Universidad de Concepción

Dirección de Postgrado

Facultad de Cs. Físicas y Matemáticas - Programa Magíster en Matemática

Arcos y MDS-códigos de tipo generalizado.

(Arcs and MDS-codes of generalized type.)

Tesis para optar al grado de Magíster en Matemática.

ALEXIS EDUARDO ALMENDRAS VALDEBENITO

CONCEPCIÓN-CHILE

2016

Profesor Guía: Andrea Luigi Tironi

Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas

Universidad de Concepción

Universidad de Concepción

Dirección de Postgrado

Facultad de Cs. Físicas y Matemáticas - Programa Magíster en Matemática

Arcos y MDS-códigos de tipo generalizado.

(Arcs and MDS-codes of generalized type.)

Tesis para optar al grado de Magíster en Matemática.

ALEXIS EDUARDO ALMENDRAS VALDEBENITO

CONCEPCIÓN-CHILE

2016

Profesor Guía : Andrea Luigi Tironi

Comisión Evaluadora : Antonio Laface

Maximiliano Leyton A.

Carlos Martinez R.

A mis padres.

Agradecimientos

Deseo agradecer en primer lugar a mi profesor guía, Andrea Luigi Tironi, quien en todos estos meses de trabajo me entrego los conocimientos necesarios para realizar esta tesis, su tiempo cada vez que fue necesario y su infinita paciencia al momento de juntarnos a trabajar. Aunque no puedo nombrarlos a todos, mi gratitud es para todos aquellos profesores y funcionarios del Departamento de Matemáticas, sin su apoyo no hubiese sido posible alcanzar mi objetivo.

No puedo dejar de lado a mis padres, Hector y Alicia, fueron ellos quienes me entregaron todos los valores que me llevaron a cumplir mis metas, nunca les podré compensar todo lo que hicieron por mi. Finalmente, a mi pareja Elizabeth por su apoyo, paciencia, comprensión y compañía todos estos meses que dedique a la tesis, simplemente muchas gracias por estar siempre a mi lado.

Además, la tesis fue desarrolla en el marco del Proyecto Anillo ACT 1415 PIA CONICYT y los estudios de postgrado fueron parcialmente financiados por CONICYT-PCHA/Magíster Nacional año 2013 - Folio:221320380 y el Proyecto VRID N. 214.013.039-1.OIN.

Índice general

Índice de figuras

Índice de tablas

Introducción

La teoría de códigos, desarrollada desde un punto de vista matemático e informático surgió en 1948 cuando Claude E. Shannon publicó el artículo *The Mathematical Theory of Communication* [38]. Esta teoría trata de resolver el problema de cómo transmitir información de manera segura y fiable, a través de un canal que sea poco seguro y poco fiable. Aquí se encuentran principalmente dos temas de estudios: el análisis de la geometría de subconjuntos en espacios proyectivos finitos y la investigación de propiedades de estructura algebraica sobre un campo finito. Ambos argumentos tienen la finalidad de construir códigos que cumplan con distintas propiedades para facilitar la transmisión de la información.

En 1979, J.W.P. Hirschfeld en *Projective Geometries over Finite Field* [17] caracteriza las distintas variedades algebraicas en $\mathbb{P}^n(\mathbb{F}_q)$ como conjuntos finitos de puntos que cumplen ciertas propiedades combinatoricas. Aquí, como conjunto más general se considera un $(k, l; r, s; n, q)$-set, el cual corresponde a un conjunto de k subespacios de dimensión l en $\mathbb{P}^n(\mathbb{F}_q)$, tal que a lo más r de ellos viven sobre subespacios de dimensión s. En particular, un $(k, 0; n, n-1; n, q)$-set en $\mathbb{P}^n(\mathbb{F}_q)$ es simplemente llamado un k-arco y corresponde a un conjunto de k puntos tal que no más de n de ellos viven sobre una hiperplano de $\mathbb{P}^n(\mathbb{F}_q)$, y un k-arco en $\mathbb{P}^2(\mathbb{F}_q)$ es un conjunto de k puntos tal que no más de 2 de ellos están sobre una recta.

Un $[n, k, d]_q$-código lineal es un subespacio de dimensión k del espacio vectorial $\mathbb{F}_q^n$ y con distancia d (Definición 1.3.4), donde $\mathbb{F}_q$ es un campo finito con q elementos. Respecto

a la distancia de un código lineal, Richard Singleton en 1964 demostró en el artículo *Maximun Distance q-nary Codes* [40], que la máxima distancia de un código lineal está dada por $d \leq n-k+1$. Así, un $[n,k,n-k+1]_q$-código es llamado un *MDS código*. El estudio y construcción de este tipo de códigos puede ser hecho en el espacio proyectivo, ya que un n-arco en $\mathbb{P}^{n-k-1}(\mathbb{F}_q)$ define un $[n,k,n-k+1]$-código (Corolario 1.4.2).

Un código $\mathscr{C} \subseteq \mathbb{F}_q^n$, se llama *código cíclico* si tiene la siguiente propiedad:

$$(x_1, x_2, \ldots, x_n) \in \mathscr{C} \Longrightarrow (x_n, x_1, \ldots, x_{n-1}) \in \mathscr{C}.$$

La ventaja de este tipo de código es la relación que existe con los ideales de $\mathbb{F}_q[x]/(x^n-1)$, ya que si un polinomio $g(x) \in \mathbb{F}_q[x]$ es un divisor de x^n-1 este genera un código cíclico en $\mathbb{F}_q^n$ (Teorema 1.3.29).

De manera natural, se pueden considerar los ideales de $\mathbb{F}_q[x]/(x^n-\alpha)$ con $\alpha \in \mathbb{F}_q^*$ y donde se tiene que si un polinomio $g(x) \in \mathbb{F}_q[x]$ es un divisor de $x^n-\alpha$, este genera un código $\mathscr{C} \subseteq \mathbb{F}_q^n$ el cual se caracteriza en que si $(x_1, x_2, \ldots, x_n) \in \mathscr{C}$ implica que $(\alpha x_n, x_1, \ldots, x_{n-1}) \in \mathscr{C}$. Estos códigos son llamados *códigos α-cíclicos*, o *códigos pseudo-cíclicos* si son α-cíclicos para algún $\alpha \in \mathbb{F}_q^*$. Además, se puede observar que un código 1-cíclico es simplemente un código cíclico.

En el 2007, Delphine Boucher y Felix Ulmer en su artículo *Skew-Cyclic Codes* [9] generalizaron los códigos cíclicos. Así, un código $\mathscr{C} \subseteq \mathbb{F}_q^n$, se llama *código skew-cíclico* si $(x_1, x_2, \ldots, x_n) \in \mathscr{C}$ implica que $(\theta(x_n), \theta(x_1), \ldots, \theta(x_{n-1})) \in \mathscr{C}$, donde θ es un automorfismo de $\mathbb{F}_q$. En este caso, definiendo una estructura de anillo en el conjunto

$$R := \mathbb{F}_q[x;\theta] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{F}_q \text{ y } n \in \mathbb{N}\},$$

con la adición en R definida como la adición usual de polinomios y la multiplicación en R definida por la regla básica $x \cdot \alpha = \theta(\alpha) \cdot x$ ($\alpha \in \mathbb{F}_q$). Existe una relación uno a uno entre los códigos skew cíclicos y los los R-submódulos izquierdos del conjunto R-módulo izquierdo

$R/R(x^n-1)$, ya que si un polinomio $g(x)$ divide a la derecha a x^n-1 este genera un código skew cíclico en $\mathbb{F}_q^n$. Si $\theta = id$, un código skew cíclico es simplemente un código cíclico.

Finalmente podemos considerar los *códigos skew pseudo-cíclicos*, definidos por Boucher, Sole y Ulmer en *Skew Constacyclic Codes over Galois Rings* [5] con el nombre de *códigos skew consta-cíclicos*, en donde se dice que $\mathscr{C} \subseteq \mathbb{F}_q^n$ es un código skew α-cíclico si $(x_1, x_2, \ldots, x_n) \in \mathscr{C}$ implica que $(\alpha\theta(x_n), \theta(x_1), \ldots, \theta(x_{n-1})) \in \mathscr{C}$, donde θ es un automorfismo de $\mathbb{F}_q$ y $\alpha \in \mathbb{F}_q^*$. Así, en este caso los códigos cíclicos, pseudo-cíclicos y skew-cíclicos son casos particulares de los códigos skew pseudo-cíclico cuando $\theta = id$, o $\alpha = 1$, dependiendo del caso. Además, existe una relación como la anterior entre los R-submódulos izquierdos del R-módulo izquierdo $R/R(x^n-\alpha)$ y los códigos skew pseudo-cíclicos de $\mathbb{F}_q^n$, ya que si un polinomio $g(x)$ divide a la derecha a $x^n-\alpha$, este genera un R-submódulo izquierdo de $R/R(x^n-\alpha)$ que nos da un código skew pseudo-cíclico de $\mathbb{F}_q^n$ (ver §2.1).

En el Capítulo 1, se entregan todos los conocimientos previos para trabajar con MDS-códigos y códigos skew pseudo-cíclicos. Así, en la Sección 1.1 se encuentra todo lo referente a *Campos Finitos*, incluyendo *Polinomios* y *Skew Polinomios*. En la Sección 1.2 están los contenidos necesarios de *Geometría Proyectiva* para trabajar con *Arcos* y *Curvas Racionales Normales*. Los contenidos sobre *Códigos* se pueden encontrar en la Sección 1.3. Además, en esta última sección se desarrolla de manera extendida el Teorema 1.3.54 aclarando cada detalle de la demostración realizada por Tatsuya Maruta en *A geometric approach to semi-cyclic codes* [29]. Finalmente, en la Sección 1.4 se presenta la conexión entre la geometría proyectiva y los códigos lineales, la cual será importante para resultados del Capitulo 2 y 3.

En el Capítulo 2, se entregan definiciones y propiedades básicas sobre los códigos skew pseudo-cíclicos. En la Sección 2.1, se demuestra de una manera directa y sencilla que el código dual de un código skew α-cíclico es un código skew α^{-1}-cíclico (Teorema

2.1.12). Este último resultado permite demostrar los Teoremas 2.1.15, 2.1.16, 2.1.18, 2.2.12 y 2.3.2 que corresponden a nuevas propiedades de los códigos skew pseudo-cíclicos, las cuales están inspiradas en teoremas de Tatsuya Maruta en un contexto algebraico conmutativo (ver [29], [30] y [31]) y que son traspasadas al caso no conmutativo $\mathbb{F}_q[x;\theta]$. Además, en la Sección 2.2 se demuestran teoremas referentes a MDS códigos skew pseudo-cíclicos, a pesar que el Teorema 1.3.54 no se puede generalizar como los otros resultados de Maruta, el Teorema 2.2.5 presenta una relación entre los MDS códigos skew pseudo-cíclicos y la geometría proyectiva. En la última parte de este capítulo, en la Sección 2.3, se encuentran algunos resultados que utilizan el Teorema 2.1.16 y la factorización de skew polinomios dada por André Leroy en *Noncommutative Polynomial Maps* [24]. Cabe destacar que por medio del software MAGMA y usando los nuevos resultados sobre los códigos skew pseudo-cíclicos de este capítulo, se pueden construir distintos códigos que alcanzan la mejor distancia conocida dado el largo n del código, su dimensión k y el campo $\mathbb{F}_q$ de sus elementos (ver [14]), además de mejorar la forma de construirlos, ya que requiere de polinomios generadores de grado menor que los conocidos (ver [31]).

En el Capítulo 3, se define un nuevo conjunto de puntos en $\mathbb{P}^2(\mathbb{F}_q)$ el cual llamamos *Arco Generalizado* en $\mathbb{P}^2(\mathbb{F}_q)$, este corresponde a un conjunto de puntos tal que no más de 5 puntos viven en una curva de grado 2, es decir, viven sobre una cónica reducible o irreducible. Similar al estudio realizado en arcos en $\mathbb{P}^2(\mathbb{F}_q)$ (ver [1], [2], [19], [20]), se estudia la geometría de un arco generalizado para q pequeños, encontrando la configuración de puntos que permiten construir arcos generalizados completos. Para valores de $q \geq 7$, aunque la configuración geométrica de estos conjuntos de puntos es más compleja, se obtienen cotas superiores e inferiores para los arcos generalizados completos y que por medio del software MAGMA se encuentran ejemplos que alcanzan estos valores para algunos q pequeños. Además, en este capítulo se estudia la relación de los arcos generalizados con los Veronesian Arcos en $\mathbb{P}^2(\mathbb{F}_q)$, definidos por K. Coolsaet y H. Sticker en 2012. Respecto a este último conjunto hay muy poca información, ya que sólo existe una conje-

tura para la cota superior (Observación 3.1.4), es por esto, que en la Proposición 3.3.4 se presenta una cota inferior para los Veronesian arcos completos. Además, como se muestra en el Teorema 3.2.2 un arco generalizado en $\mathbb{P}^2(\mathbb{F}_q)$ determina un arco en $\mathbb{P}^5(\mathbb{F}_q)$, y por lo tanto, define un MDS código. Así, los arcos generalizados en $\mathbb{P}^2(\mathbb{F}_q)$ definen MDS códigos de dimensión 6, a diferencia de un arco en $\mathbb{P}^2(\mathbb{F}_q)$ que define MDS códigos de dimensión 3.

Por último, en el Capítulo 4, se entregan todos los programas usados en MAGMA para los distintos ejemplos mostrados en la tesis, tanto para códigos como para arcos. En particular, se pueden destacar el Programa 4, el cual construye MDS códigos skew pseudo-cíclicos y el Programa 10 que construye arcos de tipo generalizados para $q \leq 13$.

Además de todo lo mencionado anteriormente, se debe destacar los resultados originales presentes en este trabajo. En el Capítulo 2, del Teorema 2.1.12 al 2.3.8 son las nuevas proposiciones referentes a códigos skew pseudo-cíclico. En cuanto al Capítulo 3, dado que el concepto de arco generalizado no se ha trabajado anteriormente, todos los resultados en este capítulo son originales.

Introduction

The mathematical and computer point of view of the coding theory was considered for the first time in 1948 by Claude E. Shannon in his article *The Mathematical Theory of Communication* [38]. This theory seeks to primarily solve the problem of how to safely transmit information through a channel which is not secure and reliable. For this, there are mainly two themes of study: the analysis of the geometry of subsets in finite projective spaces and the investigation of some properties of algebraic structures over finite fields. Both of the above topics have as main purpose the construction of codes with good properties which facilitate the transmission of information.

In the book *Projective Geometries over Finite Field* [17], J.W.P. Hirschfeld characterized in 1979 algebraic varieties in $\mathbb{P}^n(\mathbb{F}_q)$ as finite sets of points which satisfy some combinatorial properties. Following the same notation as in [17], we define a $(k, l; r, s; n, q)$-set, as a set of k subspaces of dimension l in $\mathbb{P}^n(\mathbb{F}_q)$ such that at most r of them lie on subspaces of $\mathbb{P}^n(\mathbb{F}_q)$ of dimension s. A $(k, 0; n, n-1; n, q)$-set in $\mathbb{P}^n(\mathbb{F}_q)$ is simply called a k-arc and corresponds to a set of k points such that no more n of them lie on a hyperplane of $\mathbb{P}^n(\mathbb{F}_q)$. In particular, a k-arc in $\mathbb{P}^2(\mathbb{F}_q)$ is a set of k points such that no more 2 of them lie on a line.

A linear $[n, k, d]_q$-code $\mathscr{C}$ is a subspace of dimension k of the vector space $\mathbb{F}_q^n$ and distance d (see Definition 1.3.4), where $\mathbb{F}_q$ is a finite field with q elements. With respect to the distance d of a linear code $\mathscr{C}$, Richard Singleton in 1964 proved in *Maximum Distance q-nary Codes* [40] that $d \leq n - k + 1$. For this reason, an $[n, k, n-k+1]_q$-code

is called MDS (Maximum Distance Separable) code. The study and the construction of such codes can be done in projective spaces, since an n-arc in $\mathbb{P}^{n-k-1}(\mathbb{F}_q)$ defines an $[n, k, n-k+1]_q$-code (see Corollary 1.4.2).

A code $\mathscr{C} \subseteq \mathbb{F}_q^n$, is a *cyclic code* if it satisfies the following property:

$$(x_1, x_2, \ldots, x_n) \in \mathscr{C} \Longrightarrow (x_n, x_1, \ldots, x_{n-1}) \in \mathscr{C}.$$

The advantage of this kind of code is its relation with ideals of $\mathbb{F}_q[x]/(x^n-1)$, since a polynomial $g(x) \in \mathbb{F}_q[x]$ which is a divisor of x^n-1 generates an ideal in $\mathbb{F}_q[x]/(x^n-1)$ which is in one-to-one correspondence with a cyclic code in $\mathbb{F}_q^n$ (see Theorem 1.3.29).

In a similar way, we can consider ideals of $\mathbb{F}_q[x]/(x^n-\alpha)$ with $\alpha \in \mathbb{F}_q^*$ which are generated by a divisor $g(x) \in \mathbb{F}_q[x]$ of $x^n-\alpha$, which are in one-to-one correspondence with a code $\mathscr{C} \subseteq \mathbb{F}_q^n$ characterized by the following property: if $(x_1, x_2, \ldots, x_n) \in \mathscr{C}$ then $(\alpha x_n, x_1, \ldots, x_{n-1}) \in \mathscr{C}$. These codes are called *α-cyclic codes*, or more in general *pseudo-cyclic codes* if they are α-cyclic codes for some $\alpha \in \mathbb{F}_q^*$. In particular, let us note here that a 1-cyclic code is simply a cyclic code.

In the paper *Skew-Cyclic Codes* [9], Delphine Boucher and Felix Ulmer generalized in 2007 the cyclic codes. A code $\mathscr{C} \subseteq \mathbb{F}_q^n$ is called there a *skew cyclic code* if $(x_1, x_2, \ldots, x_n) \in \mathscr{C}$ implies that $(\theta(x_n), \theta(x_1), \ldots, \theta(x_{n-1})) \in \mathscr{C}$, where θ is an automorphism of $\mathbb{F}_q$. In this case, a ring structure on the set

$$R := \mathbb{F}_q[x;\theta] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{F}_q \text{ and } n \in \mathbb{N}\},$$

is given, where addition is the usual addition and the multiplication is defined by the basic rule $x \cdot a = \theta(a) \cdot x$ $(a \in \mathbb{F}_q)$. Moreover, there exists a relation between skew cyclic codes and left R-submodules of the whole left R-module $R/R(x^n-1)$, since a right divisor $g(x)$ of x^n-1 generates a left R-submodule of $R/R(x^n-1)$ which is again in one-to-one correspondence with a skew cyclic code in $\mathbb{F}_q^n$. In particular, when $\theta = id$, a

skew-cyclic code is simply a cyclic code.

Finally, we consider *skew α-cyclic codes*, or *skew pseudo-cyclic codes*, called *skew constacyclic codes* by Boucher and Ulmer in *Skew Constacyclic Codes over Galois Rings* [5] they are codes $\mathscr{C} \subseteq \mathbb{F}_q^n$ such that

$$(x_1, x_2, \ldots, x_n) \in \mathscr{C} \Longrightarrow (\alpha\theta(x_n), \theta(x_1), \ldots, \theta(x_{n-1})) \in \mathscr{C} \ ,$$

where θ is an automorphism of $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_q^*$. In particular, cyclic codes, pseudo-cyclic codes and skew cyclic codes are special cases of skew pseudo-cyclic codes. Furthermore, also in this situation, there is a similar relation as above between left R-submodules of the left R-module $R/R(x^n - \alpha)$ and skew pseudo-cyclic codes of $\mathbb{F}_q^n$, since a right divisor $g(x)$ of $x^n - \alpha$ generate a left R-submodule of $R/R(x^n - \alpha)$ which gives a skew pseudo-cyclic code of $\mathbb{F}_q^n$ (see §2.1).

In Chapter 1, we give some background material to deal with MDS codes and skew pseudo-cyclic codes. In Section 1.1 we recall basic results about *Finite Fields*, *Polynomials* and *Skew Polynomials*. In Section 1.2, we give definitions and preliminary results in *Projective Geometry* to work with *Arcs* and *Rational Normal Curves*. The main notions of *Codes* can be found in Section 1.3, where some proofs of results presented by Tatsuya Maruta in *A geometric approach to semi-cyclic codes* [29], as Theorems 1.3.49 and 1.3.54, are given for their better understanding. Finally, in Section 1.4 we show the connection between projective geometry and linear codes which will be useful in Chapters 2 and 3.

In Chapter 2, definitions and properties of skew pseudo-cyclic codes are delivered. In Section 2.1, we prove in a direct and easy way that the dual code of skew α-cyclic code is a skew α^{-1}-cyclic code (Theorem 2.1.12). This results allows us to prove Theorems 2.1.15, 2.1.16, 2.1.18, 2.2.12 and 2.3.2 which correspond to new properties of skew pseudo-cyclic

codes inspired by some Maruta's results in a commutative context (see [29], [30] and [31]). Moreover, in Section 2.2 we give some results about MDS skew pseudo-cyclic codes (see e.g. Theorem 2.2.5) which show a relation between MDS skew pseudo-cyclic codes and the projective geometry. In Section 2.3 we present some applications of Theorem 2.1.16 and the factorization algorithm for skew polynomials by André Leroy in *Noncommutative Polynomial Maps* [24]. We would like to stress that by using MAGMA software and the new results obtained in this chapter, we can construct some codes which reach the best know distance for small field (see [14]), by using generator polynomials of degree less than the known ones (see [31]).

In Chapter 3, we define a new set of points in $\mathbb{P}^2(\mathbb{F}_q)$, called a *Generalized arc* in $\mathbb{P}^2(\mathbb{F}_q)$, which corresponds to a set of points in $\mathbb{P}^2(\mathbb{F}_q)$ such that no more 5 of them lie on a curve of degree 2, i.e. on a reducible or irreducible conic. Similar to the case of arcs in $\mathbb{P}^2(\mathbb{F}_q)$ (see [1], [2], [19], [20]), we study the geometry of a generalized arc for small values of q and we find the configuration of points which gives complete generalized arcs. For $q \geq 7$, we obtain upper and lower bounds on the cardinality of some of such sets and by the MAGMA software we construct examples which reach these values for some small q. Moreover, in this chapter we study the relation between generalized arcs and Veronesian arcs in $\mathbb{P}^2(\mathbb{F}_q)$ defined by K. Coolsaet and H. Sticker in 2012. With respect to Veronesian arcs, we have only few informations and only a conjecture about an upper bound (Remark 3.1.4) is know. For this reason, in Proposition 3.3.4 we present a lower bound for the complete Veronesian arcs. Finally, as it is shown in Theorems 3.2.2, a generalized arc in $\mathbb{P}^2(\mathbb{F}_q)$ produces an arc in $\mathbb{P}^5(\mathbb{F}_q)$ and defines a MDS code. So the generalized arcs in $\mathbb{P}^2(\mathbb{F}_q)$ define MDS codes of dimension 6, instead of arcs in $\mathbb{P}^2(\mathbb{F}_q)$ which define MDS codes of only dimension 3.

Finally, in Chapter 4, all programs in MAGMA used for the main examples in this thesis about codes and arcs are given. In particular, we can highlight Programs 4 and 10 which allow us to build MDS skew pseudo-cyclic codes and generalized arcs for $q \leq 13$.

In addition to all the above, we would like to highlight Theorems 2.1.12 to 2.3.8 which are new results concerning skew pseudo-cyclic codes and all the Chapter 3, where the concept of generalized arc is new and all the theorems about this subject are original.

Capítulo 1

Geometría Proyectiva y Teoría de Códigos

1.1. Campos Finitos

1.1.1. Definiciones y Propiedades Básicas

Comenzaremos con algunas definiciones y teoremas importantes en el estudio de campos, extensiones de campos y polinomios sobre campos finitos.

Definición 1.1.1. Un *campo* es un conjunto K cerrado bajo dos operaciones $+, \cdot$ tal que

1. $(K, +)$ es un grupo abeliano con identidad 0;
2. $(K_0, \cdot)$ es un grupo abeliano con identidad 1, donde $K_0 = K \setminus \{0\}$;
3. $x \cdot (y + z) = x \cdot y + x \cdot z$ para todo $x, y, z \in K$.

Definición 1.1.2. Un *campo finito* es un campo con solo un número finito de elementos.

Definición 1.1.3. Un Campo que no contiene subcampos propios es llamado un *campo primo*.

Definición 1.1.4. Para un primo p, sea $\mathbb{F}_p$ el conjunto $\{0, 1, \ldots, p-1\}$ de enteros y sea $\phi\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{F}_p$ el mapeo definido por $\phi([a]) = a$ para $a = 0, 1, \ldots, p-1$. Entonces $\mathbb{F}_p$, dotado con la estructura de campo inducida por ϕ es un campo finito, llamado *Campo de Galois de orden p*.

Ejemplo 1.1.1. Consideremos $\mathbb{Z}/5\mathbb{Z}$, isomorfo a $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, con el isomorfismo dado por: $[0] \mapsto 0$, $[1] \mapsto 1$, $[2] \mapsto 2$, $[3] \mapsto 3$, $[4] \mapsto 4$. La tabla para las dos operaciones $+$ y $\cdot$ para elementos en $\mathbb{F}_5$ son los siguientes

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ejemplo 1.1.2. Un ejemplo simple e importante es el campo finito $\mathbb{F}_2$. Los elemento de este campo de orden dos son el 0 y el 1, y las tablas de operaciones son las siguientes

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

En este contexto, los elementos 0 y 1 son llamados *elementos binarios*.

Definición 1.1.5. La *característica* de un campo K es el entero positivo p más pequeño (y por lo tanto un primo) tal que $p \cdot x = 0$ para todo $x \in K$.

Definición 1.1.6. Si R es un anillo arbitrario y existe un entero n talque $nr = 0$ para cada $r \in R$, entonces el entero n es llamado *característica* de R y R se dice que tiene característica (positiva) n. Si tal entero n no existe, R se dice que tiene característica 0.

Teorema 1.1.7 ([25], Theorem 1.44)**.** *Un anillo $R \neq \{0\}$ de característica positiva que tiene una identidad y no tiene divisores de cero debe tener característica prima.*

Demostración. Como R contiene elementos distintos de cero, R tiene característica $n \geq 2$. Si n no es primo, podemos escribir $n = km$ donde $k, m \in \mathbb{Z}$, $1 < k, m < n$. Sea e la identidad, entonces $0 = ne = (km)e = (ke)(me)$, y esto implica que $ke = 0$ o $me = 0$ ya que R no tiene divisores de cero. Se tiene que $kr = (ke)r = 0$ para todo $r \in R$ o $mr = (me)r = 0$ para todo $r \in R$ que contradice la definición de la característica n.

□

Corolario 1.1.8 ([25], Corollary 1.45)**.** Un campo finito tiene característica prima.

Demostración. Por el Teorema 1.1.7 es suficiente mostrar que un campo finito F tiene característica positiva. Considerando los multiplos $e, 2e, 3e, \ldots$ de la identidad. Como F contiene solo una cantidad finita de elementos, existen enteros k y m con $1 \leq k \leq m$ tal que $ke = me$, o $(m-k)e = 0$, y así F tiene característica positiva.

□

Teorema 1.1.9 ([25], Theorem 1.46)**.** *Sea R un anillo conmutativo de característica prima p. Entonces*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ y } (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

para $a, b \in R$ y $n \in \mathbb{N}$.

Demostración. Usando el hecho que

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i} \equiv 0 \bmod p$$

para todo $i \in \mathbb{Z}$ con $0 < i < p$, lo cual se obtiene de que $\binom{p}{i}$ es un número entero y de la observación de que el factor p en el numerador no puede ser cancelado. Entonces por el Teorema del binomio

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p,$$

y por inducción en n completamos la demostración de la primera identidad. Por lo que hemos demostrado, obtenemos

$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n},$$

lo que demuestra la segunda identidad.

□

Teorema 1.1.10 ([25], Theorem 1.78)**.** *El subcampo primo de un campo F es isomorfo a $\mathbb{F}_p$ o $\mathbb{Q}$, de acuerdo a si la característica de F es un primo p o 0.*

Definición 1.1.11. Un polinomio $p \in F[x]$ se dice *irreducible sobre F* (o *irreducible en $F[x]$*, o *primo en $F[x]$* si p tiene grado positivo y $p = bc$ con $b, c \in F[x]$ implica que b o c es un polinomio constante.

Teorema 1.1.12 (Factorización Única en $F[x]$, [25], Theorem 1.59)**.** *Cualquier polinomio $f \in F[x]$ de grado positivo puede ser escrito en la forma*

$$f = ap_1^{e_1} \cdots p_k^{e_k},$$

donde $a \in F$, $p_1, \ldots, p_k$ son polinomios mónicos irreducibles en $F[x]$, y $e_1, \ldots, e_k$ son enteros positivos. Más aún, esta factorización es única salvo el orden de los factores.

Teorema 1.1.13 ([25], Theorem 1.61)**.** *Para $f \in F[x]$, el anillo cociente $F[x]/(f)$ es un campo si y solo si f es irreducible sobre F.*

Definición 1.1.14. Un elemento $b \in F$ es llamado una *raíz* (o *un cero*) del polinomio $f \in F[x]$ si $f(b) = 0$.

Teorema 1.1.15 ([25], Theorem 1.64)**.** *Un elemento $b \in F$ es una raíz del polinomio $f \in F[x]$ si y sólo si $x - b$ divide $f(x)$.*

Demostración. Usando el algoritmo de la división podemos escribir

$$f(x) = q(x)(x-b) + c$$

con $q \in F[x]$ y $c \in F$. Substituyendo b por x, tenemos $f(b) = c$, entonces

$$f(x) = q(x)(x - b) + f(b).$$

El Teorema queda demostrado de esta identidad.

□

Definición 1.1.16. Sea $b \in F$ una raíz del polinomio $f \in F[x]$. Si k es un entero positivo tal que $f(x)$ es divisible por $(x - b)^k$, pero no por $(x - b)^{k+1}$, entonces k es llamado la *multiplicidad* de b. Si $k = 1$, entonces b es llamada una *raíz simple* de f, y si $k \geq 2$, entonces b es llamada una *raíz múltiple* de f.

Teorema 1.1.17 ([25], Theorem 1.66)**.** *Sea $f \in F[x]$ con $deg(f) = n \geq 0$. Si $b_1, \ldots, b_m \in F$ son raíces distintas de f con multiplicidad $k_1, \ldots, k_m$ respectivamente, entonces $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$ divide $f(x)$. Consecuentemente, $k_1 + \cdots + k_m \leq n$, y f puede tener a lo más n distintas raíces en F.*

Demostración. Notamos que cada polinomio $x - b_j$, $1 \leq j \leq m$, es irreducible sobre F, y así $(x - b_j)^{k_j}$ aparece como un factor en la factorización canónica de f. Juntos, el factor $(x - b_1)^{k_1} \cdots (x - b_m)^{k_m}$ aparece en la factorización canónica de f y así este es un divisor de f. Comparando los grados, tenemos $k_1 + \cdots + k_m \leq n$, y $m \leq k_1 + \cdots + k_m \leq n$ muestra la última Proposición.

□

Definición 1.1.18. Si $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$, entonces la *derivada* f' de f es definida por $f' = f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in F[x]$.

Teorema 1.1.19 ([25], Theorem 1.68)**.** *Un elemento $b \in F$ es una raíz múltiple de $f \in F[x]$ si y solo si b es una raíz de f y f'.*

Definición 1.1.20. Sea K un subcampo del campo F y M cualquier subconjunto de F. Entonces el campo $K(M)$ es definido como la intersección de todos los subcampos de F contenidos en K y M. Para $M = \langle \theta_1, \ldots, \theta_n \rangle$ finito, escribimos $K(M) = K(\theta_1, \ldots, \theta_n)$.

Definición 1.1.21. Sea K un subcampo de F y $\theta \in F$. Si θ satisface una ecuación polinómica no trivial con coeficientes en K, esto es, si $a_n\theta^n + \cdots + a_1\theta + a_0 =$ con $a_i \in k$ no todos 0, entonces θ se dice que es *algebraico* sobre K. Una extensión L de K es llamado *algebraico* sobre K (o una *extensión algebraica de* K) si cada elemento de L es algebraico sobre K.

Definición 1.1.22. Si $\theta \in F$ es algebraico sobre K, entonces el determina el único polinomio mónico $g \in K[x]$ que genera al ideal $J = \{f \in K[x] \colon f(\theta) = 0\}$ de $K[x]$ es llamado *polinomio minimal* (*polinomio de definición* o *polinomio irreducible*) de θ sobre K. Por el grado de θ sobre K nos referimos al grado de g.

Teorema 1.1.23 ([25], Theorem 1.82)**.** *Sea $p(x)$ el polinomio minimo de un elemento α en $\mathbb{F}_q$ con $q = p^h$ y p primo. Entonces*

a) $p(x)$ es irreducible,

b) si α es la raíz de un polinomio $f(x)$ con coeficientes en $\mathbb{F}_p$, entonces $p(x)$ divide a $f(x)$,

c) $p(x)$ divide $x^q - x$,

d) si $p(x)$ es primitivo, entonces tiene grado h. En otro caso, el grado de $p(x)$ es menor o igual a h.

Definición 1.1.24. Sea L una extensión del campo K. Si L, considerándolo como espacio vectorial sobre K, es finito dimensional, entonces L es llamado *extensión finita* de K. La dimensión del espacio vectorial L sobre K es llamado el *grado* de L sobre K, denotado por $[L : K]$.

Teorema 1.1.25 ([25], Theorem 1.84)**.** *Si L es una extensión finita de K y M es una extensión finita de L, entonces M es una extensión finita de K con*

$$[M : K] = [M : L][L : K].$$

Definición 1.1.26. Sea $f \in K[x]$ de grado positivo y F una extensión del campo K. Entonces f se dice que *se descompone* en F si f puede escribirse como un producto de factores lineales en $F[x]$, esto es, si existen elementos $a_1, a_2, \ldots, a_n \in F$ tal que

$$f(x) = a(x - a_1)(x - a_2)\cdots(x - a_n),$$

donde a el coeficiente líder de f. El campo F es el *campo de descomposición* (*splitting field*) de f sobre K si f se descompone en F y si, además, $F = K(a_1, a_2, \ldots, a_n)$.

Veremos algunas propiedades fundamentales de los Campos Finitos y una descripción de los métodos para construir Campos Finitos, los cuales serán de vital importancia en el estudio de la Teoría de Códigos y Geometría Proyectiva sobre Campos Finitos.

Teorema 1.1.27 ([25], Theorem 2.1)**.** *Sea F un campo finito que contiene un subcampo K con q elementos. Entonces F tiene q^m elementos, donde $m = [F : K]$.*

Demostración. F es un espacio vectorial sobre K, y como F es finito, este es un es un espacio finito-dimensional sobre K. Si $[F : K] = m$, entonces F tiene una base sobre K conformada por m elementos, $b_1, b_2, \ldots, b_m$. Cada elemento de F puede escribirse de manera única en la forma $a_1b_1 + a_2b_2 + \cdots + a_mb_m$, donde $a_1, a_2, \ldots, a_m \in K$. Como cada a_i puede tomar q valores, F tiene exactamente q^m elementos.

□

Teorema 1.1.28 ([25], Theorem 2.2)**.** *Sea F un campo finito. Entonces F tiene p^n elementos, donde el primo p es la característica de F y n es el grado de F sobre el subcampo primo.*

Demostración. Como F es finito, la característica es un primo p por el Corolario 1.1.8. Por lo tanto el subcampo primo K es isomorfo a $\mathbb{F}_p$ por el Teorema 1.1.10 y este contiene p elementos. Por el Teorema 1.1.27 se cumple el Teorema 1.1.28.

□

Lema 1.1.29 ([25], Lemma 2.3)**.** *Si F es campo finito con q elementos, entonces cada $a \in F$ satisface $a^q = a$.*

Demostración. La identidad $a^q = a$ es trivial para $a = 0$. Por otra parte los elementos de $F \setminus \{0\}$, por el Teorema de Lagrange, forman un grupo de orden $q - 1$ bajo la multiplicación. Así $a^{q-1} = 1$ para todo $a \in F$ con $a \neq 0$, multiplicando por a se obtiene el resultado deseado.

□

Lema 1.1.30 ([25], Lemma 2.4)**.** *Si F es un campo finito con q elementos y K es un subcampo de F, entonces el polinomio $x^q - x$ en $K[x]$ se factoriza en $F[x]$ como*

$$x^q - x = \prod_{a \in F} (x - a)$$

y F es un campo de descomposición (splitting field) de $x^q - x$ sobre K.

Demostración. El polinomio $x^q - x$ de grado q tiene a lo más q raciones en F. Por el Lema 1.1.29 sabemos que esas q raíces, son todos los elementos de F. Así dado el polinomio se descompone en F de la manera indicada, y no se puede descomponer en un campo más pequeño.

□

Teorema 1.1.31 (Existencia y Unicidad de Campos Finitos, [25], Teorema 2.5)**.** *Para cualquier primo p y cada entero positivo n existe un campo finitos con p^n elementos. Cualquier campo finito con $q = p^n$ elementos es isomorfo al campo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$.*

Demostración. (Existencia) Para $q = p^n$ consideramos $x^q - x \in \mathbb{F}_p[x]$, y sea F el campo de descomposición sobre $\mathbb{F}_p$. Este polinomio tiene q raíces distintas en F como su derivada es $qx^{q-1} - 1 = -1$ en $\mathbb{F}_p[x]$, no puede tener raíces en común con $x^q - x$. Sea $S = \{a \in F : a^q - a = 0\}$. Así S es un subcampo de F ya que:

i) S contiene 0 y 1;

II) $a, b \in S$ por el Teorema 1.1.9 tenemos que $(a-b)^q = a^q - b^q = a - b$, y así $a - b \in S$;

III) para $a, b \in S$ y $b \neq 0$ tenemos $(ab^{-1})^q = a^q b^{-q} = ab^{-1}$, y así $ab^{-1} \in S$.

Por otra parte, $x^q - x$ se debe factorizar en S ya que S contiene todas sus raíces. Así $F = S$, y como S tiene q elementos, F s un campo finito con q elementos.

(Unicidad) Sea F un campo finito con $q = p^n$ elementos. Entonces F tiene característica p por el Teorema 1.1.28 y así contiene $\mathbb{F}_p$ como subcampo. Ahora, se tiene del Lema 1.1.30 que F es un campo de descomposición de $x^q - x$ sobre $\mathbb{F}_p$. Así el resultado deseado es una consecuencia de la unicidad (salvo isomorfismos) de los campos de descomposición.

□

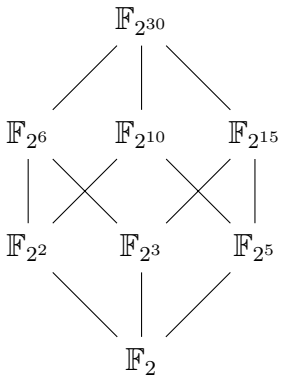
Teorema 1.1.32 (Criterio de Subcampo, [25], Theorem 2.6)**.** *Sea $\mathbb{F}_q$ un campo finito con $q = p^n$ elementos. Entonces cada subcampo de $\mathbb{F}_q$ tiene orden p^m, donde m es un divisor positivo de n. Recíprocamente, si m es un divisor positivo de n, entonces existe exactamente un subcampo de $\mathbb{F}_q$ con p^m elementos.*

Demostración. Es claro que un subcampo K de $\mathbb{F}_q$ tiene orden p^m para algún entero positivo $m \leq n$. Por el Lema 1.1.27 se muestra que $q = p^n$ debe ser una potencia de p^m, y así m es necesariamente un divisor de n.

Inversamente, si m es un divisor positivo de n, entonces $p^m - 1$ divide $p^n - 1$, y por lo tanto $x^{p^m-1} - 1$ divide a $x^{p^n-1} - 1$ en $\mathbb{F}_q[x]$. Por lo cual, $x^{p^m} - x$ divide $x^{p^n} - x = x^q - x$ en $\mathbb{F}_q[x]$. Por lo tanto, cada raíz de $x^{p^m} - x$ es una raíz de $x^q - x$ y así está en $\mathbb{F}_q$. De esto se tiene que $\mathbb{F}_q$ debe contener un campo de descomposición como subcampo de $x^{p^m} - x$ sobre $\mathbb{F}_q$, y podemos ver de la demostración del Teorema 1.1.31, un campo de división que tiene orden p^m. Si existen dos subcampos de orden p^m en $\mathbb{F}_q$, juntos contienen más de p^m raíces de $x^{p^m} - x$ en $\mathbb{F}_q$, lo cual es una contradicción.

□

Ejemplo 1.1.3. Los subcampos del campo finito $\mathbb{F}_{2^{30}}$ pueden ser determinados con la lista de todos los enteros positivos divisores de 30. Las relaciones de contención entre estos distintos subcampos se muestran en el siguiente diagrama.



Por el Teorema 1.1.32, las relaciones de contención son equivalentes a las relaciones de divisibilidad entre los divisores positivos de 30.

Teorema 1.1.33 ([25], Theorem 2.8)**.** *Para cada campo finito $\mathbb{F}_q$ el grupo multiplicativo $\mathbb{F}_q^*$ de elementos distintos de cero de $\mathbb{F}_q$ es cíclico.*

Demostración. Podemos suponer $q \geq 3$. Sea $h = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ la descomposición en factores primos del orden $h = q - 1$ del grupo $\mathbb{F}_q^*$. Para cada i, $1 \leq i \leq m$, el polinomio $x^{h/p_i} - 1$ tiene a lo más h/p_i raíces en $\mathbb{F}_q$. Como $h/p_i < h$, se tiene que existen elementos distintos de cero en $\mathbb{F}_q$ que no son raíces de este polinomio. Sea a_i, b_i elementos en $\mathbb{F}_q$ tal que $b_i = a_i^{h/p_i^{r_i}}$. Tenemos que $b_i^{p_i^{r_i}} = 1$, como el orden de b_i es un divisor de $p_i^{r_i}$ y es por lo tanto de la forma $p_i^{s_i}$. Por otro lado,

$$b_i^{p_i^{r_i - 1}} = a_i^{h/p_i} \neq 1,$$

y así el orden de b_i es $p_i^{r_i}$. Afirmamos que el elemento $b = b_1 b_2 \cdots b_m$ tiene orden h. Supongamos, por el contrario, que el orden de b es un divisor propio de h y es por lo tanto un divisor de al menos uno de los m enteros h/p_i, $1 \leq i \leq m$, supongamos de h/p_1. Entonces se tiene

$$1 = b^{h/p_1} = b_1^{h/p_1} b_2^{h/p_1} \cdots b_m^{h/p_1}.$$

Ahora si $2 \leq i \leq m$, entonces $p_i^{r_i}$ divide h/p_1, y así $b_i^{h/p_1} = 1$. Por lo tanto $b_1^{h/p_1} = 1$. Esto implica que el orden de b_1 debe dividir h/p_1, que es imposible ya que el orden de

b_1 es $p_1^{r_1}$. Así, $\mathbb{F}_q^*$ es un grupo cíclico con generador b.

□

Definición 1.1.34. Un generador de un grupo cíclico $\mathbb{F}_q^*$ es llamado un *elemento primitivo* de $\mathbb{F}_q$.

Teorema 1.1.35 ([25], Theorem 2.10)**.** *Sea $\mathbb{F}_q$ un campo finito y $\mathbb{F}_r$ una extensión de campo finito. Entonces $\mathbb{F}_r$ es una extensión algebraica simple de $\mathbb{F}_q$ para cada elemento primitivo de $\mathbb{F}_r$ puede servir como elemento para definir $\mathbb{F}_r$ sobre $\mathbb{F}_q$.*

Demostración. Sea ξ un elemento primitivo de $\mathbb{F}_r$. Claramente se tiene $\mathbb{F}_q(\xi) \subseteq \mathbb{F}_r$. Por otro lado, $\mathbb{F}_q(\xi)$ contiene al 0 y todas las potencias de ξ, y así todos los elementos de $\mathbb{F}_r$. Por lo tanto, $\mathbb{F}_r = \mathbb{F}_q(\xi)$.

□

Corolario 1.1.36 ([25], Corollary 2.11)**.** Para cada campo finito $\mathbb{F}_q$ y cada entero positivo n existe un polinomio irreducible en $\mathbb{F}_q[x]$ de grado n.

Demostración. Sea $\mathbb{F}_r$ la extensión del campo finito $\mathbb{F}_q$ de orden q^n, así que $[\mathbb{F}_r : \mathbb{F}_q] = n$. Por el Teorema 1.1.35 tenemos que $\mathbb{F}_r = \mathbb{F}_q(\xi)$ para algún $\xi \in \mathbb{F}_r$. Entonces el polinomio minimal de ξ sobre $\mathbb{F}_q$ es un polinomio irreducible en $\mathbb{F}_q[x]$ de grado n.

□

1.1.2. Polinomios

Lema 1.1.37 ([25], Lemma 2.12)**.** *Sea $f \in \mathbb{F}_q[x]$ un polinomio irreducible sobre un campo finito $\mathbb{F}_q$ y sea α una raíz de f en una extensión del campo $\mathbb{F}_q$. Entonces para un polinomio $h \in \mathbb{F}_q[x]$ se tiene que $h(\alpha) = 0$ si y solo si f divide a h.*

Demostración. Sea a el coeficiente lider de f y sea $g(x) = a^{-1}f(x)$. Entonces g es un polinomio mónico irreducible en $\mathbb{F}_q[x]$ con $g(\alpha) = 0$ y así el polinomio mínimo de α sobre $\mathbb{F}_q$ en el mismo sentido de la Definición 1.1.22. Finalmente de la segunda parte del Teorema 1.1.23 se obtiene lo querido.

