1)$$

for $k = 1, ..., r$, which is extended to all elements of R_m by linearity of addition.

We then define a product of two elements $\vec{p}(X) = (p_1(X), ..., p_r(X)) \in R_m$ and $\vec{t}(X) = (t_1(X), ..., t_r(X)) \in R_m$ by

$$\vec{p}(X) *_{\widehat{P}} \vec{t}(X) := (p_1(X)\Phi_1(t_1(X)), ..., p_r(X)\Phi_r(t_r(X))).$$

By the above commutative diagram, we can also define a Hermitian product of two elements $\vec{a}(X) := (a_1(X), ..., a_r(X))$ and $\vec{b}(X) := (b_1(X), ..., b_r(X))$ of $R_n := R/Rf_1 \times ... \times R/Rf_r$ by

$$< \vec{a}(X), \vec{b}(X) >:= j(\vec{a}(X)) *_{\widehat{P}} j(\vec{b}(X)).$$

The next two results are now an immediate generalization of [15, Proposition 3.2 and Corollary 3.3].

Proposition 4.3.32. *Assume that* $(*)$ *holds. Let* $\vec{a} = (\vec{a_1}, ..., \vec{a_r}), \vec{b} = (\vec{b_1}, ..., \vec{b_r}) \in \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ *and denote by*

$$\vec{a}(X) := (\pi_1(\vec{a_1}), ..., \pi_r(\vec{a_r})) := (a_1(X), ..., a_r(X))$$

and

$$\vec{b}(X) := (\pi_1(\vec{b_1}), ..., \pi_r(\vec{b_r})) := (b_1(X), ..., b_r(X))$$

their polynomial representation in $R/Rf_1 \times ... \times R/Rf_r$ *via* $\pi = (\pi_1, ..., \pi_r)$ *respectively. If* $(\diamond\diamond)$ *holds, then*

$$\vec{a_i} \cdot_{*_i} \vec{b_i}(\Theta \circ M_i)^{h_i} = 0, \quad \text{for all } 0 \leq h_i \leq m_i - 1, \; i = 1, ..., r \quad \Longleftrightarrow \quad < \vec{a}(X), \vec{b}(X) >= \vec{0}.$$

Proof. Without loss of generality, we can assume that $r = 1$, since the statement will follow easily by applying the below argument to each component of $< \vec{a}(X), \vec{b}(X) >\in R_m$. Moreover, for simplicity we omit the subindexes.

Since $\theta^m = id$, the condition $< a(X), b(X) >= 0$ is equivalent to

$$\begin{aligned} j(a(X)) *_{\widehat{P}} j(b(X)) = 0 &\Longleftrightarrow a(X) q_f \Phi(b(X) q_f) = 0 \\ &\Longleftrightarrow \left(\sum_{i=0}^{m-1} a'_i X^i\right) \Phi \left(\sum_{k=0}^{m-1} b'_k X^k\right) = 0 \\ &\Longleftrightarrow \left(\sum_{i=0}^{m-1} a'_i X^i\right) \left(\sum_{k=0}^{m-1} \theta^{-k}(b'_k) X^{m-k}\right) = 0 \\ &\Longleftrightarrow \sum_{h=0}^{m-1} \left(\sum_{i=0}^{m-1} a'_{i+h} \theta^h(b'_i)\right) X^h = 0, \end{aligned}$$

where the subscript $i+h$ is taken modulo m. Comparing the coefficients of X^h on both sides of the last equation, we get

$$\sum_{i=0}^{m-1} a'_{i+h}\theta^h(b'_i) = 0, \text{ for all } 0 \leq h \leq m-1.$$

By Proposition 4.3.12 the above equation is equivalent for all $0 \leq h \leq m-1$ to

$$\begin{aligned} \vec{a'} \cdot \vec{b'}(\Theta^h \circ P^h) = 0 &\iff \vec{a'} \cdot \vec{b'}(\Theta \circ P)^h = 0 \\ &\iff i(\vec{a}) \cdot i(\vec{b})(\Theta \circ P)^h = 0 \\ &\iff i(\vec{a}) \cdot i(\vec{b}(\Theta \circ M)^h) = 0 \\ &\iff \vec{a}Q \cdot (\vec{b}(\Theta \circ M)^h)Q = 0, \end{aligned}$$

i.e. $\vec{a} \cdot_* \vec{b}(\Theta \circ M)^h = 0$ for all $0 \leq h \leq m-1$. □

Let I be a left R-submodule of R_n. We define the dual I^ν of I in R_n taken with respect to the Hermitian product $<,>$ as

$$I^\nu := \{\vec{a}(X) \in R_n \mid \ < \vec{a}(X), \vec{t}(X) >= \vec{0}\ , \ \forall \vec{t}(X) \in I\ \}.$$

Definition 4.3.33. *Let T be a semi-linear transformation of $\mathbb{F}_q^n$ as in $(*)$. We define the Hermitian dual code $\mathscr{C}^\nu$ of a linear code $\mathscr{C}$ with respect to $<,>$ as the linear code*

$$\mathscr{C}^\nu := \left\{\vec{x} \in \mathbb{F}_q^n \mid \ < \vec{x}(X), \vec{c}(X) >= 0 \text{ for every } \vec{c} \in \mathscr{C}\right\}.$$

Remark 4.3.34. *If $I \subseteq R_n$ is a left R-submodule, then I^ν is again a left R-submodule of R_n. Consequently, from* Theorem 4.1.6 *we can deduce that if $\mathscr{C}'$ is a code invariant under D as in $(*)$, then $\mathscr{C}'^\nu = \pi^{-1}(\pi(\mathscr{C}')^\nu)$ is again a code invariant by D.*

From Proposition 4.3.32 we can deduce the following results which relate the quasi-Euclidean duals with the Hermitian duals of product T-codes.