□

Lema 1.1.38 ([25], Lemma 2.13)**.** *Sea $f \in F_q[x]$ un polinomio irreducible sobre $\mathbb{F}_q$ de grado m. Entonces $f(x)$ divide a $x^{q^n} - x$ si y solo si m divide a n.*

Demostración. Supongamos que $f(x)$ divide a $x^{q^n} - x$. Sea α una raíz de f en el campo de descomposición de f sobre $\mathbb{F}_q$. Entonces $\alpha^{q^n} = \alpha$, así $\alpha \in \mathbb{F}_{q^n}$. De esto, se tiene que $\mathbb{F}_q(\alpha)$ es un subcampo de $\mathbb{F}_{q^n}$. Pero como $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$ y $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$, por el Teorema 1.1.25 muestra que m divide n.

Por otro lado, si m divide a n, entonces el Teorema 1.1.32 implica que $\mathbb{F}_{q^n}$ contiene a $\mathbb{F}_{q^m}$ como un subcampo. Si α es una raíz de f en el campo de descomposición de f sobre $\mathbb{F}_q$, entonces $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, y así $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$. Por lo tanto, tenemos que $\alpha \in \mathbb{F}_{q^n}$, entonces $\alpha^{q^n} = \alpha$, y α es una raíz de $x^{q^n} - x \in \mathbb{F}_q[x]$. Podemos inferir del Lema 1.1.37 que $f(x)$ divide $x^{q^n} - x$.

□

Teorema 1.1.39 ([25], Theorem 2.14)**.** *Si f es un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m, entonces f tiene una raíz α en $\mathbb{F}_{q^m}$. Más aún, todas las raíces de f son simples y están dadas por los m elementos distintos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ de $\mathbb{F}_{q^m}$.*

Demostración. Sea α una raíz de f en el campo de descomposición de f sobre $\mathbb{F}_q$. Entonces $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = m$, de aquí $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$, y en particular $\alpha \in \mathbb{F}_{q^m}$. Ahora mostraremos que si $\beta \in \mathbb{F}_{q^m}$ es una raíz de f, entonces β^q es también una raíz de f. Tomando $f(x) = a_m x^m + \cdots + a_1 x + a_0$ con $a_i \in \mathbb{F}_q$ para $0 \leq i \leq m$. Entonces, usando el Lema 1.1.29 y el Teorema 1.1.9, se tiene

$$\begin{aligned} f(\beta^q) &= a_m \beta^{qm} + \cdots + a_1 \beta^q + a_0 \\ &= a_m^q \beta^{qm} + \cdots + a_1^q \beta^q + a_0^q \\ &= (a_m \beta^m + \cdots + a_1 \beta + a_0)^q \\ &= f(\beta)^q \\ &= 0. \end{aligned}$$

Por lo tanto, los elementos $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}$ son raíces de f. Queda por demostrar

que los elementos son distintos. Supongamos, por el contrario, que $\alpha^{q^j} = \alpha^{q^k}$ para algún entero j y k con $0 \leq j < k \leq m-1$. Elevando esta identidad a la potencia q^{m-k}, tenemos

$$\alpha^{q^{m-k+j}} = \alpha^{q^m} = \alpha.$$

Luego del Teorema 1.1.37 que $f(x)$ divide a $x^{q^{m-k+j}} - x$. Por Lema 1.1.38, esto solo es posible si m divide a $m-k+j$. Pero tenemos que $0 < m-k+j < m$, y esto nos lleva a una contradicción.

□

Corolario 1.1.40 ([25], Corollary 2.15)**.** Sea f un polinomio irreducible en $\mathbb{F}_q[x]$ de grado m. Entonces el campo de descomposición de f sobre $\mathbb{F}_q$ está dado por $\mathbb{F}_{q^m}$.

Demostración. El Teorema 1.1.39 muestra que f se descompone en $\mathbb{F}_{q^m}$, Más aún, $\mathbb{F}_q(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{m-1}}) = \mathbb{F}_q(\alpha) = \mathbb{F}_{q^m}$ para una raíz α de f en $\mathbb{F}_{q^m}$, donde la segunda identidad viene de la demostración del Teorema 1.1.39.

□

Sea $\mathbb{F}_q$ un campo finito con $q = p^h$ elementos, donde p es un número primo y $r \geq 1$ es un entero. Con cada polinomio $f(x) \in \mathbb{F}_q[x]$ está asociada una función polinómica $f\colon \mathbb{F}_q \to \mathbb{F}_q$, definida por $\alpha \mapsto f(\alpha)$, donde $f(\alpha)$ es el resultado de sustituir x por α.

Lema 1.1.41 ([37], Lemma 1.1)**.** *Para cualquier función $\Phi\colon \mathbb{F}_q \to \mathbb{F}_q$ existe una única función polinomial $f \in \mathbb{F}_q[x]$ de grado a lo más $q-1$ tal que la función polinomial asociada $f\colon \alpha \mapsto f(\alpha)$ satisface $\Phi(\alpha) = f(\alpha)$ para todo $\alpha \in \mathbb{F}_q$.*

Demostración. La siguiente formula (*Carlitz Interpolation Formula*) entrega un polinomio adecuado:

$$f(x) = \sum_{\alpha \in \mathbb{F}_q} \Phi(\alpha)(1 - (x-\alpha)^{q-1}).$$

Para mostrar que es única, suponemos que existen polinomios $f, g \in \mathbb{F}_q[x]$ de grado $\leq q-1$ que satisfacen $f(\alpha) = g(\alpha)$ para todo $\alpha \in \mathbb{F}_q$. Si $f \neq g$ entonces se tiene que la diferencia $(f-g)$ es un polinomio distinto del polinomio nulo y que se anula en los q

elementos de $\mathbb{F}_q$. Pero $\deg(f-g) \leq q-1$, así $f-g$ puede tener a lo más $q-1$ raíces en $\mathbb{F}_q$, lo que es una contradicción.

□

Lema 1.1.42 ([37], Lemma 1.2)**.** *Para cualquier $f, g \in \mathbb{F}_q[x]$ se tiene que $f(\alpha) = g(\alpha)$ para todo $\alpha \in \mathbb{F}_q$ si y solo si $f(x) \equiv g(x) \, mod \, (x^q - x)$.*

Demostración. Por el algoritmo de división podemos escribir

$$f(x) - g(x) = h(x)(x^q - x) + r(x), \text{ donde } \deg(r) < q.$$

Entonces $f(\alpha) - g(\alpha) = r(\alpha)$ para todo $\alpha \in \mathbb{F}_q$, así $f(\alpha) = g(\alpha)$ para todo $\alpha \in \mathbb{F}_q$ si y solo si r se anula en cada elemento de $\mathbb{F}_q$. Como $\deg(r) < q$ esto es equivalente a $r(x) = 0$.

□

Entre las funciones polinomiales que podemos considerar, las funciones de más interés para el trabajo que se realizará más adelante, son del tipo $f\colon \mathbb{F}_q \to \mathbb{F}_q$ que permutan los elementos de $\mathbb{F}_q$. Por el Lema 1.1.41 podemos asumir que las funciones son polinomios de grado a lo más $q-1$.

Definición 1.1.43. Un polinomio $f \in \mathbb{F}_q[x]$ es llamado Polinomio de Permutación (PP) de $\mathbb{F}_q$ si la función polinomial asociada $f\colon c \to f(c)$ es una permutación de $\mathbb{F}_q$.

Lema 1.1.44 ([37], Lemma 1.3)**.** *El polinomio $f \in \mathbb{F}_q$ es un polinomio de permutación de $\mathbb{F}_q$ si y solo si una de las siguientes condiciones se cumple:*

1. *la función $f\colon c \to f(c)$ es uno a uno;*
2. *la función $f\colon c \to f(c)$ es inyectiva;*
3. *$f(x) = a$ tiene una solución en $\mathbb{F}_q$ para cada $a \in \mathbb{F}_q$;*
4. *$f(x) = a$ tiene solución unica en $\mathbb{F}_q$ para cada $a \in \mathbb{F}_q$.*

Ejemplo 1.1.4. Consideremos el polinomio $f(x) = x^3 + 1 \in \mathbb{F}_{11}[x]$. Evaluando los valores $\{0, 1, \ldots, 10\} = \mathbb{F}_{11}$ en f, se tiene

x	0	1	2	3	4	5	6	7	8	9	10
$f(x)$	1	2	9	6	10	5	8	3	7	4	0

Podemos ver que f es un PP de $\mathbb{F}_{11}$ con estructura cíclica $(0, 1, 2, 9, 4, 10)(3, 6, 8, 7)$.

1.1.3. Skew Polinomios

En esta sección representamos la construcción de un anillo no conmutativo $R = \mathbb{F}_q[x; \theta]$, donde $q = p^h$ y p es número primo. La estructura de este anillo no conmutativo depende de los elementos de un campo finito $\mathbb{F}_q$ y de un automorfismo θ de $\mathbb{F}_q$. Denotamos por $|\langle\theta\rangle|$ el orden del automorfismo θ.

Sea $\mathbb{F}_q$ un campo finito de característica p y θ un automorfismo de $\mathbb{F}_q$ con $|\langle\theta\rangle| = m$. Sea K un subcampo de $\mathbb{F}_q$ fijado bajo θ. Entonces, $[\mathbb{F}_q : K] = m$ y $K = \mathbb{F}_{p^t}$, donde $q = p^{tm}$. Por otra parte, K ya es fijado bajo θ, así tenemos $\theta(a) = a^{p^t}$ para todo $a \in \mathbb{F}_q$.

Ejemplo 1.1.5. Consideremos el campo finito $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ donde $\alpha^2 + \alpha + 1 = 0$. Definimos el automorfismo

$$\begin{aligned} \theta \colon \mathbb{F}_4 &\longrightarrow \mathbb{F}_4 \\ a &\longmapsto \theta(a) = a^2. \end{aligned}$$

Entonces $\theta(0) = 0$, $\theta(1) = 1$, $\theta(\alpha) = \alpha^2$ y $\theta(\alpha^2) = \alpha$. Así el campo fijado K es sólo el campo binario $\mathbb{F}_2$.

Definición 1.1.45. Siguiendo la notación anterior, definimos el conjunto de polinomios torcidos (skew) $\mathbb{F}_q[x; \theta]$ como

$$\mathbb{F}_q[x; \theta] = \{f(x) = a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}, a_i \in \mathbb{F}_q \text{ para todo } i = 0, 1, \ldots, n\}$$

donde la adición de estos polinomios es definida de la forma estándar, mientras que la multiplicación es definida usando la regla de la distributividad y la regla $xa = \theta(a)x$, para todo $a \in \mathbb{F}_q$.

Ejemplo 1.1.6. Usando la misma regla del automorfismo del ejemplo 1.1.5 se tiene

$$\begin{aligned}(\alpha x)\cdot(\alpha^2 x) &= \alpha\cdot\theta(\alpha^2)x^2\\ &= \alpha\cdot\alpha x^2\\ &= \alpha^2 x^2.\end{aligned}$$

Por otro lado, tenemos:

$$\begin{aligned}(\alpha^2 x)\cdot(\alpha x) &= \alpha^2\cdot\theta(\alpha)x^2\\ &= \alpha^2\cdot\alpha^2 x^2\\ &= \alpha x^2.\end{aligned}$$

Esto muestra que $(\alpha x)\cdot(\alpha^2 x) \neq (\alpha^2 x)\cdot(\alpha x)$.

Teorema 1.1.46 ([32])**.** *El conjunto $\mathbb{F}_q[x;\theta]$, con respecto a la adición y multiplicación definidas arriba, es un anillo no conmutativo llamado anillo de polinomios torcidos (skew).*

Los siguientes resultados son conocidos para el anillo $\mathbb{F}_q[x;\theta]$:

Lema 1.1.47 ([32], Lemma II.10)**.** *Sean $f, g \in \mathbb{F}_q[x;\theta]$. Entonces*

1. *$\mathbb{F}_q[x;\theta]$ no tiene divisores de cero distintos de cero.*
2. *Las unidades de $\mathbb{F}_q[x;\theta]$ son las de $\mathbb{F}_q$.*
3. *$deg(f+g) \leq max\{deg(f), deg(g)\}$.*
4. *$deg(f\cdot g) = deg(f) + deg(g)$.*

Teorema 1.1.48 ([32], Theorem II.10, Algoritmo de División Derecha)**.** *Para cualquier polinomio f y g en $\mathbb{F}_q[x;\theta]$ con $f \neq 0$ existe un único polinomio q y r tal que*

$$g = q \cdot f + r \text{ donde } deg(r) < deg(f).$$

El resultado anterior es llamado división derecha por f. Un resultado similar puede ser probado respecto a la división izquierda por f.

Teorema 1.1.49 ([32], Teorema II.12)**.** *$\mathbb{F}_q[x;\theta]$ es anillo ideal principal izquierdo (derecho) no conmutativo. Más aún, cualquier ideal bilátero debe ser generado por un polinomio $f(x)$ de la forma*

$$f(x) = (a_0 + a_m x^m + a_{2m} x^{2m} + \cdots + a_{nm} x^{nm}) \cdot x^t$$

donde $m = |\langle\theta\rangle|$, $t \in \mathbb{N}$.

Teorema 1.1.50 ([39], Lemma 7)**.** *$(x^n - 1) \in Z(\mathbb{F}_q[x;\theta])$ si y solo si $m \mid n$, donde $Z(\mathbb{F}_q[x;\theta])$ es el centro de $\mathbb{F}_q[x;\theta]$ y $m = |\langle\theta\rangle|$.*

Como resultado del Teorema 1.1.49, el ideal generado por el polinomio $x^n - \alpha$ es un ideal bilatero en $\mathbb{F}_q[x;\theta]$ si sólo si $m \mid n$. Más aún, $(x^n - \alpha)$ conmuta con los elementos de $F[x;\theta]$. Este resultado es muy importante en la estructura de los elementos en el conjunto $R_n = \mathbb{F}_q[x;\theta]/(x^n - \alpha)$. Sea $R = \mathbb{F}_q[x;\theta]$, si $m \mid n$ entonces el conjunto R_n es un anillo, donde la multiplicación es definida por

$$(f_1(x) + R(x^n - \alpha)) * (f_2(x) + R(x^n - \alpha)) = f_1(x) * f_2(x) + (x^n - \alpha).$$

Si $m \nmid n$ entonces $(x^n - \alpha) \notin Z(\mathbb{F}_q[x;\theta])$, lo que implica que en general

$$(f_1(x) + R(x^n - \alpha)) * (f_2(x) + R(x^n - \alpha)) \neq f_1(x) * f_2(x) + (x^n - \alpha).$$

Por lo cual, si $m \nmid n$, la multiplicación no es bien definida en R_n y no es un anillo.

Sea $(f(x) + R(x^n - \alpha))$ un elemento en R_n, y sea $r(x) \in \mathbb{F}_q[x;\theta]$. Definimos la multiplicación a la izquierda como:

$$r(x)*(f(x)+R(x^n-\alpha)) = r(x)*f(x)+R(x^n-\alpha) \text{ para cualquier } r(x) \in \mathbb{F}_q[x;\theta]. \quad (1.1)$$

Esta multiplicación es bien definida de los elementos de $\mathbb{F}_q[x;\theta]$ por los elementos de R_n. Bajo esta definición tenemos el siguiente resultado:

Teorema 1.1.51 ([39], Teorema 9)**.** *R_n es un $F[x;\theta]$-módulo izquierdo donde la multiplicación es definida en 1.1.*

Definición 1.1.52. Sea $f(x) = \sum_{i=0}^{n} a_i x^i$ un polinomio en $\mathbb{F}_q[x;\theta]$, con θ un automorfismo de $\mathbb{F}_q$ y $\alpha \in \mathbb{F}_q$. La *evaluación residual (derecha)* de f en α es denotada por $f(\alpha)$ y es definida como el resto de la división derecha de f por $x - \alpha$. También se define $\mathcal{N}_i^{\theta}(\alpha)$ recursivamente como

$$\mathcal{N}_0^{\theta}(\alpha) := 1,$$
$$\mathcal{N}_{i+1}^{\theta}(\alpha) := \theta(\mathcal{N}_i^{\theta}(\alpha)) \cdot \alpha = \theta^i(\alpha)\theta^{i-1}(\alpha)\cdots\theta(\alpha)\alpha.$$

Lema 1.1.53 ([8], Lemma 1)**.** *Sea $f(x) = \sum_{i=0}^{n} a_i x^i$ un polinomio en $\mathbb{F}_q[x;\theta]$, con θ un autmorfismo de $\mathbb{F}_q$. Para $\alpha \in \mathbb{F}_q$, se tiene*

$$f(\alpha) = \sum_{i=0}^{n} a_i \mathcal{N}_i^{\theta}(\alpha).$$

Definición 1.1.54. Sea $\mathbb{F}_q$ un campo finito y θ un automorfismo de $\mathbb{F}_q$. Dado $A = \{\alpha_1, \alpha_2 \ldots, \alpha_n\} \subset \mathbb{F}_q$, la matriz θ-Vandermonde de A es definida por

$$V_n^{\theta}(A) = \begin{pmatrix} \mathcal{N}_0^{\theta}(\alpha_1) & \mathcal{N}_0^{\theta}(\alpha_2) & \cdots & \mathcal{N}_0^{\theta}(\alpha_n) \\ \mathcal{N}_1^{\theta}(\alpha_1) & \mathcal{N}_1^{\theta}(\alpha_2) & \cdots & \mathcal{N}_1^{\theta}(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{N}_n^{\theta}(\alpha_1) & \mathcal{N}_n^{\theta}(\alpha_2) & \cdots & \mathcal{N}_n^{\theta}(\alpha_n) \end{pmatrix} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \mathcal{N}_1^{\theta}(\alpha_1) & \mathcal{N}_1^{\theta}(\alpha_2) & \cdots & \mathcal{N}_1^{\theta}(\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathcal{N}_n^{\theta}(\alpha_1) & \mathcal{N}_n^{\theta}(\alpha_2) & \cdots & \mathcal{N}_n^{\theta}(\alpha_n) \end{pmatrix}$$

En $\mathbb{F}_q$ con $q = p^h$, donde p es primo y considerando ϑ el automorfismo de Frobenius, es decir $\vartheta(a) = a^p$. La factorización de polinomios en $\mathbb{F}_q[x;\vartheta]$ puede ser trasladada a factorización de polinomios en $\mathbb{F}_q[x]$ con algoritmo de André Leroy (Teorema 1.1.56). Esto proceso se puede generalizar considerando como automorfismo una potencia de Frobenius, es decir, $\theta(a) = a^{p^s}$, con $s = 1, \ldots, h-1$.

Definición 1.1.55. Dado un número primo p y un entero $i \geq 1$, se define

$$[i] := \frac{(p^s)^i - 1}{p-1} = p^{i-1} + p^{i-2} + \cdots + 1.$$

Consideramos el siguiente subconjunto de $\mathbb{F}_q[x]$:

$$\mathbb{F}_q[x^{[]}] := \left\{ \sum_{i \geq 0} \alpha_i x^{[i]} \in \mathbb{F}_q[x] \right\}.$$

Un polinomio perteneciente a este conjunto, es llamado $[p^s]$-polinomio. Se tiene que $\mathbb{F}_q[t;\theta] \subset \mathbb{F}_q[x][t;\theta]$, luego considerando $f \in \mathbb{F}_q[t;\theta]$ como un elemento de $\mathbb{F}_q[x][t;\theta]$ podemos evaluarlo en x. Se denota el polinomio resultante por $f^{[]}[x] \in \mathbb{F}_q[x]$, es decir, $f(t)(x) = f^{[]}(x)$.

Teorema 1.1.56 ([24], Theorem 2.5)**.** *Sea $f(t) = \sum_{i=0}^{n} a_i t^i$ un polinomio en $\mathbb{F}_q[t;\theta] \subset \mathbb{F}_q[x][t;\theta]$, con θ el automorfismo de Frobenius. Se tiene:*

(1) para cualquier $h = h(x) \in \mathbb{F}_q[x]$, $f(h) = \sum_{i=0}^{n} a_i h^{[i]}$;

(2) $\{f^{[]} | f \in \mathbb{F}_q[t;\theta]\} = \mathbb{F}_q[x^{[]}]$;

(3) para cualquier $h(t) \in R = \mathbb{F}_q[t;\theta]$, $f(t) \in Rh(t)$ si y sólo si $f^{[]} \in \mathbb{F}_q[x]h^{[]}(x)$.

Este Teorema muestra que el problema de irreducibilidad de un polinomio $f(t) \in \mathbb{F}_q[x;\theta]$ puede ser traslado en términos de factorizaciones en $\mathbb{F}_q[x]$. Esto se puede observar en el siguiente Corolario obvio, pero importante.

Corolario 1.1.57 ([24], Corollary 2.6)**.** Un polinomio $f(t) \in \mathbb{F}_q[t;\theta]$ es irreducible si y sólo si su $[p^s]$-polinomio asociado $f^{[]} \in \mathbb{F}_q[x^{[]}] \subset \mathbb{F}_q[x]$ no tiene factores triviales en $\mathbb{F}_q[x^{[]}]$.

De esta forma, se obtiene fácilmente un algoritmo de factorización de polinomios en $\mathbb{F}_q[t;\theta]$. Dado un $f(t) \in \mathbb{F}_q[t;\theta]$ primero se debe encontrar el polinomio $h^{[]} \in \mathbb{F}_q[x^{[]}]$ tal que $h^{[]}$ divide a $f^{[]}$(si es posible) y escribimos $f^{[]}(x) = g(x)h^{[]}(x)$ para algún $g(x)$ en $\mathbb{F}_q[x]$. Esto entrega que $f(t) = \widetilde{g}(t)h(t) \in \mathbb{F}_q[t;\theta]$, para algún $\widetilde{g}(t) \in \mathbb{F}_q[t;\theta]$, el cual encontramos al dividir $f(t)$ a la derecha por $h(t)$. Ahora se aplica el mismo procedimiento a $\widetilde{g}(t)$ y encontramos un factor derecho $\widetilde{g}(t)$ en $\mathbb{F}_q[t;\theta]$ encontrando (si es posible) un $[p^s]$-factor de $\widetilde{g}^{[]}$. Este proceso se repite hasta que el $[p^s]$-polinomio asociado sea irreducible en $\mathbb{F}_q[x^{[]}]$.

Ejemplo 1.1.7. Considerando $\mathbb{F}_4$ y θ como en el ejemplo 1.1.5, sea

$$f(t) = t^4 + \alpha^2 t^3 + \alpha^2 t2 + \alpha^2 t + 1 \in \mathbb{F}_4[t;\theta].$$

Su [2]-polinomio asociado es

$$f^{[]}(x) = x^{15} + \alpha^2 x^7 + \alpha^2 x^3 + \alpha^2 x + 1 \in \mathbb{F}_4[x^{[]}].$$

Este puede ser factorizado de la siguiente forma

$$f^{[]}(x) = (x^6 + x^4 + \alpha^2 x^2 + \alpha^2 x + \alpha)(x^6 + \alpha^2 x^4 + x^3 + \alpha^2 x^2 + \alpha x + \alpha^2)(x^3 + \alpha x + 1).$$

Este último factor es un [2]-polinomio que corresponde a

$$h(t) = t^2 + \alpha t + 1 \in \mathbb{F}_4[t;\theta].$$

Más aún, $h^{[]}(x) = x^3 + \alpha x + 1$ es irreducible en $\mathbb{F}_4[x]$, así $h(t)$ también es irreducible en $\mathbb{F}_4[t;\theta]$. Luego, podemos concluir que

$$f(t) = \widetilde{g}(t)(t^2 + \alpha t + 1).$$

De donde $\widetilde{g}(t) = (t^2 + t + 1)$ y su [2]-polinomio asociado está dado por

$$g^{[]}(x) = x^3 + x + 1.$$

Como $g^{[]}$ es irreducible en $\mathbb{F}_4[x]$, se tiene que

$$f(t) = (t^2 + t + 1)(t^2 + \alpha t + 1)$$

es la descomposición de $f(t)$ en factores irreducibles en $\mathbb{F}_4[t;\theta]$.

1.2. Geometría Proyectiva

1.2.1. Definiciones Básicas y Propiedades Numéricas

Sea $V = V(n+1, K)$ un espacio vectorial de dimensión $(n+1)$ sobre el campo K con origen $\vec{0}$. Considerando la relación de equivalencia en los puntos de $V \setminus \{\vec{0}\}$, donde las clases son los subespacios de dimensión uno de V sin el origen; esto es, si $\vec{x}, \vec{y} \in V \setminus \{0\}$ y para alguna base $\vec{x} = (x_0, x_1, \ldots, x_n)$, $\vec{y} = (y_0, y_1, \ldots, y_n)$, $\vec{x}$ es equivalente a $\vec{y}$ si, para algún $\lambda \in K_0 := K \setminus \{0\}$, $y_i = \lambda x_i$ para todo i. Entonces el conjunto de clases de equivalencias es el *espacio proyectivo n-dimensional sobre* K y se denota por $\mathbb{P}^n(K)$ o $PG(n, K)$, si $K = \mathbb{F}_q$ entonces se denota por $\mathbb{P}^n(\mathbb{F}_q)$ o simplemente $PG(n, q)$.

Los elementos de $\mathbb{P}^n(K)$ son llamados puntos. Si el punto $[x]$ es la clase de equivalencia del vector $\vec{x}$, entonces se dice que $\vec{x}$ es un vector que representa $[x]$. Los puntos $[x_1], \ldots, [x_r]$ son *linealmente independientes* si el conjunto de vectores $\vec{x_1}, \ldots, \vec{x_r}$ que los representa son linealmente independiente.

Un *subespacio de dimensión* m de $\mathbb{P}_n(K)$ es el conjunto de todos los puntos cuyos vectores que representan forman (junto con el origen) un subespacio de dimensión $m+1$ de $V(n+1, K)$. Subespacios de dimensión cero, uno, dos y tres son llamados respectiva-

mente *punto*, *linea*, *plano* y *espacio* respectivamente. Un subespacio de dimensión $n-1$ es llamado un *hiperplano*.

Un m-espacio Π_m es un conjunto de puntos representados por los vectores $t_0\vec{x_0} + t_1\vec{x_1} + \cdots + t_m\vec{x_m}$, donde $\vec{x_0}, \vec{x_1}, \ldots, \vec{x_m}$ son $m+1$ vectores linealmente independiente y $(t_0, t_1, \ldots, t_m) \in K^{m+1} \setminus \{\vec{0}\}$; o equivalentemente, Π_m es el conjunto de puntos cuyos vectores representantes $\vec{x}$ satisfacen la ecuación $\vec{x}A = 0$, donde A es una matriz $(n+1) \times (n-m)$ de rango $n-m$ con coeficientes en K.

Definición 1.2.1. Si un punto P está en un hiperplano Π, entonces P es *incidente* con Π.

Definición 1.2.2. Si S y S' son dos espacios $\mathbb{P}^n(K)$, entonces un *colineación* $\mathfrak{L}\colon S \to S'$ es una biyección que preserva la incidencia; esto es, si $\Pi_r \subset \Pi_s$, entonces $\mathfrak{L}(\Pi_r) \subset \mathfrak{L}(\Pi_s)$.

Definición 1.2.3. Una *proyectividad* $\mathfrak{L}\colon S \to S'$ es una biyección dada por una matriz T. Si $\mathfrak{L}[x] = [x']$, entonces $\lambda\vec{x'} = \vec{x}T$ donde $\vec{x'}$ y $\vec{x}$ son los vectores coordenadas para $[x']$ y $[x]$ respectivamente, y $\lambda \in K_0$.

Teorema 1.2.4 ([17], Theorem 3.1.1)**.** *El número de puntos en un espacio proyectivo de dimensión n sobre el campo $\mathbb{F}_q$ está dado por $q^n + q^{n-1} + \cdots + q + 1$.*

Teorema 1.2.5 ([17], Theorem 3.1.1)**.** *El número de subespacios de dimensión r en un espacio proyectivo de dimensión n sobre el campo $\mathbb{F}_q$ está dado por $\dfrac{[n-r+1, n+1]\_}{[1, r+1]\_}$, donde $[a, b]\_ = \prod_{i=a}^{b}(q^i - 1)$ para $b \geq a$, e igual a 1 en otro caso.*

Corolario 1.2.6.

1. El número de puntos en una recta proyectiva es $q+1$.
2. El número de puntos en un plano proyectivo es $q^2 + q + 1$.
3. El número de rectas en un plano proyectivo es $q+1$.
4. El número de puntos en un espacio proyectivo es $(q+1)(q^2+1)$.

Ejemplo 1.2.1. El plano proyectivo $\mathbb{P}^2(\mathbb{F}_3)$ (Figura 3.1) está formado por los puntos:

- $[0:0:1]$
- $[1:0:1]$
- $[1:1:2]$
- $[1:0:2]$
- $[0:1:0]$
- $[0:1:1]$
- $[1:2:0]$
- $[1:0:0]$
- $[1:1:0]$
- $[1:2:1]$
- $[1:1:1]$
- $[1:2:2]$
- $[0:1:2]$

Además, la recta $L = \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{F}_3) \mid x_0 + 2x_2 = 0\}$ contiene a los puntos $[0:1:0]$, $[1:0:1]$, $[1:2:1]$ y $[1:1:1]$.

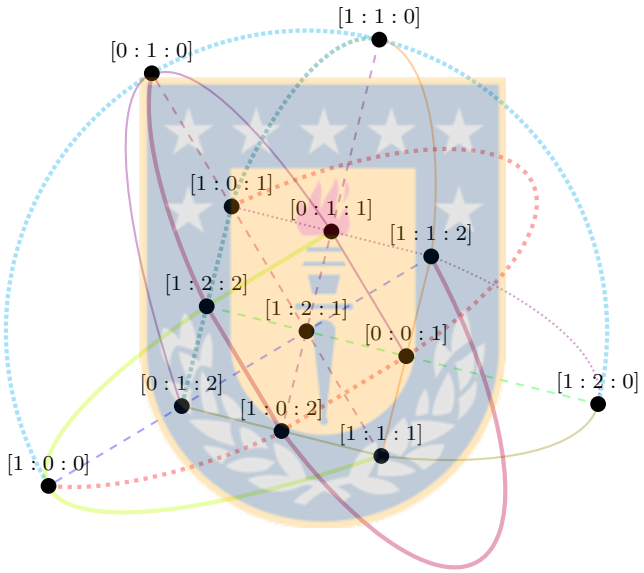


Figura 1.1: Plano Proyectivo sobre el Campo Finito $\mathbb{F}_3$.

1.2.2. Arco y Curva Racional Normal

Una *cónica no-singular* de $\mathbb{P}^2(\mathbb{F}_q)$ consiste de $q+1$ puntos donde 3 de ellos no son colineales. Es natural preguntar si la condición de no colinealidad de $q+1$ son suficientes para tener una cónica no singular. En otras palabras, ¿esta propiedad combinatoria caracteriza a las cónicas no-singulares? Esta pregunta tuvo respuesta de forma afirmativa

por Segre [33]. Generalizando Segre consideró conjunto de k puntos en $\mathbb{P}^2(\mathbb{F}_q)$, $k \geq 3$, que no tengan 3 puntos colineales.

Definición 1.2.7. Un *k-arco* en $\mathbb{P}^2(\mathbb{F}_q)$ es un conjunto de k puntos no tres de los cuales son colineales. Un *k-arco se dice completo* si no está contenido en un $(k+1)$-arco.

Definición 1.2.8. Sea $v \in \mathbb{Z}_{\geq 2}$. Un *$(k, v)$-arco* en $\mathbb{P}^2(\mathbb{F}_q)$ es un conjunto de k puntos no $v+1$ de los cuales son colineales. Un (k, v)-arco se dice *completo*, si no está contenido en un $(k+1, v)$-arco.

Definición 1.2.9. Un *k-arco* en $\mathbb{P}^n(\mathbb{F}_q)$ es un conjunto de k puntos no $n+1$ de los cuales están sobre un hiperplano. Un k-arco en $\mathbb{P}^n(\mathbb{F}_q)$ se dice *completo* si no esta contenido en un $(k+1)$-arco.

Teorema 1.2.10 ([22], Subsection 3.1)**.** *Para cada potencia de primo q y cada entero $N \geq q-1$, existe un $(N+2)$-arco en $\mathbb{P}^N(\mathbb{F}_q)$ equivalente a $\{[1:0:0\cdots:0], [0:1:0:\cdots:0], \ldots, [0:0:\cdots:0:1], [1:1:\cdots:1]\}$ y es de tamaño máximo.*

Definición 1.2.11. Una *curva racional normal* de $\mathbb{P}^n(\mathbb{F}_q)$, $n \geq 2$, es un conjunto de puntos en $\mathbb{P}^n(\mathbb{F}_q)$ que es proyectivamente equivalente a

$$\{[t^n : t^{n-1} : \cdots : t : 1] \mid t \in \mathbb{F}_q\} \cup \{[1:0:\cdots:0]\}.$$

Una curva racional normal contiene $q+1$ puntos. Para $n = 2$, esta es una cónica no-singular. Para $n = 3$, esta es una *cubica twisted*. Cualquier $(n+3)$-arco en $\mathbb{P}^n(\mathbb{F}_q)$ está contenida en una única curva racional normal de este espacio ([18], Teorema 21.1.1).

Teorema 1.2.12 ([20], Theorem 4.10)**.** *Para q impar y $n \geq 3$, sea $\mathcal{K}$ un k-arco en $\mathbb{P}^n(\mathbb{F}_q)$. Si*

$$k > q - \frac{1}{4}\sqrt{q} + n - \frac{1}{4},$$

entonces $\mathcal{K}$ se encuentra en una única curva racional normal de $\mathbb{P}^n(\mathbb{F}_q)$.

Teorema 1.2.13 ([20], Theorem 4.11)**.** *Para q par, $q \neq 2$, $n \geq 3$, sea $\mathcal{K}$ e un arco en $\mathbb{P}^n(\mathbb{F}_q)$. Si*

$$k > q - \frac{1}{2}\sqrt{q} + n - \frac{3}{4},$$

entonces $\mathcal{K}$ se encuentra en una única curva racional normal de $\mathbb{P}^n(\mathbb{F}_q)$.

Teorema 1.2.14 ([17], Chapter 8)**.** *Sea K un k-arco de $\mathbb{P}^2(\mathbb{F}_q)$. Entonces*

1. *$k \leq q + 2$;*
2. *para q impar, $k \leq q + 1$;*
3. *cualquier cónica no-singular es un $(q+1)$-arco;*
4. *para q par, un $(q+1)$-arco se extiende a un $(q+2)$-arco.*

Definición 1.2.15. En $\mathbb{P}^2(\mathbb{F}_q)$,

1. un $(q+1)$-arco es un *óvalo*;
2. un $(q+2)$-arco, q par, es un *óvalo completo* o *hiperóvalo*.

Lema 1.2.16 ([17] Lemma 8.1.4)**.** *Las $q+1$ tangentes a un $(q+1)$-arco K en $\mathbb{P}^2(\mathbb{F}_q)$ con q par se intersectan en un punto, el cual llamamos núcleo.*

Teorema 1.2.17 ([33], Theorem I)**.** *En $\mathbb{P}^2(\mathbb{F}_q)$, q impar, cada óvalo es una cónica no-singular (es decir, puede ser representado por una ecuación de segundo grado).*

Definición 1.2.18. En $\mathbb{P}^2(\mathbb{F}_q)$, el tamaño más grande de un arco completo es denotado por $m(2,q)$, el segundo más grande se denota por $m'(2,q)$, y el más pequeño por $t(2,q)$.

Los progresos para $m'(2,q)$ son los siguientes.

Teorema 1.2.19.

$m'(2,q)$

$\leq q-1$	$q \geq 7$	*Segre 1955* [33]
$\leq q-\frac{1}{4}\sqrt{q}+\frac{7}{4}$	q *impar*	*Segre 1967* [36]
$=q-\sqrt{q}+1$	q *par*	*Segre 1967* [36]
$\leq \frac{44}{45}q+\frac{8}{9}$	q *primo*	*Thas 1987* [43]
$\leq q-\frac{1}{2}\sqrt{q}+5$	$q=p^h$, $p \geq 5$	*Hirschfeld-Korchmáros 1996* [16].

Respecto a los k-arcos completos, Coolsaet y Sticker [10] entregaron una clasificación completa de estos para $q \leq 31$, la cual fue realizada por medio de programas escritos en Java.

Denotando por $m_v(2,q)$ al tamaño máximo de un (k,v)-arco, se tiene además el siguiente resultado.

Teorema 1.2.20 ([27],[22] Theorem 3.2.5)**.** *Si* $4 \leq v < q$*, entonces*

$$m_v(2,q) \leq (v-1)q + v - 3.$$

1.2.3. Hiperóvalos

En $\mathbb{P}^2(\mathbb{F}_q)$, q par, existen hiperóvalos conformados por los puntos de una cónica y su núcleo, Lema 1.2.14; este tipo de ovalo es llamado *hiperóvalo regular*.

Lema 1.2.21 ([17], Lemma 8.4.1; [34])**.** *Para* $q = 2, 4, 8$*, cada óvalo en* $\mathbb{P}^2(\mathbb{F}_q)$ *es regular.*

Demostración. En $\mathbb{P}^2(\mathbb{F}_2)$, un hiperóvalo está formado por cuatro puntos, cualquiera tres de ellos siempre forman una cónica. Por lo tanto, no es solo un óvalo, pero está formado por la cónica unido con su núcleo.
De forma similar en $\mathbb{P}^2(\mathbb{F}_4)$, un hiperóvalo está formado por 6 puntos, cualquiera de sus 5 puntos forman una cónica.Por lo tanto, no es solo un óvalo, pero está formado por la cónica unido con su núcleo.
Para el caso $q = 8$, ver [34].

□

Teorema 1.2.22 ([17], Lemma 8.4.2)**.** *Un hiperóvalo de* $\mathbb{P}^2(\mathbb{F}_q)$*,* $q = 2^h$*,* $h > 0$*, es proyectivamente equivalente a un hiperóvalo,*

$$\{[F(t) : t : 1] \mid t \in \mathbb{F}_q\} \cup \{[0 : 1 : 0], [1 : 0 : 0]\},$$

donde F *es un polinomio de permutación sobre* $\mathbb{F}_q$ *de grado a lo más* $q-2$*, que satisface* $F(0) = 0$*,* $F(1) = 1$ *y tal que para cada* $s \in \mathbb{F}_q$*,*

$$F_s(x) = \frac{F(x+s) + F(s)}{x},$$

es un polinomio de permutación con $F_s(0) = 0$*.*

Demostración. Sea $\mathcal{K}$ un $(q+1)$-arco. Llamando U_1 al núcleo de $\mathcal{K}$ y sean U_0, U_1 y U puntos de $\mathcal{K}$. Entonces el hiperóvalo $\mathcal{O}$ está formado por $\mathcal{K} \cup \{U_1\}$.
Sea u_2 la recta que contiene a U_0 y U_1, como ambos puntos están en $\mathcal{O}$, esta recta no contiene más puntos del hiperóvalo. Por lo tanto, podemos considerar $\mathcal{O} \setminus \{U_0, U_1\} = \{[s_i : t_1 : 1] \mid i \in \{1, \ldots, q\}\}$. Cada otra recta que contiene a U_0, tiene exactamente un punto de $\mathcal{O}$, $t_1 \neq t_j$ para $i \neq j$. De manera similar, cada recta que contiene a U_1 contiene exactamente otro punto de $\mathcal{O}$, $s_1 \neq s_j$ para $i \neq j$. Así $\{s_i \mid i \in \{1, \ldots, q\}\} = \{t_i \mid i \in \{1, \ldots, q\}\} = \mathbb{F}_q$ y existe un único polinomio de permutación F en $\mathbb{F}_q[x]$ tal que $F(t_i) = s_i$, para todo i. Por lo tanto $\mathcal{O} \setminus \{U_0, U_1\} = \mathcal{K} \setminus \{U_0\} = \{[F(t) : t : 1] \mid t \in \mathbb{F}_q\}$. Ahora, el grado de F debe ser mayor a 1, de otra forma los puntos de $\mathcal{K} \setminus \{U_0\}$ pueden estar en una linea, que es imposible para $q > 2$. Por lo tanto, podemos escribir $\mathcal{O} = \{[P(t) : t : 1] \mid t \in \mathbb{F}_q\} \cup \{U_0\}$, donde $U_0 = \{[0 : 1 : 0]\}$. Además como U_2 y U están en $\mathcal{K}$, se tiene $F(0) = 0$ y $F(1) = 1$.
La condición para cada $s \in \mathbb{F}_q$,

$$F_s(x) = \frac{F(x+s) + F(s)}{x},$$

es un polinomio de permutación con $F_s(0) = 0$, es equivalente a que no existan 3 puntos

colineales de $\{[P(t) : t : 1] \mid t \in \mathbb{F}_q\} \setminus \{U_0, U_1, U_2\}$. Esto es cierto si y solo si

$$\begin{vmatrix} F(t_1) & t_1 & 1 \\ F(t_2) & t_2 & 1 \\ F(t_3) & t_3 & 1 \end{vmatrix} \neq 0,$$

para t_1, t_2, t_3 distintos en $\mathbb{F}_q$; esto es,

$$\frac{F(t_1) + F(t_2)}{t_1 + t_2} \neq \frac{F(t_1) + F(t_3)}{t_1 + t_3}.$$

Equivalentemente, para cada s en $\mathbb{F}_q$, $\dfrac{F(t) + F(s)}{t + s}$ toma un valor distinto en $\mathbb{F}_q \setminus \{0\}$ para cada t en $\mathbb{F}_q \setminus \{s\}$; como no se tiene $\dfrac{F(t) + F(s)}{t + s} = 0$, ya que luego $F(t) = F(s)$ y $t = s$. Usando la sustitución $x + s$ por t se tiene que $\dfrac{F(x + s) + F(s)}{x}$ toma valores diferentes para cada $\mathbb{F}_q \setminus \{0\}$; esto es, cada s en $\mathbb{F}_q$, el polinomio $F_s(x)$ define un polinomio de permutación de $\mathbb{F}_q \setminus \{0\}$. Sin embargo, el grado de F_s es menor que $q - 1$. Así, $F_s(0) = 0$ y F_s es un polinomio de permutación de $\mathbb{F}_q[x]$.

□

Cuando las condiciones del Teorema sean satisfechas para el polinomio F, nos referiremos al ovalo como $\mathscr{D}(F)$.

Corolario 1.2.23 ([17], Corollary 1)**.** Si $\mathscr{D}(F)$ con $F(x) = \sum_{i=1}^{q-2} a_i x^i$ es un ovalo en $\mathbb{P}^2(\mathbb{F}_q)$ con q par y $q > 2$, entonces $F(x) = \sum_{j=1}^{(q-2)/2} a_{2j} x^{2j}$ es una función par.

Ejemplo 1.2.2. (Programa 12) En $\mathbb{P}^2(\mathbb{F}_8)$, con $\mathbb{F}_8 = \mathbb{F}_2[w]$, el conjunto de puntos

$$\{[F(x) : x : 1] \mid x \in \mathbb{F}_8\} \cup \{[0 : 1 : 0], [1 : 0 : 0]\}$$

con $F(x) = x^6 + x^4 + x^2$ corresponde a los puntos:

- $[0:1:0]$
- $[1:0:0]$
- $[0:0:1]$
- $[1:1:1]$
- $[w^5:w:1]$
- $[w^3:w^2:1]$
- $[w^2:w^3:1]$
- $[w^6:w^4:1]$
- $[w:w^5:1]$
- $[w^4:w^6:1]$

Para $q=2^h$, $h\geq 4$, existen *hiperóvalos irregulares*, o sea, hiperóvalos que no son la unión de una cónica y su núcleo. Varias clases infinitas de hiperóvalos irregulares son conocidas. El problema es la clasificación de hiperóvalos parece ser demasiado difícil. En general solo se tiene el Teorema 1.2.22. La tabla 1.1 presenta algunas clases de hiperóvalos conocidos.

Nombre	$F(x)$	$q=2^h$	Condición	
Regular	x^2			[4]
Traslación	x^{2^i}		$(h,i)=1$	[34]
Segre	x^6	h impar		[35]
Glynn I	$x^{3\sigma+4}$	h impar	$\sigma=2^{(h+1)/2}$	[13]
Gynn II	$x^{\sigma+\lambda}$		$\sigma=2^{(h+1)/2}$;	[13]
			$\lambda=2^m$ si $h=4m-1$;	
			$\lambda=2^{3m+1}$ si $h=4m+1$	

Tabla 1.1: Hiperóvalos en $\mathbb{P}^2(\mathbb{F}_q)$, q par.

1.3. Teoría de Códigos

1.3.1. Códigos Lineales

Un código lineal de largo n sobre el campo finito $\mathbb{F}_q$ es simplemente un subespacio del espacio vectorial $\mathbb{F}_q^n=\underbrace{\mathbb{F}_q\times\cdots\times\mathbb{F}_q}_{n-\text{veces}}$ con $n\geq 2$.

Definición 1.3.1. Un *código lineal* $\mathscr{C}$ sobre $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$.

Definición 1.3.2. Sea $\mathscr{C}\subseteq\mathbb{F}_q^n$ un código lineal.

1. El *código dual* de $\mathscr{C}^\perp$ es el complemento ortogonal de $\mathscr{C}$ en $\mathbb{F}_q^n$.

2. La *dimensión* $\dim(\mathscr{C})$ de $\mathscr{C}$ es la dimensión de $\mathscr{C}$ como un espacio vectorial sobre $\mathbb{F}_q$, i.e. $\dim(\mathscr{C}) := \dim_{\mathbb{F}_q}\mathscr{C}$.

Teorema 1.3.3 ([26], Theorem 4.2.4)**.** *Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código lineal. Entonces,*

1. *$|\mathscr{C}| = q^{dim(\mathscr{C})}$, i.e. $dim(\mathscr{C}) = \log_q |\mathscr{C}|$, donde $|\mathscr{C}|$ es la cardinalidad de $\mathscr{C} \subseteq \mathbb{F}_q^n$;*

2. *$\mathscr{C}^\perp$ es un código lineal y $dim(\mathscr{C}) + dim(\mathscr{C}^\perp) = n$;*

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

Demostración.

1. Sea $\dim(\mathscr{C}) = k$. Si $\{\vec{v_1}, \vec{v_2}, \ldots, \vec{v_k}\}$ una base para $\mathscr{C}$, luego

$$\mathscr{C} = \{\lambda_1\vec{v_1} + \lambda_2\vec{v_2} + \cdots + \lambda_k\vec{v_k} \colon \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}_q\}.$$

   Como $|\mathbb{F}_q| = q$, existen exactamente q opciones para cada $\lambda_1, \lambda_2, \ldots, \lambda_k$; por lo tanto $\mathscr{C}$ tiene exactamente $q^{\dim(\mathscr{C})}$ elementos.

2. Es fácil verificar que dado un subespacio vectorial sobre $\mathbb{F}_q$, su complemento ortogonal también es un subespacio vectorial de $\mathbb{F}_q$.
   Si $\mathscr{C} = \{\vec{0}\}$, el resultado se cumple de forma trivial. Supongamos que $\dim(\mathscr{C}) = k \geq 1$, con base $\{\vec{v_1}, \vec{v_2}, \ldots, \vec{v_k}\}$. Se debe probar que $\dim(\mathscr{C}^\perp) = n - k$.
   Se tiene que $\vec{x} \in \mathscr{C}^\perp$ si y solo si

$$\vec{v_1} \cdot \vec{x} = \vec{v_2} \cdot \vec{x} = \cdots = \vec{v_k} \cdot \vec{x} = 0,$$

   lo que es equivalente a decir que $\vec{x}$ satisface $A\vec{x}_t = \vec{0}$, donde A es una matriz $k \times n$ donde las i-esima fila es $\vec{v_i}$.
   Las filas de A son linealmente independientes, si $A\vec{x}_t = \vec{0}$ es un sistema lineal de k ecuaciones linealmente independientes en n variables, el cual tiene un espacio de solución de dimensión $n - k$.

3. Usando la igualdad anterior y reemplazando $\mathscr{C} \subseteq \mathbb{F}_q^n$ por $\mathscr{C}^\perp$, se obtiene que $\dim(\mathscr{C}) = \dim((\mathscr{C}^\perp)^\perp)$. Por lo cual, es suficiente mostrar que $\mathscr{C} \subseteq (\mathscr{C}^\perp)^\perp$. Sea $\vec{c} \in \mathscr{C}$. Para mostrar que $\vec{c} \in (\mathscr{C}^\perp)^\perp$, se debe tener que $\vec{c} \cdot \vec{x} = 0$ para todo $\vec{x} \in \mathscr{C}^\perp$. Como $\vec{c} \in \mathscr{C}$ y $\vec{x} \in \mathscr{C}^\perp$, por la definición de $\mathscr{C}^\perp$, se tiene que $\vec{c} \cdot \vec{x} = 0$.

□

Ejemplo 1.3.1.

1. En $\mathbb{F}_2$. Sea $\mathscr{C} = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$, luego $\dim(\mathscr{C}) = \log_2 |\mathscr{C}| = \log_2 4 = 2$. Además, se tiene que $\mathscr{C}^\perp = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$, así $\dim(\mathscr{C}^\perp) = 2$. En particular, los puntos 1 y 2 del Teorema 1.3.3 quedan verificados.

2. En $\mathbb{F}_3$. Sea $\mathscr{C} = \{(0,0,0), (0,0,1), (0,0,2), (0,1,0), (0,2,0), (0,1,1), (0,1,2), (0,2,1), (0,2,2)\}$, por lo tanto $\dim(\mathscr{C}) = \log_3 |\mathscr{C}| = \log_3 9 = 2$. Además $\mathscr{C}^\perp = \{(0,0,0), (1,0,0), (2,0,0)\}$, así $\dim(\mathscr{C}^\perp) = 1$.

Otras nociones importantes en la teoría de códigos son la distancia y el peso, definidos de la siguiente forma.

Definición 1.3.4. Si $\vec{x}, \vec{y} \in \mathbb{F}_q^n$, la *distancia* (Hamming) $d(\vec{x}, \vec{y})$ de $\vec{x}$ y $\vec{y}$ está dada por

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

mientras que el *peso* $w(\vec{x})$ de $\vec{x} \in \mathbb{F}_q^n$ es definido por

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

donde $\vec{0} := (0, \ldots, 0) \in \mathbb{F}_q^n$.

Observación 1.3.5. Equivalentemente, para $\vec{x}, \vec{y} \in \mathbb{F}_q^n$ se puede definir distancia entre

$\vec{x} = (x_1, \ldots, x_n)$ e $\vec{y} = (y_1, \ldots, y_n)$ como

$$d(\vec{x}, \vec{y}) := d(x_1, y_1) + \cdots + d(x_n, y_n), \tag{1.2}$$

donde, para cada $i \in \{1, \ldots, n\}$ se define

$$d(x_i, y_i) := \begin{cases} 1 & , x_i \neq y_i \\ 0 & , x_i = y_i \end{cases}.$$

Proposición 1.3.6 ([26], Proposition 2.3.3)**.** *Sea $\vec{x}, \vec{y}, \vec{z} \in \mathbb{F}_q^n$. Entonces se tiene*

1. $0 \leq d(\vec{x}, \vec{y}) \leq n$,
2. $d(\vec{x}, \vec{y}) = 0$ *si y sólo si* $\vec{x} = \vec{y}$,
3. $d(\vec{x}, \vec{y}) = d(\vec{y}, \vec{x})$,
4. *(Desigualdad Triangular)* $d(\vec{x}, \vec{z}) \leq d(\vec{x}, \vec{y}) + d(\vec{y}, \vec{z})$.

Observación 1.3.7. Para cada elemento x de $\mathbb{F}_q$, se puede definir el peso de Hamming de la siguiente forma:

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

Luego, para $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, el peso de Hamming de $\vec{x}$ puede definirse también como

$$w(\vec{x}) := w_h(x_1) + \cdots + w_h(x_n). \tag{1.3}$$

Definición 1.3.8. Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código lineal tal que $\mathscr{C} \neq \{\vec{0}\}$. La *distancia mínima* de $\mathscr{C}$ es definida como

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

Equivalentemente el *peso mínimo* de $\mathscr{C}$ puede definirse como

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

Lema 1.3.9. *Si $\vec{x}, \vec{y} \in \mathbb{F}_q^n$, luego $d(\vec{x}, \vec{y}) = w(\vec{x} - \vec{y})$.*

Demostración. Para $\vec{x} = (x_1, \ldots, x_n), \vec{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$, $d(\vec{x}, \vec{y}) = 0$ si y sólo si $\vec{x} = \vec{y}$, lo que es cierto si y sólo si $x_i = y_i$ para todo $i = 1, \ldots, n$, o equivalentemente, $w(\vec{x} - \vec{y}) = 0$. Usando ahora 1.2 y 1.3, el Lema queda demostrado.

□

Teorema 1.3.10 ([26], Theorem 4.3.8)**.** *Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código lineal. Entonces $d(\mathscr{C}) = w(\mathscr{C})$.*

Demostración. Por definición, existe $\vec{x}, \vec{y} \in \mathscr{C}$ tal que $d(\vec{x}, \vec{y}) = d(\mathscr{C})$, por lo tanto

$$d(\mathscr{C}) = d(\vec{x}, \vec{y}) = w(\vec{x} - \vec{y}) \geq w(\mathscr{C}),$$

donde $\vec{x} - \vec{y} \in \mathscr{C}$.
Por otra parte, existe un $\vec{z} \in \mathscr{C} \setminus \{\vec{0}\}$ tal que $w(\mathscr{C}) = w(\vec{z})$, así

$$w(\mathscr{C}) = w(\vec{z}) = d(\vec{z}, \vec{0}) \geq d(\mathscr{C}).$$

□

Ejemplo 1.3.2. Considerando el código binario $\mathscr{C} \subseteq \mathbb{F}_2^4$, dado por

$$\mathscr{C} = \{(0,0,0,0), (1,0,0,0), (0,1,0,0), (1,1,0,0)\}.$$

Se puede ver que

$$w((1,0,0,0)) = 1,$$
$$w((0,1,0,0)) = 1,$$
$$w((1,1,0,0)) = 2.$$

Por lo tanto, $d(\mathscr{C}) = 1$.

Observación 1.3.11. Un código lineal $\mathscr{C} \subseteq \mathbb{F}_q^n$ con $\dim(\mathscr{C}) = k$ se denota por $[n,k]_q$-código o, si q es claro en el contexto, un $[n,k]$-código. Si este además tiene distancia d, se denota por $[n,k,d]$-código.

Definición 1.3.12.

1. Una *matriz generadora* para un código lineal $\mathscr{C}$ es una matriz G cuyas filas forman una base para $\mathscr{C}$.

2. Una *matriz de control de paridad* H de un código lineal $\mathscr{C}$ es una matriz generadora para el código dual $\mathscr{C}^{\perp}$.

Observación 1.3.13.

1. Si $\mathscr{C}$ es un $[n,k]$-código lineal, entonces la matriz generadora de $\mathscr{C}$ debe ser una matriz $k \times n$ y la matriz de control de paridad para $\mathscr{C}$ debe ser una matriz $(n-k) \times n$.

2. Las filas de una matriz generadora son linealmente independientes. Lo mismo se tiene para la matriz de control de paridad. Para mostrar que una matriz $k \times n$ G es de hecho una matriz generadora para un determinado $[n,k]$-código lineal $\mathscr{C}$, es suficiente mostrar que las filas de G son vectores en $\mathscr{C}$ y que son linealmente independiente.

Definición 1.3.14.

1. Una matriz generadora de la forma $(I_k|X)$ se dice que está en la *forma estandar*.
2. Una matriz de control de paridad en la forma $(Y|I_{n-k})$ se dice que está en la *forma estándar*.

Lema 1.3.15 ([26], Lemma 4.5.4)**.** *Sea $\mathscr{C}$ un $[n,k]$-código lineal sobre $\mathbb{F}_q$, con matriz generadora G. Entonces $\vec{v} \in \mathbb{F}_q^n$ pertenece a $\mathscr{C}^\perp$ si y sólo si $\vec{v}$ es ortogonal a cada fila de G; i.e., $\vec{v} \in \mathscr{C}^\perp \Leftrightarrow \vec{v}G_t = \vec{0}$. En particular, una matriz H $(n-k) \times n$ es una matriz de control de paridad para $\mathscr{C}$ si y sólo si las filas de H son linealmente independiente y $HG_t = O$.*

Demostración. Sea $\vec{r_i}$ la i-esima fila de G. En particular, $\vec{r_i} \in \mathscr{C}$ para todo $1 \leq i \leq k$, y cada $\vec{c} \in \mathscr{C}$ puede escribirse como

$$\vec{c} = \lambda_1 \vec{r_1} + \cdot + \lambda_k \vec{r_k},$$

donde $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q$.
Si $\vec{v} \in \mathscr{C}^\perp$, entonces $\vec{v} \cdot \vec{c} = 0$ para todo $\vec{c} \in \mathscr{C}$. En particular, $\vec{v}$ es ortogonal a $\vec{r_i}$, para todo $1 \leq i \leq k$; i.e., $\vec{v}G_t = \vec{0}$.
Por otra parte, si $\vec{v} \cdot \vec{r_i} = 0$ para todo $1 \leq i \leq k$, luego claramente, para cualquier $\vec{c} = \lambda_1 \vec{r_1} + \cdot + \lambda_k \vec{r_k} \in \mathscr{C}$,

$$\vec{v} \cdot \vec{c} = \lambda_1(\vec{v} \cdot \vec{r_1}) + \cdot + \lambda_k(\vec{v} \cdot \vec{r_k}) = 0.$$

Para la última parte, si H es una matriz de control de paridad para $\mathscr{C}$, entonces las filas de H son linealmente independientes por definición. Como las filas de H son códigos en $\mathscr{C}^\perp$, de lo anterior se tiene que $HG_t = O$.
Ahora, si $HG_t = O$, entonces lo anterior muestra que las filas de H, y por lo tanto el espacio de filas de H, están contenidas en $\mathscr{C}$. Como las filas de H son linealmente independientes, el espacio de filas de H tiene dimensión $n-k$, así el espacio de filas de

H es de hecho $\mathscr{C}^{\perp}$. En otras palabras, H es la matriz de control de paridad para $\mathscr{C}$.

□

Teorema 1.3.16 ([26], Theorem 4.5.6)**.** *Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código lineal y sea H su matriz de control de paridad. Entonces:*

1. *$\mathscr{C}$ tiene distancia $\geq d$ si y sólo si cualquier $d-1$ columnas de H son linealmente independientes;*

2. *$\mathscr{C}$ tiene distancia $\leq d$ si y sólo si H tiene d columnas que son linealmente dependientes.*

Demostración. Sea $\vec{v} = (v_1, \ldots, v_n) \in \mathscr{C}$ un vector con peso $w(\vec{v}) = e > 0$. Supongamos que las coordenadas distintas de cero están en las posiciones $i_1, \ldots, i_e$, así $v_j = 0$ si $j \notin \{i_1, \ldots, i_e\}$. Sea $\vec{c_i}$ $(1 \leq i \leq n)$ la i-ésima columna de H.
Por el Lema 1.3.15, $\mathscr{C}$ contiene un vector distinto de cero $\vec{v} = (v_1, \ldots, v_n)$ de peso e (con coordenadas distintas de cero $v_{i_1}, \ldots, v_{1_e}$) si y sólo si

$$\vec{0} = \vec{v}H_t = v_{i_1}\left(\vec{c_{i_1}}\right)_t + \cdots + v_{1_e}\left(\vec{c_{i_e}}\right)_t,$$

que es válido si y sólo si existen e columnas de H (sean estas, $\vec{c_{i_1}}, \ldots, \vec{c_{i_e}}$) que son linealmente dependiente.
Para decir que la distancia de $\mathscr{C}$ es $\geq d$ es equivalente a decir que $\mathscr{C}$ no contiene ningún vector no nulo de peso $\leq d_1$, que es lo mismo que decir que cualquier $\leq d-1$ columnas de H son linealmente independientes. Esto prueba (1).
De manera similar, para decir que la distancia de $\mathscr{C}$ es $\leq d$ es equivalente a decir que $\mathscr{C}$ contiene un vector no nulo de peso $\leq d$, que es equivalente a decir que H tiene $\leq d$ columnas (y entonces d columnas) que son linealmente dependientes. Esto prueba (2).

□

Corolario 1.3.17. Sea $\mathscr{C}$ un código lineal y sea H su matriz de control de paridad. Entonces las siguientes proposiciones son equivalentes:

1. $\mathscr{C}$ tiene distancia d;

2. cualquier $d-1$ columnas de H son linealmente independientes y H tiene d columnas que son linealmente dependientes.

Ejemplo 1.3.3. Sea $\mathscr{C}$ un código binario con matriz de control de paridad

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

Se puede observar que no existen columnas nulas y ningún par de columnas de H suman $\vec{0}_t$, así cualquier par de columnas de H son linealmente independiente. Sin embargo, las columnas 1, 3 y 4 suman $\vec{0}_t$, y por lo tanto son linealmente dependientes. Así, la distancia de $\mathscr{C}$ es $d = 3$.

Teorema 1.3.18 ([26], Theorem 4.5.9)**.** *Si $G = (I_k \mid X)$ es la matriz generadora en forma estándar de un $[n, k]$-código $\mathscr{C}$, entonces la matriz de control de paridad para $\mathscr{C}$ es $H = (-X_t \mid I_{n-k})$.*

Demostración. Obviamente, le ecuación $HG_t = O$ es satisfecha. Considerando las últimas $n - k$ coordenadas, es claro que las filas de H son linealmente independientes. Por lo tanto, la conclusión viene del Lema 1.3.15.

□

1.3.2. MDS-códigos

De manera más general, podemos definir un código (no necesariamente lineal) como un subconjunto de $\mathbb{F}_q^n$. En este caso, un código de largo n, con M elementos y distancia mínima d se denota como un (n, M, d)-código.

Definición 1.3.19. Dado un campo finito $\mathbb{F}_q$ y dado los valores n y d, $A_q(n, d)$ denota al tamaño M más grande posible para el cual existe un (n, M, d)-código sobre $\mathbb{F}_q$. Esto

es,

$$A_q(n,d) = \max\{M : \text{ existe un } (n,M,d)\text{-código sobre } \mathbb{F}_q\}.$$

Cualquier (n,M,d)-código $\mathscr{C}$ que tiene el tamaño máximo, esto es, $M = A_q(n,d)$, es llamado *código optimo*.

Teorema 1.3.20 (Singleton Bound, [26], Theorem 5.4.1)**.** *Para cualquier entero $q > 1$, cualquier entero positivo n y d tal que $1 \leq d \leq n$, se tiene*

$$A_q(n,d) \leq q^{n-d+1}.$$

En particular, cuando q es la potencia de un primo, los parametros $[n,k,d]$ de un código lineal sobre $\mathbb{F}_q$ satisface

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

Demostración. Para probar que $A_q(n,d) \leq q^{n-d+1}$, consideramos un (n,M,d)-código $\mathscr{C}$ sobre un campo $\mathbb{F}_q$, donde $M = A_q(n,d)$. Borrando la últimas $d-1$ coordenadas de todos los vectores de $\mathscr{C}$. Ya que la distancia es d, después de borrar las últimas $d-1$ coordenadas de todos los vectores, los restantes vectores (de largo $n-d+1$) aún son todos distintos. El número máximo de vectores de largo $n-d+1$ es q^{n-d+1}, por lo tanto $A_q(n,d) = M \leq q^{n-d+1}$.
Para mostrar que $d \leq n-k+1$, se obtiene de lo anterior, ya que por definición de $A_q(n,d)$, $q^k \leq A_q(n,d)$.

□

Definición 1.3.21. Un código lineal con parámetros $[n,k,d]$ tal que $d = n-k+1$ es llamado *Maximun Distance Separable (MDS)* código.

Teorema 1.3.22 ([26], Theorem 5.4.5)**.** *Sea $\mathscr{C}$ un código lineal sobre $\mathbb{F}_q$ con parámetros $[n,k,d]$. Sea G, H la matrices generadoras y la matriz de control de paridad, respectivamente para $\mathscr{C}$. Entonces, las siguientes proposiciones son equivalentes:*

1. *$\mathscr{C}$ es un MDS código;*

2. *cada conjunto de $n-k$ columnas de H es linealmente independientes;*

3. *cada conjunto de k columnas de G es linealmente independientes;*

4. *$\mathscr{C}^{\perp}$ es un MDS código.*

Demostración. La equivalencia de (1) y (2) viene directamente del Corolario 1.3.17, con $d = n - k + 1$.

Como G es la matriz de control de paridad para $\mathscr{C}^{\perp}$, (3) y (4) también son equivalentes por el Corolario 1.3.17.

Ahora, probaremos que (1) implica (4).

Recordemos que H es la matriz generadora para $\mathscr{C}^{\perp}$, así el largo de $\mathscr{C}^{\perp}$ es n y su dimensión es $n-k$. Para mostrar que $\mathscr{C}^{\perp}$ es MDS, debemos mostrar que la distancia mínima d' es $k+1$.

Supongamos $d' \leq k$. Entonces existe un vector $\vec{c} \in \mathscr{C}^{\perp}$ con a lo más k entradas distintas de cero (y por lo tanto al menos $n-k$ coordenadas ceros). Permutando las coordenadas no cambia el peso de los vectores, así podemos asumir que las últimas $n-k$ coordenadas de $\vec{c}$ son 0.

Escribiendo H como $H = (A \mid H')$, donde A es alguna matriz $(n-k) \times k$ y H' es una matriz cuadrada $(n-k) \times (n-k)$. Ya que las columnas de H' son linealmente independientes (porque (1) y (2) son equivalentes), H' es invertible. Por lo tanto, las filas de H' son linealmente independientes. La única manera de que todas las últimas coordenadas sean 0 (como es $\vec{0}$) es usar la combinación 0-lineal de filas de H' (por independencia lineal). Por lo tanto, todos los vectores $\vec{c}$ son todos los vectores nulos $\vec{0}$. Así, $d' \geq k+1$. Usando el Singleton Bound, se tiene que $d' = k+1$.

Ya que $(\mathscr{C}^{\perp})^{\perp} = \mathscr{C}$, lo anterior también muestra que (4) implica (1).

□

Definición 1.3.23. Un MDS código $\mathscr{C}$ sobre $\mathbb{F}_q$ es *trivial* si y sólo si $\mathscr{C}$ satisface una las siguientes condiciones:

1. $\mathscr{C} = \mathbb{F}_q^n$;

2. $\mathscr{C}$ es equivalente al código generado por $\vec{1} = (1, \ldots, 1)$;

3. $\mathscr{C}$ es equivalente al código dual generado por $\vec{1}$.

Teorema 1.3.24 ([28], Theorem 11.4.8)**.** *Un $[n, k, d]$-código $\mathscr{C}$ con matriz generadora $G = [I|G']$, donde G' es una matriz $k \times (n-k)$, es MDS si y sólo si cada submatriz cuadrada (formada por cualquier i filas y cualquier i columnas, para cualquier $i = 1, 2, \ldots, min\{k, n-k\}$) de G' es no singular.*

1.3.3. Códigos Cíclicos y Pseudo-Cíclicos

Definición 1.3.25. Un código lineal $\mathscr{C} \subseteq \mathbb{F}_q^n$ es llamado *código cíclico* si es invariante bajo la transformación lineal

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

Observación 1.3.26. Decir que un código lineal $\mathscr{C}$ es invariante bajo ϕ es equivalente a decir que $\mathscr{C}$ es invariante bajo la acción de la matriz de permutación

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

es decir, $\mathscr{C} = \{\vec{c}P : \vec{c} \in \mathscr{C}\}$.

Ejemplo 1.3.4. Los siguientes códigos, son códigos cíclicos:

1. los tres códigos triviales $\{\vec{0}\}$, $\{\lambda \cdot \vec{1} : \lambda \in \mathbb{F}_q\}$ y $\mathbb{F}_q^n$;

2. el $[3, 2, 2]$-código lineal binario $\{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$.

Teorema 1.3.27 ([26], Theorem 7.3.7)**.** *Si $\mathscr{C} \subseteq \mathbb{F}_q^n$ es un código cíclico entonces el código dual $\mathscr{C}^\perp \subseteq \mathbb{F}_q^n$ es también un código cíclico.*

Demostración. Si $\vec{h} = (h_1, \ldots, h_n) \in \mathscr{C}^{\perp}$ entonces $\vec{h} \cdot \vec{c} = 0$ para todo $\vec{c} = (c_1, \ldots, c_n) \in \mathscr{C}$. Así tenemos

$$\begin{aligned}\phi(\vec{h}) \cdot \vec{c} &= (h_n, h_1, \ldots, h_{n-2}) \cdot (c_1, c_2 \ldots, c_n) \\ &= h_n c_0 + h_1 c_2 + \cdots + h_{n-2} c_n \\ &= \vec{h} \cdot \phi^{n-1}(\vec{c}) = 0,\end{aligned}$$

como $\mathscr{C}$ es un código cíclico, $\phi^{n-1}(\vec{c}) \in \mathscr{C}$, donde $\phi^k = \underbrace{\phi \circ \cdots \circ \phi}_{k\text{-veces}}$, para todo $k \in \mathbb{N}$. Luego, $\mathscr{C}^{\perp}$ es un código cíclico.

□

Con el fin de convertir la estructura de códigos cíclicos en una estructura algebraica, consideramos la siguiente correspondencia:

$$\begin{aligned}\pi : \quad \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q[x]/(x^n - 1) \\ (a_0, a_1, \ldots, a_{n-1}) &\longmapsto a_0 + a_1 x + \cdots a_{n-1} x^{n-1}\end{aligned} \tag{1.4}$$

Observamos que π es un $\mathbb{F}_q$-isomorfismo lineal de espacios vectoriales sobre $\mathbb{F}_q$. Así, podemos identificar en algunos casos $\mathbb{F}_q^n$ con $\mathbb{F}_q[x]/(x^n - 1)$ y un vector $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$ con el polinomio $\pi(\vec{a}) = \sum_{i=0}^{n-1} a_i x^i$. Ya que $\mathbb{F}_q[x]/(x^n - 1)$ es un anillo, tenemos la operación multiplicación en $\mathbb{F}_q[x]/(x^n - 1)$ además de la adición heredada de $\mathbb{F}_q^n$.

Ejemplo 1.3.5. Consideremos el código cíclico $\mathscr{C} = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$; luego $\pi(\mathscr{C}) = \{0, 1+x, 1+x^2, x+x^2\} \subset \mathbb{F}_2[x]/(x^3 - 1)$.

Teorema 1.3.28 ([26], Theorem 7.2.1)**.** *Sea π definida en (1.4). Luego un subconjunto no vacío $\mathscr{C}$ de $\mathbb{F}_q^n$ es un código cíclico si y sólo si $\pi(\mathscr{C})$ es un ideal de $\mathbb{F}_q[x]/(x^n - 1)$.*

Demostración. Supongamos que $\pi(\mathscr{C})$ es un ideal de $\mathbb{F}_q[x]/(x^n - 1)$. Luego, para cualquier $\alpha, \beta \in \mathbb{F}_q \subset \mathbb{F}_q[x]/(x^n - 1)$ y $\vec{a}, \vec{b} \in \mathscr{C}$, se tiene que $\alpha\pi(\vec{a}), \beta\pi(\vec{b}) \in \pi(\mathscr{C})$. Así $\pi(\alpha\vec{a} + \beta\vec{b}) = \alpha\pi(\vec{a}) + \beta\pi(\vec{b}) \in \pi(\mathscr{C})$, es decir, $\alpha\vec{a} + \beta\vec{b} \in \mathscr{C}$. Esto muestra que $\mathscr{C}$ es un código lineal.

Ahora sea $\vec{c} = (c_0, \ldots, c_{n-1}) \in \mathscr{C}$ y $\pi(\vec{c}) = c_0 + c_1x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1} \in \pi(\mathscr{C})$. Como $\pi(\mathscr{C})$ es un ideal, el polinomio

$$\begin{aligned} x\pi(\vec{c}) &= c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n \\ &= c_{n-1} + c_0x + \cdots + c_{n-2}x^{n-1} \in \pi(\mathscr{C}), \text{ ya que } x^n - 1 = 0 \text{ en } \mathbb{F}_q[x]/(x^n - 1), \end{aligned}$$

es decir, $(c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathscr{C}$.

Por otro lado, supongamos que $\mathscr{C} \subseteq \mathbb{F}_q^n$ es un código cíclico. Para cualquier polinomio

$$f(x) = f_0 + f_1x + \cdots + f_{n-2}x^{n-2} + f_{n-1}x^{n-1} = \pi(f_0, f_1, \ldots, f_{n-2}, f_{n-1})$$

de $\pi(\mathscr{C})$ con $(f_0, f_1, \ldots, f_{n-2}, f_{n-1}) \in \mathscr{C}$, el polinomio

$$x \cdot f(x) = f_{n-1} + f_0x + f_1x^2 + \cdots + f_{n-2}x^{n-1}$$

es también un elemento de $\pi(\mathscr{C})$ ya que $\mathscr{C}$ es cíclico. Así $x^2 \cdot f(x) = x(x \cdot f(x)) \in \pi(\mathscr{C})$ y por inducción podemos ver que $x^i \cdot f(x) \in \pi(\mathscr{C})$ para todo entero $i \geq 0$. Como $\mathscr{C}$ es un código lineal y π es una transformación lineal, $\pi(\mathscr{C}) \subseteq \mathbb{F}_q[x]/(x^n - 1)$ es un grupo con respecto a la suma y para cualquier $g(x) = g_0 + g_1x + \cdots + g_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n - 1)$ el polinomio

$$g(x) \cdot f(x) = \sum_{i=o}^{n-1} g_i(x^i f(x))$$

es un elemento de $\pi(\mathscr{C})$. Por lo tanto, $\pi(\mathscr{C})$ es un ideal de $\mathbb{F}_q[x]/(x^n - 1)$.

□

Ejemplo 1.3.6.

1. El código $\mathscr{C} = \{(0,0,0), (1,1,1), (2,2,2)\}$ en $\mathbb{F}_3$ es un código cíclico. El ideal correspondiente en $\mathbb{F}_3[x]/(x^3 - 1)$ es $\pi(\mathscr{C}) = \{0, 1 + x + x^2, 2 + 2x + 2x^2\}$.

2. El conjunto $I = \{0, 1+x^2, x+x^3, 1+x+x^2+x^3\}$ es un ideal en $\mathbb{F}_2[x]/(x^4-1)$. El correspondiente código cíclico es $\pi^{-1}(I) = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$.

Teorema 1.3.29 ([26], Theorem 7.2.3)**.** *Sea I un ideal distinto del nulo en $\mathbb{F}_q[x]/(x^n-1)$ y sea g un polinomio mónico no nulo de menor grado en I. Entonces $g(x)$ es un generador de I y divide a x^n-1.*

Demostración. Para cualquier polinomio $f(x)$ de I, tenemos por el algoritmo de división

$$f(x) = s_1(x)g(x) + r_1(x)$$

para algún polinomio $s_1(x), r_1(x) \in \mathbb{F}_q[x]$ con $\deg(r_1(x)) < \deg(g(x))$. Esto fuerza a que $r(x) = 0$, ya que $r_1(x) = f(x) - s_1(x)g(x) \in I$ y $g(x)$ tiene el grado menor de los polinomios de I. Por lo tanto, $I = \langle g(x) \rangle$.
Considerando ahora el algoritmo de división en

$$x^n - 1 = s_2(x)g(x) + r_2(x)$$

con $\deg(r_2(x)) < \deg(g(x))$. Por lo tanto,

$$r_2(x) = (x^n - 1) - s_2(x)g(x)$$

es un elemento de I (notar que $x^n - 1$ es el cero d $\mathbb{F}_q[x]/(x^n - 1)$). Esto implica que $r_2(x) = 0$ ya que $g(x)$ tiene el menor grado. Así, $g(x)$ es un divisor de $x^n - 1$.

□

Ejemplo 1.3.7. En el ejemplo 1.3.6 (1), el polinomio $1 + x + x^2$ es de menor grado, así este divide a $x^3 - 1$. En el ejemplo 1.3.6 (2), el polinomio $1 + x^2$ es de grado mínimo y este divide a $x^4 - 1$.

Teorema 1.3.30 ([26], Theorem 7.2.5)**.** *Existe un único polinomio mónico de grado mínimo en cada ideal I de $F_q[x]/(x^n - 1)$.*

Demostración. Sea $g_1(x)$ y $g_2(x)$ dos polinomios mónicos generadores de menor grado en el ideal I. Entonces, un múltiplo escala de $g_1(x) - q_2(x)$ es un polinomio mónico de

menor grado en I. Esto es una contradicción.

□

Definición 1.3.31. El único polinomio mónico de grado mínimo de un ideal no nulo I de $\mathbb{F}_q[x]/(x^n-1)$ es llamado el *polinomio generador* de I. Para un código cíclico $\mathscr{C}$, el polinomio generado de $\pi(\mathscr{C})$ es llamado también el *polinomio generador* de $\mathscr{C}$.

Ejemplo 1.3.8. El polinomio generador del código cíclico $\{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}$ es $1+x$.

Teorema 1.3.32 ([26], Theorem 72.8)**.** *Cada divisor mónico de x^n-1 es el polinomio generador de algún código cíclico en $\mathbb{F}_q^n$.*

Demostración. Sea $g(x)$ un divisor mónico de x^n-1 y sea I el ideal $\langle g(x)\rangle$ de $\mathbb{F}_q[x]/(x^n-1)$ generado por $g(x)$. Sea $\mathscr{C}$ el correspondiente código cíclico. Asumimos que $h(x)$ es el polinomio generador de $\mathscr{C}$. Entonces existe un polinomio $b(x)$ tal que

$$h(x) \equiv g(x)b(x) \pmod{x^n-1}.$$

Así, $g(x)$ es un divisor de $h(x)$. Por lo tanto, $g(x)$ es el mismo $h(x)$ ya que $h(x)$ tiene grado mínimo y es mónico.

□

De los teoremas 1.3.30 y 1.3.32, se obtiene el siguiente resultado.

Corolario 1.3.33. Existe una correspondencia uno a uno entre los códigos cíclicos en $\mathbb{F}_q^n$ y los divisores mónicos de $x^n-1 \in \mathbb{F}_q[x]$.

Observación 1.3.34. Los polinomios 1 y x^n-1 corresponden $\mathbb{F}_q^n$ y $\{\vec{0}\}$ respectivamente.

Ejemplo 1.3.9. Para encontrar todos los códigos cíclicos binarios de largo 6, factorizamos el polinomio $x^6-1 \in \mathbb{F}_2[x]$:

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

Todos los divisores mónicos de $x^6 - 1$:

$$\begin{array}{lll} 1, & 1+x, & 1+x+x^2 \\ (1+x)^2, & (1+x)(1+x+x^2), & (1+x)^2(1+x+x^2), \\ (1+x+x^2), & (1+x)(1+x+x^2)^2 & 1+x^6 \end{array}$$

Así, existen nueve códigos cíclicos de largo 6. Usando la mapa π (1.4), podemos escribir fácilmente todos los códigos cíclicos. Por ejemplo, el código cíclico correspondiente al polinomio $(1+x+x^2)^2$ es

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

.

Del ejemplo anterior, encontrar el número de códigos cíclicos de largo n puede ser determinado si se conoce el número de factorizaciones de $x^n - 1$. Para esto, se tiene el siguiente resultado.

Teorema 1.3.35 ([26], Theorem 7.2.12)**.** *Sea $x^n - 1 \in \mathbb{F}_q[x]$ dada la factorización*

$$x^n - 1 = \prod_{i=1}^{r} p_i^{e_i}(x),$$

donde $p_1(x), p_2(x), \ldots, p_r(x)$ son polinomios mónicos irreducibles distintos y $e_i \geq 1$ para todo $i = 1, 2, \ldots, r$. Entonces existen $\prod_{i=1}^{r}(e_i + 1)$ códigos cíclicos de largo n sobre $\mathbb{F}_q$.

Demostración. La demostración sigue del Corolario 1.3.33 al contar el número de todos los polinomios mónicos divisores de $x^n - 1$.

□

Dado un código cíclico $\mathscr{C}$, este está totalmente determinado por su polinomio generador $g(x)$, todos los parámetros de $\mathscr{C}$ también son determinados por el polinomio generador. El siguiente resultado entrega la dimensión del código en términos de su polinomio generador.

Teorema 1.3.36 ([26], Theorem 7.2.14)**.** *Sea $g(x)$ el polinomio generador de un ideal de $\mathbb{F}_q[x]/(x^n-1)$. Entonces el correspondiente código cíclico tiene dimensión k si el grado de $g(x)$ es $n-k$.*

Demostración. Para dos polinomios $c_1(x) \neq c_2(x)$ con $\deg(c_i) \leq k-1$ $(i=1,2)$, claramente $g(x)c_1(x) \not\equiv g(x)c_2(x) \pmod{x^n-1}$. Así, el conjunto

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

tiene q^k elementos y es un subconjunto de el ideal $\langle g(x)\rangle$. Por otra parte, para cualquier vector $g(x)a(x)$ con $a(x) \in \mathbb{F}_q[x]/(x^n-1)$, escribimos

$$a(x)g(x) = u(x)(x^n-1) + v(x) \tag{1.5}$$

con $\deg(v(x)) < n$. Por 1.5, tenemos que $v(x) = a(x)g(x) - u(x)(x^n-1)$. Así, $g(x)$ divide $v(x)$. Escribiendo $v(x) = g(x)b(x)$ para algún polinomio $b(x)$. Entonces $\deg(b(x)) < k$, por lo cual $v(x)$ está en A. Esto muestra que A es lo mismo que $\langle g(x)\rangle$. Por lo tanto, la dimensión de el código es $\log_q |A| = k$.

□

Ejemplo 1.3.10.

1. Basados en la factorización: $x^7-1 = (1+x)(1+x^2+x^3)(1+x+x^3) \in \mathbb{F}_2[x]$, conocemos que existen solo dos $[7,3]$-códigos cíclicos binarios :

$$\begin{aligned}\langle(1+x)(1+x^2+x^3)\rangle =& \{(0,0,0,0,0,0,0),(1,1,1,0,1,0,0),(0,1,1,1,0,1,0),\\ & (0,0,1,1,1,0,1),(1,0,0,1,1,1,0),(0,1,0,0,1,1,1),\\ & (1,0,1,0,0,1,1),(1,1,0,1,0,0,1)\}\\ \langle(1+x)(1+x+x^3)\rangle =& \{(0,0,0,0,0,0,0),(1,0,1,1,1,0,0),(0,1,0,1,1,1,0),\\ & (0,0,1,0,1,1,1),(1,0,0,1,0,1,1),(1,1,0,0,1,0,1),\\ & (1,1,1,0,0,1,0),(0,1,1,1,0,0,1)\}.\end{aligned}$$

2. Basados en la factorización: $x^7-1=(2+x)(1+x+x^2+x^3+x^4+x^5+x^6)\in\mathbb{F}_3[x]$, no existe ningún $[7,2]$-código cíclico.

Teorema 1.3.37 ([26], Theorem 7.3.1)**.** *Sea $g(x)=g_0+g_1x+\cdots+g_{n-k}x^{n-k}$ el polinomio generador de un código cíclicos $\mathscr{C}$ en $\mathbb{F}_q^n$ con $deg(g(x))=n-k$. Entonces la matriz*

$$G=\begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}=\begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & g_0 & g_1 & \cdots & \cdots & g_{n-k} \end{pmatrix}$$

es la matriz generadora de $\mathscr{C}$ (notar que se identifica un vector con un polinomio).

Demostración. Es suficiente mostrar que $g(x)$, $xg(x)$,..., $x^{k-1}g(x)$ forman una base de $\mathscr{C}$. Es claro que estas son linealmente independiente sobre $\mathbb{F}_q$. Por el Teorema 1.3.36, se tiene que la $\dim(\mathscr{C})=k$.

□

Ejemplo 1.3.11. Considerando el $[7,4]$-código cíclico binario con polinomio generador $g(x)=1+x^2+x^3$. Entonces este código tiene matriz generadora

$$G=\begin{pmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ x^3g(x) \end{pmatrix}=\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Esta matriz no está en forma estándar. Si la cuarta fila se suma a la segunda fila y la suma de estas dos es agregada a la primera fila, la matriz generadora en forma estándar:

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

Así, por el Teorema 1.3.18, podemos obtener la matriz de control de paridad.

Del ejemplo anterior, podemos observar que se puede obtener la matriz de control de paridad a partir de la matriz generadora mediante operaciones elementales de filas. Sin embargo, ya que el código dual de un código cíclico $\mathscr{C}$ también es cíclico, tenemos que ser capaces de encontrar una matriz de control de paridad del polinomio generador del código dual.

Definición 1.3.38. Sea $h(x) = \sum_{i=0}^{k} a_i x^i$ un polinomio de grado k ($a_k \neq 0$) sobre $\mathbb{F}_q$. El *polinomio reciproco* de $h(x)$ está dado por

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

Observación 1.3.39. Si $h(x)$ es un divisor de $x^n - 1$, entonces también lo es $h_R(x)$.

Ejemplo 1.3.12.

1. Para el polinomio $h(x) = 1 + 2x + 3x^5 + x^7 \in \mathbb{F}_5[x]$, el reciproco de $h(x)$ es

$$\begin{aligned} h_R(x) &= x^7 h(1/x) \\ &= x^7(1 + 2(1/x) + 3(1/x)^5 + (1/x)^7) \\ &= 1 + 3x^2 + 2x^6 + x^7. \end{aligned}$$

2. Considerando el divisor $h(x) = 1 + x + x^3 \in \mathbb{F}_2[x]$ de $x^7 - 1$. Entonces $h_R(x) = 1 + x^2 + x^3$ es también divisor de $x^7 - 1$.

Teorema 1.3.40 ([26], Theorem 7.3.7)**.** *Sea $g(x)$ el polinomio generador de $[n, k]$-código cíclico $\mathscr{C}$ sobre $\mathbb{F}_q$. Sea $h(x) = (x^n - 1)/g(x)$. Entonces $h_0^{-1} h_R(x)$ es el polinomio generador de $\mathscr{C}^\perp$, donde h_0 es el término constante de $h(x)$.*

Demostración. Sea $g(x) = \sum_{i=0}^{n-1} g_i x^i$ y sea $h(x) = \sum_{i=0}^{n-1} h_i x^i$. Entonces

$$h_R(x) = \frac{1}{x^{n-k-1}} \sum_{i=0}^{n-1} h_{n-i-1} x^i,$$

donde $k = \deg(h(x))$.

Considerando el producto

$$\begin{aligned} 0 &\equiv g(x)h(x) \\ &\equiv (g_o h_0 + g_1 h_{n-1} + \cdots + g_{n-1}h_1) + (g_0 h_1 + g_1 h_0 + \cdots g_{n-1}h_2)x + \\ &\quad + (g_0 h_2 + g_1 h_1 + \cdots + g_{n-1}h_3)x^2 + \cdots + (g_0 h_{n-1} + \\ &\quad + g_1 h_{n-2} + \cdots + g_{n-1}h_0)x^{n-1} (\text{mod } x^n - 1). \end{aligned}$$

Por lo tanto, el coeficiente de cada potencia de x en la última línea de la igualdad anterior debe ser cero. Al observar el coeficiente de cada potencia de x, obtenemos $\vec{g_i} \cdot (h_{n-1}, h_{n-2}, \cdots, h_1, h_0) = 0$, para todo $i = 0, 1, \ldots, n-1$, donde $\vec{g_i}$ es el vector obtenido de $(g_0, g_1, \ldots, g_{n-1})$ mediante desplazamiento cíclico de i posiciones. Por lo tanto, $(h_{n-1}, h_{n-2}, \ldots, h_1, h_0)$ es vector de $\mathscr{C}^{\perp}$ donde $\{\vec{g_0}, \vec{g_1}, \ldots, \vec{g_{n-1}}\}$ generan a $\mathscr{C}$ por el Teorema 1.3.37.

Mediante desplazamiento del vector $(h_{n-1}, h_{n-2}, \ldots, h_1, h_0)$ en $k+1$ posiciones, obtenemos el vector correspondiente a $h_R(x)$. Esto implica que $h_R(x)$ es un vector en $\mathscr{C}^{\perp}$ que también es código cíclico.

Como $\deg(h_R(x)) = \deg(h(x)) = k$, el conjunto $\{h_R(x), xh_R(x), \ldots, x^{n-k-1}h_R(x)\}$ es una base de $\mathscr{C}^{\perp}$. Por lo tanto, $\mathscr{C}^{\perp}$ es generado por $h_R(x)$. Así, el polinomio mónico $h^{-1}h_R(x)$ es el polinomio generador de $\mathscr{C}^{\perp}$.

□

Definición 1.3.41. Sea $\mathscr{C}$ un código cíclico en $\mathbb{F}_q$ de largo n con polinomio generador $g(x)$. Sea $h(x) = (x^n - 1)/g(x)$. Entonces, $h_0^{-1}h_R(x)$ es llamado el *polinomio control de paridad* de $\mathscr{C}$, donde h_0 es el término constante de $h(x)$.

Corolario 1.3.42. ([26], Corollary 7.3.9) Sea $\mathscr{C}$ un $[n, k]$-código cíclico en $\mathbb{F}_q$ con polinomio generador $g(x)$. Con $h(x) = (x^n - 1)/g(x)$. Sea $h(x) = h_0 + h_1 x + \cdots + h_k x^k$. Entonces la matriz

$$H = \begin{pmatrix} h_R(x) \\ xh_R(x) \\ \vdots \\ x^{n-k-1}h_R(x) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & h_k & h_{k-1} & \cdots & \cdots & h_0 \end{pmatrix}$$

es la matriz de control de paridad de $\mathscr{C}$.

Demostración. El resultado es inmediato de los teoremas 1.3.37 y 1.3.40.

□

Ejemplo 1.3.13. Sea $\mathscr{C}$ el $[7, 4]$-código cíclico binario generado por $g(x) = 1 + x^2 + x^3$ como en el ejemplo 1.3.11. Con $h(x) = (x^7 - 1)/g(x) = 1 + x^2 + x^3 + x^4$. Entonces $h_R(x) = 1 + x + x^2 + x^4$ es el polinomio control de paridad de $\mathscr{C}$. Entonces

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

es la matriz de control de paridad de $\mathscr{C}$.

Los códigos pseudo-cíclicos o semi-cíclicos fueron introducidos por Elwyn Berlekamp [3] usando el nombre de códigos consta-cíclicos (*constacyclic codes*).

Definición 1.3.43. Sea α un elemento distinto de cero en $\mathbb{F}_q$. Un código lineal $\mathscr{C} \subseteq \mathbb{F}_q^n$ es llamado *código α-cíclico* si es invariante bajo la transformación lineal

$$\phi_\alpha : (c_0, c_1 \ldots, c_{n-1}) \mapsto (\alpha c_{n-1}, c_0, \ldots, c_{n-2}).$$

Un código es llamado *pseudo-cíclico* si $\mathscr{C}$ es α-cíclico para algún $\alpha \in \mathbb{F}_q^*$, $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

Observación 1.3.44. Decir que un código lineal $\mathscr{C}$ es invariante bajo ϕ_α es equivalente

a decir que $\mathscr{C}$ es invariante bajo la acción de la matriz de permutación

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

es decir, $\mathscr{C} = \{\vec{c}P \colon \vec{c} \in \mathscr{C}\}$.

Observación 1.3.45. Un código 1-cíclico es simplemente un código cílcico.