Theorem 4.3.35. *Let $\mathscr{C}_T = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$ be a product T-code and define the isomorphism $\overline{\pi} = \pi \circ \varphi$. If $(\diamond\diamond)$ holds, then*

$$\overline{\pi}(\mathscr{C}_T^*) = \overline{\pi}(\mathscr{C}_T)^\nu\ .$$

Proof. Since $\mathscr{C}_T = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$, from Corollary 4.3.30 we deduce that $\mathscr{C}_T^* = (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star C$. Thus it is sufficient to prove that

$$\pi(\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) = \pi(\mathscr{C}_1 \times ... \times \mathscr{C}_r)^\nu \ .$$

Moreover, without loss of generality, we can assume that $r = 1$. Therefore, let $\pi(\vec{b}) = \pi_1(\vec{b}) \in \pi_1(\mathscr{C}_1^*)$ for some $\vec{b} \in \mathscr{C}_1^*$. Then for every $\vec{a} \in \mathscr{C}_1$ and $h \in \mathbb{Z}_{\geq 0}$ we have $\vec{b} \cdot_* \vec{a}(\Theta \circ M_1)^h = 0$. Thus by Proposition 4.3.32 we get $< \pi_1(\vec{b}), \pi_1(\vec{a}) >= 0$ for all $\vec{a} \in \mathscr{C}_1$, i.e. $\pi_1(\vec{b}) \in \pi_1(\mathscr{C}_1)^\nu$. Hence $\pi_1(\mathscr{C}_1^*) \subseteq \pi_1(\mathscr{C}_1)^\nu$. Finally, let $b(X) \in \pi_1(\mathscr{C}_1)^\nu$. Then we get $< b(X), \pi_1(\vec{a}) >= 0$, $\forall \vec{a} \in \mathscr{C}_1$. By Proposition 4.3.32 with $h = 0$, this implies that $\pi_1^{-1}(b(X)) \cdot_* \vec{a} = 0$, $\forall \vec{a} \in \mathscr{C}_1$, i.e. $\pi_1^{-1}(b(X)) \in \mathscr{C}_1^*$. This shows that $b(X) = \pi_1(\pi_1^{-1}(b(X))) \in \pi_1(\mathscr{C}_1^*)$, that is, $\pi_1(\mathscr{C}_1)^\nu \subseteq \pi_1(\mathscr{C}_1^*)$. □

Corollary 4.3.36. *Let $\mathscr{C}_T = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$ be a product T-code, where C is as in $(*)$. If $(\diamond\diamond)$ holds, then*

$$\mathscr{C}_T = \mathscr{C}_T^* \iff \overline{\pi}(\mathscr{C}_T) = \overline{\pi}(\mathscr{C}_T)^\nu \ ,$$

i.e., $\mathscr{C}_T$ is self-dual with respect to $\cdot_*$ $\iff$ $\overline{\pi}(\mathscr{C}_T)$ is self-dual with respect to $<,>$.

Proof. Since $\overline{\pi}$ is an isomorphism, this follows immediately from Theorem 4.3.35. □

Theorem 4.3.37. *Let $\mathscr{C}_T = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$ be a product T-code, where $\mathscr{C}_i = (g_i)_{n_i,q}^{k_i,\theta}$ is an f_i-module θ-codes for every $i = 1, ..., r$. If $(\diamond\diamond)$ holds, then $\mathscr{C}_T^* = (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star C$ is a product T-code, where $\mathscr{C}_i^* = (\mathscr{C}_i \star B_i)^\perp$ with $B_i := Q_i(Q_i)_t$ for $i = 1, ..., r$. Furthermore, a generator matrix for $\mathscr{C}_T^*$ is given by*

$$G^* := \begin{pmatrix} G_1^* & & & \\ & G_2^* & & \\ & & \ddots & \\ & & & G_r^* \end{pmatrix} \cdot C \ ,$$

where

$$G_i^* := \begin{pmatrix} \pi_i^{-1}(g_i^*) \\ \pi_i^{-1}(g_i^*)(\Theta \circ M_i) \\ \vdots \\ \pi_i^{-1}(g_i^*)(\Theta \circ M_i)^{s_i - 1} \end{pmatrix} \ ,$$

with $s_i := \dim \mathscr{C}_i^*$, $g_i^* q_{f_i} = l.l.c.m(h_i^\perp, q_i) \mod (X_i^m - 1)$, $h_i^\perp = \sum_{j=0}^{k_i} \theta^i(h_{k_i-j})X^j$ *and* $X^{m_i} - 1 = g_i q_{f_i}(\sum_{j=0}^{k_i} h_j X^j)$*, is the generator matrix of the quasi-Euclidean code* $\mathscr{C}_i^*$ *for every* $i = 1, ..., r$*.*

Proof. Since $\mathscr{C}_T = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$ is a product T-code, then $\overline{\pi}(\mathscr{C}_T)$ is a left R-submodule of R_n. Hence $\overline{\pi}(\mathscr{C}_T)^\nu$ is a left R-submodule. By Proposition 4.3.30 and Theorems 4.3.35 and 4.1.6, we conclude that $\mathscr{C}_T^* = (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star C$ is a product T-code.

Consider the following commutative diagrams

$$\begin{tikzcd}
\mathscr{C}_k \arrow[r, "i_k"] \arrow[d, "\pi_k"'] & i_k(\mathscr{C}_k) \arrow[d, "\pi'_k"] \\
(g_k) \arrow[r, "j_k"'] & (g_k q_{f_k})
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathscr{C}_k^* \arrow[r, "i_k"] \arrow[d, "\pi_k"'] & i_k(\mathscr{C}_k^*) \arrow[d, "\pi'_k"] \\
(g_k^*) \arrow[r, "j_k"'] & (G_k)
\end{tikzcd}$$

for every $k = 1, ..., r$. By Proposition 4.3.12 we see that $i_k(\mathscr{C}_k)$ is a θ-cyclic code. So from [6, Theorem 8] we know that $i_k(\mathscr{C}_k)^\perp$ is again a θ-cyclic code generated by the skew polynomial $h_k^\perp := h_k^* \in R$ such that $X^{m_k} - 1 = g_k q_{f_k} h_k$, where h^* is as in [4, Definition 3]. Since $\mathscr{I}_k := \text{Im } i_k$ is generated by $q_{f_k} \in R$, from Proposition 4.3.22 (v) it follows that $\pi'_k(i_k(\mathscr{C}_k^*)) = (h_k^\perp) \cap (q_{f_k})$, i.e. $\pi'_k(i_k(\mathscr{C}_k^*)) = (G_k)$ with $G_k = l.l.c.m.(h_k^\perp, q_{f_k})$. From Proposition 4.3.11 we deduce that $\pi_k(\mathscr{C}_k^*) = (g_k^*)$ with g_k^* such that $G_k = g_k^* q_{f_k}$. □

Corollary 4.3.38. *Let* $\mathscr{C} = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$ *be a product* T*-code, where* C *is as in* $(*)$*. If* $(\diamond\diamond)$ *holds, then*

$$\mathscr{C}^* \textit{ is a product } T\textit{-code} \iff \mathscr{C} + \text{Ker } B \textit{ is a product } T\textit{-code.}$$

Proof. Suppose that $\mathscr{C}^* = (\mathscr{C}_1^* \times ... \times \mathscr{C}_r^*) \star C$ is a product T-code. Then by Proposition 4.3.22 (iv) and Corollary 4.3.37 we see that $\mathscr{C} + \text{Ker } B = (\mathscr{C}^*)^*$ is a product T-code. Finally, assume that $\mathscr{C} + \text{Ker } B$ is a product T-code. Then by Proposition 4.3.22 (vi) and Corollary 4.3.37, we deduce that $\mathscr{C}^* = \mathscr{C}^* \cap (\text{Ker } B)^* = (\mathscr{C} + \text{Ker } B)^*$ is a product T-code. □

Let us note here that the converse of Corollary 4.3.37 is not true in general, as the following example shows.