Teorema 1.3.46 ([29], Theorem 1)**.** *Si $\mathscr{C} \subseteq \mathbb{F}_q^n$ es un código α-cíclico entonces el código dual $\mathscr{C}^\perp \subseteq \mathbb{F}_q^n$ es un código α^{-1}-cíclico.*

Demostración. Si $\vec{h} = (h_1, \ldots, h_n) \in \mathscr{C}^\perp$ entonces $\vec{h} \cdot \vec{c} = 0$ para todo $\vec{c} = (c_1, \ldots, c_n) \in \mathscr{C}$. Así tenemos

$$\begin{aligned} \phi_{\alpha^{-1}}(\vec{h}) \cdot \vec{c} &= (\alpha^{-1}h_n, h_1, \ldots, h_{n-2}) \cdot (c_1, c_2 \ldots, c_n) \\ &= \alpha^{-1}h_n c_1 + h_1 c_2 + \cdots + h_{n-2}c_n \\ &= \vec{h} \cdot \alpha^{-1}(\alpha c_2, \alpha c_3, \ldots, \alpha c_n, c_1) \\ &= \vec{h} \cdot \alpha^{-1}\phi_\alpha^{n-1}(\vec{c}) \\ &= 0, \end{aligned}$$

como $\mathscr{C}$ es un código α-cíclico, $\alpha^{-1}\phi_\alpha^{n-1}(\vec{c}) \in \mathscr{C}$, donde $\phi_\alpha^k = \underbrace{\phi_\alpha \circ \cdots \circ \phi_\alpha}_{k\text{-veces}}$, para todo $k \in \mathbb{N}$. Luego, $\mathscr{C}^\perp$ es un código α^{-1}-cíclico.

□

Con el fin de convertir la estructura de códigos cíclicos en una estructura algebraica,

consideramos la siguiente correspondencia:

$$\begin{aligned} \pi: \quad \mathbb{F}_q^n \quad &\longrightarrow \quad \mathbb{F}_q[x]/(x^n-\alpha) \\ (a_0, a_1, \ldots, a_{n-1}) &\longmapsto a_0 + a_1 x + \cdots a_{n-1}x^{n-1} \end{aligned} \tag{1.6}$$

Observamos que π es un $\mathbb{F}_q$-isomorfismo lineal de espacios vectoriales sobre $\mathbb{F}_q$. Así, podemos identificar $\mathbb{F}_q^n$ con $\mathbb{F}_q[x]/(x^n-\alpha)$ y un vector $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$ con el polinomio $\pi(\vec{a}) = \sum_{i=0}^{n-1} a_i x^i$. Ya que $\mathbb{F}_q[x]/(x^n-\alpha)$ es un anillo, tenemos la operación multiplicación en $\mathbb{F}_q[x]/(x^n-\alpha)$ además de la adición heredada de $\mathbb{F}_q^n$.

Teorema 1.3.47 ([28], Chapter 7. §2)**.** *Sea π definida en (1.6). Luego un subconjunto no vacío $\mathscr{C}$ de $\mathbb{F}_q^n$ es un código pseudo-cíclico si y sólo si $\pi(\mathscr{C})$ es un ideal de $\mathbb{F}_q[x]/(x^n-\alpha)$, para algún $\alpha \in \mathbb{F}_q^*$.*

Demostración. Supongamos que $\pi(\mathscr{C})$ es un ideal de $\mathbb{F}_q[x]/(x^n-\alpha)$. Luego, para cualquier $\beta, \gamma \in \mathbb{F}_q^n$ y $\vec{b}, \vec{c} \in \mathscr{C}$, se tiene que $\beta\pi(\vec{b}), \gamma\pi(\vec{c}) \in \pi(\mathscr{C})$. Así $\pi(\beta\vec{b} + \gamma\vec{a}+) = \beta\pi(\vec{b}) + \gamma\pi(\vec{c}) \in \pi(\mathscr{C})$, es decir, $\beta\vec{b} + \gamma\vec{c} \in \mathscr{C}$. Esto muestra que $\mathscr{C}$ es un código lineal.

Ahora sea $\vec{c} = (c_0, \ldots, c_{n-1}) \in \mathscr{C}$ y $\pi(\vec{c}) = c_0 + c_1 x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1} \in \pi(\mathscr{C})$. Como $\pi(\mathscr{C})$ es un ideal, el polinomio

$$\begin{aligned} x \cdot \pi(\vec{c}) &= c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n \\ &= \alpha c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} \in \pi(\mathscr{C}) \end{aligned}$$

ya que $x^n - \alpha = 0$ en $\mathbb{F}_q[x]/(x^n-\alpha)$, así, $(\alpha c_{n-1}, c_0, \ldots, c_{n-2}) \in \mathscr{C}$.

Por otro lado, supongamos que $\mathscr{C} \subseteq \mathbb{F}_q^n$ es un código α-cíclico, para algún $\alpha \in \mathbb{F}_q^*$. Para cualquier polinomio

$$f(x) = f_0 + f_1 x + \cdots + f_{n-2}x^{n-2} + f_{n-1}x^{n-1} = \pi(f_0, f_1, \ldots, f_{n-2}, f_{n-1})$$

de $\pi(\mathscr{C})$ con $(f_0, f_1, \ldots, f_{n-2}, f_{n-1}) \in \mathscr{C}$, el polinomio

$$x \cdot f(x) = \alpha f_{n-1} + f_0 x + f_1 x^2 + \cdots + f_{n-2}x^{n-1}$$

es también un elemento de $\pi(\mathscr{C})$ ya que $\mathscr{C}$ es α-cíclico. Así $x^2 \cdot f(x) = x(x \cdot f(x)) \in \pi(\mathscr{C})$ y por inducción podemos ver que $x^i \cdot f(x) \in \pi(\mathscr{C})$ para todo entero $i \geq 0$. Como $\mathscr{C}$ es un código lineal y π es una transformación lineal, $\pi(\mathscr{C}) \subseteq \mathbb{F}_q[x]/(x^n - \alpha)$ es un grupo con respecto a la suma y para cualquier $g(x) = g_0 + g_1 x + \cdots + g_{n-1}x^{n-1} \in \mathbb{F}_q[x]/(x^n - \alpha)$ el polinomio

$$g(x) \cdot f(x) = \sum_{i=o}^{n-1} g_i(x^i f(x))$$

es un elemento de $\pi(\mathscr{C})$. Por lo tanto, $\pi(\mathscr{C})$ es un ideal de $\mathbb{F}_q[x]/(x^n - \alpha)$.

□

Teorema 1.3.48 ([29], Theorem 1)**.** *Sea $\mathscr{C}$ un ideal no nulo de $\mathbb{F}_q[x]/(x^n - \alpha)$, esto es, un código α-cíclico de largo n. Entonces existe un único polinomio de grado mínimo en $\mathscr{C}$, que satisface:*

(a) $\mathscr{C} = \langle g(x) \rangle$, es decir, $g(x)$ es el polinomio generador de $\mathscr{C}$.

(b) $g(x)$ es un factor de $x^n - \alpha$.

(c) Cualquier $c(x) \in \mathscr{C}$ puede escribirse de manera única como $c(x) = f(x)g(x)$ en $\mathbb{F}_q[x]$, donde $f(x) \in \mathbb{F}_q[x]$ tiene grado menor que $n - k$, $k = \deg g(x)$. La dimensión de $\mathscr{C}$ es $n - k$.

(d) Si $g(x) = \sum_{i=0}^{k} g_i x^i$, entonces $\mathscr{C}$ tiene la siguiente matriz generadora

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_k & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_k & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & g_0 & g_1 & \cdots & \cdots & g_k \end{pmatrix}.$$

(e) El código dual de $\mathscr{C}$ es un código α^{-1}-cíclico.

Ejemplo 1.3.14 (Programa 1)**.** Con $\mathbb{F}_4[x]$ con $\mathbb{F}_4 = \mathbb{F}_2(w)$, donde $w^2 + w + 1 = 0$.

Como $w^4 = w$, el polinomio $x^4 - w$, se puede escribir como

$$\begin{aligned} x^4 - w &= x^4 - w^4 \\ &= (x-w)^4 \\ &= (x-w)^2(x-w)^2 = (x^2-w^2)(x^2-w^2) \\ &= (x-w)(x-w)^3 = (x-w)(x^3+wx^2+w^2x+1) \end{aligned}$$

Donde la segunda igualdad viene del Teorema 1.1.9. Tomando $g(x) = (x-w)$, este genera un código w-cíclico de largo 4, dimensión 3 y distancia 2, cuya matriz generadora H está dada por

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

Teorema 1.3.49 ([29], Theorem 2)**.** *Sea $\mathscr{C}$ un $[n, n-k]$-código sobre $\mathbb{F}_q$. Entonces $\mathscr{C}$ es α-cíclico si y sólo si $\mathscr{C}$ tiene matriz de control de paridad de la forma*

$$[P_t, (PT)_t, (PT^2)_t, \ldots, (PT^{n-1})_t],$$

con $P \in \mathbb{F}_q^k$ y $T \in GL(k,q)$ tal que $PT^n = \alpha P$, donde S_t es la transpuesta de S.

Teorema 1.3.50 ([29], Theorem 3; [30], Theorem B)**.** *Sea $g(x)$ un polinomio de grado k en $\mathbb{F}_q[x]$ que divide a $x^n - \alpha$, $\alpha \in \mathbb{F}_q^*$. Entonces C es un $[n, n-k]$-código α-cíclico sobre $\mathbb{F}_q$ con polinomio generador $g(x)$ si y sólo si $\mathscr{C}$ es un código con matriz de control de paridad $[P_t, (PT)_t, (PT^2)_t, \ldots, (PT^{n-1})_t]$, donde $P = (1, 0, \ldots, 0)$ y T es la matriz*

compañera de $g(x)$*, es decir,*

$$T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix}$$

si $g(x) = \sum_{i=0}^{k} a_i x^i$ *con* $a_k = 1$.

Observación 1.3.51. Un código $\mathscr{C}$ con matriz de control de paridad de la forma

$$[P_t, (PT)_t, (PT^2)_t, \ldots, (PT^{n-1})_t],$$

con $P \in \mathbb{F}_q^k$ y $T \in GL(k,q)$ se dice *definido por* (T, P, n). Se define el conjunto

$$\Gamma_k^\alpha := \{(T,P,n) \in GL(k,q) \times \mathbb{F}_q^k \times \mathbb{Z} \mid (T,P,n) \text{ define un } (n, n-k)\text{-código } \alpha\text{-cíclico}\}.$$

Teorema 1.3.52 ([29], Theorem 4)**.** *Sea* $(T_i, P_i, n) \in \Gamma_k^\alpha$*, y sea* $\mathscr{C}$ *el código definido por* (T_i, P_i, n) $(i = 1, 2)$*. Entonces las siguientes proposiciones son equivalentes:*

(*i*) $\mathscr{C}_1 = \mathscr{C}_2$,

(*ii*) T_1 *y* T_2 *son equivalentes,*

(*iii*) $\varphi_{T_1} = \varphi_{T_2}$*, donde* φ_T *es el polinomio característico de* T*. En particular,* (T, P, n) *y* (T, Q, n) *define el mismo código si ellos están en* Γ_k^α.

Demostración.

(*i*) $\Rightarrow$ (*ii*): Como $\mathscr{C}_1 = \mathscr{C}_2$, existe $S \in GL(k,q)$ con $S_t G^{(n)}_{T_1,P_1} = G^{(n)}_{T_2,P_2}$, donde $G^{(n)}_{T_i,P_i}$ es la matriz de control de paridad definida por (T_i, P_i, n), es decir,

$$S_t[(P_1)_t, (P_1T_1)_t, (P_1T_1^2)_t, \ldots, (P_1T_1^{n-1})_t] = [(P_1S)_t, (P_1T_1S)_t, (P_1T_1^2S)_t, \ldots, (P_1T_1^{n-1}S)_t]$$
$$= [(P_2)_t, (P_2T_2)_t, (P_2T_2^2)_t, \ldots, (P_2T_2^{n-1})_t]$$

Como $\mathscr{C}_1$ y $\mathscr{C}_2$ tienen la misma dimensión y $P_2T_2^i = P_1T_1^iS = P_2(S^{-1}T_1S)^i$, $i = 1, \ldots, n$, tenemos que $S^{-1}T_1S = T_2$.

$(ii) \Rightarrow (iii)$: Como T_1 y T_2 son equivalentes, estas tienen el mismo polinomio característico, es decir, $\varphi_{T_1} = \varphi_{T_2}$.

$(iii) \Rightarrow (i)$: se obtiene fácilmente de parte de "$(i) \Rightarrow (ii)$" y el Teorema 1.3.50.

□

Corolario 1.3.53 ([29], Corollary 5)**.** Sea $\mathscr{C}$ un $[n, n-k]$-código α-cíclico con polinomio generador $g(x) = \sum_{i=0}^{k} a_i x^i$. Si $q = p^h$, $r|p^h$ y $(n, p) = 1$, entonces $\mathscr{C}$ y $\overline{\mathscr{C}}$ son equivalentes, donde $\overline{\mathscr{C}}$ es el código α^r-cíclico generado por $g_r(x) = \sum_{i=0}^{k} a_i^r x^i$.

Demostración. Notamos que $g(x) = \prod_i (x - \lambda_i)$ implica que $g_r(x) = \prod_i (x - \lambda_i^r)$. Como $\mathscr{C}$ es un código α-cíclico, existe $(T, P, n) \in \Gamma_k^{\alpha}$ que define $\mathscr{C}$.

Por $r|p^h$ y $(n, p) = 1$, (T^r, P, n) está en $\Gamma_k^{\alpha^r}$, y este define un código equivalente a $\mathscr{C}$. Se tiene de $g(x) = \varphi_T$ que $g_r(x) = \varphi_{T^r}$ y del Teorema 1.3.52 que $\mathscr{C}$ y $\overline{\mathscr{C}}$ son equivalentes.

□

Existe una correspondencia uno a uno entre las todas clases de equivalencia de (n, k)-códigos MDS sobre $\mathbb{F}_q$ y todas las clases de n-arcos en $\mathbb{P}^{k-1}(\mathbb{F}_q)$ (Corolario 1.4.2). A un (n, k)-código sobre $\mathbb{F}_q$, lo llamaremos *código Reed-Solomon generalizado* (*código GRS*) si este corresponde a la clase de un n-arco en $\mathbb{P}^{k-1}(\mathbb{F}_q)$, cada uno de los cuales está contenido en una curva racional normal. En particular, un código GRS de largo $q+1$ sobre $\mathbb{F}_q$ es llamado *código racional normal* (*código NR*); este está en correspondencia de la clase de curvas racional normal.

Teorema 1.3.54 ([29], Theorem 6)**.** *Existe un (n, k)-código MDS pseudo-cíclico sobre $\mathbb{F}_q$ con $(n, q) \neq 1$, $2 \leq k \leq n-2$, si y sólo si $n = p$, donde $q = p^h$, con p primo. Más aún, un (p, k)-código pseudo-cíclico sobre $\mathbb{F}_q$ es GRS.*

Demostración.

"$\Rightarrow$"

Por reducción al absurdo, supongamos que $n \neq p$, pero como $(n, q) \neq 1$, se tiene que $n = \lambda \cdot \mu$, con μ la mayor potencia de p que divide a n. Estudiaremos por separado, cuando $n = q$, y donde h debe ser mayor que 0, y cuando $n \neq q$.

Caso 1: $n = q$, $h > 1$. Sea $\mathscr{C}$ un $[q, k]$-código α-cíclico con polinomio generador $g(x)$. Por el Teorema 1.3.48, $g(x)$ es un factor de $x^n - \alpha$ y de grado $n-k$. Además, como $n = q$ por el Teorema 1.1.9, podemos escribir $(x^n - \alpha) = (x - \alpha)^n = (x - \alpha)^{p^h}$, así $g(x) = (x - \alpha)^r$, $r = q - k$.

Si $r \leq p^{h-1}$, entonces $(x - \alpha)^{p^{h-1}} = x^{p^{h-1}} - \alpha^{p^{h-1}}$ debe estar en $\mathscr{C}$. Para que $\mathscr{C}$ sea MDS, su distancia debe ser $d = n - k + 1$, y de la hipótesis sabemos que $k \leq n - 2$, o sea $d \geq 3$, y por lo tanto $\mathscr{C}$ no puede ser MDS ya que $g(x)$ está en el código.

Si $p^{h-1} < r < p^h - 1$ y $\mathscr{C}$ es MDS, entonces todos los coeficientes de $g(x)$ deben ser distintos de cero, o si no, $g(x)$ tendría $n - k$ o menos términos. De esto sigue que $r = sp^{h-1} - 1$, para algún s, $2 \leq s \leq p$. Entonces $f(x) = (x - \alpha)^{r+1} = (x^{p^{h-1}} - \alpha^{p^{h-1}})^s \neq 0 \in \mathscr{C}$. Como la distancia mínima d de $\mathscr{C}$ es $d = n - k + 1 = d = r + 1 = sp^{h-1} \geq s + 1 \geq w(f)$, lo cual es una contradicción.

Caso 2: $n \neq q$. Sea $\mathscr{C} = \langle g(x) \rangle$ con $g(x) \mid x^n - \alpha$. Debemos mostrar la existencia de $f(x)$ $(\neq 0 \in \mathbb{F}_q[x]/(x^n - \alpha))$ en $\mathscr{C}$ con peso $w(f)$ menor que $n - k + 1$, para esto, usaremos un argumento similar a la demostración del Teorema de Zehendner [45]. Tomando $\lambda = n/\mu$ donde μ es la potencia más grande de q que divide a n, por el por el Teorema 1.1.9, podemos escribir $x^n - \alpha = x^{\lambda\mu} - \alpha = (x^\lambda - \alpha)^\mu$. Luego, $x^\lambda - \alpha$ lo podemos factorizar en el campo de descomposición sobre $\mathbb{F}_q$, por el Teorema 1.1.39. Si ξ representa una raíz primitiva λ-ésima de α, tenemos

$$x^\lambda - \alpha = \prod_{i=1}^{\lambda} (x - \xi^i).$$

Así

$$g(x) = \prod_{i=1}^{\lambda} (x - \xi^i)^{t_i}$$

con un entero adecuado $t_i \geq 0$. El polinomio $g(x)$ tiene grado $n-k$, por lo cual $\sum_{i=1}^{\lambda} t_i = n-k$. Sea t el máximo valor de los t_i. Como $g(x)$ es un factor de $x^n - \alpha$, podemos concluir que $0 < t \leq n-k$ y $t \leq \mu$.

Supongamos $t < n-k$ y $t < \mu$. Podemos elegir $f(x) = (x^\lambda - \alpha)^t$. Entonces tenemos que $\deg(f(x)) = \lambda t < \lambda\mu = n$, luego $f(x)$ es un polinomio distinto de cero y tiene a lo más $t+1 < n-k+1$ términos distintos de cero. Por el Teorema 1.3.48(c), $f(x) \in \mathscr{C}$, y este no puede ser MDS.

Supongamos $t = n-k$. Entonces $g(x) = (x - \xi^i)^{n-k}$ para un cierto entero i. Si $n-k \not\equiv -1 (\text{mod } p)$ y $p \leq n-k$, usamos $m = n-k-p\left[\frac{(n-k)}{p}\right]$, así $0 < m < n-k$. Considerando el desarrollo binomial de $g(x)$ tenemos,

$$\begin{aligned} g(x) &= (x - \xi^i)^{n-k} \\ &= \sum_{j=0}^{n-k} \binom{n-k}{j} x^{n-k-j} (-\xi^i)^j \\ &= x^{n-k} + (n-k)x^2(-\xi^i) + \cdots + \binom{n-k}{m+1} x^{n-k-m-1}(-\xi^i)^{m+1} + \cdots + (-\xi^i)^{n-k}. \end{aligned}$$

Analizando el término $\binom{n-k}{m+1}$ tenemos,

$$\binom{n-k}{m+1} = \frac{(n-k)!}{(m+1)!(n-k-m-1)!},$$

multiplicando esta igualdad por $(n-k+1)$,

$$\begin{aligned}(n-k+1)\binom{n-k}{m+1} &= \frac{(n-k+1)!}{(m+1)!(n-k-m-1)!} \\ &= \frac{(n-k+1)!}{(m+1)!(n-k-m)(n-k-m-1)!}(n-k-m) \\ &= \frac{(n-k+1)!}{(m+1)!(n-k-m)!}(n-k-m) \\ &= \binom{n-k+1}{m+1}(n-k-m).\end{aligned}$$

De $m = n-k-p\left[\frac{(n-k)}{p}\right]$, tenemos que $n-k-m = p\cdot c$ con $c \in \mathbb{N}$. Además, como $n-k \not\equiv -1(\text{mod } p)$, p no divide a $(n-k+1)$ y como p es primo, p debe dividir a $\binom{n-k}{m+1}$.

Como p divide a $\binom{n-k}{m+1}$, $g(x)$ tiene a lo más $n-k$ términos, por lo cual $\mathscr{C}$ no puede ser MDS. Ahora si $n-k \equiv -1(\text{mod } p)$, de la expansión binomial de $g(x)$, podemos observar del término $(n-k)x(-\xi^i)$, que $\xi^i \in \mathbb{F}_q$. Luego podemos tomar $f(x) = (x-\xi^i)^{n-k+1}$, y por el Teorema 1.3.48(c), $f(x) \in \mathscr{C}$. Tomando $m = (n-k+1)/p$, se tiene

$$\begin{aligned}f(x) &= (x-\xi^i)^{n-k+1} \\ &= (x-\xi^i)^{mp} \\ &= (x^p-\xi^{ip})^m.\end{aligned}$$

Tenemos que $\deg(f(x)) < n$ y además el peso $w(f)$ es a lo más $m+1 < n-k+1$, luego $\mathscr{C}$ no puede ser MDS.

Si $p > n-k$, entonces de la expansión binomial de $g(x)$ se tiene nuevamente que $\xi^i \in \mathbb{F}_q$. Como n es diferente de p, podemos tomar el polinomio distinto de cero en $\mathscr{C}$, $f(x) = (x-\xi^i)^p = x^p - \xi^{ip}$. Por lo cual $\mathscr{C}$ no es MDS.

Supongamos $t = \mu < n-k$. El $[n, n-k]$-código cíclico con polinomio generador $r(x) = (x^n-\alpha)/g(x)$ es MDS si y sólo si $\mathscr{C}$ es MDS. Sea u la máxima multiplicidad

de las raíces de $r(x)$. Usando el mismo argumento de $g(x)$ pero aplicado a $r(x)$, entonces podemos asumir que $u = \mu$. Así, no todas las raíces de $x^\lambda - \alpha$ son raíces de $g(x)$. Sea W el conjunto de todas las raíces de $g(x)$. Si ξ^i es una raíz de $g(x)$, entonces por el Teorema 1.1.23 cada raíz del polinomio minimal correspondiente $M^{(i)}(x)$ es también una raíz de $g(x)$, y así el polinomio

$$s(x) = \prod_{\xi^i \in W} (x - \xi^i)$$

corresponde al producto de polinomios minimales con coeficientes en $\mathbb{F}_q$, luego $s(x)$ tiene coeficientes en $\mathbb{F}_q$. De esto, tenemos que $g(x)$ tiene al menos una raíz múltiple y como este tiene grado $n - k$, tenemos que el grado del polinomio $s(x)$ es menor que $n - k$. Considerando ahora $f(x)$ como

$$\begin{aligned} f(x) &= [s(x)]^\mu \\ &= \left[\prod_{\xi^i \in W} (x - \xi^i) \right]^\mu, \end{aligned}$$

se tiene que $g(x)$ es un factor de $f(x)$, y así, $f(x) \in \mathscr{C}$. El grado de $f(x)$ es menor que n y como μ es una potencia de p se tiene que

$$\begin{aligned} wt(f(x)) &\leq wt(s(x)) \\ &\leq 1 + \deg(s(x)) \\ &< n - k + 1. \end{aligned}$$

Es decir, $\mathscr{C}$ no es MDS.

"$\Leftarrow$"

Supongamos ahora que $n = p$. Sea $\overline{\alpha}^p = \alpha$ y $\mathscr{C} = \langle g(x) \rangle$ con $g(x) = (x - \overline{\alpha}^p)^{p-k}$. Sea

$$f_i(x) = \sum_{j=0}^{p-1} j^i \overline{\alpha}^{p-1-j} x^j, \quad 0 \leq i \leq k-1,$$

y definimos $0^0 \equiv 1$ (Lema 2.2.2). Se tiene que $p-i-1 \geq p-k$, así $g(x)$ divide a $(x-\overline{\alpha})^{p-i-1}$. Luego $(x-\overline{\alpha})^{p-i-1}$ divide a $f_i(x)$, por lo cual, $f_i(x)$ está en $\mathscr{C}$, $0 \leq i \leq k-1$. Sea G la matriz formada por todos los coeficientes de f_i, $0 \leq i \leq k-1$. Entonces

$$G = \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_{k-2} \\ f_{k-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & p-1 \\ 0 & 1^2 & 2^2 & \cdots & (p-1)^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1^{k-2} & 2^{k-2} & \cdots & (p-1)^{k-2} \\ 0 & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{pmatrix} \cdot \begin{pmatrix} \overline{\alpha}^{p-1} & 0 & 0 & \cdots & 0 & 0 \\ 0 & \overline{\alpha}^{p-2} & 0 & \cdots & 0 & 0 \\ 0 & 0 & \overline{\alpha}^{p-3} & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \overline{\alpha} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

es decir, G se puede escribir como una matriz cuyas columnas forman un curva racional normal (definición 1.2.11) y que en el espacio proyectivo no se ve afectada al multiplicarse por la matriz diagonal.

Como cada f_i, $0 \leq i \leq k-1$, está en $\mathscr{C}$ y G está formada por k filas linealmente independientes, G es la matriz generadora de C y así $\mathscr{C}$ es un código NR, o sea, es un código MDS.

□

Ejemplo 1.3.15 (Programa 3)**.** Con $\mathbb{F}_{25}$, en el software Magma se puede verificar para $n \leq 100$, que un (n,k)-código MDS pseudo-cíclico con $(n,q) \neq 1$, $2 \leq k \leq n-2$, sólo existe para $n = 5$. Por ejemplo, el polinomio $g(x) = x^2 + 2x + 1$ genera un $(5,3)$-código MDS 4-cíclico.

Teorema 1.3.55 ([29], Theorem 7)**.** *Para cualquier k, $1 \leq k \leq q$, existe un $[q+1,k]$-código MDS pseudo-cíclico sobre $\mathbb{F}_q$.*

Para un (n,k)-código α^{-1}-cíclico $\mathscr{C}$, $\alpha \in \mathbb{F}_q^*$, el polinomio generador $g(x)$ del código dual $\mathscr{C}^\perp$ es llamado el *polinomio control* de $\mathscr{C}$. Por el Teorema 1.3.50, $\mathscr{C}$ tiene una matriz generadora de la forma $[P_t, (PT)_t, (PT^2)_t, \ldots, (PT^{n-1})_t]$, donde $P = (1,0,\ldots,0)$

y T es la matriz compañera de $g(x)$. Por otra parte, $g(x)$ puede escribirse como

$$g(x) = \prod_{i=1}^{k}(x - \eta_i),\ \eta_1, \ldots, \eta_k \in K,$$

para alguna extensión K del campo $\mathbb{F}_q$. Luego $g(\eta_i) = 0$, para cada η_i, es decir,

$$g_0 + g_1\eta_i + g_2\eta_i^2 + \cdots + g_k\eta_i^k = 0,$$

con $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_kx^k$ y $\eta_i^n = \alpha$, ya que $g(x)$ divide a $x^n - \alpha$. Como $\mathscr{C}^\perp$ corresponde al ideal de $\mathbb{F}_q[x]/(x^n - \alpha)$ generado por $g(x)$, tenemos que

$$\begin{pmatrix} g_0 & g_1 & \cdots & g_k & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_k & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & g_0 & g_1 & \cdots & \cdots & g_k \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \eta_1 & \eta_2 & \cdots & \eta_k \\ \eta_1^2 & \eta_2^2 & \cdots & \eta_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ \eta_1^{n-1} & \eta_2^{n-1} & \cdots & \eta_k^{n-1} \end{pmatrix} = O.$$

Así, $\mathscr{C}^\perp$ tiene matriz de control de paridad de la forma

$$\begin{pmatrix} 1 & \eta_1 & \eta_1^2 & \cdots & \eta_1^{n-1} \\ 1 & \eta_2 & \eta_2^2 & \cdots & \eta_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \eta_k & \eta_k^2 & \cdots & \eta_1^{n-1} \end{pmatrix}, \text{ con } \eta_i^n = \alpha \text{ para todo } i.$$

Claramente, el $\mathbb{F}_{q^r}$-span de un código α-cíclico sobre $\mathbb{F}_q$ es un código α-cíclico sobre $\mathbb{F}_{q^r}$. Además se tiene que cada submatriz cuadrada de tamaño k de una matriz generadora G de un (n, k)-código MDS es no singular y que cada submatriz cuadrada de G' es no singular cuando $G = [I_k|G']$ (Teorema 1.3.24). Entonces el $\mathbb{F}_{q^r}$-span de un código MDS sobre $\mathbb{F}_q$ es un código MDS sobre $\mathbb{F}_{q^r}$.

Si $\mathscr{C}$ es un $[n, k]$-código pseudo-cíclico con polinomio control $g(x)$. Luego si asumimos

que $g(x) = \prod_{i=1}^{k}(n - \eta_i)$, $\eta_i \in K$, donde K es alguna extensión del campo $\mathbb{F}_q$. Entonces $\mathscr{C}$ es MDS si

$$\det \begin{pmatrix} \eta_1^{i_1} & \eta_1^{i_2} & \cdots & \eta_1^{i_k} \\ \eta_2^{i_1} & \eta_2^{i_2} & \cdots & \eta_2^{i_k} \\ \vdots & \vdots & \ddots & \vdots \\ \eta_k^{i_1} & \eta_k^{i_2} & \cdots & \eta_k^{i_k} \end{pmatrix} \neq 0 \qquad \text{para cualquier } i_1, \ldots, i_k \text{ distintos, con } 1 \leq i_j \leq n.$$

El recíproco es verdadero si $g(x)$ es irreducible sobre $\mathbb{F}_q$.

Teorema 1.3.56 ([30], Theorem 2.10)**.** *Sea $\mathscr{C}$ un $[n,k]$-código pseudo-cíclico y sea $g(x)$ el polinomio generador del código dual $\mathscr{C}$. Si $g(x)$ es irreducible sobre $\mathbb{F}_q$, es decir, $g(x) = \prod_{i=1}^{k}(x - \eta^{q^i})$ para algún $\eta \in K = \mathbb{F}_{q^k}$. Entonces $\mathscr{C}$ es MDS si y sólo si $det(\eta^{i_j q^l})_{1\leq j,l\leq k} \neq 0$ para cualquier $i_1, \ldots, i_k$ distintos con $1 \leq i_j \leq n$.*

Definición 1.3.57. Sea α un elemento distinto de cero de $\mathbb{F}_q$ y sea $R = \mathbb{F}_q[x]/(x^N - \alpha)$ el anillo de polinomios sobre $\mathbb{F}_q$ módulo $x^N - \alpha$. Para $\boldsymbol{g} = (g_1(x), g_2(x), \ldots, g_m(x)) \in R^m$,

$$\mathscr{C}_{\boldsymbol{g}} = \{(r(x)g_1(x), r(x)g_2(x), \ldots, r(x)g_m(x)) \mid r(x) \in R\} \subseteq \mathbb{F}_q^{mN},$$

es llamado el *código Quasi-Twisted (QT) 1-generador*. Si $\alpha = 1$ es llamado *código Quasi-Cíclico (QC)* con generador $\boldsymbol{g}$.

Observación 1.3.58. De la definición anterior, cuando $m = 1$, $\mathscr{C} = \mathscr{C}_{\boldsymbol{g}}$ corresponde a un código α-cíclico.

Del Teorema 1.3.50 un $[n, n-k]$-código sobre $\mathbb{F}_q$, es α-cíclico con polinomio generador $g(x)$ si y sólo si $\mathscr{C}$ es un código con matriz de control de paridad $[g^n] := [P_t, (PT)_t, (PT^2)_t, \ldots, (PT^{n-1})_t]$, donde $P = (1, 0, \ldots, 0)$ y T es la matriz compañera

de $g(x)$, es decir,

$$T = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix}$$

si $g(x) = \sum_{i=0}^{k} a_i x^i$ con $a_k = 1$. Ahora, sea $\mathcal{T}$ la proyectividad de $\mathbb{P}^{k-1}(\mathbb{F}_q)$ definida por T. Podemos decir que $\mathcal{T}$ es la proyectividad definida por $g(x)$. Entonces las columnas de $[g^n]$ pueden ser consideradas como una órbita de $\mathcal{T}$. Recíprocamente, podemos obtener un código pseudo-cíclico desde una órbita de una proyectividad de $\mathbb{P}^{k-1}(\mathbb{F}_q)$.

Ahora, tomando m órbitas $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m$ de $\mathcal{T}$ con largo N, y seleccionar un punto P_i de cada $\mathcal{O}_i$. Luego, por simplicidad, podemos tomar P_1 como $P = (1, 0, \ldots, 0)$. Podemos denotar la matriz

$$[P_t, (PT)_t, \ldots, (PT^{n_1-1})_t;\ (P_2)_t, (P_2T)_t, \cdots,$$
$$\cdots, (P_2T^{n_2-1})_t;\ \cdots;(P_m)_t, (P_mT)_t, \ldots, (P_mT^{n_m-1})_t]$$

por $[g^{n_1}] + P_2^{n_2} + \cdots + P_m^{n_m}$. Entonces, la matriz $[g^N] + P_2^N + \cdots + P_m^N$ definida por m órbitas $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m$ de τ generan un código QT.

Teorema 1.3.59 ([31], Theorem 2.3)**.** *$[g^N] + P_2^N + \cdots + P_m^N$ genera un $[mN, k]$-código Quasi-Twisted (QT) 1-generador con generador*

$$\boldsymbol{g} = \left(h^*(x), b_2(x^{-1})h^*(x), \ldots, b_m(x^{-1})h^*(x)\right),$$

donde $h^*(x) = h_0^{-1}x^{N-k}h(x^{-1})$, $h(x) = \sum_{j=0}^{N-k} h_j x^j = (x^N - \alpha)/g(x)$, $b_i(x) = (1, x, \ldots, x^{k-1})P_i$ $(2 \leq i \leq m)$.

1.4. De la Geometría a los Códigos Lineales

Hemos introducido la geometría proyectiva sobre campos finitos y hemos visto los códigos lineales sobre campos finitos. Como estas dos teorías están relacionadas por el campo finito en cual se trabaja, se espera que exista una conexión entre ellas. Ahora explicaremos la relación entre la geometría proyectiva en campos finitos y los MDS códigos.

Teorema 1.4.1 ([11], Theorem 4.1.2)**.** *Un n-arco en $\mathbb{P}^{n-k-1}(\mathbb{F}_q)$ define un MDS $[n, k, n-k+1]$-código $\mathscr{C}$.*

Demostración. Sea K un n-arco en $\mathbb{P}^{n-k-1}(\mathbb{F}_q)$. Cualquier punto del arco tiene la forma $[x_0 : x_1 : \cdots : x_{n-k-1}]$. Si tomamos cada punto del arco y lo transformamos en la columna de una matriz H, entonces H tiene $(n-k)$ filas y n columnas. Esta matriz es una matriz de control de paridad para un código. Como las columnas de H vienen de un n-arco, entonces cualquier $n-k-1+1 = n-k$ de ellas son linealmente independientes. Por el Corolario 1.3.17 se tiene que $\mathscr{C}$, el código definido por H, es un MDS código.

□

Corolario 1.4.2 ([11], Corollary 4.1.1)**.** Un n-arco en $\mathbb{P}^{k-1}(\mathbb{F}_q)$ corresponde a un MDS $[n, n-k, k+1]_q$-código lineal, y viceversa.

Ejemplo 1.4.1. Considerando el plano proyectivo de orden 3, es decir, $\mathbb{P}^2(\mathbb{F}_3)$. Considerando el 4-arco formado por los puntos $\{[1:0:0], [1:2:1], [1:1:0], [1:1:1]\}$ (figura 1.2). Podemos tomar los vectores y crear la matriz H con columnas igual a estos vectores.

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

Donde H es la matriz generadora de $\mathscr{C}^{\perp}$, un MDS $[4, 3, 2]$-código. Así, H es la matriz de control de paridad de $\mathscr{C}$ un MDS $[4, 1, 4]$-código.

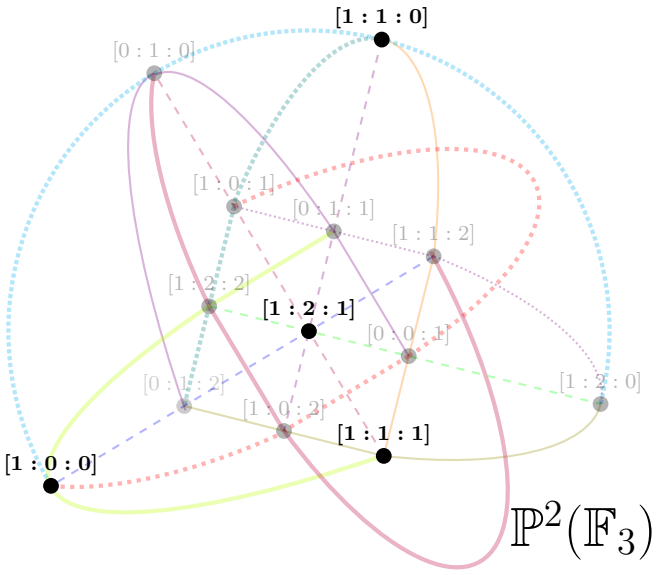


Figura 1.2: 4-arco en $\mathbb{P}^2(\mathbb{F}_3)$.

Ejemplo 1.4.2. Considerando el plano proyectivo de orden 4, es decir, $\mathbb{P}^2(\mathbb{F}_4)$. Donde el campo finito $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$. Entonces con el polinomio de permutación $F(t) = t^2$, podemos obtener el hiperóvalo regular formado por los 6 puntos

$$\mathcal{K} = \{[0:0:1], [0:1:0], [1:0:0], [1:1:1], [\alpha:\alpha^2:1], [\alpha^2:\alpha:1]\}.$$

Podemos crear la matriz H con columnas iguales a los vectores del hiperóvalo:

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

Esta es la matriz de control de paridad para un $[6, 3, 4]$-código lineal MDS. Podemos observar también que el código dual $\mathscr{C}^{\perp}$ es un $[6, 3, 4]$-código lineal MDS. Este código tiene un nombre especial, *Hexacódigo*.

Ejemplo 1.4.3 (MDS de un 10-arco de Glynn)**.** Consideramos el espacio proyectivo

$\mathbb{P}^4(\mathbb{F}_9)$. Construimos $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2+x+2)$ donde el polinomio $p(x) = (x^2+x+2)$ es irreducible sobre $\mathbb{F}_3$. Los elementos de $\mathbb{F}_9$ corresponden al conjunto

$$\{0, 1, 2, \eta, \eta+1, \eta+2, 2\eta, 2\eta+1, 2\eta+2\}$$

donde $\eta^2+\eta+2=0$ y $\eta^4=-1$. Llamamos ahora un 10-arco de Glynn al conjunto L definico como

$$L = \{[1 : t : t^2+\eta t^6 : t^3 : t^4] \mid t \in \mathbb{F}_9\} \cup \{[0:0:0:0:1]\}.$$

Usando esto podemos construir explícitamente los 10 puntos del arco de Glynn. En primer lugar, debemos notar las siguientes relaciones que se cumplen para η:

1. $\eta^2 = 2\eta+1$,
2. $\eta^3 = 2\eta+2$,
3. $\eta^4 = 2 = -1$,
4. $\eta^6 = \eta+2$.

Tomando cada punto de L como una columna de H donde H es entonces la siguiente matriz:

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

Así, vemos que se crea un $[10, 5, 6]$-código MDS. Este es código MDS no trivial. Esto es una buena razón, por la cual los arcos son un objeto deseado en espacios proyectivos.

Capítulo 2

Códigos Skew Pseudo-Cíclicos

2.1. Definiciones y Propiedades

Definición 2.1.1. Sea $\alpha \in \mathbb{F}_q^*$ y θ un automorfismo de $\mathbb{F}_q$. Un código lineal $\mathscr{C} \subseteq \mathbb{F}_q^n$ es llamado *código skew α-cíclico* si es invariante bajo la transformación lineal

$$\phi_{\alpha,\theta} : (c_0, c_1 \ldots, c_{n-1}) \mapsto (\alpha\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})).$$

Un código es llamado *skew pseudo-cíclico* si $\mathscr{C}$ es skew α-cíclico para algún $\alpha \in \mathbb{F}_q^*$ y θ un automorfismo de $\mathbb{F}_q$.

Teorema 2.1.2 ([7], Proposition 1)**.** *Un código $\mathscr{C}$ es un código skew α-cíclico con el automorfismo θ si y sólo si es invariante bajo la aplicación semi-lineal $\mathcal{T} := \Theta \circ A$, es decir, $(\vec{c})\mathcal{T} \in \mathscr{C}$ para todo $\vec{c} \in \mathscr{C}$, donde $\Theta \colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ es definida por $\Theta((c_0, \ldots, c_{n-1})) = (\theta(c_0), \ldots, \theta(c_{n-1}))$ y A es una matriz $n \times n$ dada por*

$$A = \left(\begin{array}{c|ccc} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \hline \alpha & 0 & \cdots & 0 \end{array}\right), \text{ con } \alpha \in \mathbb{F}_q^*.$$

Observación 2.1.3. Si $\mathscr{C}$ es un código skew pseudo-cíclico invariante bajo la aplicación semi-lineal $\mathcal{T} := \Theta \circ A$, entonces $\mathscr{C} \star (\Theta \circ A) \subseteq \mathscr{C}$, donde $\mathscr{C} \star (\Theta \circ A) := \{\Theta(\vec{c})A \mid \vec{c} \in \mathscr{C}\}$.

Observación 2.1.4. Un código skew pseudo-cíclico con $\theta = Id$, es simplemente un código pseudo-cíclico.

Con el fin de convertir la estructura de códigos cíclicos en una estructura algebraica, con $R := \mathbb{F}_q[x;\theta]$, consideramos la siguiente correspondencia:

$$\begin{array}{rccc} \pi: & \mathbb{F}_q^n & \longrightarrow & R/R(x^n-\alpha) \\ & (a_0, a_1, \ldots, a_{n-1}) & \longmapsto & a_0 + a_1 x + \cdots a_{n-1}x^{n-1} \end{array} \tag{2.1}$$

Observamos que π es un $\mathbb{F}_q$-isomorfismo lineal de espacios vectoriales sobre $\mathbb{F}_q$. Así, podemos identificar en algunos casos $\mathbb{F}_q^n$ con $R/R(x^n-\alpha)$ y un vector $\vec{a} = (a_0, a_1, \ldots, a_{n-1})$ con el polinomio $\pi(\vec{a}) = \sum_{i=0}^{n-1} a_i x^i$.

Definición 2.1.5. Denotamos por $\mathbb{F}_q^\theta$, al subconjunto de $\mathbb{F}_q$ formado por los elementos invariantes bajo el automorfismo θ, es decir, $\mathbb{F}_q^\theta := \{\alpha \in \mathbb{F}_q \mid \theta(\alpha) = \alpha\}$.

Observación 2.1.6. Si $m \nmid n$, donde $m = |\langle\theta\rangle|$ o si $\alpha \notin \mathbb{F}_q^\theta$, $R/R(x^n-\alpha)$ no es un anillo y no podemos discutir de la estructura de sus ideales, como lo es en el caso conmutativo. Por ejemplo, en literatura de códigos skew cíclicos, la condición $m \mid n$ es asumida, entonces se tiene una correspondencia uno a uno entre los códigos skew-cíclicos y los ideales de $R/R(x^n-1)$.

El conjunto $R/R(x^n-\alpha)$ puede ser considerado como un $\mathbb{F}_q$-módulo izquierdo o como un $\mathbb{F}_q[x;\theta]$-módulo izquierdo.

El siguiente Teorema entrega una definición correcta de un código skew pseudo-cíclico para cualquier largo n.

Teorema 2.1.7. *Sea π definida en (2.1) y $R := \mathbb{F}_q[x;\theta]$. Luego un subconjunto no vacío $\mathscr{C}$ de $\mathbb{F}_q^n$ es un código skew pseudo-cíclico si y sólo si $\pi(\mathscr{C})$ es un R-submódulo izquierdo del R-módulo izquierdo $R/R(x^n-\alpha)$, para algún $\alpha \in \mathbb{F}_q^*$.*

Teorema 2.1.8. *Sea $\mathscr{C}$ un R-submódulo izquierdo de $R/R(x^n-\alpha)$ con $R := \mathbb{F}_q[x;\theta]$, esto es, un código skew α-cíclico de largo n. Entonces existe un único polinomio mónico de grado mínimo en $\mathscr{C}$, que satisface*

(a) $\mathscr{C} = Rg$, es decir, $g(x)$ es el polinomio generador de $\mathscr{C}$;

(b) $g(x)$ es un divisor derecho de $x^n-\alpha$;

(c) Cualquier $c(x) \in \mathscr{C}$ puede escribirse de manera única como $c(x) = f(x)g(x) \in R/R(x^n-\alpha)$, donde $f(x) \in R$ tiene grado menor que $n-k$ y $k = \deg g(x)$. La dimensión de $\mathscr{C}$ es $n-k$;

(d) Si $g(x) = \sum_{x=0}^{k} g_i x^i$, entonces $\mathscr{C}$ tiene la siguiente matriz generadora

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_k & 0 & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_k) & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \theta^{n-k-1}(g_0) & \theta^{n-k-1}(g_1) & \cdots & \cdots & \theta^{n-k-1}(g_k) \end{pmatrix}.$$

Lema 2.1.9. *Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código lineal y $\mathcal{T}\colon \mathbb{F}_q^n \to \mathbb{F}_q^n$ una aplicación semi-lineal dada por $\mathcal{T} := \Theta \circ A$ (como en el Teorema 2.1.2), tal que $\mathscr{C} \star \mathcal{T} \subseteq \mathscr{C}$. Si $\mathcal{T}$ es invertible, entonces $\mathscr{C} \star \mathcal{T} = \mathscr{C}$. Además, $\mathscr{C} \star \mathcal{T} = \mathscr{C}$, si sólo si, $\mathscr{C} \star (\mathcal{T})^{-1} = \mathscr{C}$.*

Demostración. Como $\mathcal{T}$ es invertible, la aplicación semi-lineal es inyectiva, por lo cual $|\mathscr{C} \star \mathcal{T}| = |\mathscr{C}|$ y $\mathscr{C} \star \mathcal{T} \subseteq \mathscr{C}$, por lo tanto $\mathscr{C} \star \mathcal{T} = \mathscr{C}$. □

Definición 2.1.10. Para cualquier matriz $M = [m_{ij}]$, con $m_{ij} \in \mathbb{F}_q$ y θ un automorfirsmo de $\mathbb{F}_q$, se define $M_\theta := [\theta(m_{ij})]$.

Proposición 2.1.11 ([41], Proposition 25). *Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código skew pseudo-cíclico invariante bajo la transformación semi-lineal $\mathcal{T} = \Theta \circ M$. Entonces el código dual $\mathscr{C}^\perp$ es un código skew pseudo-cíclico invariante bajo $\mathcal{T}' = \Theta^{-1} \circ (M_t)_{\theta^{-1}}$.*

Teorema 2.1.12 ([12], Theorem 6.1). *Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código lineal y $\alpha \in \mathbb{F}_q^*$. Entonces $\mathscr{C}$ es un código skew α-cíclico si y solo si su código dual $\mathscr{C}^\perp$ es un código skew α^{-1}-cíclico.*

Demostración.

"$\Rightarrow$"

Supongamos que $\mathscr{C}$ es un código skew α-cíclico, invariante bajo la transformación semi-lineal $\Theta \circ A$, es decir, $\mathscr{C} \star (\Theta \circ A) \subseteq \mathscr{C}$. De la Proposición 2.1.11, tenemos que

$$\mathscr{C}^\perp \star \left(\Theta^{-1} \circ (A_t)_{\theta^{-1}}\right) \subseteq \mathscr{C}^\perp.$$

Además, como $(\Theta^{-1} \circ (A_t)_{\theta^{-1}})$ es invertible, del Lema 2.1.9, podemos concluir que

$$\mathscr{C}^\perp \star \left(\Theta^{-1} \circ (A_t)_{\theta^{-1}}\right) = \mathscr{C}^\perp.$$

Considerando $\Theta \circ M_\theta = M \circ \Theta$, para cualquier matriz M, por el Lema 2.1.9 tenemos que

$$\begin{aligned} \mathscr{C}^\perp \star \left(\Theta^{-1} \circ (A_t)_{\theta^{-1}}\right) = \mathscr{C}^\perp &\iff \mathscr{C}^\perp \star \left(\Theta^{-1} \circ (A_t)_{\theta^{-1}}\right)^{-1} = \mathscr{C}^\perp \\ &\iff \mathscr{C}^\perp \star \left(((A_t)^{-1})_{\theta^{-1}} \circ \Theta\right) = \mathscr{C}^\perp \\ &\iff \mathscr{C}^\perp \star \left(\Theta \circ (A_t)^{-1}\right) = \mathscr{C}^\perp. \end{aligned}$$

Dado que la matriz

$$(A_t)^{-1} = \left(\begin{array}{c|ccc} 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ \hline \alpha^{-1} & 0 & \cdots & 0 \end{array}\right),$$

podemos concluir que $\mathscr{C}^\perp$ es un código skew α^{-1}-cíclico.

"$\Leftarrow$"

Considerando que $(\mathscr{C}^{\perp})^{\perp} = \mathscr{C}$, el reciproco del Teorema se obtiene de forma inmediata con la parte anterior. □

Corolario 2.1.13 ([12], Corollary 6.2)**.** Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un skew código α-cíclico. Si $\mathscr{C} = \mathscr{C}^{\perp}$, entonces n es par y $\alpha = \pm 1$.

Demostración. Primero, podemos observar que $n = \dim(\mathscr{C}) + \dim(\mathscr{C}^{\perp}) = 2\dim(\mathscr{C})$. Como $g(x)$ es el polinomio generador de $\mathscr{C}$, por el Teorema 2.1.12 tenemos

$$x^n - \alpha = h_1(x)g(x) \quad \text{y} \quad x^n - \alpha^{-1} = h_2(x)g(x),$$

para algún $h_1(x), h_2(x) \in R$. Así, se tiene que $\deg((h_1(x) - h_2(x))g(x)) = 0$ y como $\deg(g(x)) > 0$, podemos concluir que $h_2(x) = h_1(x)$ y esto muestra que $\alpha = \alpha^{-1}$, es decir, $\alpha^2 = 1$. □

Proposición 2.1.14 ([12], Theorem 6.1)**.** *Sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código skew α-cíclico generado por el polinomio $g(x) = g_0 + g_1 x + \cdots + g_n x^{n-k}$. Entonces el código dual $\mathscr{C}^{\perp}$ es generado por*

$$h(x) := \theta^k(\hbar_0^{-1}) \left[\sum_{i=0}^{k} \theta^i(\hbar_{k-i}) x^i \right],$$

donde $\hbar(x) := \hbar_0 + \hbar_1 x + \cdots + \hbar_k x^k$ es tal que $x^n - \theta^{-k}(\alpha) = g(x)\hbar(x)$.

Demostración. Como $\mathscr{C}$ es un código skew α-cíclico, por el Teorema 2.1.12 sabemos que el código $\mathscr{C}^{\perp}$ es un código skew α^{-1}-cíclico. Luego, desde el Teorema 2.1.8 se tiene que existe un único polinomio mónico $h(x)$ de grado mínimo en $R := \mathbb{F}_q[x;\theta]$ tal que $\mathscr{C}^{\perp} = Rh(x)$. Por el Theorem 3 en [6], podemos deducir que existe $\hbar(x) \in R$ y $c \in \mathbb{F}_q^*$ tal que

$$x^n - c = g(x)\hbar(x)$$

y $h(x) = \theta^k(\hbar_0^{-1})g^{\perp}(x)$, donde $g^{\perp}(x) := \sum_{i=0}^{k} \theta^i(\hbar_{k-i})x^i$. Como $g(x) \in R$ es mónico y $x^n - \alpha = t(x)g(x)$ para algún polinomio mónico $t(x) \in R$, por el Lemma 2 en [7] tenemos

que

$$x^n - \theta^{-k}(\alpha) = g(x)s(x)$$

para algún $s(x) \in R$. Por lo tanto $c - \theta^{-k}(\alpha) = g(x)(s(x) - \hbar(x))$ y como $\deg(g(x)) \geq 1$, podemos concluir que $c = \theta^{-k}(\alpha)$. □

Ejemplo 2.1.1 (Programa 2)**.** Consideremos el campo finito $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ donde $\alpha^2 + \alpha + 1 = 0$ y θ el automorfismo de Frobenius, es decir, $\theta(a) = a^2$. Sea $\mathscr{C}$ el $[8, 2, 4]_4-$código skew α-cíclico generado por el polinomio $\alpha^2 x^6 + x^4 + \alpha x^2 + \alpha^2$, con matriz generadora

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

Su respectivo código dual $\mathscr{C}^\perp$ es el $[8, 6, 2]_4$-código skew α^2-cíclico ($\alpha^2 = \alpha^{-1}$) generado por el polinomio $\alpha^2 x^2 + 1$, con matriz generadora

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

Teorema 2.1.15. *Sea $\mathscr{C}$ un $[n, n-k]$-código lineal sobre $\mathbb{F}_q$. Entonces $\mathscr{C}$ es skew α-cíclico si y sólo si $\mathscr{C}$ tiene matriz de control de paridad de la forma $[P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$, con $P \in \mathbb{F}_q^k$, $\tau = \Theta \circ T$ y $T \in GL(k, q)$ tal que $P\tau^n = \alpha P$.*

Demostración.

"$\Rightarrow$"

Sea $\mathscr{C}$ un $[n, n-k]$-código skew α-cíclico sobre $\mathbb{F}_q$ con una matriz de control de paridad $H = [(P_1)_t, (P_2)_t, \ldots, (P_n)_t]$, donde $(P_i)_t$ son los vectores columnas. Entonces por el Teorema 2.1.12, tenemos que $H' = [\alpha^{-1}\Theta((P_n)_t), \Theta((P_1)_t), \Theta((P_2)_t), \ldots, \Theta((P_{n-1})_t)]$ es también una matriz de control de paridad para $\mathscr{C}$. Luego, existe una matriz $T_t \in GL(k, q)$

tal que $H = T_t \cdot H'$. Por lo tanto, se tiene

$$\begin{aligned}
(P_1)_t &= T_t(\alpha^{-1}\Theta((P_n)_t)) = (\alpha^{-1}(P_n)\Theta \circ T)_t \\
(P_2)_t &= T_t\Theta((P_1)_t) = ((P_1)\Theta \circ T)_t \\
(P_3)_t &= T_t\Theta((P_2)_t) = ((P_2)\Theta \circ T)_t = ((P_1)(\Theta \circ T)^2)_t \\
&\vdots \\
(P_n)_t &= T_t\Theta((P_n)_t) = ((P_{n-1})\Theta \circ T)_t = ((P_1)(\Theta \circ T)^{n-1})_t
\end{aligned}$$

Además,

$$P_1 = \alpha^{-1}(P_n)(\Theta \circ T) \Rightarrow P_1 = \alpha^{-1}(P_1)(\Theta \circ T)^n \Rightarrow \alpha P_1 = P_1(\Theta \circ T)^n$$

Así, con $\tau = \Theta \circ T$ y $P = P_1$, se tiene que $H = [P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$ con $\alpha P = P \cdot \tau^n$.

"$\Leftarrow$"

Sea $\mathscr{C}$ un código con matriz de control de paridad $H = [P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$ con $P \in \mathbb{F}_q^k$, $\tau = \Theta \circ T$ y $T \in GL(k, q)$ tal que $P\tau^n = \alpha P$. Luego, para cualquier $\vec{c} = (c_0, c_1, \ldots, c_{n-1}) \in \mathscr{C}$ se tiene que $\vec{c}H_t = \vec{0}$, lo que implica que

$$\begin{aligned}
\sum_{i=0}^{n-1} c_i(P\tau^i) = \vec{0} &\Longrightarrow \left(\sum_{i=0}^{n-1} c_i(P\tau^i)\right)\tau = (\vec{0})\tau \\
&\Longrightarrow \sum_{i=0}^{n-2} \theta(c_i)(P\tau^{i+1}) + \theta(c_{n-1})(P\tau^n) = \vec{0} \\
&\Longrightarrow \sum_{i=0}^{n-2} \theta(c_i)(P\tau^{i+1}) + \theta(c_{n-1})(\alpha P) = \vec{0} \\
&\Longrightarrow (\alpha\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2}))H_t = \vec{0},
\end{aligned}$$

es decir, $(\alpha\theta(c_{n-1}), \theta(c_0), \ldots, \theta(c_{n-2})) \in \mathscr{C}$ y por lo tanto, $\mathscr{C}$ es un código skew α-cíclico. □

Teorema 2.1.16. *Sea* $g(x) = \sum_{i=0}^{k} a_i x^i$ *con* $a_k = 1$ *un polinomio de grado* k *en* $\mathbb{F}_q[x; \theta]$

que divide a la derecha a $x^n - \alpha$, $\alpha \in \mathbb{F}_q^*$. *Entonces* $\mathscr{C}$ *es un* $[n, n-k]$*-código skew* α*-cíclico sobre* $\mathbb{F}_q$ *con polinomio generador* $g(x)$ *si y sólo si* $\mathscr{C}$ *es un código con matriz de control de paridad* $[P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$, *donde* $P = (1, 0, \ldots, 0)$, $\tau = \Theta \circ T_g$ *y* T_g *es la matriz compañera de* $g(x)$, *es decir,*

$$T_g = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix}.$$

Demostración. Consideremos la siguiente aplicación lineal

$$\begin{aligned} \pi\colon \quad \mathbb{F}_q^k &\longrightarrow R/Rg \\ (c_0, c_1, \ldots, c_{k-1}) &\longmapsto c_0 + c_1 x + \cdots c_{k-1} x^{k-1} \end{aligned} \tag{2.2}$$

con $R = \mathbb{F}_q[x; \theta]$. Luego, se puede observar que $\pi(P\tau^i) = x^i$ con $P = (1, 0, \ldots, 0)$, para cada $i \in \mathbb{Z}_{\geq 0}$. Así, se tiene que

$$\begin{aligned} \pi(a_0 P + a_1 P\tau + \cdots + a_{k-1} P\tau^{k-1} + P\tau^k) &= \pi(a_0 P) + \pi(a_1 P\tau) + \cdots + \pi(P\tau^k) \\ &= a_0\pi(P) + a_1\pi(P\tau) + \cdots + \pi(P\tau^k) \\ &= a_0(1) + a_1(x) + \cdots + (x^k) \\ &= g(x) = 0 \in R/Rg(x), \end{aligned}$$

es decir, $a_0 P + a_1 P\tau + \cdots + a_{k-1} P\tau^{k-1} + P\tau^k = (0, \ldots, 0) = \vec{0}$. Además, como $g(x)$ es un divisor derecho de $x^n - \alpha$,

$$\begin{aligned} \pi(P\tau^n - \alpha P) &= \pi(P\tau^n) - \alpha\pi(P) \\ &= x^n - \alpha = 0 \in R/Rg(x), \end{aligned}$$

lo que implica que $P\tau^n - \alpha P = (0, 0, \ldots, 0)$, o sea, $P\tau^n = \alpha P$.

Tomamos $H = [(P_0)_t, (P_1)_t, \ldots, (P_{n-1})_t]$, $P_i = P\tau^i$, $P_0 = P = (1, 0, \ldots, 0)$ y $\tau = \Theta \circ T_g$.

"$\Leftarrow$"

Observamos que $\vec{g} = (a_0, a_1, \ldots, a_{k-1}, 1, 0, \ldots, 0) \in \mathbb{F}_q^n$ es un elemento de $\mathscr{C}$, pues $\vec{g}H_t = \vec{0}$. Además, $\vec{g}\tau^i H_t = \vec{0}$ para cada $i = 0, \ldots, n-k-1$, es decir, $\{\vec{g}, \vec{g}\tau, \ldots, \vec{g}\tau^{n-k-1}\}$ son $n-k$ elementos de $\mathscr{C}$ linealmente independientes. Luego $\mathscr{C}$ tiene una matriz generadora dada por

$$G = \begin{pmatrix} a_0 & a_1 & \cdots & a_{k-1} & 1 & 0 & 0 & \cdots & 0 \\ 0 & \theta(a_0) & \theta(a_1) & \cdots & \theta(a_{k-1}) & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \theta^{n-k-1}(a_0) & \theta^{n-k-1}(a_1) & \cdots & \cdots & \theta^{n-k-1}(a_{k-1}) & 1 \end{pmatrix}, \quad (2.3)$$

.

Como $P\tau^n = \alpha P$, por el Teorema 2.1.15, H forma una matriz de control de paridad de un $[n, n-k]$-código skew α-cíclico. En fin, pues $g(x)$ es un polinomio mónico que se corresponde con el vector $\vec{g} \in \mathscr{C}$, se concluye que $\mathscr{C}$ es un $[n, n-k]$-código skew α-cíclico sobre $\mathbb{F}_q$ con polinomio generador $g(x)$.

"$\Rightarrow$"

Sea $\mathscr{C}$ un $[n, n-k]$-código skew α-cíclico sobre $\mathbb{F}_q$ con polinomio generador $g(x) = a_0 + a_1 x + \cdots + a_{k-1}x^{k-1} + x^k$. Luego la matriz generadora en forma canónica de $\mathscr{C}$, es como (2.3) y mostraremos que H es la matriz de control de paridad de $\mathscr{C}$. Ya sabemos

que $a_0P + a_1P\tau + \cdots + a_{k-1}P\tau^{k-1} + P\tau^k = \vec{0}$. Luego

$$\begin{aligned}
(a_0P + a_1P\tau + \cdots + P\tau^k)\tau = \vec{0} &\Leftrightarrow (\theta(a_0)P\tau + \theta(a_1)P\tau^2 + \cdots + P\tau^{k+1}) = \vec{0} \\
(a_0P + a_1P\tau + \cdots + P\tau^k)\tau^2 = \vec{0} &\Leftrightarrow (\theta^2(a_0)P\tau^2 + \theta^2(a_1)P\tau^3 + \cdots + P\tau^{k+2}) = \vec{0} \\
\vdots \qquad\qquad & \qquad\qquad \vdots \\
(a_0P + a_1P\tau + \cdots + P\tau^k)\tau^{n-k-1} = \vec{0} &\Leftrightarrow (\theta^{n-k-1}(a_0)P\tau^{n-k-1} + \cdots + P\tau^{n-1}) = \vec{0},
\end{aligned}$$

lo que implica que $GH_t = O$, es decir $HG_t = O$. Por el Lema 1.3.15 H es la matriz de control de paridad de $\mathscr{C}$. □

Ejemplo 2.1.2. Consideremos el campo finito $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, donde $\alpha^2 + \alpha + 1 = 0$, y θ el automorfismo de Frobenius, es decir $\theta(a) = a^2$. El $[7, 3]$-código skew α-cíclico generado por el polinomio $g(x) = x^4 + x^2 + \alpha^2 x + 1$ tiene matriz generadora

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

y matriz de control de paridad de la forma $H := [P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^5)_t]$, donde $P = (1, 0, 0, 0)$, $\tau = \Theta \circ T_g$ y T_g es la matriz compañera de $g(x)$, es decir,

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

Así, la matriz H está dada por

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

Además, se puede comprobar que $G \cdot H_t = O$.

Observación 2.1.17. Un código $\mathscr{C} \subseteq \mathbb{F}_q^n$ con matriz de control de paridad de la forma $[P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$, con $P \in \mathbb{F}_q^k$, $\tau = \Theta \circ T$ y $T \in GL(k,q)$ se llama código $\mathscr{C}$ *definido por* (τ, P, n). Además, se define el conjunto

$$\Gamma_k^\alpha := \{(\tau, P, n) \mid (\tau, P, n) \text{ define un } [n, n-k]_q\text{-código skew } \alpha\text{-cíclico}\}.$$

Proposición 2.1.18. *Sea $(\tau_i, P_i, n) \in \Gamma_k^\alpha$ y sea $\mathscr{C}$ el código definido por (τ_i, P_i, n), con $i = 1, 2$. Entonces, $\mathscr{C}_1 = \mathscr{C}_2$ si y solo si existe una $S \in GL(k,q)$ tal que $\tau_1 = S \cdot \tau_2 \cdot S^{-1}$ y $P_1 S = P_2$.*

Demostración.
"$\Rightarrow$"
Como $\mathscr{C}_1 = \mathscr{C}_2$, existe $S \in GL(k,q)$ tal que

$$\begin{aligned} S_t[(P_1)_t, (P_1\tau_1)_t, (P_1\tau_1^2)_t, \ldots, (P_1\tau_1^{n-1})_t] &= [(P_1S)_t, (P_1\tau_1 S)_t, (P_1\tau_1^2 S)_t, \ldots, (P_1\tau_1^{n-1}S)_t] \\ &= [(P_2)_t, (P_2\tau_2)_t, (P_2\tau_2^2)_t, \ldots, (P_2\tau_2^{n-1})_t] \end{aligned}$$

De la igualdad de la primera columna se tiene que $P_1S = P_2$, lo que implica que $P_2S^{-1} = P_1$. Además, $P_2\tau_2^i = P_1\tau_1^i S = (P_2S^{-1})\,\tau_1^i S = P_2\,(S^{-1}\tau_1 S)^i$, con $i = 1, \ldots, n-1$.

Tenemos que $\{P_2\tau_2^{j_1}, P_2\tau_2^{j_2}, \ldots, P_2\tau_2^{j_k}\}$ son vectores linealmente independiente sobre $\mathbb{F}_q^n$ para $j_i \in \{1, \ldots, n-1\}$. Luego, un vector $\vec{v} \in \mathbb{F}_q^n$ se puede escribir como $\vec{v} =$

$\sum_{i=0}^{k-1} \lambda_i \left(P_2\tau_2^{j_i}\right)$. Así, se tiene que

$$\begin{aligned}
\vec{v}\tau_2 &= \sum_{i=0}^{k-1} \lambda_i \left(P_2\tau_2^{j_i}\right)\tau_2 \\
&= \sum_{i=0}^{k-1} \lambda_i \left(P_2\tau_2^{j_{i+1}}\right) \\
&= \sum_{i=0}^{k-1} \lambda_i \left(P_2\left(S^{-1}\tau_1 S\right)^{j_{i+1}}\right)
\end{aligned}
\quad , \quad
\begin{aligned}
\vec{v}\left(S^{-1}\tau_1 S\right) &= \sum_{i=0}^{k-1} \lambda_i \left(P_2\tau_2^{j_i}\right)\left(S^{-1}\tau_1 S\right) \\
&= \sum_{i=0}^{k-1} \lambda_i \left(P_2\left(S^{-1}\tau_1 S\right)^{j_i}\right)\left(S^{-1}\tau_1 S\right) \\
&= \sum_{i=0}^{k-1} \lambda_i \left(P_2\left(S^{-1}\tau_1 S\right)^{j_{i+1}}\right)
\end{aligned}$$

Al tomar $\vec{v} = \vec{e_j}$, $\vec{e_j}$ vector canónico para $j = 1, \ldots, k$, se cumple $\vec{e_j}\tau_2 = \vec{e_j}S^{-1}\tau_1 S$ y podemos concluir que $S^{-1}\tau_1 S = \tau_2$.

"$\Leftarrow$"

Dado que existe una matriz $S \in GL(k, q)$ tal que $S\tau_2^i = \tau_1^i S$ y $P_2 = P_1 S$, se tiene que $P_2\tau_2^i = P_1 S\tau_2^i = P_1\tau_1^i S$ para $i = 0, \ldots, n-1$, es decir

$$\begin{aligned}
[(P_2)_t, (P_2\tau_2)_t, (P_2\tau_2^2)_t, \ldots, (P_2\tau_2^{n-1})_t] &= [(P_1 S)_t, (P_1\tau_1 S)_t, (P_1\tau_1^2 S)_t, \ldots, (P_1\tau_1^{n-1} S)_t] \\
&= S_t[(P_1)_t, (P_1\tau_1)_t, (P_1\tau_1^2)_t, \ldots, (P_1\tau_1^{n-1})_t].
\end{aligned}$$

Por el Teorema 2.1.15, las matrices definidas por (τ_1, P_1, n) y (τ_2, P_2, n) son las matrices control de paridad de códigos skew α-cíclicos, que difieren por una matriz invertible, es decir, corresponden al mismo código. Luego $\mathscr{C}_1 = \mathscr{C}_2$. □

Contrariamente al caso conmutativo (ver 1.3.52), cuando $\theta \neq id$, se trabaja con el polinomio mínimo m_τ de una aplicación τ semi-lineal [42] en lugar del polinomio característico. En este contexto, un polinomio mínimo puede estar asociado a dos códigos distintos, es decir, si $\mathscr{C}_1 = \mathscr{C}_2$ entonces $m_{\tau_1} = m_{\tau_2}$, pero en general no es valido el reciproco, como muestra el siguiente ejemplo.

Ejemplo 2.1.3. Consideremos el campo finito $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, donde $\alpha^2+\alpha+1 = 0$ y θ el automorfismo de Frobenius, es decir, $\theta(a) = a^2$. Con $R := \mathbb{F}_4[x; \theta]$, $g_1 = 1+\alpha x+x^2+x^3$ y $g_2 = 1 + \alpha^2 x + x^2 + x^3$ en R. Sean $\mathscr{C}_1 := Rg_1$ y $\mathscr{C}_1 := Rg_2$, dos $[14, 11]$-códigos skew

1-cíclicos. Como $g_1(x) \neq g_2(x)$, y se tiene que $\mathscr{C}_1 \neq \mathscr{C}_2$. Además

$$\tau_1 = \Theta \circ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix} \quad , \quad \tau_2 = \Theta \circ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix}$$

con polinomios mínimos respectivos $m_{\tau_1}(x) = m_{B_1}(x^2)$ y $m_{\tau_2}(x) = m_{B_2}(x^2)$ (ver [42]), donde

$$\begin{aligned} B_1 &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix}_\theta \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix} \quad , \quad B_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix}_\theta \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & \alpha & 1 \\ 1 & \alpha^2 & \alpha \end{pmatrix} \qquad = \begin{pmatrix} 0 & 0 & 1 \\ 1 & \alpha^2 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix} \end{aligned}$$

Así, se tiene que

$$\begin{aligned} m_{B_1}(t) &= det \begin{pmatrix} -t & 0 & 1 \\ 1 & \alpha - t & 1 \\ 1 & \alpha^2 & \alpha - t \end{pmatrix} \quad , \qquad m_{B_2}(t) = det \begin{pmatrix} -t & 0 & 1 \\ 1 & \alpha^2 - t & 1 \\ 1 & \alpha & \alpha^2 - t \end{pmatrix} \quad , \\ &= t^3 + t + 1 \qquad\qquad = t^3 + t + 1. \end{aligned}$$

Por lo tanto, existen dos códigos diferentes con el mismo polinomio mínimo.

2.2. MDS Códigos Skew Pseudo-Cíclicos

Lema 2.2.1. *Dado* $\mathbb{F}_q$ *con* $q = p^h$, p *primo,* $0 \leq i \leq k-1$ *y* $\beta \in \mathbb{F}_q^*$. *El polinomio* $(x-\beta)^{p-i-1} \in \mathbb{F}_q[x]$ *divide al polinomio* $f_i(x) = \sum_{j=0}^{p-1} j^i \beta^{p-1-j} x^j \in \mathbb{F}_q[x]$, *considerando* $0^0 = 1$.

Demostración. Con $h \leq p-i-2$, se tiene que la derivada de orden h del polinomio f_i está dada por

$$f_i^{(h)}(x) = \sum_{j=0}^{p-1} j^i \beta^{p-1-j} \cdot j \cdot (j-1) \cdots (j-h+1) x^{j-h}.$$

Evaluando $f_i^{(h)}$ en β, tenemos

$$\begin{aligned}
f_i^{(h)}(\beta) &= \sum_{j=0}^{p-1} j^i \beta^{p-1-j} \cdot j \cdot (j-1) \cdots (j-h+1) \beta^{j-h} \\
&= \sum_{j=0}^{p-1} j^i \beta^{p-1-h} \cdot j \cdot (j-1) \cdots (j-h+1) \\
&= \beta^{p-1-h} \sum_{j=0}^{p-1} j^i \cdot j \cdot (j-1) \cdots (j-h+1) \\
&= \beta^{p-1-h} \sum_{j=0}^{p-1} \left(\lambda_{i+h} j^{i+h} + \cdots + \lambda_1 j + \lambda_0 \right), \qquad \text{con } \lambda_n \in \mathbb{F}_q \\
&= \beta^{p-1-h} \left(\lambda_{i+h} \sum_{j=0}^{p-1} j^{i+h} + \cdots + \lambda_1 \sum_{j=0}^{p-1} j^1 + \cdots + \lambda_0 \sum_{j=0}^{p-1} 1 \right)
\end{aligned}$$

Además, para $s+1 \leq i+h+1 \leq p-1$ se tiene que

$$\begin{aligned}
& (t+1)^{s+1} - t^{s+1} = \sum_{k=0}^{s+1} \binom{s+1}{k} t^k - t^{s+1} \\
\Longrightarrow \quad & (t+1)^{s+1} - t^{s+1} = \sum_{k=1}^{s} \binom{s+1}{k} t^k + 1 \\
\Longrightarrow \quad & \sum_{t=0}^{p-1} \left[(t+1)^{s+1} - t^{s+1}\right] = \sum_{t=0}^{p-1} \left[\sum_{k=1}^{s} \binom{s+1}{k} t^k + 1\right] \\
\Longrightarrow \quad & p^{s+1} = \sum_{k=1}^{s} \binom{s+1}{k} \left[\sum_{t=0}^{p-1} t^k\right] + p \\
\Longrightarrow \quad & p^{s+1} - p = \binom{s+1}{s} \sum_{t=0}^{p-1} t^s + \sum_{k=1}^{s-1} \binom{s+1}{k} \left[\sum_{t=0}^{p-1} t^k\right].
\end{aligned}$$

Si $\sum_{t=0}^{p-1} t^k$ es un múltiplo de p, para todo $k = 1, \ldots, s-1$ por hipótesis de inducción, entonces $\binom{s+1}{s} \left[\sum_{t=0}^{p-1} t^s\right]$ es un múltiplo de p, es decir, $p \mid \binom{s+1}{s}$ o bien $p \mid \left[\sum_{t=0}^{p-1} t^s\right]$. Notar que, $\binom{s+1}{s} = s+1 \leq p-1$ lo que implica que $p \mid \left[\sum_{t=0}^{p-1} t^s\right]$ con s tal que $s \leq i+h$.

Así, $\sum_{j=0}^{p-1} j^s$ es un múltiplo de p y $f_i^{(h)}(\beta) = 0$.

Por lo tanto, como β es solución de $f_i^{(h)}$ con $h \leq p-i-2$, se tiene que

$$(x-\beta)^{p-i-1} \mid f_i(x).$$

□

Lema 2.2.2. *Dado $\mathbb{F}_q$ con $q = p^h$, p primo, $0 \leq i \leq k-1$, $\beta \in \left(\mathbb{F}_q^{\theta}\right)^*$. El polinomio $(x-\beta)^{p-i-1} \in \mathbb{F}_q[x;\theta]$ divide al polinomio $f_i(x) = \sum_{j=0}^{p-1} j^i \beta^{p-1-j} x^j \in \mathbb{F}_q[x;\theta]$, considerando $0^0 = 1$.*

Demostración. Como $\beta \in \left(\mathbb{F}_q^{\theta}\right)^*$ se tiene que los polinomios $(x-\beta)^{p-i-1}$ y $f_i(x)$ están en $\mathbb{F}_q^{\theta}[x;\theta]$.

Considerando la división de $f_i(x)$ por $(x-\beta)^{p-i-1}$ en $\mathbb{F}_q^{\theta}[x]$, por el Lema 2.2.1, se

tiene que

$$f_i(x) = q_i(x) \cdot (x-\beta)^{p-i-1} \text{ en } \mathbb{F}_q^\theta[x]$$

para algún $q_i(x) \in \mathbb{F}_q^\theta[x]$. Como el producto de polinomios en $\mathbb{F}_q^\theta[x;\theta]$ lo podemos interpretar en $\mathbb{F}_q^\theta[x]$, se tiene que

$$f_i(x) = q_i(x) \cdot (x-\beta)^{p-i-1} \text{ en } \mathbb{F}_q^\theta[x;\theta] \ .$$

Además, $\mathbb{F}_q^\theta[x;\theta] \subseteq \mathbb{F}_q[x;\theta]$ y se tiene que el cociente, resto son únicos, por el Teorema 1.1.48, se puede concluir que $(x-\beta)^{p-i-1}$ divide a $f_i(x)$.

□

Proposición 2.2.3. *Sea $\mathbb{F}_q$, con $q = p^h$, con p primo y $\alpha \in \mathbb{F}_p^*$. Entonces existe un $[p,k]$-código MDS skew α-cíclico sobre $\mathbb{F}_q$, con $2 \leq k \leq p-2$.*

Demostración. Como $\alpha \in \mathbb{F}_p^*$, se tiene que $\alpha^p = \alpha$. Así, un $[p,k]$-código skew α-cíclico $\mathscr{C}$ está generado por un polinomio $g(x)$ divisor de $x^p - \alpha = x^p - \alpha^p = (x-\alpha)^p$, por ejemplo $g(x) = (x-\alpha)^{p-k}$. Sea

$$f_i(x) = \sum_{j=0}^{p-1} j^i \alpha^{p-1-j} x^j, \quad 0 \leq i \leq k-1,$$

con $0^0 \equiv 1$. Se tiene que $p-i-1 \geq p-k$, así $g(x)$ divide a $(x-\alpha)^{p-i-1}$. Además, $(x-\alpha)^{p-i-1}$ divide a $f_i(x)$ por el Lema 2.2.2, por lo cual, $f_i(x)$ está en $\mathscr{C}$ para $0 \leq i \leq k-1$.

Sea G la matriz formada por todos los coeficientes de f_i, $0 \leq i \leq k-1$. Entonces

$$G = \begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_{k-2} \\ f_{k-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & p-1 \\ 0 & 1^2 & 2^2 & \cdots & (p-1)^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1^{k-2} & 2^{k-2} & \cdots & (p-1)^{k-2} \\ 0 & 1^{k-1} & 2^{k-1} & \cdots & (p-1)^{k-1} \end{pmatrix} \cdot \begin{pmatrix} \alpha^{p-1} & 0 & 0 & \cdots & 0 & 0 \\ 0 & \alpha^{p-2} & 0 & \cdots & 0 & 0 \\ 0 & 0 & \alpha^{p-3} & \cdots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix},$$

es decir, G ses una matriz cuyas columnas son múltiplos de puntos de un curva racional normal (definición 1.2.11) en $\mathbb{P}^{k-1}(\mathbb{F}_q)$ y que en el espacio proyectivo no se ve afectada al multiplicarse por la matriz diagonal.
Como cada f_i, $0 \leq i \leq k-1$, está en $\mathscr{C}$ y G está formada por k filas linealmente independientes, G es la matriz generadora de un MDS código $\mathscr{C}$.

□

Observación 2.2.4. En el caso conmutativo, por el Teorema 1.3.54, existe un $[n,k]$-código MDS pseudo-cíclico sobre $\mathbb{F}_q$ con $(n,q) \neq 1$, $2 \leq k \leq n-2$, si y sólo si $n = p$, donde $q = p^h$, con p primo. En el caso no conmutativo, existen códigos MDS pseudo-cíclicos también cuando $n \neq p$. A continuación se presenta un ejemplo de esta situación.

Ejemplo 2.2.1 (Programa 4)**.**

- Existe un $[4,2]$-código MDS α-cíclico, sobre $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ generado por α, donde $q = 4$, $n = 4$ y $k = 2$, por lo cual $(n,q) \neq 1$, $2 \leq k \leq n-2$. El código está generado por $g(x) = \alpha x^2 + \alpha^2 x + \alpha^2$ y tiene matriz de control de paridad

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

- Existe un $[6,4]$-código MDS 1-cíclico, sobre $\mathbb{F}_9 = \mathbb{F}_3[\omega]$ generado por ω. El código está generado por el polinomio $g(x) = \omega^5 x^2 + \omega^7 x + \omega^7$ y tiene matriz de control de paridad

$$\begin{pmatrix} \omega^7 & \omega^7 & \omega^5 & 0 & 0 & 0 \\ 0 & \omega^5 & \omega^5 & \omega^7 & 0 & 0 \\ 0 & 0 & \omega^7 & \omega^7 & \omega^5 & 0 \\ 0 & 0 & 0 & \omega^5 & \omega^5 & \omega^7 \end{pmatrix}.$$

Por el Teorema 2.1.15, la matriz de control de paridad de un MDS $[n, n-k]$-código skew pseudo-cíclico depende de $\tau = \Theta \circ T$ y es del siguiente tipo:

- $[P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$, con $P \in \mathbb{F}_q^k$, $\tau = \Theta \circ T$, $T \in GL(k,q)$ y tal que $P\tau^n = \alpha P$, con $n \leq \text{ord}(\tau)$.

Bajo ciertas condiciones sobre q, k y n, la existencia de los MDS $[n,k]_q$-códigos skew pseudo-cíclicos se relaciona con condiciones algebraicas, como se muestra en el siguiente resultado.

Teorema 2.2.5. *Si existe un $\mathscr{C} \subseteq \mathbb{F}_q^n$ MDS $[n, n-k]$-código skew pseudo-cíclico con $q > 2$, n y k tales que $k = 4, \ldots, n-1$ y*

$$\begin{cases} q + k - \dfrac{\sqrt{q}+5}{4} < n & , q \text{ impar} \\ q + k - \dfrac{2\sqrt{q}+7}{4} < n & , q \text{ par}, \end{cases}$$

entonces, existen $f(x), p(x) \in \mathbb{F}_q[x;\theta]$ con $deg(f(x)) = 2$ y $deg(p(x)) \leq 1$ tales que $(x^i - \lambda)p(x) \not\equiv 0 \ mod\ f(x)$, para todo $\lambda \in \mathbb{F}_q^*$ e $i = 1, \ldots, n-1$.

Demostración. Un $[n, n-k]$-código MDS skew pseudo-cíclico $\mathscr{C} \subseteq \mathbb{F}_q$, por el Teorema 2.1.15 tiene una matriz de control de paridad de la forma $[P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$, con $P \in \mathbb{F}_q^k$, $\tau = \Theta \circ T$ y $T \in GL(k,q)$ tales que $P\tau^n = \alpha P$.
El conjunto

$$\mathcal{K} := \{[P\tau^i] \colon i = 0, \ldots, n-1\} \subseteq \mathbb{P}^{k-1}(\mathbb{F}_q),$$

por el Teorema 1.3.24 forma un n-arco en $\mathbb{P}^{k-1}(\mathbb{F}_q)$. Por los Teoremas 1.2.12 y 1.2.13 y la hipótesis

$$\begin{cases} q - \frac{1}{4}\sqrt{q} + (k-1) - \frac{1}{4} < n & , q \text{ impar} \\ q - \frac{1}{2}\sqrt{q} + (k-1) - \frac{3}{4} < n & , q \text{ par} \end{cases},$$

el conjunto $\mathcal{K}$ vive sobre una única curva racional normal.

Así, a través de una proyectividad dada por $A \in GL(k,q)$ podemos llevar los puntos de $\mathcal{K}$ a la curva racional normal canónica, imagen de la aplicación de Veronese

$$\begin{aligned} \nu_k \colon \mathbb{P}^1(\mathbb{F}_q) &\longrightarrow \quad \mathbb{P}^{k-1}(\mathbb{F}_q) \\ [x_0 : x_1] &\longmapsto [x_0^{k-1} : x_0^{k-2}x_1 : \cdots : x_0x^{k-2} : x^{k-1}] \ . \end{aligned}$$

Luego, tomando $\tau' := A^{-1}\tau A$, podemos definir el conjunto

$$\mathcal{K}' := \{[P\tau^i A] \colon i = 0, \ldots, n-1\} = \{[PA(\tau')^i] \colon i = 0, \ldots, n-1\} \subseteq \mathbb{P}^{k-1}(\mathbb{F}_q),$$

donde $\tau' = A^{-1}(\Theta \circ T)A = \Theta(A_\theta^{-1}TA) = \Theta \circ M'$ con $M' := A_\theta^{-1}TA$. Ahora, consideremos el siguiente diagrama conmutativo

$$\begin{array}{ccc} \mathbb{P}^{k-1}(\mathbb{F}_q) & \xrightarrow{\tau' := \Theta \circ M'} & \mathbb{P}^{k-1}(\mathbb{F}_q) \\ {\scriptstyle \nu_k}\uparrow & & \uparrow{\scriptstyle \nu_k} \\ \mathbb{P}^1(\mathbb{F}_q) & \xrightarrow[\Theta \circ M]{} & \mathbb{P}^1(\mathbb{F}_q) \end{array},$$

con $M \in GL(2,q)$ tal que $(\Theta \circ M) \circ \nu_k = \nu_k \circ \tau'$. De esta forma, podemos identificar los elementos de $\mathcal{K}'$ con los elementos del conjunto

$$\left\{[p(\Theta \circ M)^i] \colon i = 0, \ldots, n-1\right\} \subseteq \mathbb{P}^1(\mathbb{F}_q),$$

donde $[p] = \nu_k^{-1}([PA])$. Notar que $\deg(m_M) = 1, 2$, donde m_M es el polinomio mínimo de M.

Caso 1:

Sea $\deg(m_M) = 1$. Entonces se tiene que $M = \beta I$, para algún $\beta \in \mathbb{F}_q^*$ y esto implica que $\Theta \circ M = \Theta$ en $\mathbb{P}^1(\mathbb{F}_q)$, con $n \leq \operatorname{ord}(\Theta)$. Así, de la hipótesis se deduce que

$$\begin{cases} q + k - \dfrac{\sqrt{q}+5}{4} < n \leq \operatorname{ord}(\Theta) \leq r & , q \text{ impar} \\ q + k - \dfrac{2\sqrt{q}+7}{4} < n \leq \operatorname{ord}(\Theta) \leq r & , q \text{ par}, \end{cases}$$

donde $q = p^r$ para algún $r \in \mathbb{Z}_{\geq 1}$ y p primo. Pero estas desigualdades no se cumplen para ningún q, es decir, este caso no es posible.

Caso 2:

Sea $\deg(m_M) = 2$. La matriz M no es un múltiplo de I. Supongamos que para todo $\vec{v} \in \mathbb{P}^1(\mathbb{F}_q)$ se tiene que $\vec{v}M$ es múltiplo de $\vec{v}$. Luego la proyectividad dada por M lleva

todos los puntos de $\mathbb{P}^1(\mathbb{F}_q)$ en sí mismos. Como $\#\left(\mathbb{P}^1(\mathbb{F}_q)\right) = q+1 > 3$, M es un múltiplo de I, absurdo. Por lo cual, existe $\vec{v} \in \mathbb{P}^1(\mathbb{F}_q)$ tal que $\vec{v}M$ no es un múltiplo de $\vec{v}$. Así $\vec{v}$, $\vec{v}M$ son linealmente independientes y existe $C \in GL(2,k)$ tal que $M = CM_CC^{-1}$ con

$$M_C = \begin{pmatrix} 0 & 1 \\ \gamma & \beta \end{pmatrix}.$$

Ahora, se tiene que $\Theta \circ M = \Theta(CM_CC^{-1}) = C_{\theta^{-1}}(\Theta M_C)C^{-1}$ y de esta forma, podemos considerar el siguiente diagrama conmutativo

$$\begin{array}{ccc} \mathbb{P}^1(\mathbb{F}_q) & \xrightarrow{\Theta\circ M} & \mathbb{P}^1(\mathbb{F}_q) \\ {\scriptstyle C_{\theta^{-1}}}\downarrow & & \uparrow{\scriptstyle C^{-1}} \\ \mathbb{P}^1(\mathbb{F}_q) & \xrightarrow[\Theta\circ M_C]{} & \mathbb{P}^1(\mathbb{F}_q) \end{array}.$$

Así, podemos considerar el conjunto

$$\left\{[\overline{p}(\Theta \circ M_C)^i] \colon i = 0, \ldots, n-1\right\} \subseteq \mathbb{P}^1(\mathbb{F}_q),$$

donde $\overline{p} := pC_{\theta^{-1}}$.

Ahora, sea $f(x)$ el polinomio característico de M_C, es decir, $f(x) = x^2 - \beta x - \gamma$ y consideremos la siguiente biyección

$$\begin{aligned} \pi \colon \quad \mathbb{F}_q^2 \quad &\longrightarrow \mathbb{F}_q[x;\theta]/(x^2 - \beta x - \gamma) := R \\ (v_0, v_1) &\longmapsto \pi(v_0, v_1) = v_0 + v_1 x \end{aligned}$$

Observamos que

$$\begin{aligned} \pi\left(\vec{v}\ (\Theta \circ M_C)\right) &= x \cdot \pi(\vec{v}) \\ &= x(v_0 + v_1 x) \end{aligned}$$

La aplicación π induce la biyección

$$\begin{aligned}\widehat{\pi}\colon \left(\mathbb{F}_q^2 \setminus \{(0,0)\}\right) / \mathbb{F}_q^* &\longrightarrow (R \setminus \{0\}) \ / \mathbb{F}_q^* \\ [(v_0, v_1)] \qquad &\longmapsto \widehat{\pi}[(v_0, v_1)] := [\pi(v_0, v_1)]\end{aligned}.$$

Así, $\widehat{\pi}[\vec{v}\ (\Theta \circ M_C)] = [x(v_0 + v_1 x)]$.

Como $\left(\mathbb{F}_q^2 \setminus \{(0,0)\}\right) / \mathbb{F}_q^* \cong \mathbb{P}^1(\mathbb{F}_q)$, se tiene que para todo $i = 1, \ldots, n-1$

$$\begin{aligned}[\overline{p}] \neq [(\overline{p})(\Theta \circ M_C)^i] &\Longrightarrow \widehat{\pi}[\overline{p}] \neq \widehat{\pi}[(\overline{p}(\Theta \circ M_C)^i] \\ &\Longrightarrow [\pi(\overline{p})] \neq [\pi((\overline{p})(\Theta \circ M_C)^i)] \\ &\Longrightarrow [p(x)] \neq [x^i p(x)] \\ &\Longrightarrow \lambda p(x) \neq x^i \cdot p(x) \qquad (\ \forall \lambda \in \mathbb{F}_q^*) \\ &\Longrightarrow (x^i - \lambda)p(x) \not\equiv 0 \bmod f(x) \qquad (\ \forall \lambda \in \mathbb{F}_q^*)\end{aligned}$$

es decir, existen $f(x), p(x) \in \mathbb{F}_q[x;\theta]$ con $\deg(f(x)) = 2$ y $\deg(p(x)) \leq 1$ tales que $(x^i - \lambda)p(x) \not\equiv \bmod f(x)$, para todo $\lambda \in \mathbb{F}_q^*$ e $i = 1, \ldots, n-1$. □

Observación 2.2.6. Desde la demostración del Teorema 2.2.5, se pueden deducir los siguientes resultados:

(1) Sean $q > 2$, n y k tales que $k = 4, \ldots, n-1$ y

$$\begin{cases} q + k - \dfrac{\sqrt{q}+5}{4} < n & , q \text{ impar} \\ q + k - \dfrac{2\sqrt{q}+7}{4} < n & , q \text{ par} \end{cases}.$$

Entonces existe un $\mathscr{C} \subseteq \mathbb{F}_q^n$ MDS $[n, n-k]$-códgo skew pseudo-cíclico si y sólo si existen $f(x), p(x) \in \mathbb{F}_q[x;\theta]$ con $\deg(f(x)) = 2$ y $\deg(p(x)) \leq 1$ tales que $(x^i - \lambda)p(x) \not\equiv\ 0 \bmod f(x)$, para todo $\lambda \in \mathbb{F}_q^*$ e $i = 1, \ldots, n-1$.