Example 4.3.39. *In $\mathbb{F}_4^3$, where $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ with $\alpha^2 + \alpha + 1 = 0$, consider the polynomial $f_2 = X^3 + X^2 + \alpha X + \alpha^2$. Then from* Example 4.3.26 *we know that $m = 6$ and*

$$B_2 = \begin{pmatrix} 0 & \alpha^2 & 0 \\ \alpha^2 & 0 & \alpha \\ 0 & \alpha & 0 \end{pmatrix},$$

with $\mathrm{rk}\ B_2 = 2$. *Consider the linear code $\mathscr{C} \subset \mathbb{F}_4^3$ generated by the vectors $\vec{e}_2 = (0,1,0)$ and $\vec{e}_3 = (0,0,1)$. Since*

$$(\vec{e}_3)\ \Theta \circ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha^2 & \alpha & 1 \end{pmatrix} = \vec{e}_3 \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ \alpha^2 & \alpha & 1 \end{pmatrix} = (\alpha^2, \alpha, 1) \notin \mathscr{C},$$

we see that $\mathscr{C}$ is not an f_2-module θ-code. On the other hand, since Ker B_2 *is generated by the vector $(\alpha^2, 0, 1)$ and $\mathscr{C} \cap \mathrm{Ker}\ B_2 = \{\vec{0}\}$, we obtain that*

$$\mathscr{C} + \mathrm{Ker}\ B_2 = \mathscr{C} \oplus \mathrm{Ker}\ B_2 = \mathbb{F}_4^3$$

is an f_2-module θ-code. By Corollary 4.3.38 *we get that $\mathscr{C}^*$ is an f_2-module θ-code.*

Remark 4.3.40. *If $(\diamond\diamond)$ holds, then* Ker $B \subseteq \mathbb{F}_q^n$ *is a T-code such that* Ker $B = ($Ker $B_1 \times ... \times$ Ker $B_r)$, Ker $B^\perp =$ Im B, $($Ker $B^\perp)^\perp =$ Ker B *and* Ker $B^* = \mathbb{F}_q^n$, $($Ker $B^*)^* =$ Ker B. *In particular,* Ker $B \subseteq \mathbb{F}_q^n$ *does not contain any T-code $\mathscr{C} \subseteq \mathbb{F}_q^n$ with $\mathscr{C}^* \neq \mathbb{F}_q^n$.*

4.4 An encoding and decoding algorithm

Given a θ-semi-linear transformation $T = \Theta \circ M$ and a product T-code $\mathscr{C}_T \subset \mathbb{F}_q^n$ of dimension $k < n$, a classical codification of a message $\vec{M} \in \mathbb{F}_q^k$ is given by $\vec{M} G_T C^{-1}$, where G_T is a generator matrix of $\mathscr{C}_T$ and C is the invertible matrix such that $\mathscr{C}_T = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$. Note that $\vec{M} G_T \in \mathscr{C}_T$ and

$$\vec{m} := \vec{M} G_T C^{-1} \in \mathscr{C}_T \star C^{-1} = \mathscr{C}_1 \times ... \times \mathscr{C}_r$$

for some f_i-module θ-codes $\mathscr{C}_i = (g_i)$, where the g_i's are right divisors of the f_i's respectively (see Remark 4.1.4 and assumption (*)). However, this encoding method is not systematic, i.e. it is not strictly related with an easy decoding algorithm.

So, let us give here a non-trivial and systematic encoding method for product T-codes. Let $\vec{M} \in \mathbb{F}_q^k = \mathbb{F}_q^{k_1} \times ... \times \mathbb{F}_q^{k_r}$ be the original message such that $\vec{M} = (\vec{M}_1, ..., \vec{M}_r)$, where $\vec{M}_i \in \mathbb{F}_q^{k_i}$ for every $i = 1, ..., r$. Let $\mathscr{C}_T = (\mathscr{C}_1 \times ... \times \mathscr{C}_r) \star C$ be a product T-code such that $\dim_{\mathbb{F}_q} \mathscr{C}_i = k_i$ for any $i = 1, ..., r$. Note that $\mathscr{C}_i \subseteq \mathbb{F}_q^{n_i}$ with $n_i \geq k_i$ for every $i = 1, ..., r$. Therefore, consider the natural injective map $i_j : \mathbb{F}_q^{k_j} \to \mathbb{F}_q^{n_j}$ such that $i_j(a_1, ..., a_{k_j}) := (a_1, ..., a_{k_j}, 0, ..., 0)$ for any $j = 1, ..., r$, and define the injective map

$$i := (i_1, ..., i_r) : \mathbb{F}_q^{k_1} \times ... \times \mathbb{F}_q^{k_r} \to \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}.$$

Define $\vec{m} := i(\vec{M}) = ((\vec{M}_1, \vec{0}), \ldots, (\vec{M}_r, \vec{0})) \in \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ and denote by $m = (m_1, \ldots, m_r) \in R_n$ the representation of the message $\vec{m} = i(\vec{M}) \in \mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$, via the vector isomorphism

$$\pi := (\pi_1, ..., \pi_r) : \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r} \to R_n := R/Rf_1 \times ... \times R/Rf_r \ .$$

At this point, we can encode the original message $\vec{m} := i(\vec{M})$ by working equivalently on either (i) R_n, or (ii) $\mathbb{F}_q^n := \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$.