(2) Si existen $f(x), p(x) \in \mathbb{F}_q[x;\theta]$ con $\deg(f(x)) = 2$ y $\deg(p(x)) \leq 1$ tales que $(x^i - \lambda)p(x) \not\equiv\ 0 \bmod f(x)$, para todo $\lambda \in \mathbb{F}_q^*$ e $i = 1, \ldots, n-1$, entonces existe un $\mathscr{C} \subseteq \mathbb{F}_q^n$ MDS $[n, n-k]$-código skew pseudo-cíclico.

El Teorema 2.2.5, se puede extender también para el caso $k = 3$ y q impar, ya que en el plano $\mathbb{P}^2(\mathbb{F}_q)$ los n-arcos con $n > q - \sqrt{q}/4 + 7/4$ están sobre cónicas no singulares (Teoremas 1.2.17 y 1.2.19).

Teorema 2.2.7. *Sea q impar y n tal que*

$$q - \frac{\sqrt{q} - 7}{4} < n.$$

Entonces existe un $\mathscr{C} \subseteq \mathbb{F}_q^n$ MDS $[n, n-3]$-código skew pseudo-cíclico si y sólo si existen $f(x), p(x) \in \mathbb{F}_q[x;\theta]$ con $deg(f(x)) = 2$ y $deg(p(x)) \leq 1$ tales que $(x^i - \lambda)p(x) \not\equiv 0$ mod $f(x)$, para todo $\lambda \in \mathbb{F}_q^*$ e $i = 1, \ldots, n-1$.

Observación 2.2.8. En el caso $k = 3$ y q par, la situación es más compleja, ya que un arco completo máximal tiene $q + 2$ puntos, donde no todos son hiperóvalos regulares (Teorema 1.2.22). Por lo tanto, que su cardinalidad sea mayor que $m'(2, q)$ (Definición 1.2.18) no implica que estos puntos estén sobre una cónica.

Del Teorema 1.2.22, un hiperóvalo de $\mathbb{P}^2(\mathbb{F}_q)$, $q = 2^h$, $h > 0$, es proyectivamente equivalente a un hiperóvalo,

$$\{[F(t) : t : 1] \mid t \in \mathbb{F}_q\} \cup \{[0 : 1 : 0], [1 : 0 : 0]\}, \tag{2.4}$$

donde F es un polinomio de permutación sobre $\mathbb{F}_q$ de grado a lo más $q-2$, que satisface $F(0) = 0$, $F(1) = 1$ y tal que para cada $s \in \mathbb{F}_q$,

$$F_s(x) = \frac{F(x+s) + F(s)}{x},$$

es un polinomio de permutación con $F_s(0) = 0$.

Cuando las condiciones anteriores sean satisfechas para el polinomio F, nos referiremos al hiperóvalo (2.4) como $\mathscr{D}(F)$.

Definición 2.2.9. A menos de proyectividades, llamamos $\mathcal{K}_{\mathscr{C}} \subseteq \mathbb{P}^2(\mathbb{F}_q)$ al conjunto de

puntos de $\mathbb{P}^2(\mathbb{F}_q)$ definidos por las columnas de una matriz de control de paridad de un $[n, n-3]_q$-código $\mathscr{C} \subseteq \mathbb{F}_q^n$.

Teorema 2.2.10. *Sea q par y $n \geq e^2+3$ para algún $e \in \mathbb{Z}_{\geq 2}$. Si existe un $\mathscr{C} \subseteq \mathbb{F}_q^n$ MDS $[n, n-3]$-código skew pseudo-cíclico definido por (τ, P, n), con $\tau = \Theta \circ T$ y $T \in GL(k, q)$, tal que $\mathcal{K}_{\mathscr{C}} \subseteq \mathbb{P}^2(\mathbb{F}_q)$ sea proyectivamente equivalente mediante $A \in GL(3, q)$ a un subconjunto de $\mathcal{G}_{\mathscr{C}} \subseteq \mathscr{D}(F) \subseteq \mathbb{P}^2(\mathbb{F}_q)$ con $deg(F(t)) = m \leq e$, entonces se tiene el siguiente diagrama conmutativo*

$$\begin{array}{ccccc}
\mathcal{K}_{\mathscr{C}} & \xrightarrow{\Theta} & \mathcal{K}_{\mathscr{C}} & \xrightarrow{T} & \mathcal{K}_{\mathscr{C}} \\
\downarrow A & & \downarrow A & & \downarrow A \\
\mathcal{G}_{\mathscr{C}} & \xrightarrow[\Theta]{} & \mathcal{G}_{\mathscr{C}} & \xrightarrow[M]{} & \mathcal{G}_{\mathscr{C}} \\
\uparrow \varphi & & \uparrow \varphi & & \uparrow \varphi \\
\mathbb{P}^1(\mathbb{F}_q) & \xrightarrow[\Theta']{} & \mathbb{P}^1(\mathbb{F}_q) & \xrightarrow[M']{} & \mathbb{P}^1(\mathbb{F}_q)
\end{array},$$

con $[x_0 : x_1]\Theta' = [\theta(x_0) : \theta(x_1)]$, $\varphi\colon \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^2(\mathbb{F}_q)$ *definida por* $[x_0 : x_1]\varphi = \left[x_0^m : x_0^{m-1}x_1 : x_0^m F\left(\frac{x_1}{x_0}\right)\right]$ *y se cumple uno de los siguientes casos:*

a) $m = 2$, $F(t) = t^2$ *y*

(1) $m = 2$, $M = \begin{pmatrix} a_0 & a_1 & \frac{a_1^2}{a_0} \\ 0 & a_2 & 0 \\ 0 & 0 & \frac{a_2^2}{a_0} \end{pmatrix}$ *y* $M' = \begin{pmatrix} a_0 & a_1 \\ 0 & a_2 \end{pmatrix}$, *con* $a_1 \in \mathbb{F}_q$ *y* $a_0, a_2 \in \mathbb{F}_q^*$,

(2) $m = 2$, $M = \begin{pmatrix} b_0^2 & 0 & 0 \\ 0 & b_0 b_1 & 0 \\ 1 & b_1 & b_1 \end{pmatrix}$ *y* $M' = \begin{pmatrix} b_0 & 0 \\ 1 & b_1 \end{pmatrix}$ *con* $b_0 \in \mathbb{F}_q$ *y* $b_1 \in \mathbb{F}_q^*$.

(3) $m = 2$, $M = \begin{pmatrix} 0 & 0 & c_0^2 \\ 0 & c_0 & 0 \\ 1 & c_1 & c_1^2 \end{pmatrix}$ *y* $M' = \begin{pmatrix} 0 & c_0 \\ 1 & c_1 \end{pmatrix}$ *con* $c_1 \in \mathbb{F}_q$ *y* $c_0 \in \mathbb{F}_q^*$.

(b) m *es par y mayor que* 2,

$$M = \begin{pmatrix} 1 & d_0 & F(d_0) \\ 0 & d_1 & 0 \\ 0 & 0 & F(d_0)+F(d_0+d_1) \end{pmatrix} \text{ y } M' = \begin{pmatrix} 1 & d_0 \\ 0 & d_1 \end{pmatrix} \text{ con } d_0 \in \mathbb{F}_q,\ d_1 \in \mathbb{F}_q^*,\ y$$
$$F(d_0) + (F(d_0) + F(d_0+d_1))\, F(t) = F(d_0 + d_1 t), \text{ para todo } t \in \mathbb{F}_q.$$

Demostración. Sea $\mathscr{C}$ un MDS $[n, n-3]$-código skew α-cíclico. Por el Teorema 2.1.15 $\mathscr{C}$ tiene una matriz de control de paridad de la forma $[P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$, con $P \in \mathbb{F}_q^3$, $\tau = \Theta \circ T$ y $T \in GL(3,q)$ tal que $P\tau^n = \alpha P$. Esta matriz de control de paridad define un n-arco $\mathcal{K}_{\mathscr{C}}$ en $\mathbb{P}^2(\mathbb{F}_q)$ y por hipótesis este es proyectivamente equivalente a un conjunto $\mathcal{G}_{\mathscr{C}}$ tal que

$$\mathcal{G}_{\mathscr{C}} \subseteq \{[1 : t : F(t)] \mid t \in \mathbb{F}_q\} \cup \{[0:1:0], [0:0:1]\} := \mathscr{D}(F) \subseteq \mathbb{P}^2(\mathbb{F}_q).$$

Sea $A \in GL(3,q)$ la matriz que define la proyectividad que lleva los puntos de $\mathcal{K}_{\mathscr{C}}$ en $\mathcal{G}_{\mathscr{C}}$. Así, se tiene el siguiente diagrama conmutativo

$$\begin{array}{ccccc} \mathcal{K}_{\mathscr{C}} & \xrightarrow{\Theta} & \mathcal{K}_{\mathscr{C}} & \xrightarrow{T} & \mathcal{K}_{\mathscr{C}} \\ \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A} & & \downarrow{\scriptstyle A} \\ \mathcal{G}_{\mathscr{C}} & \xrightarrow[\Theta]{} & \mathcal{G}_{\mathscr{C}} & \xrightarrow[M]{} & \mathcal{G}_{\mathscr{C}} \end{array}.$$

Haciendo el cambio de variables $t = \frac{x_1}{x_0}$ los puntos de la forma $[1 : t : F(t)]$ los podemos escribir como $\left[1 : \frac{x_1}{x_0} : F\left(\frac{x_1}{x_0}\right)\right] = \left[x_0^m : x_0^{m-1}x_1 : x_0^m F\left(\frac{x_1}{x_0}\right)\right] \in \mathbb{P}^2(\mathbb{F}_q)$ con m igual al grado de $F(t)$, par y menor o igual a $q-2$.

Luego, podemos considerar la aplicación inyectiva

$$\begin{aligned} \varphi\colon \mathbb{P}^1(\mathbb{F}_1) &\longrightarrow \mathbb{P}^2(\mathbb{F}_q) \\ [x_0 : x_1] &\longmapsto [x_0 : x_1]\varphi = \left[x_0^m : x_0^{m-1}x_1 : x_0^m F\left(\frac{x_1}{x_0}\right)\right], \end{aligned}$$

Cuya imagen vive en la curva plana $\Gamma\colon G(z_0, z_1, z_2) = 0$, donde

$$G(z_0, z_1, z_2) := z_0^{m-1} z_2 + z_0^m F\left(\frac{z_1}{z_0}\right).$$

Esta es una curva de grado m, donde el punto $N := [0 : 1 : 0] \notin \Gamma$ y

$$\mathcal{G}_{\mathscr{C}} \subseteq \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{F}_q) \colon G(x_0, x_1, x_2) = 0\} \cup \{N\}.$$

Considerando la matriz de control de paridad $[(P\tau)_t, (P\tau^2)_t, (P\tau^3)_t, \ldots, (P\tau^n)_t]$ esta define un n-arco $\mathcal{K}'_{\mathscr{C}} \subseteq \mathbb{P}^2(\mathbb{F}_q)$, análogamente al caso anterior, es proyectivamente equivalente a

$$\mathcal{G}'_{\mathscr{C}} \subseteq \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{F}_q) \colon G'(x_0, x_1, x_2) = 0\} \cup \{N'\},$$

donde $G' = G \circ \tau^{-1}$ y como $0 \neq G'(N') = G \circ \tau^{-1}(N') = G(N'\tau^{-1})$, se tiene que $N' = N\tau$. Llamando además $\Gamma' \colon G'(z_0, z_1, z_2) = 0$, se tiene que $\#(\Gamma \cap \Gamma') \geq n - 2$, ya que Γ y Γ' comparten por lo menos los puntos $\mathcal{G}_{\mathscr{C}}$ distintos de N y N'.

Caso 1:

Supongamos que $m = 2$. Luego, $F(t) = t^2$ y esto implica que $G(z_0, z_1, z_2) = z_0 z_2 + z_1^2 = 0$. Además, por hipótesis $n - 2 > 4$ por lo cual las cónicas Γ y Γ' coinciden, lo que implica que $\mathcal{K}_{\mathscr{C}}$ es proyectivamente equivalente a un conjunto $\mathcal{G}_{\mathscr{C}}$ tal que

$$\mathcal{G}_{\mathscr{C}} \subseteq \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{F}_q) \colon G(x_0, x_1, x_2) = 0\}.$$

Esto permite obtener una relación entre los puntos de $\mathcal{G}_{\mathscr{C}}$ y los puntos de la recta proyectiva $\mathbb{P}_1(\mathbb{F}_q)$, y tener además el siguiente diagrama conmutativo

$$\begin{array}{ccccc} \mathcal{G}_{\mathscr{C}} & \xrightarrow{\Theta} & \mathcal{G}_{\mathscr{C}} & \xrightarrow{M} & \mathcal{G}_{\mathscr{C}} \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} \\ \mathbb{P}^1(\mathbb{F}_q) & \xrightarrow[\Theta']{} & \mathbb{P}^1(\mathbb{F}_q) & \xrightarrow[M']{} & \mathbb{P}^1(\mathbb{F}_q) \end{array},$$

donde $[a_0 : a_1]\Theta' = [\theta(a_0) : \theta(a_1)]$, para todo $[a_0 : a_1] \in \mathbb{P}^1(\mathbb{F}_q)$, $M' \in GL(2, q)$ y la

aplicación φ está definida por

$$\begin{aligned}\varphi\colon \mathbb{P}^1(\mathbb{F}_1) &\longrightarrow \mathbb{P}^2(\mathbb{F}_q)\\ [x_0 : x_1] &\longmapsto [x_0 : x_1]\varphi = \left[x_0^2 : x_0x_1 : x_1^2\right].\end{aligned}$$

Podemos considerar que las matrices M y M' están dadas por

$$M = \begin{pmatrix} a_{00} & a_{01} & a_{02}\\ a_{10} & a_{11} & a_{12}\\ a_{20} & a_{21} & a_{22}\end{pmatrix} \quad \text{y} \quad M' = \begin{pmatrix} b_{00} & b_{01}\\ b_{10} & b_{11}\end{pmatrix}.$$

Ahora, analizando el caso

$$\begin{array}{ccc} [0:0:1] & \xrightarrow{M} & [a_{20} : a_{21} : a_{22}] \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} \\ [0:1] & \xrightarrow[M']{} & [a:b] \end{array},$$

podemos estudiar por separado cuando $a = 0$ y $a \neq 0$, en este último caso se puede separar a su vez en $q > 4$ y $q = 4$, y tomando $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, el caso $q = 4$ se puede analizar para los distintos valores de b_{00}.

$(a = 0)$ Tenemos que $[a_{20} : a_{21} : a_{22}] = [0 : 0 : a_{22}]$, con $a_{22} \neq 0$. Además, como $[0 : 1]M' = [0 : 1]$ se tiene que $b_{10} = 0$, así

$$M' = \begin{pmatrix} b_{00} & b_{01}\\ 0 & b_{11}\end{pmatrix}$$

se tiene que $b_{00}, b_{11} \neq 0$. Luego, considerando el punto $[1 : t]$ para todo $t \in \mathbb{F}_q$, podemos obtener que

$$\begin{aligned} b_{00} &= \lambda(t) \cdot (a_{00} + a_{10}t + a_{20}t^2)\\ b_{01} + b_{11}t &= \lambda(t) \cdot (a_{01} + a_{11}t + a_{21}t^2),\end{aligned}$$

con $\lambda(t) \in \mathbb{F}_q^*$. Así, podemos escribir

$$\frac{b_{01}+b_{11}t}{b_{00}} = \frac{a_{01}+a_{11}t+a_{21}t^2}{a_{00}+a_{10}t+a_{20}t^2},$$

lo que implica que

$$(b_{11}a_{20})t^3+(b_{01}a_{20}+b_{11}a_{10}+b_{00}a_{21})t^2+(b_{01}a_{10}+b_{11}a_{00}+b_{00}a_{11})t+(b_{01}a_{00}+b_{00}a_{01}) = 0$$

para todo $t \in \mathbb{F}_q$. Como la ecuación anterior se divide por $t^q - t = \prod_{\alpha_i \in \mathbb{F}_q} (t-\alpha_i)$ y $q \geq 4$, cada factor debe ser 0. Así, el factor $(b_{11}a_{20}) = 0$ y como $b_{01} \neq 0$ se tiene que $a_{20} = a_{21} = 0$. Luego, se deduce también que $b_{11}a_{00} = b_{00}a_{11}$ y $b_{01}a_{00} = b_{00}a_{01}$ y las matrices están dadas por

$$M = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ 0 & a_{11} & a_{12} \\ 0 & 0 & a_{22} \end{pmatrix}, \quad M' = \begin{pmatrix} a_{00} & a_{01} \\ 0 & a_{11} \end{pmatrix}.$$

Utilizando estas matrices, ahora se tiene que

$$\begin{array}{ccc} [1:t:t^2] & \xrightarrow{M} & [a_{00}:a_{01}+a_{11}t:a_{02}+a_{12}t+a_{22}t^2] \\ \uparrow \varphi & & \uparrow \varphi \\ [1:t] & \xrightarrow[M']{} & [a_{00}:a_{01}+a_{11}t] \end{array}.$$

Como

$$\begin{aligned} [a_{00}:a_{01}+a_{11}t]\varphi &= \left[1:\frac{a_{01}+a_{11}t}{a_{00}}\right]\varphi \\ &= \left[1:\frac{a_{01}+a_{11}t}{a_{00}}:\frac{a_{01}^2+a_{11}^2t^2}{a_{00}^2}\right] \\ &= \left[a_{00}:a_{01}+a_{11}t:\frac{a_{01}^2+a_{11}^2t^2}{a_{00}}\right], \end{aligned}$$

se deduce que $a_{02}+a_{12}t+a_{22}t^2 = \frac{a_{01}^2+a_{11}^2t^2}{a_{00}}$, es decir $a_{12} = 0$, $a_{02} = \frac{a_{01}^2}{a_{00}}$ y $a_{22} = \frac{a_{11}^2}{a_{00}}$.

Por lo tanto,

$$M = \begin{pmatrix} a_{00} & a_{01} & \frac{a_{01}^2}{a_{00}} \\ 0 & a_{11} & 0 \\ 0 & 0 & \frac{a_{11}^2}{a_{00}} \end{pmatrix}, \quad M' = \begin{pmatrix} a_{00} & a_{01} \\ 0 & a_{11} \end{pmatrix}, \quad \text{con } a_{00}, a_{11} \neq 0,$$

y esto nos da el caso (1) del teorema.

$(a \neq 0,\ q > 4)$ En este caso, podemos considerar el siguiente diagrama

$$\begin{array}{ccc} [0:0:1] & \xrightarrow{M} & [a_{20}:a_{21}:a_{22}] \\ \uparrow\varphi & & \uparrow\varphi \\ [0:1] & \xrightarrow[M']{} & [1:\gamma] \end{array},$$

con $[a:b] = [1:\gamma]$. Así, las matrices están dadas por

$$M = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ 1 & \gamma & \gamma^2 \end{pmatrix}, \quad M' = \begin{pmatrix} b_{00} & b_{01} \\ 1 & \gamma \end{pmatrix}.$$

Como $([1:t]\varphi)\,M = ([1:t]M')\varphi$, si $t = b_{00}$ se tiene las siguientes igualdades

(1') $a_{00} + a_{10}b_{00} + b_{00}^2 = 0$,

(2') $a_{01} + a_{11}b_{00} + \gamma b_{00}^2 = 0$.

Si $t \neq b_{00}$ se tiene que

$$\begin{aligned} &[a_{00} + a_{10}t + t^2 : a_{01} + a_{11}t + \gamma t^2 : a_{02} + a_{12}t + \gamma^2 t^2] \\ &\qquad = [b_{00}^2 + t^2 : b_{00}b_{01} + (b_{00}\gamma + b_{01})t + \gamma t^2 : b_{01}^2 + \gamma^2 t^2], \quad (2.5) \end{aligned}$$

lo que se traduce en las igualdades

$$\frac{a_{01} + a_{11}t + \gamma t^2}{a_{00} + a_{10}t + t^2} = \frac{b_{01} + \gamma t}{b_{00} + t}, \qquad \frac{b_{01}^2 + \gamma^2 t^2}{b_{00}^2 + t^2} = \frac{a_{02} + a_{12}t + \gamma^2 t^2}{a_{00} + a_{10}t + t^2}.$$

De la primera igualdad, se tiene

(3') $a_{01}b_{00} = a_{00}b_{01}$,

(4') $a_{01} + a_{11}b_{00} = \gamma a_{00} + a_{10}b_{01}$,

(5') $a_{11} + \gamma b_{00} = \gamma a_{10} + b_{01}$.

Para la segunda igualdad, como es válida para todo $t \neq b_{00}$ y $q > 4$, el polinomio obtenido es idénticamente cero y así se tienen las igualdades

(6') $a_{00}b_{01}^2 = a_{02}b_{00}^2$,

(7') $b_{01}^2 a_{10} = a_{12}b_{00}^2$,

(8') $b_{01}^2 + \gamma^2 a_{00} = a_{02} + b_{00}^2\gamma^2$,

(9') $\gamma^2 a_{10} = a_{12}$.

Considerando todas estas ecuaciones, con $q > 4$, para todo $\gamma \in \mathbb{F}_q$ y $b_{00} \neq 0$, las matrices podemos escribirlas como

$$M = \begin{pmatrix} b_{00}^2 & 0 & 0 \\ 0 & \gamma b_{00} & 0 \\ 1 & \gamma & \gamma^2 \end{pmatrix}, \quad M' = \begin{pmatrix} b_{00} & 0 \\ 1 & \gamma \end{pmatrix},$$

de esta forma, obtenemos el caso (2) del teorema.

($a \neq 0$, $q = 4$, $b_{00} = 0$) Las ecuaciones (1') a (5') del caso anterior, también son válidas con $q = 4$, usando ademas que $b_{00} = 0$, se tiene que

- $a_{00}b_{01} = 0$,
- $a_{11} = \gamma a_{10} + b_{01}$,
- $a_{01} = 0$.
- $a_{01} = \gamma a_{00} + a_{10}b_{01}$,
- $a_{00} = 0$,

Reemplazando los valores de a_{00} y a_{01}, se tiene que $a_{10}b_{01} = 0$ y como $b_{01} \neq 0$, necesariamente $a_{10} = 0$. Así, desde la expresión (2.5) se obtiene que $a_{02} = b_{01}^2 + a_{12}t$,

para todo $t \in \mathbb{F}_q$, por lo tanto $a_{12} = 0$. Con esto, las matrices están dadas por

$$M = \begin{pmatrix} 0 & 0 & a_{11}^2 \\ 0 & a_{11} & 0 \\ 1 & \gamma & \gamma^2 \end{pmatrix}, \quad M' = \begin{pmatrix} 0 & a_{11} \\ 1 & \gamma \end{pmatrix},$$

y de esta manera, tenemos el caso (3) del teorema.

$(a \neq 0,\ q = 4,\ b_{00} = 1)$ Considerando la igualdad

$$\frac{b_{01}^2 + \gamma t^2}{b_{00}^2 + t^2} = \frac{a_{02} + a_{12}t + \gamma t^2}{a_{00} + a_{10}t + t^2},$$

se tiene que

$$\left(b_{01}^2 a_{00} + a_{02} b_{00}^2\right) + \left(b_{01}^2 a_{10} + a_{12} b_{00}^2\right) t + \\ + \left(b_{01}^2 + a_{00}\gamma^2 + b_{00}^2\gamma^2 + a_{02}\right) t^2 + \left(a_{12} + \gamma^2 a_{10}\right) t^3 = 0. \quad (2.6)$$

Como esta ecuación es válida para todo $t \neq b_{00} = 1$, su parte izquierda debe ser igual a

$$\lambda\left(t(t+\omega)(t+\omega^2)\right) = \lambda\left(t + t + t^3\right), \quad (2.7)$$

con $\lambda \in \mathbb{F}_4^*$, ya que estas son del mismo grado y son validas para $t \in \{0, \omega, \omega^2\}$ deben diferir a lo más por una constante. Así, además de las 5 ecuaciones (1')-(5') usadas en los casos anteriores, se tiene que

- $a_{12} + \gamma^2 a_{10} = \lambda$,
- $b_{01}^2 + a_{00}\gamma^2 + \gamma^2 + a_{02} = \lambda$,
- $b_{01}^2 a_{10} + a_{12} = \lambda$,
- $b_{01}^2 a_{00} + a_{02} = 0$.

Dado que $a_{02} = a_{00}b_{01}^2$, $a_{10} = a_{00} + 1$ y $a_{12} + \lambda = \gamma^2 a_{10} = b_{01}^2 a_{10}$ se tiene

$$\begin{aligned} b_{01}^2 + a_{00}\gamma^2 + \gamma^2 + a_{02} = \lambda &\Longrightarrow b_{01}^2 + a_{00}\gamma^2 + \gamma^2 + a_{00}b_{01}^2 = \lambda \\ &\Longrightarrow b_{01}^2(1 + a_{00}) + \gamma^2(1 + a_{00}) = \lambda \\ &\Longrightarrow b_{01}^2 a_{10} + \gamma^2 a_{10} = \lambda \\ &\Longrightarrow a_{12} + \lambda + a_{12} + \lambda = \lambda \\ &\Longrightarrow 0 = \lambda. \end{aligned}$$

Como la última igualdad es una contradicción, se tiene que necesariamente $b_{00} \neq 1$.

$(a \neq 0,\ q = 4,\ b_{00} = \omega)$ En este caso, la parte izquierda de 2.6 debe ser igual

$$\lambda\left(t(t+1)(t+\omega^2)\right) = \lambda\left(\omega^2 t + \omega t + t^3\right),$$

con $\lambda \in \mathbb{F}_4^*$. Similar al caso anterior, ahora tenemos las siguientes igualdades

(1") $a_{12} + \gamma a_{10} = \lambda$,

(2") $b_{01}^2 + a_{00}\gamma^2 + \omega^2\gamma^2 + a_{02} = \lambda\omega$,

(3") $b_{01}^2 a_{10} + a_{12}\omega^2 = \lambda\omega^2$,

(4") $b_{01}^2 a_{00} + a_{02}\omega^2 = 0$.

De aquí, se tiene que $\omega \cdot b_{01}^2 \cdot a_{10} = \gamma^2 \cdot a_{10}$.

Si $a_{10} = 0$, de la ecuación (4') se tiene que $a_{00} = \omega^2$. Luego, de la ecuación (4") se tiene que $a_{02} = b_{01}^2$ y así, al reemplazar en (2"), se tiene que $\lambda\omega = 0$, lo cual no es posible.

Si $a_{10} \neq 0$, se debe tener que $\omega \cdot b_{01}^2 = \gamma^2$, es decir $b_{01} = \omega\gamma$ y considerando la ecuación (4"), $a_{02} = \gamma^2 a_{00}$. Reemplazando estos valores en (2"), se tiene que $\lambda\omega = 0$, lo cual tampoco es posible.

Por lo tanto, necesariamente $b_{00} \neq \omega$.

$(a \neq 0,\ q = 4,\ b_{00} = \omega^2)$ De manera análoga al caso anterior, se obtiene que b_{00} no puede tomar tampoco el valor ω^2.

Caso 2:

Supongamos que $m \geq 4$. Luego la curva $G(z_0, z_1, z_2) := z_0^{m-1} z_2 + z_0^m F\left(\frac{z_1}{z_0}\right)$ tiene un punto singular, el cual podemos obtener al igualar a cero sus derivadas parciales (ver [44], Lemma 2.10):

$$\frac{\partial G}{\partial z_0} = (m-1) z_0^{m-2} z_2 + m z_0^{m-1} F\left(\frac{z_1}{z_0}\right) + z_0^{m-2} F'\left(\frac{z_1}{z_0}\right) z_1 = 0 \ ,$$

$$\frac{\partial G}{\partial z_1} = z_0^{m-1} F'\left(\frac{z_1}{z_0}\right) = 0 \ ,$$

$$\frac{\partial G}{\partial z_2} = z_0^{m-1} = 0 \ .$$

Notar que la curva G es irreducible, de grado m y tiene un solo punto singular dado por $[0:0:1]$. Además, de manera similar se puede probar que G' también es una curva irreducible, de grado m y tiene el mismo punto singular $[0:0:1]$. Por lo tanto, $[0:0:1]$ es invariante bajo $\tau = \Theta \circ M$ y como $[0:1:0]$ no pertenece $\mathcal{G}_{\mathscr{C}}$, tampoco pertenece a ${\mathcal{G}'}_{\mathscr{C}}$, es decir, $[0:1:0]$ también es invariante bajo τ. Más aún, se tiene que la recta que contiene a los puntos $[0:0:1]$ y $[0:1:0]$ es invariante bajo τ.

Sabemos además, que $\mathcal{G}_{\mathscr{C}} \subseteq \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{F}_q) \colon G(x_0, x_1, x_2) = 0\} \cup \{[0:1:0]\}$, donde la cardinalidad de $\mathcal{G}_{\mathscr{C}}$ es n y $\mathcal{G}_{\mathscr{C}}(\Theta \circ M) = \mathcal{G}_{\mathscr{C}}$.

Considerando la hipótesis $n \geq e^2 + 3$ y que $m \leq e$, se tiene que

$$\#(\Gamma \cap \Gamma') \geq n - 2 \geq e^2 + 1 > e^2 \geq m^2.$$

Por lo tanto, por el Teorema de Bezout (ver [23], Theorem 25.1), se tiene que $\Gamma = \Gamma'$ y lo que implica que $\mathcal{K}_{\mathscr{C}}$ es proyectivamente equivalente a un conjunto $\mathcal{G}_{\mathscr{C}}$ tal que

$$\mathcal{G}_{\mathscr{C}} \subseteq \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(\mathbb{F}_q) \colon G(x_0, x_1, x_2) = 0\}.$$

Esto permite obtener una relación entre los puntos de $\mathcal{G}_{\mathscr{C}}$ y los puntos de la recta proyectiva $\mathbb{P}_1(\mathbb{F}_q)$, y tener además el siguiente diagrama conmutativo

$$\begin{array}{ccccc} \mathcal{G}_{\mathscr{C}} & \xrightarrow{\Theta} & \mathcal{G}_{\mathscr{C}} & \xrightarrow{M} & \mathcal{G}_{\mathscr{C}} \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} \\ \mathbb{P}^1(\mathbb{F}_q) & \xrightarrow[\Theta']{} & \mathbb{P}^1(\mathbb{F}_q) & \xrightarrow[M']{} & \mathbb{P}^1(\mathbb{F}_q) \end{array},$$

donde $[a_0 : a_1]\Theta' = [\theta(a_0) : \theta(a_1)]$, para todo $[a_0 : a_1] \in \mathbb{P}^1(\mathbb{F}_q)$ y $M' \in GL(2, q)$.

Con $m \geq 4$, sabemos que φ está dada por

$$\begin{aligned} \varphi\colon \mathbb{P}^1(\mathbb{F}_1) &\longrightarrow \mathbb{P}^2(\mathbb{F}_q) \\ [x_0 : x_1] &\longmapsto [x_0 : x_1]\varphi = \left[x_0^m : x_0^{m-1}x_1 : x_0^m F\left(\frac{x_1}{x_0}\right)\right]. \end{aligned}$$

Además, se tiene que el punto singular de $G(z_0, z_1, z_2) = 0$ y $N = [0 : 1 : 0]$ son invariantes bajo $\Theta \circ M$, es decir, $[0 : 0 : 1](\Theta \circ M) = [0 : 0 : 1]$ y $[0 : 1 : 0](\Theta \circ M) = [0 : 1 : 0]$. Así, podemos considerar que la matriz M está dada por

$$M = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ 0 & a_{11} & 0 \\ 0 & 0 & a_{22} \end{pmatrix}.$$

Considerando el diagrama

$$\begin{array}{ccc} [0 : 0 : 1] & \xrightarrow{M} & [0 : 0 : 1] \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} \\ [0 : 1] & \xrightarrow[M']{} & [0 : 1] \end{array},$$

se tiene necesariamente que $b_{10} = 0$ y $b_{00}, b_{11} \neq 0$, es decir, la matriz M' está dada por

$$M' = \begin{pmatrix} b_{00} & b_{01} \\ 0 & b_{11} \end{pmatrix}.$$

Así, considerando un punto cualquiera $[1 : t]$, con $t \in \mathbb{F}_q$, se tiene el siguiente diagrama

$$\begin{array}{ccc} [1 : t : F(t)] & \xrightarrow{M} & [a_{00} : a_{01} + a_{11}t : a_{02} + a_{22}F(t)] \\ \uparrow{\scriptstyle \varphi} & & \uparrow{\scriptstyle \varphi} \\ [1 : t] & \xrightarrow[M']{} & [b_{00} : b_{01} + b_{11}t] \end{array} .$$

Además, $[b_{00} : b_{01} + b_{11}t]\varphi = \left[b_{00}^m : b_{00}^{m-1}(b_{01} + b_{11}t) : b_{00}^m F\left(\frac{b_{01} + b_{11}t}{b_{00}}\right)\right]$. Por lo tanto, existe $\lambda \in \mathbb{F}_q^*$ tal que

- $a_{00} = \lambda \cdot b_{00}^m \neq 0$,
- $a_{01} + a_{11}t = \lambda \cdot b_{00}^{m-1}(b_{01} + b_{11}t)$,
- $a_{02} + a_{22}F(t) = \lambda \cdot b_{00}^m F\left(\frac{b_{01} + b_{11}t}{b_{00}}\right)$.

De esto, tenemos que para todo $t \in \mathbb{F}_q$ se cumple la igualdad

$$\frac{a_{01} + a_{11}t}{a_{00}} = \frac{b_{01} + b_{11}t}{b_{00}} .$$

Así, se tiene que

- $a_{01} = \frac{b_{01}}{b_{00}} \cdot a_{00}$,
- $a_{11} = \frac{b_{11}}{b_{00}} \cdot a_{00}$.

Luego,

$$F\left(\frac{b_{01} + b_{11}t}{b_{00}}\right) = \frac{a_{02}}{a_{00}} + \frac{a_{22}}{a_{00}}F(t).$$

Como $a_{00} = \lambda b_{00}^n \neq 0$, implica que $a_{00} = 1$. Así $F(a_{01} + a_{11}t) = a_{02} + a_{22}F(t)$ para todo $t \in \mathbb{F}_q$. Como F es un polinomio de permutación que define un hiperóvalo se tiene que $\deg(F(t)) = m \leq q - 2$, $F(0) = 0$ y $F(1) = 1$, así podemos deducir que

- $a_{02} = F\left(\frac{b_{01}}{b_{00}}\right)$,
- $a_{22} = F\left(\frac{b_{01}}{b_{00}}\right) + F\left(\frac{b_{01} + b_{11}}{b_{00}}\right)$.

Finalmente, llamando $\alpha := \frac{b_{01}}{b_{00}}$ y $\beta := \frac{b_{11}}{b_{00}}$, las matrices M y M' se pueden escribir

como

$$M = \begin{pmatrix} 1 & \alpha & F(\alpha) \\ 0 & \beta & 0 \\ 0 & 0 & F(\alpha) + F(\alpha+\beta) \end{pmatrix}, \qquad M' = \begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix},$$

con $F(\alpha) + (F(\alpha) + F(\alpha+\beta))\, F(t) = F(\alpha + \beta t)$, para todo $t \in \mathbb{F}_q$ y así, finalmente tener el caso (b) del teorema.

□

Similar a los Teoremas 2.2.5 y 2.2.7, como en la demostración del Teorema 2.2.10 la función φ relaciona un conjunto en $\mathbb{P}^2(\mathbb{F}_q)$ con $\mathbb{P}^1(\mathbb{F}_q)$ se puede tener una tesis de tipo algebraica.

Proposición 2.2.11. *Sea q par y $n \geq e^2 + 3$ para algún $e \in \mathbb{Z}_{\geq 2}$. Si existe un $\mathscr{C} \subseteq \mathbb{F}_q^n$ MDS $[n, n-3]$-código skew pseudo-cíclico definido por (τ, P, n), tal que $\mathcal{K}_{\mathscr{C}}$ sea proyectivamente equivalente a un subconjunto de $\mathscr{D}(F)$ con $deg(F(t)) = m \leq e$, entonces existen $f(x) \in \mathbb{F}_q[x;\theta]$ de grado 2 y $p(x) \in \mathbb{F}_q[x;\theta]$ con $deg(p(x)) \leq 1$ tales que $(x^i - \lambda)p(x) \not\equiv 0 \ mod\ f(x)$, para todo $\lambda \in \mathbb{F}_q^*$ e $i = 1, \ldots, n-1$.*

Demostración. Sea $\mathscr{C}$ un MDS $[n, n-3]$-código skew α-cíclico. Considerando las notaciones del Teorema 2.2.10, las columnas de la matriz de control de paridad, forman un n-arco en $\mathbb{P}^2(\mathbb{F}_q)$ proyectivamente equivalente a $\mathcal{G}_{\mathscr{C}} \subseteq \mathscr{D}(F)$.

Además, como también se mostró en el Teorema 2.2.10, mediante la aplicación inyectiva

$$\begin{aligned} \varphi \colon \mathbb{P}^1(\mathbb{F}_1) &\longrightarrow \mathbb{P}^2(\mathbb{F}_q) \\ [x_0 : x_1] &\longmapsto [x_0 : x_1]\varphi = \left[x_0^m : x_0^{m-1}x_1 : x_0^m F\left(\frac{x_1}{x_0}\right) \right], \end{aligned}$$

podemos relacionar los puntos de $\mathcal{G}_{\mathscr{C}}$ con los puntos de la recta proyectiva $\mathbb{P}^1(\mathbb{F}_q)$.

Como $\mathbb{P}^1(\mathbb{F}_q) = \left(\mathbb{F}_q^2 \setminus \{(0,0)\}\right) / \mathbb{F}_q^*$, con la notación del Teorema 2.2.5, podemos

considerar la aplicación

$$\begin{aligned}\widehat{\pi}\colon \left(\mathbb{F}_q^2 \setminus \{(0,0)\}\right) / \mathbb{F}_q^* &\longrightarrow (R \setminus \{0\}) \ / \mathbb{F}_q^* \\ [(v_0, v_1)] &\longmapsto \widehat{\pi}[(v_0, v_1)] := [\pi(v_0, v_1)]\end{aligned} .$$

Así, de manera totalmente análoga al Teorema 2.2.5, se muestra que existen $f(x) \in \mathbb{F}_q[x;\theta]$ de grado 2 y $p(x) \in \mathbb{F}_q[x;\theta]$ con $\deg(p(x)) \leq 1$ tales que $(x^i - \lambda)p(x) \not\equiv 0 \bmod f(x)$, para todo $\lambda \in \mathbb{F}_q^*$ e $i = 1, \ldots, n-1$. □

Teorema 2.2.12. *Sea $\mathscr{C}$ un $[n,k]_q$-código skew pseudo-cíclico, con $k \geq 2$ y sea*

$$g(x) = l.m.c.m.\left\{x - \eta^{q^{i-1}} : i = 1, \ldots, k\right\} \in \mathbb{F}_q[x;\theta] \ ,$$

para algún $\eta \in \mathbb{F}_{q^k}^*$, el polinomio generador del código dual $\mathscr{C}^\perp$. Entonces $\mathscr{C}$ es MDS si y sólo si $\det\left[\mathcal{N}_{i_j}^\theta\left(\eta^{q^{l-1}}\right)\right]_{1\leq j,l\leq k} \neq 0$, para cualquier $i_1, \ldots, i_k$ distintos entre ellos con $0 \leq i_j \leq n-1$ y $\mathcal{N}_{i_j}^\theta$ es la evaluación residual derecha (Definición 1.1.52).

Demostración.

"$\Rightarrow$"

Sea $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_k x^k$ con $g_k \neq 0$ y H la matriz generadora de $\mathscr{C}^\perp$, o sea

$$H = \begin{pmatrix} g_0 & g_1 & \cdots & g_k & 0 & 0 & \cdots & 0 \\ 0 & \theta(g_0) & \theta(g_1) & \cdots & \theta(g_k) & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \theta^{n-k-1}(g_0) & \theta^{n-k-1}(g_1) & \cdots & \cdots & \theta^{n-k-1}(g_k) \end{pmatrix}.$$

Por simplicidad, sean $\eta_i := \eta^{q^{i-1}}$ y

$$\mathcal{N}_k := \begin{pmatrix} \mathcal{N}_0^\theta(\eta_1) & \mathcal{N}_1^\theta(\eta_1) & \cdots & \mathcal{N}_{n-1}^\theta(\eta_1) \\ \mathcal{N}_0^\theta(\eta_2) & \mathcal{N}_1^\theta(\eta_2) & \cdots & \mathcal{N}_{n-1}^\theta(\eta_2) \\ \vdots & \vdots & & \vdots \\ \mathcal{N}_0^\theta(\eta_k) & \mathcal{N}_1^\theta(\eta_k) & \cdots & \mathcal{N}_{n-1}^\theta(\eta_k) \end{pmatrix},$$

donde $\mathcal{N}_j^\theta(\eta_i)$ para $i = 1, \ldots, k$ y $j = 0, \ldots, n-1$, corresponde a la Definición 1.1.52. Notar que

$$\begin{aligned} \mathcal{N}_s^\theta(\eta_i) &= \theta(\mathcal{N}_{s-1}^\theta(\eta_i))\eta_i \\ &= \theta\left(\theta(\mathcal{N}_{s-2}^\theta(\eta_i))\eta_i\right)\eta_i = \theta^2\left(\mathcal{N}_{s-2}^\theta(\eta_i)\right)\theta(\eta_i)\eta_i \\ &= \theta^j(\mathcal{N}_{s-j}^\theta(\eta_i))\theta(\eta_i)^{j-1}\cdots\theta(\eta_i)\eta_i \quad . \end{aligned}$$

Así,

$$\begin{aligned} 0 &= g_0\mathcal{N}_0^\theta(\eta_i) + g_1\mathcal{N}_1^\theta(\eta_i) + \cdots + g_k\mathcal{N}_k^\theta(\eta_i) = g(\eta_i) \\ 0 &= \theta(g_0)\theta(\mathcal{N}_0^\theta(\eta_i))\eta_i + \theta(g_1)\theta(\mathcal{N}_1^\theta(\eta_i))\eta_i + \cdots + \theta(g_k)\theta(\mathcal{N}_k^\theta(\eta_i))\eta_i \\ 0 &= \theta^2(g_0)\theta^2(\mathcal{N}_0^\theta(\eta_i))\theta(\eta_i)\eta_i + \theta^2(g_1)\theta^2(\mathcal{N}_1^\theta(\eta_i))\theta(\eta_i)\eta_i + \cdots + \theta^2(g_k)\theta^2(\mathcal{N}_k^\theta(\eta_i))\theta(\eta_i)\eta_i \\ &\vdots \\ 0 &= \theta^s(g_0)\theta^s(\mathcal{N}_0^\theta(\eta_i))\theta(\eta_i)^{s-1}\cdots\theta(\eta_i)\eta_i + \theta^s(g_1)\theta^s(\mathcal{N}_1^\theta(\eta_i))\theta(\eta_i)^{s-1}\cdots\theta(\eta_i)\eta_i + \\ &\qquad + \cdots + \theta^s(g_k)\theta^s(\mathcal{N}_k^\theta(\eta_i))\theta(\eta_i)^{s-1}\cdots\theta(\eta_i)\eta_i \ . \end{aligned}$$

Como $\deg(g(x)) = k$ ya que la $\dim\mathscr{C}^\perp = n - k$, se tiene que $\text{rank}V^\theta(\{\eta_1, \ldots, \eta_k\}) = \deg(g(x)) = k$ (ver [21], página 334, §7), es decir $\text{rank}(\mathcal{N}_k) = k$. Luego la matriz $\mathcal{N}_k$ es una matriz generadora del span de $\mathscr{C}$ en $\mathbb{F}_{q^k}$, ya que $H \cdot (\mathcal{N}_k)_t = O$.

Por contradicción, supongamos sin perdida de generalidad que existe en $\mathcal{N}_k$ una

sub-matriz cuadrada

$$S_k = \begin{pmatrix} \mathcal{N}_{j_1}^{\theta}(\eta_1) & \mathcal{N}_{j_2}^{\theta}(\eta_1) & \cdots & \mathcal{N}_{j_k}^{\theta}(\eta_1) \\ \mathcal{N}_{j_1}^{\theta}(\eta_2) & \mathcal{N}_{j_2}^{\theta}(\eta_2) & \cdots & \mathcal{N}_{j_k}^{\theta}(\eta_2) \\ \vdots & \vdots & & \vdots \\ \mathcal{N}_{j_1}^{\theta}(\eta_k) & \mathcal{N}_{j_2}^{\theta}(\eta_k) & \cdots & \mathcal{N}_{j_k}^{\theta}(\eta_k) \end{pmatrix},$$

con $0 \leq j_i \leq n-1$, tal que $\det(S_k) = 0$. Esto implica, por ejemplo a menos de un renombramiento, que existe $(a_{j_1}, a_{j_2}, \ldots, a_{j_{k-1}}) \in \mathbb{F}_{q^k}^{k-1} \setminus \{\vec{0}\}$ tal que

$$\sum_{i=1}^{k-1} a_{j_i} \mathcal{N}_{j_i}^{\theta}(\eta_l) = \mathcal{N}_{j_k}^{\theta}(\eta_l), \quad l = 1, \ldots, k. \tag{2.8}$$

Notar que $\left(\mathcal{N}_i^{\theta}(\overline{a})\right)^q = \mathcal{N}_i^{\theta}(\overline{a}^q)$ para todo $\overline{a} \in \mathbb{F}_{q^k}$ y además $(\eta_l)^q = \left(\eta^{q^{l-1}}\right)^q = \eta^{q^l} = \eta_{l+1}$. Elevando la expresión (2.8) a q, se tiene que

$$\begin{aligned} \left(\sum_{i=1}^{k-1} a_{j_i} \mathcal{N}_{j_i}^{\theta}(\eta_l)\right)^q = \left(\mathcal{N}_{j_k}^{\theta}(\eta_l)\right)^q &\iff \sum_{i=1}^{k-1} (a_{j_i})^q \left(\mathcal{N}_{j_i}^{\theta}(\eta_l)\right)^q = \left(\mathcal{N}_{j_k}^{\theta}(\eta_l)\right)^q \\ &\iff \sum_{i=1}^{k-1} (a_{j_i})^q \mathcal{N}_{j_i}^{\theta}(\eta_l^q) = \mathcal{N}_{j_k}^{\theta}(\eta_l^q) \\ &\iff \sum_{i=1}^{k-1} (a_{j_i})^q \mathcal{N}_{j_i}^{\theta}(\eta_{l+1}) = \mathcal{N}_{j_k}^{\theta}(\eta_{l+1}). \end{aligned}$$

Del Lema 1.1.29, tenemos que $\{\eta^{q^l} : l = 1, \ldots, k\} = \{\eta^{q^{l+1}} : l = 1, \ldots, k\}$

Luego,

$$\sum_{i=1}^{k-1} (a_{j_i})^q \mathcal{N}_{j_i}^{\theta}(\eta_l) = \mathcal{N}_{j_k}^{\theta}(\eta_l), \quad l = 1, \ldots, k. \tag{2.9}$$

Así, igualando las expresiones (2.8) y (2.9) se obtiene

$$\sum_{i=1}^{k-1} [(a_{j_i})^q - a_{j_i}] \mathcal{N}_{j_i}^{\theta}(\eta_l) = 0.$$

Esto implica que $[(a_{j_i})^q - a_{j_i}] = 0$, para todo $i = 1, \ldots, k-1$ o que $\det(S_{k-1}) = 0$, con

$$S_{k-1} = \begin{pmatrix} \mathcal{N}^\theta_{j_1}(\eta_1) & \mathcal{N}^\theta_{j_2}(\eta_1) & \cdots & \mathcal{N}^\theta_{j_{k-1}}(\eta_1) \\ \mathcal{N}^\theta_{j_1}(\eta_2) & \mathcal{N}^\theta_{j_2}(\eta_2) & \cdots & \mathcal{N}^\theta_{j_{k-1}}(\eta_2) \\ \vdots & \vdots & & \vdots \\ \mathcal{N}^\theta_{j_1}(\eta_{k-1}) & \mathcal{N}^\theta_{j_2}(\eta_{k-1}) & \cdots & \mathcal{N}^\theta_{j_{k-1}}(\eta_{k-1}) \end{pmatrix}.$$

Si $\det(S_{k-1}) = 0$, podemos repetir el proceso anterior. Notamos que

$$\begin{aligned} \det(S_2) = 0 &\iff \det \begin{pmatrix} \mathcal{N}^\theta_{j_1}(\eta_1) & \mathcal{N}^\theta_{j_2}(\eta_1) \\ \mathcal{N}^\theta_{j_1}(\eta_2) & \mathcal{N}^\theta_{j_2}(\eta_2) \end{pmatrix} = 0 \\ &\iff \mathcal{N}^\theta_{j_1}(\eta_1) \cdot \mathcal{N}^\theta_{j_2}(\eta_2) - \mathcal{N}^\theta_{j_1}(\eta_2) \cdot \mathcal{N}^\theta_{j_2}(\eta_1) = 0 \\ &\iff \mathcal{N}^\theta_{j_1}(\eta^q) \cdot \mathcal{N}^\theta_{j_2}(\eta^{q^2}) - \mathcal{N}^\theta_{j_1}(\eta^{q^2}) \cdot \mathcal{N}^\theta_{j_2}(\eta^q) = 0 \\ &\iff \left(\mathcal{N}^\theta_{j_1}(\eta)\right)^q \cdot \left(\mathcal{N}^\theta_{j_2}(\eta)\right)^{q^2} - \left(\mathcal{N}^\theta_{j_1}(\eta)\right)^{q^2} \cdot \left(\mathcal{N}^\theta_{j_2}(\eta)\right)^q = 0 \\ &\iff \left[\mathcal{N}^\theta_{j_1}(\eta) \cdot \left(\mathcal{N}^\theta_{j_2}(\eta)\right)^q - \left(\mathcal{N}^\theta_{j_1}(\eta)\right)^q \cdot \mathcal{N}^\theta_{j_2}(\eta)\right]^q = 0 \\ &\iff \frac{\mathcal{N}^\theta_{j_1}(\eta)}{\mathcal{N}^\theta_{j_2}(\eta)} = \left(\frac{\mathcal{N}^\theta_{j_1}(\eta)}{\mathcal{N}^\theta_{j_2}(\eta)}\right)^q \\ &\iff \frac{\mathcal{N}^\theta_{j_1}(\eta)}{\mathcal{N}^\theta_{j_2}(\eta)} \in \mathbb{F}_q \\ &\iff \mathcal{N}^\theta_{j_2}(\eta) = \delta \cdot \mathcal{N}^\theta_{j_1}(\eta), \quad \text{para algún } \delta \in \mathbb{F}_q. \end{aligned}$$

Elevando la última igualdad a q^i, para todo $i \geq 0$, se tiene que

$$\mathcal{N}^\theta_{j_2}(\eta^{q^i}) = \delta^{q^i} \cdot \mathcal{N}^\theta_{j^1}(\eta^{q^i}) \Longrightarrow \mathcal{N}^\theta_{j_2}(\eta^{q^i}) = \delta \cdot \mathcal{N}^\theta_{j^1}(\eta^{q^i}).$$

Al tomar el vector $\vec{a} = (0, \ldots, 0, \delta, 0, \ldots, 0, -1, 0, \ldots, 0) \in \mathbb{F}_q^n$, con δ en la posición j_1 y -1 en la posición j_2, se tiene que $\vec{a} \in \mathscr{C}^\perp$, ya que $\mathcal{N}_k \cdot \vec{a}_t = \vec{0}$, por lo tanto $d(\mathscr{C}^\perp) \leq 2$. Como $\mathscr{C}$ es MDS, su dual también lo es, por lo cual $d(\mathscr{C}^\perp) = n - (n-k) + 1 = k + 1 \leq 2$, lo que contradice $k \geq 2$. Por lo tanto $\det(S_t) \neq 0$, para algún $t = 2, \ldots, k-1$.

Ahora, $[(a_{j_i})^q - a_{j_i}] = 0$, para todo $i = 1, \ldots, t$, con $2 \leq t \leq k-1$, implica que

$a_{j_i} \in \mathbb{F}_q$. Sea $\vec{b} = (0, \ldots, 0, a_{j_1}, 0, \ldots, 0, a_{j_2}, 0, \ldots, 0, \ldots, a_{j_t}, 0, \ldots, 0, -1, 0, \ldots, 0) \in \mathbb{F}_q^n$ y sea $b(x)$ el polinomio asociado a $\vec{b}$. Luego podemos concluir que $b(\eta_l) = 0$ para todo $l = 1, \ldots, k$. Como $g(x)$ es el polinomio mínimo no trivial que es nulo sobre todos los η_l, se tiene que $b(x) = q(x)g(x)$ para algún $q(x) \in \mathbb{F}_q[x;\theta]$. Luego $\vec{b} \in \mathscr{C}^\perp$ y como $wt(\vec{b}) \leq t + 1 \leq k$, se deduce que $\mathrm{d}(\mathscr{C}^\perp) \leq k$. Por lo tanto, $\mathscr{C}^\perp$ no es MDS. Así $\mathscr{C}$ tampoco lo es, lo que contradice a la hipótesis.

"$\Leftarrow$"

Supongamos que $\mathscr{C}$ no es MDS, lo que implica que $\mathscr{C}^\perp$ no es MDS. Por lo cual existe $\vec{v} \in \mathscr{C}^\perp$ no nulo, tal que $wt(\vec{v}) \leq k$. Sea $v(x)$ el polinomio asociado a $\vec{v}$. Luego $v(x) = a(x)g(x)$ y esto implica $v(\eta_i) = 0$ para todo $i = 1, \ldots, k$. Por lo tanto, existe una submatriz cuadrada S_k de

$$\mathcal{N}_k = \begin{pmatrix} \mathcal{N}_0^\theta(\eta_1) & \mathcal{N}_1^\theta(\eta_1) & \cdots & \mathcal{N}_{n-1}^\theta(\eta_1) \\ \mathcal{N}_0^\theta(\eta_2) & \mathcal{N}_1^\theta(\eta_2) & \cdots & \mathcal{N}_{n-1}^\theta(\eta_2) \\ \vdots & \vdots & & \vdots \\ \mathcal{N}_0^\theta(\eta_k) & \mathcal{N}_1^\theta(\eta_k) & \cdots & \mathcal{N}_{n-1}^\theta(\eta_k) \end{pmatrix}, \tag{2.10}$$

tal que, $\det(S_k) = 0$, lo que contradice a la hipótesis. □

Corolario 2.2.13. Sea $\mathscr{C}$ un $[n, n-k]_q$-código skew pseudo-cíclico, con $2 \leq k \leq n-1$ y polinomio generador $g(x) = \text{l.m.c.m.}\left\{x - \eta^{q^{i-1}} : i = 1, \ldots, k\right\}$, para algún $\eta \in \mathbb{F}_{q^k}$. Entonces

$$d(\mathscr{C}) \leq \text{Mín}\left\{\text{rank}\left(\mathcal{N}_{i_1,\ldots,i_k}\right) : 1 \leq i_1 < \cdots < i_h \leq n\right\} + 1,$$

donde $\mathcal{N}_{i_1,\ldots,i_k}$ es una submatriz $k \times k$ de $\mathcal{N}_k$ y $\mathcal{N}_k$ es definida como (2.10).

Demostración. Con la notación de la demostración del Teorema 2.2.12, H es la matriz generadora de $\mathscr{C}$ y $\mathcal{N}_k$ es la matriz generadora del span del código $\mathscr{C}^\perp$ en $\mathbb{F}_{q^k}$, ya que $H \cdot (\mathcal{N}_k)_t = O$.

Podemos considerar en $\mathcal{N}_k$ una submatriz S_t de orden $t \times t$, con $t = 1, \ldots, k$, tal que

S_t realice la característica de una matriz cuadrada $k \times k$ en $\mathcal{N}_k$ y luego $\det(S_t) \neq 0$. Además, supongamos que S_t está formada por las columnas $j_1, j_2, \ldots, j_t$ de la matriz $\mathcal{N}_k$. Así, considerando el vector

$$\vec{b} = (0, \ldots, 0, a_{j_1}, 0, \ldots, 0, a_{j_2}, 0, \ldots, 0, \ldots, a_{j_t}, 0, \ldots, 0, -1, 0, \ldots, 0) \in \mathbb{F}_q^n$$

y la demostración del Teorema 2.2.12, se deduce que este vector pertenece, en este caso, al código $\mathscr{C}$ y así $\mathrm{d}(\mathscr{C}) \leq t + 1$.

Repitiendo este proceso, para todas las submatrices cuadradas $k \times k$ de $\mathcal{N}_k$, podemos concluir que

$$d(\mathscr{C}) \leq \text{Mín}\left\{\text{rank}\left(\mathcal{N}_{i_1,\ldots,i_k}\right) : 1 \leq i_1 < \cdots < i_k \leq n\right\} + 1.$$

□

2.3. Otros Resultados sobre Códigos Skew Pseudo-Cíclicos

2.3.1. Códigos Skew Quasi-Twisted

A partir de los quasi-twisted códigos podemos definir los skew quasi-twisted códigos, como sigue.

Definición 2.3.1. Sea $\alpha \in \mathbb{F}_q^*$, θ un automorfismo de $\mathbb{F}_q$ y sea $R = \mathbb{F}_q[x;\theta]/(x^N - \alpha)$ el anillo de polinomios sobre $\mathbb{F}_q$ módulo $x^N - \alpha$. Para $\boldsymbol{g} = (g_1(x), g_2(x), \ldots, g_m(x)) \in R^N$,

$$\mathscr{C}_{\boldsymbol{g}} = \{(r(x)g_1(x), r(x)g_2(x), \ldots, r(x)g_m(x)) \mid r(x) \in R\}$$

es llamado el *código Skew Quasi-Twisted (SQT)* con generador $\boldsymbol{g}$. Si $\alpha = 1$, $\mathscr{C}_{\boldsymbol{g}}$ es llamado *código Skew Quasi-Cíclico (SQC)*.

Inspirados en el trabajo de Maruta (*Constructing linear codes from some orbits of projectivities* [31]) y usando el Teorema 2.1.16, podemos obtener el resultado que se presenta a continuación.

Del Teorema 2.1.16 un $[n, n-k]$-código sobre $\mathbb{F}_q$, es un código skew α-cíclico con polinomio generador $g(x)$ si y sólo si $\mathscr{C}$ es un código con matriz de control de paridad $[g^n] := [P_t, (P\tau)_t, (P\tau^2)_t, \ldots, (P\tau^{n-1})_t]$, donde $P = (1, 0, \ldots, 0)$, $\tau = \Theta \circ T_g$ y T_g es la matriz compañera de $g(x)$, es decir,

$$T_g = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{k-1} \end{pmatrix}$$

si $g(x) = \sum_{i=0}^{k} a_i x^i$ con $a_k = 1$. Ahora, sea $\mathcal{T}$ la transformación de $\mathbb{P}^{k-1}(\mathbb{F}_q)$ en sí mismo definida por τ. Podemos decir que $\mathcal{T}$ es definida por $g(x)$. Entonces las columnas de $[g^n]$ pueden ser consideradas como una órbita de $\mathcal{T}$. Recíprocamente, podemos obtener un código skew pseudo-cíclico desde una órbita de una proyectividad de $\mathbb{P}^{k-1}(\mathbb{F}_q)$. Ahora, tomemos m órbitas $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m$ de $\mathcal{T}$ con largo N, y seleccionemos un punto P_i de cada $\mathcal{O}_i$. Por simplicidad, podemos tomar P_1 como $P = (1, 0, \ldots, 0)$ y denotar la matriz

$$[P_t, (P\tau)_t, \ldots, (P\tau^{n_1-1})_t;\ (P_2)_t, (P_2\tau)_t, \cdots, (P_2\tau^{n_2-1})_t; \cdots \\ \cdots; (P_m)_t, (P_m\tau)_t, \ldots, (P_m\tau^{n_m-1})_t]$$

por $[g^{n_1}] + P_2^{n_2} + \cdots + P_m^{n_m}$. Entonces, la matriz $[g^N] + P_2^N + \cdots + P_m^N$ definida por m órbitas $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_m$ de $\mathcal{T}$ generan un código SQT.

Teorema 2.3.2. *Si $P_i \in (\mathbb{F}_q^\theta)^k$ para $i = 1, \ldots, m$ son como arriba, entonces $[g^N] + P_2^N +$*

$\cdots + P_m^N$ *genera un* $[mN,k]_q$*-código Skew Quasi-Twisted (SQT) con generador*

$$\boldsymbol{g} = \left(h^*(x), b_2(x^{-1})h^*(x), \ldots, b_m(x^{-1})h^*(x)\right) \in R^N,$$

donde $h^*(x)$ *es como* $h(x)$ *en la Proposición 2.1.14 y* $b_i(x) = (1, x, \ldots, x^{k-1})P_i$ *para* $2 \leq i \leq m$.

Demostración. Definimos $H := [g^N] + P_2^N + \cdots + P_m^N$ y observamos que

$$H = [P_t, (P\tau)_t, \ldots, (P\tau^{N-1})_t;\ (P_2)_t, (P_2\tau)_t, \ldots, \\ \ldots, (P_2\tau^{N-1})_t;\ \cdots;\ (P_m)_t, (P_m\tau)_t, \ldots, (P_m\tau^{N-1})_t]$$

con $P_i \in (\mathbb{F}_q^\theta)^k$, $\tau = \Theta \circ T_g$ y $T_g \in GL(k,q)$ tal que $P\tau^N = \alpha P$. Llamando $H_i := [(P_i)_t, (P_i\tau)_t, \ldots, (P_i\tau^{N-1})_t]$ para todo $i = 1, \ldots, n$, tenemos $H = [H_1|H_2|\cdots|H_m]$.

Tomamos $P_1 \equiv P := (1, 0, \ldots, 0) = \vec{e_1}$ y notamos que $P\tau^{j-1} = \vec{e_j}$ para todo $j = 1, \ldots, k$, donde e_j es el j-ésimo vector canónico de $\mathbb{F}_q^k$. Entonces, para $P_i \in (\mathbb{F}_q^\theta)^k$ y $\lambda_{ij} \in \mathbb{F}_q^\theta$, tenemos

$$P_i = \sum_{j=0}^{k-1} \lambda_{ij} P\tau^j = (P)\left(\sum_{j=0}^{k-1} \lambda_{ij}\tau^j\right) =: P \cdot P_i(\tau),$$

donde $P_i(x) := \sum_{j=0}^{k-1} \lambda_{ij} x^j$. Así

$$P_i\tau^h = \sum_{j=0}^{k-1} \lambda_{ij} P\tau^{j+h} = P\tau^h \cdot P_i(\tau), \quad \forall h = 0, \ldots, N-1$$

y, para $i = 1, \ldots, m$, esto implica que

$$\begin{aligned} H_i &= [(P_i)_t, (P_i\tau)_t, \ldots, (P_i\tau^{N-1})_t] \\ &= [(P \cdot P_i(\tau))_t, (P\tau \cdot P_i(\tau))_t, \ldots, (P\tau^{N-1} \cdot P_i(\tau))_t] \\ &= P_i(\tau)_t \cdot [P_t, (P\tau)_t, \ldots, (P\tau^{N-1})_t] \\ &= P_i(\tau)_t \cdot H_1\ . \end{aligned}$$

Sea H_1^* la matriz generadora de $\mathscr{C}^\perp$ con $\mathscr{C} =< g(x) >$ escrita como

$$H_1^* := \begin{pmatrix} h^*(x) \\ xh^*(x) \\ \vdots \\ x^{k-1}h^*(x) \end{pmatrix} = [J \mid \widehat{H}_1^*]$$

con $det(J) \neq 0$, para alguna matriz cuadrada de tamaño $k \times k$ y alguna matriz $\widehat{H}_1^*$ de tamaño $k \times N - k$, donde $h^*(x)$ es como en el teorema. Por hipótesis, H_1 es también la matriz de control de paridad de $\mathscr{C}$ que puede ser escrita como $H_1 = [I_k \mid \widehat{H}_1]$, donde I_k es la matriz identidad de tamaño $k \times k$. Esto implica que $J^{-1}H_1^* = H_1$ y $J^{-1}\widehat{H}_1^* = \widehat{H}_1$.

Sea A una matriz con N columnas y definimos el operador lineal $\diamond$ como sigue:

$$x^{-1} \diamond A := A \cdot \left(\begin{array}{ccc|c} 0 & \cdots & 0 & \alpha \\ \hline 1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \end{array}\right).$$

Observamos que $x^{-1} \diamond (B \cdot C) = B \cdot (x^{-1} \diamond C)$ para dos matrices cualquieras B y C tal que $B \cdot C$ está bien definido y C tiene N columnas.

Más aún, para $h = 0, \ldots, N-1$, tenemos

$$\begin{aligned}
x^{-1} \diamond H_1 &= x^{-1} \diamond [P_t, (P\tau)_t, \ldots, (P\tau^{N-1})_t] \\
&= [(P\tau)_t, \ldots, (P\tau^{N-1})_t, \alpha P_t] \\
&= [(P\tau)_t, \ldots, (P\tau^{N-1})_t, (P\tau^N)_t] \\
&= (\tau)_t \cdot H_1 \\
x^{-2} \diamond H_1 &= x^{-1} \diamond (x^{-1} \diamond H_1) \\
&= x^{-1}((\tau)_t \cdot H_1) \\
&= (\tau^2)_t \cdot H_1 \\
&\vdots \\
x^{-h} \diamond H_1 &= (\tau^h)_t \cdot H_1
\end{aligned}$$

Por lo tanto, tenemos

$$H_i = P_i(\tau)_t \cdot H_1 = P_i(x^{-1}) \diamond (J^{-1} \cdot H_1^*) = J^{-1} \cdot (P_i(x^{-1}) \diamond H_1^*) =$$

$$= J^{-1} \cdot \begin{pmatrix} \\ P_i(x^{-1}) \diamond \begin{pmatrix} h^*(x) \\ xh^*(x) \\ \vdots \\ x^{k-1}h^*(x) \end{pmatrix} \end{pmatrix} = J^{-1} \cdot \begin{pmatrix} P_i(x^{-1}) \cdot h^*(x) \\ P_i(x^{-1}) \cdot xh^*(x) \\ \vdots \\ P_i(x^{-1}) \cdot x^{k-1}h^*(x) \end{pmatrix}$$

$$= J^{-1} \cdot \begin{pmatrix} P_i(x^{-1}) \cdot h^*(x) \\ x \cdot P_i(x^{-1})h^*(x) \\ \vdots \\ x^{k-1} \cdot P_i(x^{-1})h^*(x) \end{pmatrix} =: J^{-1} \cdot H_i^*$$

Así, podemos concluir que

$$H = [H_1|H_2|\cdots|H_m] = [J^{-1}H_1^*|J^{-1}H_2^*|\cdots|J^{-1}H_m^*] = J^{-1}[H_1^*|H_2^*|\cdots|H_m^*],$$

donde $\begin{pmatrix} P_i(x^{-1})\cdot h^*(x) \\ x\cdot P_i(x^{-1})h^*(x) \\ \vdots \\ x^{k-1}\cdot P_i(x^{-1})h^*(x) \end{pmatrix}$, es decir, $[H_1|H_2|\cdots|H_m]$ y $[H_1^*|H_2^*|\cdots|H_m^*]$ son dos matrices generadoras del mismo $[mN,k]_q$-código. □

2.3.2. Aplicación de la Factorización de Leroy

En el trabajo de André Leroy (*Noncommutative Polynomial Maps* [24]) se presenta un modo de factorizar un polinomio en un campo no conmutativo, mediante factorizaciones en un campo conmutativo. En base a esto, en los siguientes resultados se traspasa propiedades de códigos pseudo-cíclicos a códigos skew pseudo-cíclicos.

En $\mathbb{F}_q$ con $q = p^r$, donde p es primo y considerando θ el automorfismo de Frobenius, es decir $\theta(a) = a^p$. La factorización de polinomios en $\mathbb{F}_q[x;\theta]$ puede ser trasladada a factorización de polinomios en $\mathbb{F}_q[x]$ con algoritmo de André Leroy (Teorema 1.1.56). En donde para un número primo p y un entero $i \geq 1$ se define $[i] := \dfrac{p^i-1}{p-1}$ y el conjunto

$$\mathbb{F}_q[x^{[]}] := \left\{ \sum_{i\geq 0} \alpha_i x^{[i]} \in \mathbb{F}_q[x] \right\}.$$

Esto último, se puede generalizar considerando como automorfismo una potencia de Frobenius, $\theta(a) = a^{p^s}$, donde en este caso, tenemos que definir $[i]_s := \dfrac{(p^s)^i-1}{p^s-1}$. Además, se denotará $[i]_1 = [i]$.

Consideramos de aquí en adelante, un campo finito $\mathbb{F}_q$ con $q = p^t$ y p primo, además del automorfismo $\theta(a) = a^{p^s}$, para todo $a \in \mathbb{F}_q$.

Definición 2.3.3. Se define un $[p^s]$-código en $\mathbb{F}_q^m$ con $m = [n]_s$, si este es generado por

un $[p^s]$-polinomio en $\mathbb{F}_q[x^{[]}]$ y lo denotamos por $\mathscr{C}^{[]}$.

Proposición 2.3.4. *Dado un código skew pseudo-cíclico $\mathscr{C} \subseteq \mathbb{F}_q^n$ generado por $f(t) \in \mathbb{F}_q[t;\theta]$, entonces el código $\mathscr{C}^{[]} \subseteq \mathbb{F}_q^m$ con $m = [n]_s$, generado por el $[p^s]$-polinomio asociado a $f(t)$ es un código pseudo-cíclico.*

Demostración. Como $\mathscr{C}$ es generado por $f(t)$, por el Teorema 2.1.8, $f(t)$ es divisor derecho de $x^n - \alpha$ para algún $\alpha \in \mathbb{F}_q^*$. Por el Teorema 1.1.56, el $[p^s]$-polinomio asociado a $f(t)$, es decir, $f^{[]}(x) \in \mathbb{F}_q[x^{[]}]$, es un divisor de $x^m - \alpha$, con $m = [n]_s$. Por lo tanto, del Teorema 1.3.48, se deduce que el código $\mathscr{C}^{[]} \subseteq \mathbb{F}_q^m$ es un código pseudo-cíclico. □

Teorema 2.3.5. *Dado un código $\mathscr{C}$ generado por $f(t) \in \mathbb{F}_q[t;\theta]$ y el código $\mathscr{C}^{[]}$ generado por $f^{[]}(x) \in \mathbb{F}_q[x^{[]}]$, entonces se tiene que $d(\mathscr{C}^{[]}) \leq d(\mathscr{C})$. Además, $d(\mathscr{C}^{[]}) = d(\mathscr{C})$ si y sólo si existe un polinomio de peso mínimo de $\mathscr{C}^{[]}$ que pertenece a $\mathbb{F}_q[x^{[]}]$.*

Demostración. Sea $w(t) \in \mathscr{C}$ de peso mínimo. Por el Teorema 2.1.8, $w(t) = a(t) \cdot f(t)$, para algun $a(x) \in \mathbb{F}_q[t;\theta]$. Luego por el Teorema 1.1.56, $w^{[]}(x) = b(x) \cdot f^{[]}(x)$, para algún $b(x) \in \mathbb{F}_q[x]$ y por el Teorema 1.3.48, $w^{[]}(x) \in \mathscr{C}^{[]}$. Por lo tanto, $d(\mathscr{C}^{[]}) \leq wt(w^{[]}(x)) = wt(w(t)) = d(\mathscr{C})$.

"$\Rightarrow$"

Sea $v(t) \in \mathscr{C}$ tal que $wt(v(t)) = d(\mathscr{C})$. Luego se tiene que $v(t) = q(t) \cdot f(t)$, para algún $q(t) \in \mathbb{F}_q[x;\theta]$. Así, por el Teorema 1.1.56, $v^{[]}(x) = g(x) \cdot f^{[]}(x)$, para algún $g(x) \in \mathbb{F}_q[x]$, es decir, $v^{[]}(x) \in \mathscr{C}^{[]}$. Como $d(\mathscr{C}^{[]}) = d(\mathscr{C}) = wt(v(t)) = wt(v^{[]}(x))$, se tiene que el polinomio $v^{[]}(x)$ es de peso mínimo en $\mathscr{C}^{[]}$, el cual pertenece a $\mathbb{F}_q[x^{[]}]$.

"$\Leftarrow$"

Sea $w^{[]}(x) \in \mathbb{F}_q[x^{[]}]$ de peso mínimo en $\mathscr{C}^{[]}$, luego $w^{[]}(x) = a(x) \cdot f^{[]}(x)$, para algún $a(x) \in \mathbb{F}_q[x]$. Así, $w(t) = b(t) \cdot f(t)$, es decir $w(t) \in \mathscr{C}$. Por lo tanto, se concluye que

$$d(\mathscr{C}^{[]}) \leq d(\mathscr{C}) \leq wt(w(t)) = wt(w^{[]}(x)) = d(\mathscr{C}^{[]}),$$

es decir $d(\mathscr{C}^{[]}) = d(\mathscr{C})$. □

Proposición 2.3.6. *Un $[p^s]$-código $\mathscr{C}^{[]}$ con $dim(\mathscr{C}^{[]}) < [n]_s$, no es un MDS código.*

Demostración. Supongamos que existe un MDS código $\mathscr{C}^{[]} \subseteq \mathbb{F}_q^{[n]}$. Luego

$$\begin{aligned} d(\mathscr{C}^{[]}) &= [n] - \dim(\mathscr{C}^{[]}) + 1 \\ &= \deg(f^{[]}(x)) + 1 \\ &= [\deg(f(t))] + 1, \end{aligned}$$

donde $f^{[]}(x)$ es el polinomio generador de $\mathscr{C}^{[]}$. Además, por el Singleton Bound (Teorema 1.3.20) se tiene que $d(\mathscr{C}) \leq \deg(f(t)) + 1$, donde $\mathscr{C}$ es el código generado por $f(t)$. Por hipótesis, $\deg(f^{[]}(t)) \geq 1$ y como $[i]_s > i$ para todo $i \in \mathbb{Z}_{>0}$, se tiene que $\deg(f(t)) < \deg(f^{[]}(t))$. Así, por el Teorema 2.3.5, $d(\mathscr{C}^{[]}) \leq d(\mathscr{C}) \leq \deg(f(t)) + 1 < \deg(f^{[]}(x)) + 1$, lo que se contradice con el supuesto que el código $\mathscr{C}^{[]}$ sea un código MDS. □

Proposición 2.3.7. *Sea $\mathbb{F}_{q^{[k]}}^* = \langle w \rangle$ y $\mathbb{F}_{q^{[k]}} \subseteq \mathbb{F}_{q^{[n]}}$. Se tiene que $[n] \leq q^{[k]} - 1$, si sólo si,*

$$rank\left(V_{[n]}^{Id}(w, w^2, \ldots, w^{[n]-1})\right) = [n].$$

Demostración.

"$\Rightarrow$"

Sea

$$\mathcal{N} = \left(V_{[n]}^{Id}(w, w^2, \ldots, w^{[n]-1})\right) = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{[n]-1} \\ 1 & w^2 & (w^2)^2 & \cdots & \left(w^{[n]-1}\right)^2 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & w^{[n]-1} & (w^2)^{[n]-1} & \cdots & \left(w^{[n]-1}\right)^{[n]-1} \end{pmatrix}.$$

Con

$$det(\mathcal{N}) = \prod_{0 \leq i < j \leq [n]-1} (w^j - w^i).$$

Si $w^j = w^i$, es decir, $w^{j-i} = 1$, se tiene que el orden de w es menor o igual que $[n]-1$. Así,

$[n] \leq q^{[k]} - 1 = ord(w) \leq [n] - 1$, lo que es una contradicción. Por lo tanto $det(\mathcal{N}) \neq 0$, lo que implica $rank(\mathcal{N}) = [n]$.

"$\Leftarrow$"

Notar que $rank\left(V_{[n]}^{Id}(w, w^2, \ldots, w^{[n]-1})\right) = [n]$, implica que $w^{j-i} \neq 1$ para $0 \leq i < j \leq [n] - 1$. Luego $q^{[k]} - 1 = ord(w) > [n] - 1$, es decir $[n] \geq q^{[k]} - 1$. □

Teorema 2.3.8. *Dado el campo finito $\mathbb{F}_q$, donde $q = p^r$ con p un número primo, sea $\mathscr{C} \subseteq \mathbb{F}_q^n$ un código skew pseudo-cíclico con polinomio generador $g(t) \in \mathbb{F}_q[x;\theta]$ de grado k. Si*

$$k \geq \log_p \left[1 + \left(\frac{p-1}{r}\right) \cdot \log_p \left(\frac{p^n + p - 2}{p-1}\right)\right],$$

y $g^{[]}(\omega^{l+ci}) = 0$ para $i = 0, \ldots, \Delta - 2$, $l \in \mathbb{Z}_{\geq 0}$ y c es tal que $(c, q^{[k]} - 1) = 1$, donde $\mathbb{F}_{q^{[k]}} = \langle \omega \rangle$, entonces $d(\mathscr{C}) \geq \Delta$.

Demostración. El código $\mathscr{C}^{[]}$ es un código skew pseudo-cíclico con polinomio generador $g^{[]}(x) \in \mathbb{F}_q[x]$, $\mathbb{F}_{q^{[k]}} = \langle \omega \rangle$, con $\omega \in \mathbb{F}_{q^{[]}}$ y por hipótesis $g^{[]}(\omega^{l+ci}) = 0$ para $i = 0, \ldots, \Delta - 2$, $l \in \mathbb{Z}_{\geq 0}$.

Notar que

$$\begin{aligned} k \geq \log_p \left[1 + \left(\frac{p-1}{r}\right) \cdot \log_p \left(\frac{p^n + p - 2}{p-1}\right)\right] &\iff r\left(\frac{p^k - 1}{p-1}\right) \geq \log_p (1 + [n]) \\ &\iff p^{r \cdot [k]} \geq (1 + [n]) \\ &\iff q^{[k]} - 1 \geq [n], \end{aligned}$$

así que el $ord(\omega) = q^{[k]} - 1 \geq [n]$. Además, $\mathcal{N}_j^{id}(\omega^c) = (\omega^c)^j$ y como $(c, q^{[k]} - 1) = 1$, se tiene que

$$(\omega^c)^j \neq 1, \text{ para } j = 1, \ldots, [n] - 1.$$

Por lo tanto, por el Teorema 3.9 en [42], $d(\mathscr{C}^{[]}) \geq \Delta$ y por el Teorema 2.3.5, $d(\mathscr{C}) \geq d(\mathscr{C}^{[]}) \geq \Delta$. □

Capítulo 3

Arcos Generalizados

3.1. Definiciones y Propiedades

Definición 3.1.1. Un *k-arco generalizado (arco generalizado, o k_g-arco)* en $\mathbb{P}^2(\mathbb{F}_q)$ es un conjunto de k puntos no seis de los cuales están sobre una cónica reducible o irreducible. Un *k_g-arco se dice completo* si no está contenido en un $(k+1)_g$-arco.

Observación 3.1.2. De la definición, tenemos que un conjunto $\mathcal{K}_g \subseteq \mathbb{P}^2(\mathbb{F}_q)$ es un arco generalizado, si $|\mathcal{K}_g \cap \Gamma| \leq 5$, para toda cónica $\Gamma \subseteq \mathbb{P}^2(\mathbb{F}_q)$, ya sea reducible o irreducible.

Observación 3.1.3. Dado que dos rectas determinan una cónica reducible, un arco generalizado puede interceptar una cónica formada por dos rectas a lo más en 2 y 3 puntos respectivamente. Así, un k-arco generalizado es a lo más un $(k,3)$-arco en $\mathbb{P}^2(\mathbb{F}_q)$ (ver Definición 1.2.8).

Observación 3.1.4. Los Veronesian Arcos, definidos como k-arcos tales que a los más 5 puntos estén sobre una cónica, son un caso particular de los arcos generalizados. Coolsaet y Sticker, conjeturaron que si $\mathcal{K}$ es un Veronesian arco, entonces

$$|\mathcal{K}| \leq \frac{1}{3}(\sqrt{q}+1)^2.$$

3.2. Cotas Superiores

Proposición 3.2.1. *Sea $\mathcal{K}_g \subseteq \mathbb{P}^2(\mathbb{F}_q)$ un arco generalizado. Si $\mathcal{L}_1$ es una recta en $\mathbb{P}^2(\mathbb{F}_q)$ tal que $|\mathcal{K}_g \cap \mathcal{L}_1| = 3$, entonces para toda recta $\mathcal{L}$ en $\mathbb{P}^2(\mathbb{F}_q)$ se tiene que*

$$|(\mathcal{K}_g \setminus \mathcal{L}_1) \cap \mathcal{L}| \leq 2,$$

es decir, $(\mathcal{K}_g \setminus \mathcal{L}_1)$ es un k-arco en $\mathbb{P}^2(\mathbb{F}_q)$.

Demostración. Sea $\mathcal{K}_g$ un arco generalizado. Por la Observación 3.1.3 anterior tenemos que

$$|\mathcal{K}_g \cap \mathcal{L}| \leq 3, \text{ para cada recta } \mathcal{L} \text{ en } \mathbb{P}^2(\mathbb{F}_q).$$

Supongamos que existe $\mathcal{L}_2$ tal que $|(\mathcal{K}_g \setminus \mathcal{L}_1) \cap \mathcal{L}_2| = 3$. Se tiene que $(\mathcal{L}_1 \cap \mathcal{K}_g) \cap (\mathcal{L}_2 \cap \mathcal{K}_g) = \varnothing$, por lo cual $\mathcal{L}_1$ y $\mathcal{L}_2$ forman una cónica reducible Γ tal que $|\mathcal{K}_g \cap \Gamma| = 6$, lo que contradice la hipótesis que $\mathcal{K}_g$ es un arco generalizado. □

En $\mathbb{P}^2(\mathbb{F}_q)$, la mayor cardinalidad de un arco generalizado completo lo denotamos por $m_g(2,q)$ y el más pequeño por $t_g(2,q)$.

Teorema 3.2.2. *Sea q impar con $q \geq 7$. Entonces se tiene que*

$$m_g(2,q) \leq \text{mín}\{m(2,q)+3,\ m(5,q),\ m'(2,q)+3\},$$

donde $m(2,q)$ es el tamaño máximo de un arco completo en $\mathbb{P}^2(\mathbb{F}_q)$, $m(5,q)$ es el tamaño máximo de un arco completo en $\mathbb{P}^5(\mathbb{F}_q)$ (Definición 1.2.9) y $m'(2,q)$ es el segundo tamaño máximo de un arco completo en $\mathbb{P}^2(\mathbb{F}_q)$.

Demostración.

(1) De la Proposición 3.2.1, un arco generalizado está formado a lo más por un arco unido con 3 puntos colineales. Por lo tanto, $m_g(2,q) \leq m(2,q)+3$.

(2) Consideremos la incrustación de Veronese

$$\begin{aligned}\nu_2 \colon \mathbb{P}^2(\mathbb{F}_q) &\longrightarrow \mathbb{P}^5(\mathbb{F}_q)\\ [x_0 : x_1 : x_2] &\longmapsto [x_0^2 : x_1^2 : x_2^2 : x_0x_1 : x_0x_2 : x_1x_2]\end{aligned}$$

y sean $S := \nu_2(\mathbb{P}^2(\mathbb{F}_q)) \subseteq \mathbb{P}^5(\mathbb{F}_q)$, $[z_0 : z_1 : z_2 : z_3 : z_4 : z_5] \in \mathbb{P}^5(\mathbb{F}_q)$ y $H \colon \sum_{i=0}^{5} \alpha_i z_i = 0$ un hiperplano, con $\alpha_i \in \mathbb{F}_q$. Luego $\nu_2^{-1}(H \cap S)$ es una cónica en $\mathbb{P}^2(\mathbb{F}_q)$. Si un conjunto $\mathcal{K}_g$ es un arco generalizado en $\mathbb{P}^2(\mathbb{F}_q)$, significa que a lo más 5 puntos viven sobre una cónica, es decir $|\nu_2(\mathcal{K}_g) \cap H| \leq 5$. Por lo tanto, el conjunto $\nu(\mathcal{K}_g)$ es un arco en $\mathbb{P}^5(\mathbb{F}_q)$. Así, tenemos que $m_g(2,q) \leq m(5,q)$.

(3) En $\mathbb{P}^2(\mathbb{F}_q)$ un arco completo de tamaño máximal, es decir con $m(2,q)$ puntos, está formado por una cónica.

El segundo tamaño mayor de un arco completo con $q \geq 7$, es $m'(2,q) \geq 6$, es decir cualquier arco con más puntos se puede extender a un arco completo y por lo tanto vive sobre una cónica. Por lo cual, $m_g(2,q) \leq m'(2,q)+3$ por la Proposición 3.2.1.

□

Para $q = 2^h$, $h \geq 4$, existen hiperóvalos irregulares, es decir, estos no están formados por una cónica y su núcleo. Por ende, no es posible aplicar el punto (3) de la demostración anterior en estos casos.

Teorema 3.2.3. *Si q es par y $q \geq 16$, entonces* $m_g(2,q) \leq q - \dfrac{\sqrt{q}}{2} + \dfrac{17}{4}$.

Demostración. Supongamos que existe un conjunto $\mathcal{K} \subseteq \mathbb{P}^2(\mathbb{F}_q)$ tal que $|\mathcal{K}| > q - \dfrac{\sqrt{q}}{2} + \dfrac{17}{4}$. Considerando la incrustación de Veronese

$$\begin{aligned}\nu_2 \colon \mathbb{P}^2(\mathbb{F}_q) &\longrightarrow \mathbb{P}^5(\mathbb{F}_q)\\ [x_0 : x_1 : x_2] &\longmapsto [x_0^2 : x_1^2 : x_2^2 : x_0x_1 : x_0x_2 : x_1x_2]\end{aligned}$$

el conjunto $\nu_2(\mathcal{K})$ es un arco en $\mathbb{P}^5(\mathbb{F}_q)$. Por el Teorema 1.2.13, $\nu_2(\mathcal{K})$ está contenido en una única curva racional normal Γ de grado 5 en $\mathbb{P}^5(\mathbb{F}_q)$. Luego $\nu_2(\mathcal{K}) \subseteq \nu_2(\mathbb{P}^2(\mathbb{F}_q)) =: S$. Como la superficie de Veronese S está definida por cuádricas (ver [15], Example 2.7), se tiene que $\Gamma \not\subseteq S$. Además, existe una cuádrica $\mathbb{Q}^4 \subseteq \mathbb{P}^5(\mathbb{F}_q)$ tal que $S \subseteq \mathbb{Q}^4$ y $\Gamma \not\subseteq \mathbb{Q}^4$, así se tiene que

$$|\Gamma \cap S| \leq |\Gamma \cap \mathbb{Q}^4| \leq \deg(\Gamma) \cdot \deg(\mathbb{Q}^4) = 10,$$

donde la última desigualdad esta dada por el Teorema de Bezout (ver [23], Theorem 25.1). Esto implica que

$$q - \frac{\sqrt{q}}{2} + \frac{17}{4} < |\nu_2(\mathcal{K})| = |\nu_2(\mathcal{K}) \cap S \cap \Gamma| \leq |S \cap \Gamma| \leq 10.$$

Como $q \geq 16$, se tiene una contradicción en esta última desigualdad. Por lo tanto, $m_g(2,q) \leq q - \frac{\sqrt{q}}{2} + \frac{17}{4}$.

□

Observación 3.2.4. La demostración anterior se puede adaptar al caso q impar considerando el Teorema 1.2.12, pero esto no mejora la cota superior del Teorema 3.2.2.

En lo que sigue, vamos a calcular los valores exactos de $m_g(2,q)$ para q pequeños, es decir, $q = 2, 3, 4$ y 5.

Proposición 3.2.5. $m_g(2,2) = 7$.

Demostración. Las cónicas irreducibles están formadas por $q+1 = 3$ puntos (Corolario 1.2.6) y por lo tanto en $\mathbb{P}^2(\mathbb{F}_2)$ siempre su intersección con cualquier conjunto es menor que 4. Respecto a las cónicas reducibles, estas son formadas por dos rectas, las cuales tienen 3 puntos cada una en $\mathbb{P}^2(\mathbb{F}_2)$ y al menos un punto en común, luego la intersección con cualquier conjunto será menor que 6. Por lo tanto, del Teorema 1.2.4, $m_g(2,2) = |\mathbb{P}^2(\mathbb{F}_q)| = 7$. □

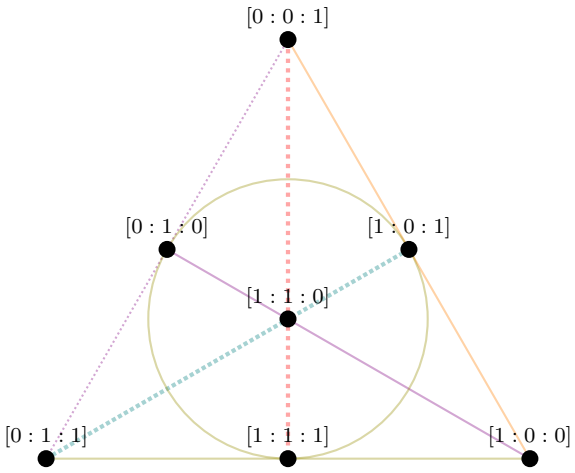


Figura 3.1: Plano Proyectivo sobre el Campo Finito $\mathbb{F}_2$.

Proposición 3.2.6. $m_g(2,3) = 7$.

Demostración. Cualquier conjunto en $\mathbb{P}^2(\mathbb{F}_3)$ intersectado con una cónica irreducible siempre tiene cardinalidad menor que 5. Las cónicas reducibles contienen a lo más 7 puntos, ya que están formadas por dos rectas que siempre tienen al menos un punto en común.

Por la Proposición 3.2 y el Teorema 1.2.14, tenemos que $m_g(2,3) \leq m(2,3) + 3 = 7$.

Sea $\mathcal{K} = \{p_1, p_2, p_3, p_4\}$ un arco completo en $\mathbb{P}^2(\mathbb{F}_3)$ y llamamos $\mathcal{L}_{ij}$ la recta que pasa por los puntos p_i y p_j. Sea q_1 la intersección de $\mathcal{L}_{12}$ y $\mathcal{L}_{34}$, y q_2 la intersección de $\mathcal{L}_{13}$ y $\mathcal{L}_{24}$. Tomamos q_3 en la recta que pasa por q_1 y q_2, intersectada con $\mathcal{L}_{14}$. Así, el conjunto $\mathcal{K} = \{p_1, p_2, p_3, p_4, q_1, q_2, q_3\}$ forma un 7-arco generalizado. Luego $m_g(2,3) = 7$. □

Lema 3.2.7. $m_g(2,4) \geq 7$.