(i) Multiply the original messages m_i by $X^{n_i - k_i}$, where $m_i = m_{i,0} + m_{i,1}X + ... + m_{i,k_i-1}X^{k_i-1}$ and $k_i = \dim_{\mathbb{F}_q} \mathscr{C}_i$. The result is $X^{n_i-k_i} \cdot m_i = \theta^{n_i-k_i}(m_{i,0})X^{n_i-k_i} + \theta^{n_i-k_i}(m_{i,1})X^{n_i-k_i+1} + ... + \theta^{n_i-k_i}(m_{i,k_i-1})X^{n_i-1}$ for $i = 1, \ldots, r$. Write $X^{n_i-k_i} \cdot m_i = q_i g_i + r_i$ for every $i = 1, ..., r$, where $\deg r_i < n_i - k_i$. Since $q_i g_i \in \mathscr{C}_i$, we can encode the original message $\vec{m} \in \mathbb{F}_q^n$ by

$$\vec{m}' := (\pi_1^{-1}(X^{n_1-k_1} - r_1), ..., \pi_r^{-1}(X^{n_r-k_r} - r_r)) \in \mathscr{C}_1 \times ... \times \mathscr{C}_r.$$

Since $\deg r_i < n_i - k_i$ for every $i = 1, ..., r$, observe that all the information about the original messages m_i is contained in the last powers $X^{n_i-k_i}, ..., X^{n_i-1}$ of $X^{n_i-k_i} \cdot m_i - r_i \in \pi_i(\mathscr{C}_i)$.

(ii) Define the map

$$\overline{\Theta} : \begin{array}{ccc} \mathbb{F}_q^{n_1} \times \cdots \times \mathbb{F}_q^{n_r} & \longrightarrow & \mathbb{F}_q^{n_1} \times \cdots \times \mathbb{F}_q^{n_r} \\ (\vec{x}_1, \ldots, \vec{x}_r) & \longmapsto & (\vec{x}_1(\Theta \circ M_1)^{n_1-k_1}, \ldots, \vec{x}_r(\Theta \circ M_r)^{n_r-k_r}) \end{array},$$

where the M_i's are matrices as in Theorem 4.1.3. By applying $\overline{\Theta}$ to $\vec{m}$ we have

$$\begin{aligned} \vec{m}\overline{\Theta} &= ((\vec{M}_1, \vec{0})(\Theta \circ M_1)^{n_1-k_1}, \ldots, (\vec{M}_r, \vec{0})(\Theta \circ M_r)^{n_r-k_r}) \\ &= ((\vec{0}, (\vec{M}_1)\Theta^{n_1-k_1}), \ldots, (\vec{0}, (\vec{M}_r)\Theta^{n_r-k_r})) \end{aligned}$$

If $\vec{m}' := ((\vec{c}_1, (\vec{M}_1)\Theta^{n_1-k_1}), \dots, (\vec{c}_r, (\vec{M}_r)\Theta^{n_r-k_r}))$ is such that $\vec{m}'H_t = \vec{0}$, where

$$H = \begin{pmatrix} H_1 & & \\ & \ddots & \\ & & H_r \end{pmatrix}$$

is the parity check matrix of $\mathscr{C}_1 \times ... \times \mathscr{C}_r$ and the matrices $H_i = (I_{n_i-k_i} \mid (T_i)_t)$ are given by Proposition 4.3.1 for every $i = 1, ..., r$. Then $\vec{m}' \in \mathscr{C}_1 \times \cdots \times \mathscr{C}_r$ is the encoded message of $\vec{m} \in \mathbb{F}_q^n$.

Now, let $\vec{m}''$ be the received message. If during the transmission of the encoded message $\vec{m}'$ there were not errors, i.e. $\vec{m}'' \in \mathscr{C}_1 \times \cdots \times \mathscr{C}_r$, then in both cases (i) and (ii) we can decode $\vec{m}'' = (\vec{m}_1'', ..., \vec{m}_r'')$ by applying $\Theta^{-n_i+k_i}$ to each component $\vec{m}_i''$ of $\vec{m}''$. The original components $\vec{m}_i$ of $\vec{m} = (\vec{m}_1, ..., \vec{m}_r)$ will be given by the last k_i coordinates of $(\vec{m}_i'')\Theta^{-n_i+k_i}$ for every $i = 1, ..., r$.

Finally, if there were errors during the transmission of the message $\vec{m}'$, i.e. $\vec{m}'' \notin \mathscr{C}_1 \times \cdots \times \mathscr{C}_r$, then by assuming that the error $\vec{e}$, defined as

$$\vec{e} := \vec{m}'' - \vec{m}' \in \vec{m}'' + (\mathscr{C}_1 \times ... \times \mathscr{C}_r),$$

where $\vec{m}''$ and $\vec{m}'$ are the received and the encoded messages respectively, has small weight $wt(\vec{e})$, we can use the below error detecting and correcting algorithm inspired by [12] and then the above decoding procedure.

A Meggitt type error correcting algorithm.

Put $d_{min} := \min_{i=1,\dots,r}\{d(\mathscr{C}_i)\}$, where $d(\mathscr{C}_i) := d_i$ is the minimum Hamming distance of the code $\mathscr{C}_i$ for $i = 1, ..., r$, and assume that

$$wt(\vec{e}) \leq \frac{d_{min} - 1}{2}.$$

Let $\pi_j : \mathbb{F}_q^{n_j} \to R/Rf_j$ be the usual isomorphism for every $j = 1, ..., r$.

For any vector $\vec{v} = (\vec{v}_1, ..., \vec{v}_r) \in \mathbb{F}_q^n = \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ put $\pi(\vec{v}) := (\pi_1(\vec{v}_1), ..., \pi_r(\vec{v}_r))$ and define the syndrome of $\pi(\vec{v})$ as follows:

$$S(\pi(\vec{v})) := (R_{g_1}(\pi_1(\vec{v}_1)), ..., R_{g_r}(\pi_r(\vec{v}_r))),$$

where $R_{g_i}(\pi_i(\vec{v}_i))$ is the rest of the division of $\pi_i(\vec{v}_i)$ by g_i for every $i = 1, ..., r$.

Observe that $S(\pi(\vec{m}')) = (0, ..., 0)$. Hence $S(\pi(\vec{e})) = S(\pi(\vec{m}''))$. Denote by t_i the polynomials in R such that $t_i \cdot X = 1$ in R/Rf_i for every $i = 1, ..., r$.

Algorithm 4**:**

Input: $\vec{m}'' = (\vec{m}''_1, ..., \vec{m}''_r)$

- **Step 1**: Compute all the syndromes

$$S(\pi(\vec{e'})) = S((\pi_1(\vec{e'}_1), ..., \pi_r(\vec{e'}_r)),$$

where $\pi_i(\vec{e'}_i) = \sum_{j=0}^{n_i-1} e'_{j,i}X^j$ is such that $wt(\vec{e'}_i) = wt(\pi_i(\vec{e'}_i)) \leq \frac{d_i-1}{2}$ with d_i the minimum Hamming distance of $\mathscr{C}_i$ and $e'_{i,n_i-1} \neq 0$;

- **Step 2**: Compute $S(\pi(\vec{m}''))$ and define $\vec{s} := S(\pi(\vec{m}''))$;

- **Step 3**: If $\vec{s} = \vec{0} \in R/Rf_1 \times ... \times R/Rf_r$ then write $\vec{e} = \vec{0}$;

- **Step 4**: If $\vec{s}$ is equal to some of the syndromes $S(\pi(\vec{e'}))$ of Step 1, then write $\vec{e} = \vec{e'}$;

- **Step 5**: If $\vec{s}$ is not in the list of Step 1, then

$$\vec{m}'' = \vec{m}' + \vec{e''}$$

for some error $\vec{e''} = (\vec{e''}_1, ..., \vec{e''}_r) \in \mathbb{F}_q^{n_1} \times ... \times \mathbb{F}_q^{n_r}$ such that $wt(\vec{e''}) \leq \frac{d_{min}-1}{2}$ and $\pi(\vec{e''}) = (\sum_{j=0}^{h_1} e''_{j,1}X^j, ..., \sum_{j=0}^{h_r} e''_{j,r}X^j)$ with $e''_{h_i,i} \neq 0$, $h_i \leq n_i - 1$ and $h_k < n_k - 1$ for some $k = 1, ..., r$. Since θ is an automorphism of $\mathbb{F}_q$, there exists an integer $\delta_k := n_k - h_k - 1$ such that

$$\overline{e}_k := X^{\delta_k} \cdot \left(\sum_{j=0}^{h_k} e''_{j,k}X^j \right),$$

i.e. $\pi_k(\vec{E}_k) := \overline{e}_k = \sum_{j=0}^{n_k-1} \overline{e}_{j,k}X^j$ is such that $wt(\vec{E}_k) \leq \frac{d_k-1}{2}$ and $\overline{e}_{n_k-1,k} \neq 0$. Thus the syndrome

$$S((\pi_1(\vec{e'}_1), ..., \overline{e}_k, ..., \pi_r(\vec{e'}_r))$$

is as in Step 1, where $\pi_i(\vec{e'}_i) = \sum_{j=0}^{n_i-1} e'_{j,i}X^j$ is such that $wt(\pi_i(\vec{e'}_i)) \leq \frac{d_i-1}{2}$ and $e'_{i,n_i-1} \neq 0$ for $i \neq k$. Then write

$$\vec{e} = (\vec{e'}_1, ..., \pi_k^{-1}(t_k^{\delta_k} \cdot \overline{e}_k), ..., \vec{e'}_r);$$

Output: $\vec{m}' = \vec{m}'' - \vec{e}$.

4.5 A construction method for T-codes

Observe that to construct a product T-code (see Definition 4.2.3) it is sufficient to construct module θ-codes (see Definition 4.2.1).

Note that in R there are exactly $q^{r-1}(q-1)$ different polynomials of the form $g = g_0 + g_1X + ... + g_{r-1}X^{r-1} + X^r$ with $g_0 \neq 0$. Thus if h is another monic polynomial of degree r, then it follows that $(g) \neq (h)$ whenever $g \neq h$. Furthermore, for any given monic polynomial $g \in R$ of degree $r < n$ as above there exists a polynomial $f \in R$ of degree n such that g is a (right) divisor of f. This shows that there exist $q^{r-1}(q-1)$ module θ-codes with parameters of $[n, n-r]_q$.

From now on, a linear code $\mathscr{C}$ of type $[n,k]_q$ with Hamming distance equal to d will be called simply a code of type $[n,k,d]_q$.

So, let us give here the following

Definition 4.5.1.

$$D_q^\theta(n,k) := \max\{d \mid \exists \text{ a module } \theta\text{−code of type } [n,k,d]_q\}$$

Similarly to [14, Proposition 3.1], we can obtain the following

Proposition 4.5.2.

$$D_q^\theta(n,k) \geq D_q^\theta(n+1,k+1).$$

Proof. Let $g = g_0 + g_1X + ... + g_{n-k}X^{n-k}$ be the generator polynomial of a module θ-code $\mathscr{C}_{n+1,k+1}$ with parameters $[n+1, k+1, D_q^\theta(n+1,k+1)]$. Observe that g_0 and g_{n-k} are distinct to zero and that the generator matrix $G_{n+1,k+1}$ of $\mathscr{C}_{n+1,k+1}$ has the form

$$\left(\begin{array}{c|cccccc} g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ \hline 0 & & & & & & \\ \vdots & & & G_{n,k} & & & \\ 0 & & & & & & \end{array}\right),$$

where $G_{n,k}$ is the following matrix

$$\begin{pmatrix} \theta(g_0) & \dots & \theta(g_{n-k}) & 0 & \dots & 0 \\ 0 & \theta^2(g_0) & \dots & \theta^2(g_{n-k}) & \dots & 0 \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & \dots & 0 & \theta^k(g_0) & \dots & \theta^k(g_{n-k}) \end{pmatrix}.$$

Note that the minimum (Hamming) distance decided by $G_{n,k}$ is at least $D_q^\theta(n+1,k+1)$. Define $G := \theta(g_0) + \theta(g_1)X ... + \theta(g_{n-k})X^{n-k}$. Then G is the generator polynomial of a module θ-code $\mathscr{C}_{n,k}$ of type $[n,k,d]_q$ with $d \geq D_q^\theta(n+1,k+1)$. Hence we get $D_q^\theta(n,k) \geq d \geq D_q^\theta(n+1,k+1)$. □

Remark 4.5.3. *If $\mathscr{C}$ is a module θ-code of type $[n,k,\Delta]_q$ with distance $\Delta \geq 1$, then we have $D_q^\theta(n,k) \geq \Delta$. Therefore by* Proposition 4.5.2 *we see that for any integer δ such that $0 \leq \delta < k$ there exists at least a module θ-code $\mathscr{C}'$ of type $[n-\delta, k-\delta, d]_q$ with $d \geq \Delta$. Thus the above result can be useful to ensure the existence and the construction of module θ-codes of type $[n,k,d]_q$ with distance d greater than or equal to some fixed value Δ and small values for n and k.*

Denote by $\mathbb{F}_q^\theta \subseteq \mathbb{F}_q$ the field fixed by θ. In what follows we try to construct vectors $\vec{v} \in \mathbb{F}_q^n$ such that $1 \leq \dim[\vec{v}] \leq k$ for some integer $k < n$, where $[\vec{v}] \subset \mathbb{F}_q^n$ is the vector subspace generated by $\{\vec{v}, (\vec{v})(\Theta \circ A_c), (\vec{v})(\Theta \circ A_c)^2, ...\}$ and A_c is the companion matrix of $f \in R$ as in Remark 4.3.9.

For simplicity, put $A := A_c$ and note that

$$(\vec{v})(\Theta \circ A_\theta) = (\vec{v})(A \circ \Theta)$$

for any $\vec{v} \in (\mathbb{F}_q)^n$, where $A_\theta := [\theta(a_{ij})]$ if $A = [a_{ij}]$. This gives the following

Lemma 4.5.4. *For every integer $k \geq 1$, we have*

$$(\Theta \circ A)^k = \Theta^k \circ A_k,$$

where $A_k := A_{\theta^{k-1}} \cdot ... \cdot A_{\theta^2} \cdot A_\theta \cdot A$ for $k \geq 2$ and $A_1 := A$.

Let h be an integer such that $1 \leq h \leq n-1$ and consider the equation:

$$(\#) \qquad (\vec{v})(\Theta \circ A)^h x_h + ... + (\vec{v})(\Theta \circ A)^1 x_1 + (\vec{v}) x_0 = \vec{0}.$$

If there exists a non-trivial vector $\vec{v}$ and a non-zero $x_h \in \mathbb{F}_q$ which satisfies the above equation (#), we can deduce that $(\vec{v})(\Theta \circ A)^h$ can be written as a linear combination of vectors in $\{\vec{v}, (\vec{v})(\Theta \circ A), ..., (\vec{v})(\Theta \circ A)^{h-1}\}$, i.e. $1 \leq \dim[\vec{v}] \leq h$.

In order to simplify equation (#), we will consider only vectors $\vec{v} \in (\mathbb{F}_q^{\theta})^n$. In this case, by Lemma 4.5.4 (#) becomes

$$(\#') \qquad \vec{v} \cdot (A_h x_h + ... + A_1 x_1 + I x_0) = \vec{0},$$

where $\vec{v} \in (\mathbb{F}_q^{\theta})^n$. Thus the existence of a non-trivial vectors $\vec{v} \in (\mathbb{F}_q^{\theta})^n$ which satisfy equation (#′) implies the existence of non-trivial solutions $x_h, ..., x_1, x_0$ of the equation

$$(\#'') \qquad \det(A_h x_h + ... + A_1 x_1 + I x_0) = 0.$$

So we can translate the problem of finding a vector $\vec{v} \neq \vec{0}$ in $(\mathbb{F}_q^{\theta})^n$ which is a solution of (#) to the problem of finding non-trivial solutions $x_h, ..., x_1, x_0$ in $\mathbb{F}_q$ of (#″). Define

$$F_h(x_0, x_1, ..., x_h) := \det(A_h x_h + ... + A_1 x_1 + I x_0).$$

We have the following

Lemma 4.5.5. *The polynomial $F_h(x_0, x_1, ..., x_h)$ is an homogeneous polynomial of degree n in the variables $x_0, x_1, ..., x_h$.*

Proof. For any $\lambda \in \mathbb{F}_q$, we get

$$\begin{aligned} F_h(\lambda x_0, \lambda x_1, ..., \lambda x_h) &= \det(A_h(\lambda x_h) + ... + A_1(\lambda x_1) + I(\lambda x_0)) \\ &= \det(\lambda I) \cdot \det(A_h x_h + ... + A_1 x_1 + I x_0) \\ &= \lambda^n \cdot F_h(x_0, x_1, ..., x_h), \end{aligned}$$

and this gives the statement. □

From Lemma 4.5.5 it follows that the zero locus $Z(F_h(x_0, x_1, ..., x_h))$ of $F_h(x_0, x_1, ..., x_h)$ on the projective space $\mathbb{P}^h(\mathbb{F}_q)$ is well defined. Put

$$Z_{h,n} := Z(F_h(x_0, x_1, ..., x_h)) \subset \mathbb{P}^h(\mathbb{F}_q).$$

Then $Z_{h,n}$ is a hypersurface of $\mathbb{P}^h(\mathbb{F}_q)$, i.e. $\dim Z_h = h-1$, of degree $n \geq h+1$. Moreover, all the points of $Z_{h,n}$ represent no trivial solutions of $(\#'')$. This gives a relation between the construction of a module θ-code $\mathscr{C} = [\vec{v}]$ of dimension less or equal to h, where $\vec{v} \in (\mathbb{F}_q^\theta)^n \cap \mathrm{Ker}\,(A_h x_h + ... + A_1 x_1 + I x_0)$, with the existence of (rational) points on the hypersurface $Z_{h,n}$ of $\mathbb{P}^h(\mathbb{F}_q)$.

Remark 4.5.6. *When θ is the identity of $\mathbb{F}_q^n$, e.g. if q is a prime number, we know from* [10] *that the number N_q of $\mathbb{F}_q$-points of the hypersurface $Z_{h,n}$ is bounded for the following inequalities: (i) $N_q \leq (n-1)q+1$ if $h=2$, except for a curve $Z_{2,4}$ over $\mathbb{F}_4$; (ii) $N_q \leq (n-1)q^{h-1} + nq^{h-2} + \frac{q^{h-2}-1}{q-1}$ if $h \geq 3$.*

For the general case of T-codes, an argument similar to the above can be directly applied to a semi-linear transformation $\Theta \circ D := \Theta \circ \mathrm{diag}(M_1, ..., M_r)$ instead of $\Theta \circ A_c$. Recall that any T-code $\mathscr{C}_T$ can be obtained from a code $\mathscr{C}_D$ invariant by $\Theta \circ D$ by the relation $\mathscr{C}_T = \mathscr{C}_D \star C$, where C is an invertible matrix such that $CTC^{-1} = \Theta \circ D$. Therefore, to obtain a T-code it is sufficient to construct a code $\mathscr{C}_D$ invariant by $\Theta \circ D$. As above, this allows us to find (rational) solutions of the following equation

$$(\#\#) \qquad (\vec{v})(\Theta \circ D)^h x_h + ... + (\vec{v})(\Theta \circ D)^1 x_1 + (\vec{v}) x_0 = \vec{0}$$

for some integer h such that $1 \leq h \leq n-1$. By considering only non-trivial vectors $\vec{v} \in (\mathbb{F}_q^\theta)^n$, $(\#\#)$ becomes simply

$$(\#\#') \qquad \vec{v} \cdot (D_h x_h + ... + D_1 x_1 + I x_0) = \vec{0}$$

which immediately implies the existence of non-trivial solutions $x_h, ..., x_1, x_0 \in \mathbb{F}_q$ of the following equation

$$(\#\#'') \qquad \det(D_h x_h + ... + D_1 x_1 + I x_0) = 0,$$

where $D_i = \mathrm{diag}((M_1)_i, ..., (M_r)_i)$ and $(M_j)_i$ is as in Lemma 4.5.4 for every $j = 1, ..., r$ and $i = 1, ..., h$. Observe that $(\#\#'')$ is equivalent to

$$\det(\mathrm{diag}((M_1)_h x_h + ... + (M_1) x_1 + I x_0, ..., (M_r)_h x_h + ... + (M_r) x_1 + I x_0)) =$$

$$= \det((M_1)_h x_h + ... + (M_1) x_1 + I x_0) \cdot ... \cdot \det((M_r)_h x_h + ... + (M_r) x_1 + I x_0) = 0,$$

i.e.

$$F(x_0, x_1, ..., x_h) := F_{1,h}(x_0, x_1, ..., x_h) \cdot ... \cdot F_{r,h}(x_0, x_1, ..., x_h) = 0,$$

where $F_{i,h}(x_0, x_1, ..., x_h) := \det((M_i)_h x_h + ... + (M_i)x_1 + Ix_0)$ for every $i = 1, ..., r$. In this case, the zero locus $Z(F(x_0, x_1, ..., x_h))$ of $F(x_0, x_1, ..., x_h)$ on the projective space $\mathbb{P}^h(\mathbb{F}_q)$ is a complete intersection of type $(d_1, ..., d_r)$, where $d_i := \deg F_{i,h}(x_0, x_1, ..., x_h)$, and its (rational) points are solutions of (##″).

Thus by any point $(x_0, x_1, ..., x_{n-1}) \in Z_{n-1,n}$ we can construct a polynomial $p = p(X) \in \mathbb{F}_q[X]$ such that $\det p(M) = 0$. In this situation, we can say more about the polynomial $p(x) \in \mathbb{F}_q[x]$.

Proposition 4.5.7. *Assume that $\theta = id$. Let $m =\in \mathbb{F}_q[X]$ be the minimal polynomial of an invertible matrix M. If $g = gcd(p, m)$ for some polynomial $p \in \mathbb{F}_q[X]$, then*

(a) Ker $p(M) =$ Ker $g(M)$*;*

(b) Ker $p(M) \neq \vec{0} \iff g \neq 1$.

Proof. Let us note that $g(M) = p(M)a(M)$ and $p(M) = g(M)b(M)$ for some polynomials $a, b \in \mathbb{F}_q[X]$. This gives Ker $p(M) \subseteq$ Ker $g(M)$ and Ker $g(M) \subseteq$ Ker $p(M)$ respectively, i.e. Ker $p(M) =$ Ker $g(M)$.

To prove (2), observe that $g = p \cdot a + m \cdot b$ for some polynomials $a, b \in \mathbb{F}_q[X]$. If $g = 1$, then $g(M) = p(M)a(M)$ is the identity matrix. This shows that $\det p(M) \cdot \det a(M) = 1$, i.e. $\det p(M) \neq 0$, but this gives a contradiction. On the other hand, if $g \neq 1$ then $m = h \cdot g$ and $p = l'cdotg$ for some polynomials $h, l \in \mathbb{F}_q[X]$. Hence $h(M)g(M)$ is the zero matrix. Since $\deg h < \deg m$ and m is the minimal polynomial of M, we deduce that $\det g(M) = 0$. Thus we get $\det p(M) = \det(l(M)g(M)) = 0$, i.e. Ker $p(M) \neq \vec{0}$. □

Chapter 5

Appendix

5.1 A normal form of a polynomial matrix

Recall that $R := \mathbb{F}_q[X, \theta]$. First of all, let us show as follows: if $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ is a 2×2 matrix with coordinates in R, then there exist elementary matrices E, F such that EAF has the normal form

$$EAF = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}.$$

Up to exchange rows and columns by left and right multiplication of A with the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, we can assume that $a_{11} \neq 0$ and $a_{11} = p \cdot a_{21} + r$, where $p, r \in R$ and $\deg(r) < \deg(a_{21})$. Then

$$\begin{pmatrix} 1 & 0 \\ 1 & -p \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ r & a_{12} - p \cdot a_{22} \end{pmatrix}.$$

Since $deg(r) < deg(a_{11})$, we obtain that $a_{11} = p'r + r'$, where $p', r' \in \mathbb{F}_q[X, \theta]$ and $\deg(r') < \deg(r)$. Then

$$\begin{pmatrix} 1 & 0 \\ 1 & -p' \end{pmatrix} \cdot \begin{pmatrix} a_{11} & a_{12} \\ r & a_{12} - pa_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{11} - p' \cdot r & a_{12} - p' \cdot (a_{12} - p'a_{22}) \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} & a_{12} \\ r' & a_{12} - p' \cdot (a_{12} - p' \cdot a_{22}) \end{pmatrix}.$$

Thus with an inductive argument, by a finite numbers of steps we can obtain the following matrix

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & a'_{22} \end{pmatrix}.$$

The goal now is to obtain zero instead of a_{12} by a similar process. Write $a_{11} = a_{12} \cdot s + t$, where $s, t \in \mathbb{F}_q[X, \theta]$ with $\deg(t) < \deg(a_{12})$. Then

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & a'_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & -s \end{pmatrix} = \begin{pmatrix} a_{11} & a_{11} - a_{12} \cdot s \\ 0 & -a'_{22} \cdot s \end{pmatrix} = \begin{pmatrix} a_{11} & t \\ 0 & -a'_{22} \cdot s \end{pmatrix}.$$

By applying again right division between a_{11} and t, we finally obtain a matrix

$$\begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}.$$

This process can be realized by the fact that when we apply the algorithm of the left (right) division, the degrees of the remainders decrease. This gives easily the matrices E and F.

The above result can be generalized to the case of $n \times n$ matrices with $n \geq 3$. For instance, when $n = 3$, if the matrix A has the form

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix},$$

up to exchange rows and columns by permutation matrices, we can suppose again that $a_{11} \neq 0$. By multiplying the matrix A on the right and on the left with matrices as

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & -q_1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & -q_2 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 \\ 1 & -q_3 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & -q_4 \end{pmatrix}$$

for some $q_i \in \mathbb{F}_q$ respectively, we lead to the following matrix

$$A' = \begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a'_{22} & a'_{23} \\ 0 & a'_{32} & a'_{33} \end{pmatrix}.$$

By a similar argument as above, we can reduce A' to the following matrix

$$\begin{pmatrix} a_{11} & 0 & 0 \\ 0 & \alpha_2 & 0 \\ 0 & 0 & \alpha_3 \end{pmatrix}$$

by multiplying A' on the left and on the right with matrices of type

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & -a \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & -b \end{pmatrix}$$

for some $a, b \in \mathbb{F}_q$, respectively.

5.2 MAGMA programs

Program 0.

```
F<w>:=GF(4);


PcMatrix:=function(qq,g,n)
 R<x>:=TwistedPolynomials(F:q:=qq);
 g:=R!g;
 d:=Degree(g);
 ll:=[];
 for i in [0.. n-d-1] do
  a,b:=Quotrem(R![1]*R![0,1]^(d+i),g);
  ll:=ll cat [b];
 end for;
 return ll;
end function;
```

Program 1.

```
F<w>:=GF(4);
P<x>:=PolynomialRing(F);

Period := function(f)
 d:=Degree(f);
 A:=CompanionMatrix(f);
 p:=Order(Determinant(A));
 _,_,E:=PrimaryRationalForm(A^p);

 // Calculate the m'_i's
 ll:=[];
  for j in [1..#E] do
   ll := ll cat [Order(CompanionMatrix(E[j][1]))];
  end for;
  return LCM(ll);
end function;
```

Program 2.

```
F<w>:=GF(4);
P<x>:=PolynomialRing(F);

PeriodF := function(f)
```

```
 return Order(CompanionMatrix(f));
end function;
```

Program 3.

```
Order(Matrix(GF(4), 3, 3, [0,0,1,1,0,F.1,0,1,0]));
```

Program 4.

```
F<w>:=GF(4);


PeriodNc:=function(qq,g)
 R<x>:=TwistedPolynomials(F:q:=qq);
 f:=R!g;
 n:=Degree(f)-1;
 repeat
  n:=n+1;
  _,r:=Quotrem(X^n-1,f);
 until r eq R![0];
 return n;
end function;
```

Program 5.

```
F<w>:=GF(4);
E:=[x : x in F | x ne 0];


RightDivisors := function(qq,g)
 R<x>:=TwistedPolynomials(F:q:=qq);
 f:=R!g;
 n:=Degree(f);
 S:=CartesianProduct(E,CartesianPower(F,n-1));
 dd:=[];
 for ss in S do
  ll:=[ss[1]] cat [p : p in ss[2]];
  q,r:=Quotrem(f,R!ll);
  if r eq R![0] then dd := dd cat [[q,R!ll]]; end if;
 end for;
 return dd;
end function;
```

Bibliography

[1] N. Aydin, I. Siap and D. Ray- Chaudhuri, *The Structure of 1-Generator Quasi-Twisted Codes and New Linear Codes*, Des. Codes Cryptogr. **24** (2001), no. 3, 313–326.

[2] M. Bhaintwal, *Skew quasi-cyclic codes over Galois rings*, Des. Codes Cryptogr. **62** (2012), no. 1, 85–101.

[3] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265.

[4] D. Boucher, F. Ulmer, *A note on the dual codes of module skew codes*, Cryptography and coding, Lecture Notes in Comput. Sci. **7089**, Springer, Heidelberg, 2011, 230–243.

[5] D. Boucher, F. Ulmer, *Linear codes using skew polynomials with automorphisms and derivations*, Des. Codes Cryptogr. 2013, **DOI** 10.1007/s10623-012-9704-4.

[6] D. Boucher, F. Ulmer, *Codes as modules over skew polynomial rings*, Cryptography and coding, Lecture Notes in Comput. Sci. **5921**, Springer, Berlin, 2009, 38–55.

[7] D. Boucher, W. Geiselmann and F. Ulmer, *Skew-cyclic codes,* Appl. Algebra Engrg. Comm. Comput. **18** (2007), no. 4, 379–389.

[8] U. Dempwolff, J. Chris Fisher and A. Herman, *Semilinear transformations over finite fields are Frobenius maps,* Glasg. Math. J. **42** (2000), no. 2, 289-?295.

[9] I.N. Herstein, *Topics in algebra*, 2nd Edition, Xerox College Publishing, Lexington, Mass.-Toronto, Ont., 1975.

[10] M. Homma, S.J. Kim, *An elementary bound for the number of points of a hypersurface over a finite field*, Finite Fields Appl. **20** (2013), 76–83.

[11] R.A. Horn, C.R. Johnson, *Matrix analysis*, Second edition, Cambridge University Press, Cambridge, 2013.

[12] W. Cary Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003.

[13] N. Jacobson, *Pseudo-linear transformations*, Ann. of Math. (2) **38** (1937), no. 2, 484–507.

[14] Zhuo-Jun Liu, Dong-Dai Lin, *A class of generalized cyclic codes*, Acta Math. Appl. Sinica (English Ser.) **16** (2000), no. 1, 53–58.

[15] S. Ling, P. Solé, *On the algebraic structure of quasi-cyclic codes. I. Finite fields*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 2751–2760.

[16] S. Ling, C. Xing, *Coding Theory, A first course*, Cambridge University Press, Cambridge, 2004.

[17] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes. I,* North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, pp. 1–369.

[18] F.J. MacWilliams, N.J.A. Sloane, *The theory of error-correcting codes. II,* North-Holland Mathematical Library, Vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977, pp. 370–762.

[19] O. Ore, *Theory of non-commutative polynomials*, Ann. of Math. (2) **34** (1933), no. 3, 480–508.

[20] J. Rosenthal, Anna-Lena Trautmann, *A complete characterization of irreducible cyclic orbit codes and their Plücker embedding*, Des. Codes Cryptogr. **66** (2013), no. 1-3, 275–289.

[21] D. Radkova, A.J. van Zanten, *Constacyclic codes as invariant subspaces*, Linear Algebra Appl. **430** (2009), no. 2-3, 855–864.

[22] J.H. van Lint, *Introduction to coding theory*, Third edition, Graduate Texts in Mathematics, **86**, Springer-Verlag, Berlin, 1999.