Demostración. Cualquier conjunto en $\mathbb{P}^2(\mathbb{F}_4)$ interceptado con una cónica irreducible siempre es menor que 6. Las cónicas reducibles contienen a lo más 9 puntos, ya que están formadas por dos rectas que tienen al menos un punto en común.

Tomamos un arco completo $\mathcal{K} \subseteq \mathbb{P}^2(\mathbb{F}_4)$, es decir una cónica más su núcleo (ver Lema 1.2.21), y un punto $p \notin \mathcal{K}$. Supongamos que $\mathcal{K}_g = \mathcal{K} \cup \{p\}$ no es un arco generalizado. Luego existen dos rectas $\mathcal{L}_1$ y $\mathcal{L}_2$, tal que $(\mathcal{L}_1 \cap \mathcal{K}_g) \cap (\mathcal{L}_2 \cap \mathcal{K}_g) = \varnothing$ y $|\mathcal{K}_g \cap \mathcal{L}_i| = 3$, para

$i = 1, 2$. El punto $p \in \mathcal{K}_g$ puede pertenecer a una sola de las dos rectas, por lo cual, existe una recta que intersecta en 3 puntos $\mathcal{K}_g \setminus \{p\} = \mathcal{K}$, lo que contradice el hecho que $\mathcal{K}$ sea un arco en $\mathbb{P}^2(\mathbb{F}_q)$. Por lo tanto,$\mathcal{K}_q$ es un arco generalizado y $m_g(2,4) \geq |\mathcal{K}_g| = 7$. □

Proposición 3.2.8. $m_g(2,4) = 7$.

Demostración. Por el Lema 3.2.7, ya sabemos que existe un arco generalizado formado por 7 puntos. Además, en $\mathbb{P}^2(\mathbb{F}_4)$ si un conjunto $\mathcal{K}_g$ intersectado con una cónica es un conjunto de puntos con cardinalidad mayor que 5, la cónica necesariamente debe ser reducible en dos rectas distintas.

Consideremos un arco completo formado por los puntos c_1, c_2, c_3, c_4, c_5 y c_6, con c_6 el núcleo de la cónica que pasa por los otros 5 puntos. Además, tomemos una recta $\mathcal{L}$ formada por los puntos p_1, p_2, p_3, p_4 y p_5 distintos de los c_i, $i = 1, \ldots, 6$. Supongamos que la recta que pasa por c_1 y c_6 intersecte a $\mathcal{L}$ en p_1, la recta que pasa por c_1 y c_2 intersecte en p_2 y así, hasta la recta que pasa por c_1 y c_5 intersecte en p_5. Luego, como la recta que pasa por c_2 y c_3 no pueden pasar por p_2 ni p_3, podemos suponer que pasa por p_1. Repitiendo esta construcción, sin perdida de generalidad, podemos considerar las siguientes rectas:

$c_1, c_6, p_1 \in \mathcal{L}_1$, $c_1, c_5, p_5 \in \mathcal{L}_5$, $c_2, c_6, p_5 \in \mathcal{L}_9$, $c_4, c_5, p_1 \in \mathcal{L}_{13}$,

$c_1, c_2, p_2 \in \mathcal{L}_2$, $c_2, c_3, p_1 \in \mathcal{L}_6$, $c_3, c_4, p_5 \in \mathcal{L}_{10}$, $c_4, c_6, p_2 \in \mathcal{L}_{14}$,

$c_1, c_3, p_3 \in \mathcal{L}_3$, $c_2, c_4, p_3 \in \mathcal{L}_7$, $c_3, c_5, p_2 \in \mathcal{L}_{11}$, $c_5, c_6, p_3 \in \mathcal{L}_{15}$,

$c_1, c_4, p_4 \in \mathcal{L}_4$, $c_2, c_5, p_4 \in \mathcal{L}_8$, $c_3, c_6, p_4 \in \mathcal{L}_{12}$, $p_1, \ldots, p_5 \in \mathcal{L}_{16}$.

Supongamos ahora que existe un $\mathcal{K}_g$ arco generalizado con 8 puntos. Notar que $\mathcal{K}_g$ no puede ser un arco. Luego existe una recta $l \subseteq \mathbb{P}^2(\mathbb{F}_4)$ tal que $|\mathcal{K}_g \cap l| = 3$. Por el Teorema 3.2.1 se tiene que $\mathcal{K}_g \setminus l := \mathcal{K}$ es un 5-arco en $\mathbb{P}^2(\mathbb{F}_4)$. Luego $\mathcal{K}$ es una cónica, es decir $\mathcal{K} = \{c_1, c_2, c_3, c_4, c_5\}$ con la notación anterior. Así, tenemos dos casos: (i) $c_6 \in l$; (ii) $c_6 \notin l$.

Caso (i): Dado que $\mathcal{K} \cup \{c_6\}$ es completo, debe existir otro punto c_i del arco con $i = 1, \ldots, 5$, en la misma recta l, por lo cual existiría una recta l con 4 puntos de $\mathcal{K}_g$. Tomando cualquier otra secante l' de $\mathcal{K}_g$ tal que $(l \cap \mathcal{K}_g) \cap (l' \cap \mathcal{K}_g) = \varnothing$, la cónica reducible $l \cup l'$ tendría 6 puntos en común con $\mathcal{K}_g$, lo cual contradice el hecho que $\mathcal{K}_g$ es un arco generalizado.

Caso (ii): Notar que $c_i \notin l$ para $i = 1, \ldots, 6$. Luego podemos suponer que $l = \mathcal{L}_{16}$ con la notación anterior, es decir, podemos considerar $\mathcal{K}_g = \{c_1, c_2, c_3, c_4, c_5, p_1, p_2, p_3\}$. Luego las rectas $\mathcal{L}_2$ y $\mathcal{L}_{13}$ forman una cónica reducible que comparte con $\mathcal{K}_g$ seis puntos distintos, lo que contradice el hecho que $\mathcal{K}_g$ es un arco generalizado.

Por lo tanto, $m_g(2, 4) = 7$. □

Ejemplo 3.2.1 (Figura 3.2)**.** El conjunto $\mathcal{K}_g$ dado por los puntos

- $[0 : 1 : 2]$
- $[1 : 1 : 2]$
- $[1 : 2 : 0]$
- $[0 : 1 : 0]$
- $[1 : 1 : 1]$
- $[1 : 0 : 1]$
- $[1 : 1 : 0]$

forma un 7-arco generalizado completo maximal en $\mathbb{P}^2(\mathbb{F}_q)$.

Proposición 3.2.9. $m_g(2, 5) = 7$.

Demostración. Por el Teorema 3.2.2, tenemos que $m_g(2, 5) \leq m(5, 5)$, Además, por el Teorema 1.2.10, sabemos que $m(5, 5) = 7$ y que existe un 7-arco con $\mathcal{K}$ en $\mathbb{P}^5(\mathbb{F}_5)$, dado por

$$\mathcal{K} := \{[1 : 0 : \cdots : 0], [0 : 1 : 0 : \cdots : 0], [0 : \cdots : 0 : 1], [1 : 1 : \cdots : 1]\}.$$

Considerando el conjunto

$$\mathcal{K}' := \{[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1], [1 : 1 : 1], [1 : 0 : 1], [1 : 1 : 0], [0 : 1 : 1]\},$$

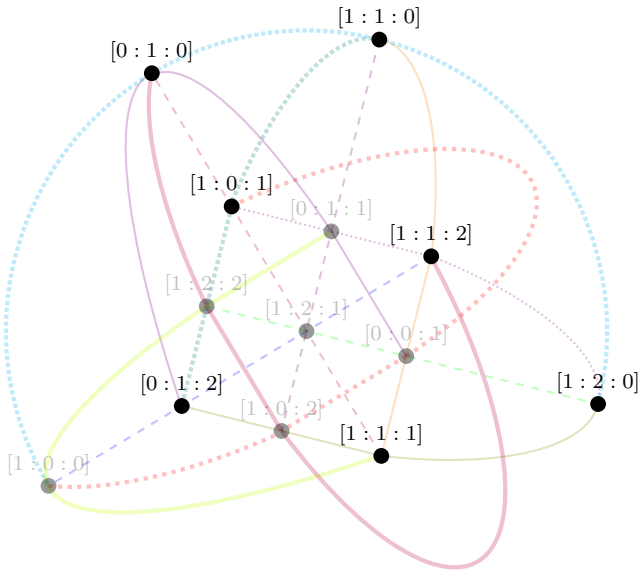


Figura 3.2: Arco Generalizado Completo en $\mathbb{P}^2(\mathbb{F}_3)$.

mediante ν_2, se tiene

$$\nu_2(\mathcal{K}') = \{[1:0:0:0:0:0], [0:1:0:0:0:0], [0:0:1:0:0:0],$$
$$[1:1:1:1:1:1], [1:0:1:0:1:0], [1:1:0:1:0:0], [0:1:1:0:0:1]\}.$$

Al usar la proyectividad dada por la matriz

$$\begin{pmatrix} 1 & 0 & 0 & 4 & 4 & 1 \\ 0 & 1 & 0 & 4 & 0 & 0 \\ 0 & 0 & 1 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 4 & 0 & 1 \end{pmatrix},$$

los puntos de $\nu_2(\mathcal{K}')$ se van en los puntos de $\mathcal{K}$. Por lo tanto, $\nu_2(\mathcal{K}')$ es un 7-arco en $\mathbb{P}^5(\mathbb{F}_5)$, es decir $\mathcal{K}'$ es un 7-arco generalizado en $\mathbb{P}^2(\mathbb{F}_q)$ formado por 7 puntos. Luego

$m_g(2,5) = 7$.

□

Para $q \geq 7$, la geometría de los puntos de un arco generalizado se vuelve mucho más compleja, por lo cual sólo se entregarán estimaciones para $m_g(2,q)$ y $t_g(2,q)$, junto con algunos ejemplos encontrados mediante el software Magma.

Observación 3.2.10. Sabemos que

$m'(2,q)$

$\leq q-1$	$q \geq 7$	Segre 1955 [33]
$\leq q - \frac{1}{4}\sqrt{q} + \frac{7}{4}$	q impar	Segre 1967 [36]
$\leq \frac{44}{45}q + \frac{8}{9}$	q primo	Thas 1987 [43]
$\leq q - \frac{1}{2}\sqrt{q} + 5$	$q = p^h$, $p \geq 5$	Hirschfeld-Korchmáros 1996 [16].

Observación 3.2.11. Para $q \geq 7$, sabemos que $m(5,q) = q+1$, excepto posiblemente para $q \in \{23, \ldots, 83\} \setminus \{32, 64\}$, Hirschfeld 1997 [19].

El siguiente teorema, es resultado directo de comparar el Teorema 3.2.2 y los resultados mostrados en la Observación 3.2.10.

Teorema 3.2.12. *Sea $q \geq 4$ impar. Entonces se tiene que*

- *para q primo:*

$$m_g(2,q) \leq \begin{cases} q+1 & , 7 \leq q \leq 21 \\ q+2 & , 23 \leq q \leq 83 \\ q+1 & , 89 \leq q \leq 131 \\ \left\lfloor \frac{44}{45}q + \frac{8}{9} \right\rfloor + 3 & , q \geq 137 \end{cases}$$

- *para $q = p^s$, con p primo mayor o igual a 5 y $s \geq 2$:*

$$m_g(2,q) \leq \begin{cases} q+1 & ,7 \leq q \leq 21 \\ q+2 & ,23 \leq q \leq 83 \\ q+1 & ,89 \leq q \leq 193 \\ \left\lfloor q - \frac{\sqrt{q}}{2} + 5 \right\rfloor + 3 & ,q \geq 197 \end{cases}$$

- *para $q = 3^s$ y $s \geq 2$:*

$$m_g(2,q) \leq \begin{cases} q+1 & ,7 \leq q \leq 21 \\ q+2 & ,23 \leq q \leq 83 \\ q+1 & ,89 \leq q \leq 181 \\ \left\lfloor q - \frac{\sqrt{q}}{4} + \frac{25}{16} \right\rfloor + 3 & ,q \geq 191 \end{cases}$$

Observación 3.2.13. Para q pequeños, por medios de los Programas 8, 9 y 10 de la Sección 4.2, se pueden encontrar los valores exactos de $m_g(2,q)$ y verificar que la cota $m_g(2,q)$ en el Teorema es alcanzado para $q = 7$. A continuación en la tabla 3.1, se presentan estos valores con sus respectivos ejemplos.

3.3. Cotas Inferiores

Observación 3.3.1. El tamaño del menor arco completo en $\mathbb{P}^2(\mathbb{F}_q)$ es denotado por $t(2,q)$. Ball en [1] mostró que

$$t(2,q) \geq \begin{cases} \lfloor \sqrt{2q} + 2 \rfloor & ,\text{para cualquier } q \\ \left\lfloor \sqrt{3q} + \frac{1}{2} \right\rfloor & ,\text{para } q = p^h,\ p \text{ primo},\ h = 1,2,3 \end{cases}.$$

Bartoli en [2], realiza un trabajo más detallado para estas cotas inferiores, con

q	$m'(2,q)$	$m(2,q)$	$m_g(2,q)$	Ejemplo de Arco Generalizado en $\mathbb{P}^2(\mathbb{F}_q)$
2	4	4	7	$\mathbb{P}^2(\mathbb{F}_2)$
3	4	4	7	$[0:1:2],[1:1:1],[1:1:2],[1:0:1],$ $[1:2:0],[1:1:0],[0:1:0]$
4	6	6	7	$[1:0:0],[0:1:0],[0:0:1],[1:1:1],$ $[\alpha:\alpha^2:1],[\alpha^2:0:1],[\alpha^2:\alpha^2:1]$
5	6	6	7	$[1:0:0],[0:1:0],[0:0:1],[1:1:1],$ $[1:0:1],[1:1:0],[0:1:1]$
7	6	8	8	$[1:0:0],[0:1:0],[0:0:1],[1:1:1],$ $[2:2:1],[5:2:1],[3:5:1],[6:1:1]$
8	6	10	9	$[1:0:0],[0:1:0],[0:0:1],[1:1:1],$ $[1:\alpha^4:1],[\alpha:1:1],[\alpha^5:\alpha^6:1],[\alpha;\alpha^4:1],$ $[\alpha^5:1:0]$
9	8	10	8	$[1:0:0],[0:1:0],[0:0:1],[1:1:1],$ $[\alpha^6:\alpha:1],[\alpha^5:0:1],[\alpha:\alpha:1],[\alpha^7:\alpha^2:1]$

Tabla 3.1: Arcos Generalizados Completos de tamaño máximal para $q \leq 9$.

$q \leq 7559$. En particular, para $q \leq 89$ muestra que $t(2,q) \leq \lfloor 3\sqrt{q} \rfloor$.

A continuación, se demuestra una cota inferior para $t(2,q)$ que mejora la de Ball para algunos q y cuyo método de demostración se adaptará para el caso de los arcos generalizados.

Teorema 3.3.2. $t(2,q) \geq \left\lceil \sqrt{2q} + \frac{3}{2} \right\rceil$ *para cualquier* q.

Demostración. Dado un conjunto de n puntos $\{p_1, p_2, \ldots, p_n\} \subseteq \mathbb{P}^2(\mathbb{F}_q)$, denotamos por $\langle p_1, \ldots, p_n \rangle$ el conjunto de puntos de todas las rectas que pasan por p_i y p_j, con $i \neq j$ e $i, j \in \{1, \ldots, n\}$.

Supongamos que el conjunto de t puntos $\{p_1, p_2, \ldots, p_t\}$ es el mínimo conjunto tal que $\langle p_1, \ldots, p_t \rangle$ cubre todo el plano $\mathbb{P}^2(\mathbb{F}_q)$, es decir

$$|\langle p_1, p_2 \ldots, p_t \rangle| = q^2 + q + 1.$$

Por un punto cualquiera del conjunto, pasan $(t-1)$ rectas que se intersectan en este punto y donde cada una tiene q puntos distintos. Por lo cual, al sacar el punto p_t, se tiene la siguiente desigualdad

$$|\langle p_1, p_2 \ldots, p_{t-1}\rangle| \geq q^2 + q + 1 - [(t-1)q + 1].$$

Ya que en el plano proyectivo todas las rectas se intersectan, al quitar otro punto, el conjunto $|\langle p_1, p_2 \ldots, p_{t-1}\rangle|$ deja de cubrir $(t-2)$ rectas que pasaban por él, con $[q+1-(t-1)]$ distintos de los que ya se habían descontado, es decir, se tiene la desigualdad

$$|\langle p_1, p_2 \ldots, p_{t-2}\rangle| \geq q^2 + q + 1 - [(t-1)q + 1] - [q+1-(t-1)](t-2).$$

Repitiendo el proceso anterior, sacando otro punto al conjunto, se tiene que

$$\begin{aligned}|\langle p_1, p_2 \ldots, p_{t-3}\rangle| \geq q^2 + q + 1 - [(t-1)q + 1] \\ - [q+1-(t-1)](t-2) - [q+1-(t-1)](t-3).\end{aligned}$$

Así, tomando una cantidad n de puntos, entre 1 y $t-1$, se puede deducir que

$$\begin{aligned}|\langle p_1, p_2 \ldots, p_{t-n}\rangle| \geq q^2 + q + 1 - [(t-1)q + 1] \\ - [q+1-(t-1)]\,(\,(t-2) + (t-3) + \cdots + (t-n)\,)\,,\end{aligned}$$

lo que implica que

$$|\langle p_1, p_2 \ldots, p_{t-n}\rangle| \geq q^2 + q - (t-1)(t-2) - (q+2-t)\left(tn - \frac{n(n+1)}{2}\right),$$

para todo $n \in \{1, \ldots, t-2\}$. Notar que existe un h tal que $1 \leq h \leq t-1$ y

$$q^2 + q - (t-1)(t-2) - [q+2-t]\left(th - \frac{h(h+1)}{2}\right) = 0.$$

Luego

$$1 \leq h = \frac{(2t-1) \pm \sqrt{4t^2 - 12t - 8q + 9}}{2} \leq t - 1,$$

es decir, $h = \dfrac{(2t-1) - \sqrt{4t^2 - 12t - 8q + 9}}{2}$ con $4t^2 - 12t - 8q + 9 > 0$. Desde esta desigualdad, se deduce entonces que

$$t \geq \sqrt{2q} + \frac{3}{2},$$

es decir, la cantidad t de puntos, tal que $\langle p_1, \ldots, p_t \rangle$ cubre todo el plano $\mathbb{P}^2(\mathbb{F}_q)$, está dada al menos por

$$t \geq \left\lceil \sqrt{2q} + \frac{3}{2} \right\rceil.$$

□

En la tabla 3.2, se presenta una comparación entre las distintas cotas inferiores para arcos y donde estos son óptimos se muestran sus respectivos ejemplos, los cuales se obtuvieron con los Programas 5, 6 y 7 de la Sección 4.2.

Observación 3.3.3. Como se puede observar en la tabla 3.2, la cota $\left\lceil \sqrt{2q} + \frac{3}{2} \right\rceil$ es mejor que la cota $\lfloor \sqrt{2q} + 2 \rfloor$ para $q = 7, 11$, además de ser optima para $q = 2, 3, 7, 8, 9, 11$.

Si todas las cónicas Γ que pasan por 5 puntos de un arco generalizado $\mathcal{K}_g \subseteq \mathbb{P}^2(\mathbb{F}_q)$ son irreducibles, este es un arco generalizado que es también un arco, es decir, $\mathcal{K}_g$ es un Veronesian Arcos.

Proposición 3.3.4. *Sea $\mathcal{K}_g \subseteq \mathbb{P}^2(\mathbb{F}_q)$, con $q \geq 4$ un Veronesian Arc completo. Entonces $|\mathcal{K}_g| \geq \lceil t_1 \rceil$, donde t_1 es la menor solución real positiva de la siguiente desigualdad:*

$$\binom{t_1}{5}(q-4) + \binom{t_1}{2}(q-1) + t_1 \geq q^2 + q + 1$$

Demostración. Dado que las cónicas irreducibles contienen $q + 1$ puntos, la cantidad de

q	$\lfloor\sqrt{2q}+2\rfloor$	$\lfloor\sqrt{3q}+\frac{1}{2}\rfloor$	$\left\lceil\sqrt{2q}+\frac{3}{2}\right\rceil$	$t(2,q)$	Ejemplos de Arcos en $\mathbb{P}^2(\mathbb{F}_q)$
2	4	2	**4**	**4**	$[0:0:1], [0:1:0], [1:0:0], [1:1:1]$
3	4	3	**4**	**4**	$[0:0:1], [0:1:0], [1:0:0], [1:1:1]$
4	4	3	4	**6**	$[0:0:1], [0:1:0], [\alpha:\alpha^2:1], [1:1:1], [1:0:0], [\alpha^2:\alpha:1]$
5	5	4	5	6	$[0:0:1], [0:1:0], [1:0:0], [1:1:1], [3:2:1], [4:3:1]$
7	5	5	**6**	**6**	$[0:0:1], [0:1:0], [1:0:0], [1:1:1], [3:2:1], [4:3:1]$
8	6	5	**6**	**6**	$[0:0:1], [0:1:0], [\alpha^2:\alpha^3:1], [1:0:0], [1:1:1], [\alpha^4:\alpha^2:1]$
9	6	5	**6**	**6**	$[0:0:1], [0:1:0], [\alpha^2:\alpha^5:1], [1:0:0], [1:1:1], [\alpha^5:\alpha^2:1]$
11	6	6	**7**	**7**	$[0:0:1], [0:1:0], [0:0:1], [1:1:1], [7:3:1], [3:2:1], [10:8:1]$
13	7	6	7	8	
16	7		8	9	
17	7	7	8	10	
19	8	8	8	10	
23	8	8	9	10	
25	9	9	9	12	
27	9	9	9	12	
29	9	9	10	13	
31	9	10	10	14	

Tabla 3.2: Comparación de Cotas Inferiores para arcos en $\mathbb{P}^2(\mathbb{F}_q)$ para $q \leq 31$.

puntos que cubren las cónicas que pasan por t_1 puntos está dado por

$$\binom{t_1}{5}(q+1-5)+t_1.$$

Además, como $\mathcal{K}_g$ es un arco, la cantidad de puntos que cubren las rectas que pasan por t_1 puntos, está dado por

$$\binom{t_1}{2}(q+1-2)+t_1.$$

Como los t_1 puntos son en común, se tiene que para que los puntos cubran el plano, estos deben satisfacer la desigualdad

$$\binom{t_1}{5}(q+1-5)+\binom{t_1}{2}(q+1-2)+t_1 \geq q^2+q+1.$$

□

Proposición 3.3.5. *Sea $\mathcal{K}_g \subseteq \mathbb{P}^2(\mathbb{F}_q)$ con $q \geq 4$ un arco generalizado que no es un arco. Entonces $|\mathcal{K}_g| \geq \lceil t_2 \rceil$, donde t_2 es la menor solución real positiva de la siguiente desigualdad:*

$$\binom{t_2-3}{5}(q-4)+\binom{t_2-2}{4}(6q-12)+\left(\binom{t_2-3}{2}+1\right)(q-2)+t_2 \geq q^2+q+1$$

Demostración. Dado un arco generalizado $\mathcal{K}_g \subseteq \mathbb{P}^2(\mathbb{F}_q)$ formado por t_2 puntos, podemos suponer que $\mathcal{K}_g = \mathcal{K} \cup \mathcal{P}$, donde $\mathcal{K}$ es un arco y $\mathcal{P}$ son 3 puntos colineales.

Las cónicas que pasan por 5 puntos de $\mathcal{K}_g$ y no contienen ningún punto de $\mathcal{P}$ son irreducibles pues es $\mathcal{K}$ es un arco y a lo más cubren

$$\binom{3}{0}\binom{t_2-3}{5}(q+1-5)+t_2 \tag{3.1}$$

puntos en el plano. Las cónicas que pasan por 4 puntos de $\mathcal{K}$ y un punto de $\mathcal{P}$, pueden ser reducibles o irreducibles. Dado que las cónicas reducibles cubren $2q+1 > q+1$ puntos, vamos a suponer que todas las cónicas anteriores son reducibles. Por ende, ellos

cubren a lo más

$$\binom{3}{1}\binom{t_2-3}{4}(2q+1-5)+t_2 \tag{3.2}$$

puntos en el plano. Las cónicas que pasan por 3 puntos de $\mathcal{K}$ y 2 puntos de $\mathcal{P}$, pueden ser reducibles o irreducibles. Como en el caso anterior, podemos suponer que estas son todas reducibles, por lo cual cubren a lo más

$$\binom{3}{2}\binom{t_2-3}{3}(2q+1-5)+t_2 \tag{3.3}$$

puntos en el plano. En fin, las cónicas que pasan por 2 puntos de $\mathcal{K}$ y 3 puntos de $\mathcal{P}$ son todas reducibles y a lo más cubren a lo más

$$\binom{3}{3}\binom{t_2-3}{2}(q+1-3)+(q+1-3)+t_2 \tag{3.4}$$

Como los t_2 puntos son en común, sumando las expresiones (3.1) a (3.4) se tiene

$$S(t_2)=\binom{t_2-3}{5}(q-4)+\binom{t_2-2}{4}(6q-12)+\left(\binom{t_2-3}{2}+1\right)(q-2)+t_2,$$

la cual es mayor o igual del número de puntos cubiertos por el span de cónicas de $\mathcal{K}_g$. Por lo tanto, si t_2 satisface $S(t_2)\geq q^2+q+1$ se tiene que $t_g(2,q)\geq\lceil t_2\rceil$. □

Observación 3.3.6. En la Tabla 3.3 se comparan la cota inferior $t(2,q)$ para un arco completo en $\mathbb{P}^2(\mathbb{F}_q)$ y la cota inferior $\lceil t_1\rceil$ de la Proposición 3.3.4, correspondiente a un Veronesian arco completo en $\mathbb{P}^2(\mathbb{F}_q)$. Es importante destacar, como se menciona en la Observación 3.1.4, un Veronesian arco es un caso particular de un arco generalizado, por lo cual, si un conjunto es completo como Veronesian arco, no necesariamente es completo como arco generalizado. Además, usando el software MAGMA (Programa 11) se pueden encontrar ejemplos que evidencian que la cota encontrada es optima para $q=5,7,8,9,11$.

Observación 3.3.7. En la Tabla 3.4 se comparan la cota inferior de un Veronesian Arco (Proposición 3.3.4), la cota inferior de un arco generalizado (Proposición 3.3.5) y

la cota inferior de un arco en $\mathbb{P}^2(\mathbb{F}_q)$. Además, para $q \leq 11$ se puede encontrar el valor exacto de $t_g(2,q)$ usando el software MAGMA (Programas 8, 9 y 10), con sus respectivos ejemplos que muestra que el bound $\lceil t_2 \rceil$ es optimo para $q = 7, 8, 9, 11$.

q	$\lceil t_1 \rceil$	$t(2,q)$	Ejemplos de Veronesian Arcos en $\mathbb{P}^2(\mathbb{F}_q)$
5	5	6	$[1:0:0], [0:1:0], [0:0:1], [1:1:1], [3:4:1]$
7	5	6	$[0:0:1], [0:1:0], [1:0:0], [1:1:1], [3:2:1], [4,3,1]$
8	6	6	$[0:0:1], [0:1:0], [1:0:0], [1:1:1], [\alpha^3 : \alpha^2 : 1],$ $[\alpha^6 : \alpha^4 : 1]$
9	6	6	$[0:0:1], [0:1:0], [1:0:0], [1:1:1], [\alpha^6 : \alpha^7 : 1]$ $[\alpha^7 : \alpha^3 : 1]$
11	6	7	$[0:0:1], [0:1:0], [0:0:1], [1:1:1], [4:3:1],$ $[5:9:1]$
13	6	8	
16	6	9	
17	6	10	
19	7	10	
23	7	10	
25	7	12	
27	7	12	
29	7	13	
31	7	14	

Tabla 3.3: Comparación de Cotas Inferiores para Arcos y Veronesian Arcos Completos en $\mathbb{P}^2(\mathbb{F}_q)$ para $5 \leq q \leq 31$.

q	$\lceil t_1 \rceil$	$\lceil t_2 \rceil$	$t_g(2,q)$	$t(2,q)$	Ejemplos de Arcos Generalizados en $\mathbb{P}^2(\mathbb{F}_q)$
5	5	6	7	6	$[1:0:0], [0:1:0], [0:0:1], [1:1:1],$ $[1:0:1], [1:1:0], [0:1:1]$
7	5	7	**7**	6	$[0:0:1], [0:1:0], [1:0:0], [1:1:1],$ $[3:0:1], [5:5:1], [2:4:1]$
8	6	7	**7**	6	$[0:0:1], [0:1:0], [1:0:0], [1:1:1],$ $[\alpha:\alpha^2:1], [\alpha^6:1:0], [\alpha^3:\alpha^6:1]$
9	6	7	**7**	6	$[0:0:1], [0:1:0], [1:0:0], [1:1:1],$ $[\alpha^3:\alpha^7:1], [1:\alpha^7:1], [\alpha^6:\alpha^3:1]$
11	6	7	**7**	7	$[0:0:1], [0:1:0], [0:0:1], [1:1:1]$ $[4:5:1], [1:5:1], [5:3:1]$
13	6	7		8	
16	6	7		9	
17	6	7		10	
19	7	7		10	
23	7	7		10	
25	7	7		12	
27	7	7		12	
29	7	7		13	
31	7	7		14	

Tabla 3.4: Comparación Cotas Inferiores para Arcos, Veronesian Arcos y Arcos Generalizado en $\mathbb{P}^2(\mathbb{F}_q)$ para $5 \leq q \leq 31$.

Capítulo 4

Programas en MAGMA

4.1. Códigos α-cíclicos

Programa 1. Códigos α-cíclicos de largo n en $\mathbb{F}_q$.

```
//Ingresar el numero q de elementos del Campo Finito

q:= ... ;
F<w>:=GF(q);
R<x> := PolynomialRing(F);

//Funcion para encontar codigos a-ciclicos de largo n en GF(q)

PCC:=function(n,a);

P:=[0];
for i in [1..n-2] do
P:=P cat [0];
end for;
T:= [-a] cat P cat [1];
f:=R!T;
n:=Degree(f);
W1:=[]; W2:=[];
for i in [1..#Factorisation(f)] do
if Factorisation(f)[i][2] eq 1 then
a:=R!Factorisation(f)[i][1];
k:=Degree(f)-Degree(R!a);
```

```
G:=Matrix(F,k,n,[[Coefficient((R!a)*x^i,j): j in {0..n-1}] :
 i in {0..k-1}]);
L:=LinearCode(G);
a;
print " ";
G;
print " ";
print "Code MDS of type: ", n, k, MinimumWeight(L);
print "-------------";
W1:= W1 cat [k];
W2:= W2 cat [MinimumWeight(L)];
end if;
if Factorisation(f)[i][2] ne 1 then
for j in [1.. Factorisation(f)[i][2]] do
a:=(R!Factorisation(f)[i][1])^j;
k:=Degree(f)-Degree(R!a);
G:=Matrix(F,k,n,[[Coefficient((R!a)*x^i,j): j in {0..n-1}] :
 i in {0..k-1}]);
L:=LinearCode(G);
a;
print " ";
G;
print " ";
print "Code of type: ", n, k, MinimumWeight(L);
print "-------------";
W1:= W1 cat [k];
W2:= W2 cat [MinimumWeight(L)];
end for; end if; end for;
print "Spectrum of the distances for", f;
print "n=", n;
print "k=";
W1;
print "d=";
return W2;
end function;
```

Programa 2. Códigos skew α-cíclicos en $\mathbb{F}_q$ y su código dual skew α^{-1}-cíclico

```
//Ingresar en qq cantidad de elementos del Campo Finito
//y en pp la potencia de Frobenius

qq:= .. ;
pp:= .. ;
```

```
F<w>:=GF(qq);
R<X>:=TwistedPolynomials(F:q:=pp);

//Funcion para encontrar un codigo skew a-ciclico de largo n
//y su codigo dual

SkewGCC:=function(n,a);

P:=[0];
for i in [1..n-2] do
P:=P cat [0];
end for;
T:= [-a] cat P cat [1];
f:=R!T;
Q:=[0];
for i in [1..n-2] do
Q:=Q cat [0];
end for;
b:=1/a;
TD:= [-b] cat P cat [1];
g:=R!TD;
V:=VectorSpace(F,n);
dd:=[]; ddd:=[];
E:=[x : x in F | x ne 0];
S:=CartesianProduct(E,CartesianPower(F,n-1));
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 [R!ll];
end if; end for;
for sss in S do
lll:=[sss[1]] cat [p : p in sss[2]];
qd,rd:=Quotrem(g,R!lll);
if rd eq R![0] then
ddd := ddd cat [R!lll];
end if; end for;
for i in [1.. #dd] do
if Degree(dd[i]) ge 1 then
k:=Degree(f)-Degree(dd[i]);
G:=Matrix(F,k,n,[V!(HorizontalJoin(Matrix(1, j+Degree(dd[i])+1,
Eltseq((R![0,1])^j*dd[i])), ZeroMatrix(F, 1, n-j-Degree(dd[i])-1))):
j in {0..k-1}]);
```

```
L:=LinearCode(G);
for t in [1.. #ddd] do
if Degree(ddd[t]) ge 1 then
kd:=Degree(g)-Degree(ddd[t]);
if kd eq n-k then
GD:=Matrix(F,kd,n,[V!(HorizontalJoin(Matrix(1, j+Degree(ddd[t])+1,
Eltseq((R![0,1])^j*ddd[t])), ZeroMatrix(F, 1, n-j-Degree(ddd[t])-1))):
j in {0..kd-1}]);
O:=ZeroMatrix(F,k,kd);
if G*Transpose(GD) eq O then
LD:=LinearCode(GD);
dd[i];
print " ";
G;
print " ";
print "Code Skew", a,"-cyclic of type: ", n, k, MinimumWeight(L);
print "--------------------------------------";
dd[t];
print " ";
GD;
print " ";
print "Code Dual Skew", b,"-cyclic of type: ", n, kd, MinimumWeight(LD);
print "======================================";
print " ";
end if; end if; end if; end for; end if; end for;
return "end";
end function;
```

Programa 3. Códigos MDS α-cíclicos en $\mathbb{F}_q$.

```
//Ingresar el numero q de elementos del Campo Finito

MDScodes:=function(q);

F<w>:=GF(q);
R<x> := PolynomialRing(F);
W1:=[];
for m in [2..100] do
FF:=[ x : x in F | x ne 0];
for l in FF do
P:=[0];
for i in [1..m-2] do
P:=P cat [0];
```

```
end for;
v:= [-l] cat P cat [1];
f:=R!v;
n:=Degree(f);
if GreatestCommonDivisor(n,q) ne 1 then
for i in [1..#Factorisation(f)] do
if Factorisation(f)[i][2] eq 1 then
a:=R!Factorisation(f)[i][1];
k:=Degree(f)-Degree(R!a);
G:=Matrix(F,k,n,[[Coefficient((R!a)*x^i,j): j in {0..n-1}] :
 i in {0..k-1}]);
L:=LinearCode(G);
if  2 le k and k le n-2 then
if MinimumWeight(L) eq n-k+1 then
print "Generator Polynomial of the", l , "-Cyclic Code:";
a;
print " ";
G;
print " ";
print "Code MDS of type: ", n, k, MinimumWeight(L);
print "-------------";
W1:= W1 cat [n];
end if; end if; end if;
if Factorisation(f)[i][2] ne 1 then
for j in [1.. Factorisation(f)[i][2]] do
a:=(R!Factorisation(f)[i][1])^j;
k:=Degree(f)-Degree(R!a);
G:=Matrix(F,k,n,[[Coefficient((R!a)*x^i,j): j in {0..n-1}] :
 i in {0..k-1}]);
L:=LinearCode(G);
if 2 le k and k le n-2 then
if n eq 2 then
f;
end if;
if MinimumWeight(L) eq n-k+1 then
print "Generator Polynomial of the", l , "-Cyclic Code:";
a;
print " ";
G;
print " ";
print "Code of type: ", n, k, MinimumWeight(L);
print "-------------";
W1:= W1 cat [n];
```

```
end if; end if; end for; end if; end for;
end if; end for; end for;
print "Spectrum of the large of codes";
return W1;
end function;
```

Programa 4. Códigos MDS skew α-cíclicos en $\mathbb{F}_q$, dado el polinomio $x^n - \alpha$.

```
//Ingresar el numero q de elementos del campo finito y la potencia t
 del automorfismo de Frobenius

q:= ...
t:= ...
F<w>:=GF(q);
R<X>:=TwistedPolynomials(F:q:=t);

//Funcion para encontrar codigos MDS skew a-cilicicos dado
 el polinomio de la forma [a,0,...,1]

SkewGCC:=function(v);
f:=R!v;
n:=Degree(f);
V:=VectorSpace(F,n);
W1:=[]; W2:=[]; dd:=[];
E:=[x : x in F | x ne 0];
S:=CartesianProduct(E,CartesianPower(F,n-1));
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 [R!ll];
end if; end for;
for i in [1.. #dd] do
if Degree(dd[i]) ge 1 then
k:=Degree(f)-Degree(dd[i]);
G:=Matrix(F,k,n,[V!(HorizontalJoin(Matrix(1, j+Degree(dd[i])+1,
Eltseq((R![0,1])^j*dd[i])), ZeroMatrix(F, 1, n-j-Degree(dd[i])-1))):
j in {0..k-1}]);
L:=LinearCode(G);
if MinimumWeight(L) eq n-k+1 then
dd[i];
print " ";
G;
```

```
print " ";
print "Code MDS of type: ", n, k, MinimumWeight(L);
print "-------------";
W1:= W1 cat [k];
W2:= W2 cat [MinimumWeight(L)];
end if; end if; end for;
print "Spectrum of the distances for", f;
print "n=", n;
print "k=";
W1;
print "d=";
return W2;
end function;
```

4.2. Arcos y Arcos Generalizados

Programa 5. k-arco completo en $\mathbb{P}^2(\mathbb{F}_q)$, con $q \geq 5$ (Versión 1).

```
//Función para  encontrar un k-arco completo en PG(2,q)

function arc(q,a)
P,V,L:=FiniteProjectivePlane(q);
PP:={ V.i : i in [1..q^2+q+1] };
repeat
K:={PP![1,0,0],PP![0,1,0],PP![0,0,1],PP![1,1,1]};
l:={@ L!a : a in Subsets(K,2) @};
pl:={ a : a in Set(l[j]), j in [1..#l] };
repeat
K:=K join { Random( PP diff pl )};
l:={@ L!a : a in Subsets(K,2) @};
pl:={ a : a in Set(l[j]), j in [1..#l] };
until #pl eq q^2+q+1;
until #K eq a;
#K;
return K;
end function;
```

Programa 6. k-arco completo en $\mathbb{P}^2(\mathbb{F}_q)$, con $q \geq 5$ (Versión 2).

```
//Función para  encontrar un k-arco completo en PG(2,q)

function arc(q,a)
K<t>:=GF(q);
P<[x]>:=ProjectivePlane(K);
R<x,y,z> := PolynomialRing(K,3);
V:={P!p : p in Points(Scheme(P,[0]))};
repeat
pts:={P![1,0,0],P![0,1,0],P![0,0,1],P![1,1,1]};
lines:=Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p)) : p in S]) |
 Degree(f) eq 1] : S in Subsets(pts,2)]);
pl:={ a : a in Points(Curve(P,[1])) , l in lines};
repeat
pts:=pts join { P!Random( V diff pl ) };
lines:=Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p)) : p in S]) |
 Degree(f) eq 1] : S in Subsets(pts,2)]);
pl:={ a : a in Points(Curve(P,[1])) , l in lines};
until #pl eq q^2+q+1;
until #pts eq a;
#pts;
return pts;
end function;
```

Programa 7. k-arco completo en $\mathbb{P}^2(\mathbb{F}_q)$ (Versión 3).

```
//Función para  encontrar  k-arco completo en PG(2,q)

function arcos(q,k);
K<t>:=GF(q);
P<[x]>:=ProjectivePlane(K);
R<x,y,z> := PolynomialRing(K,3);
V:={P!p : p in Points(Scheme(P,[0]))};
pts:={P![1,0,0],P![0,1,0],P![0,0,1],P![1,1,1]};
D:= V diff pts;
S1:={@ a : a in Subsets(D,k-4) @};
for j in [1..#S1] do
ptss := pts join S1[j];
card:={};
points:={};
T:={@ {C} : C in Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p))
 : p in S]) | Degree(f) eq 1] : S in Subsets(ptss,2)]) @};
```

```
for k in [1..#T] do
pc:={ a : a in Points(Curve(P,[l])) , l in T[k] };
points:=points join pc;
card:= card join {#(pc meet ptss)};
end for;
if forall(t){ t : t in card | t le 2 } then
if #points eq q^2+q+1 then
#points;
card;
"Cardinalidad ", #ptss;
"Conjunto ", ptss;
end if; end if; end for;
return "end";
end function;
```

Programa 8. k-arco generalizado completo en $\mathbb{P}^2(\mathbb{F}_q)$, con $q \geq 5$ (Versión 1).

```
//Función para  encontrar un k-arco generalizado completo
 en PG(2,q)

function arcg(q,a)
P,V,L:=FiniteProjectivePlane(q);
PP:={ V.i : i in [1..q^2+q+1] };
repeat
K:={PP![1,0,0],PP![0,1,0],PP![0,0,1],PP![1,1,1]};
l:={@ L!a : a in Subsets(K,2) @};
pl:={ a : a in Set(l[j]), j in [1..#l] };
D:=pl;
repeat
K:=K join { Random( PP diff D )};
l:={@ L!a : a in Subsets(K,2) @};
pl:={ a : a in Set(l[j]), j in [1..#l] };
c:={@ A : A in Subsets(K,5) @};
pc:={ A : A in Conic(c[n]) , n in [1..#c] };
D:=pl join pc;
until #D eq q^2+q+1;
if PP diff pc ne {} then
K:=K join {Random( PP diff pc )};
end if;
if #K eq a then
#K; end if;
until #K eq a; return  K;
end function;
```

Programa 9. k-arco generalizado completo en $\mathbb{P}^2(\mathbb{F}_q)$, con $q \geq 5$ (Versión 2).

```
//Función para  encontrar un k-arco generalizado completo
// en PG(2,q) en m-intentos

function arcgeq(q,a,m)
K<t>:=GF(q);
P<[x]>:=ProjectivePlane(K);
R<x,y,z> := PolynomialRing(K,3);
V:={P!p : p in Points(Scheme(P,[0]))};
for j in [1..m] do
pts:={P![1,0,0],P![0,1,0],P![0,0,1],P![1,1,1]};
lines:=Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p)) : p in S]) |
 Degree(f) eq 1] : S in Subsets(pts,2)]);
pl:={ a : a in Points(Curve(P,[l])) , l in lines};
D:=pl;
repeat
pts:=pts join { P!Random( V diff D ) };
lines:=Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p)) : p in S]) |
 Degree(f) eq 1] : S in Subsets(pts,2)]);
pl:={ a : a in Points(Curve(P,[l])) , l in lines};
conics:=Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p)) : p in S]) |
 Degree(f) eq 2] : S in Subsets(pts,5)]);
pc:={ a : a in Points(Curve(P,[l])) , l in conics};
D:= pl join pc;
until #D eq q^2+q+1;
if #pc ne q^2+q+1 then
pts:=pts join {Random( V diff pc )};
end if;
repeat
conics:=Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p)) : p in S]) |
 Degree(f) eq 2] : S in Subsets(pts,5)]);
pc:={ a : a in Points(Curve(P,[l])) , l in conics};
if #pc ne q^2+q+1 then
pts2:= pts join {Random( V diff pc )};
T:={@ {C} : C in Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p)) :
 p in S]) | Degree(f) eq 2] : S in Subsets(pts2,5)]) @};
card:={};
for k in [1..#T] do
pc:={ a : a in Points(Curve(P,[l])) , l in T[k] };
card:=card join {#(pc meet pts2)};
end for;
if forall(t){ t : t in card | t le 5 } then
pts:=pts2; F:=0;
```

```
else
F:=1; end if;
else
F:=1; end if;
until F eq 1;
if #pts eq a then
#pts; pts; end if; end for;
end function;
```

Programa 10. k-arco generalizado completo en $\mathbb{P}^2(\mathbb{F}_q)$ (Versión 3).

```
//Función para  encontrar un k-arco generalizado completo en PG(2,q)

function Arcg(q,k)
K<t>:=GF(q);
P<[x]>:=ProjectivePlane(K);
R<x,y,z> := PolynomialRing(K,3);
V:={P!p : p in Points(Scheme(P,[0]))};
pts:={P![1,0,0],P![0,1,0],P![0,0,1],P![1,1,1]};
D:= V diff pts;
S1:={@ e : e in Subsets(D,k-4) @};
for j in [1..#S1] do
ptss := pts join S1[j];
card:={};
pplane:={};
T:={@ {C} : C in Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p))
 : p in S]) | Degree(f) eq 2] : S in Subsets(ptss,5)]) @};
for g in [1..#T] do
pplane:=pplane join { b : b in Points(Curve(P,[l])) , l in T[g] };
pc:={ b : b in Points(Curve(P,[l])) , l in T[g] };
card:= card join {#(pc meet ptss)};
end for;
if forall(t){ t : t in card | t le 5 } then
if #pplane eq q^2+q+1 then
#pplane;
"Cardinalidad ", #ptss;
"Conjunto ", ptss;
end if; end if; end for;
return "fin";
end function;
```

Programa 11. k-arco generalizado y Veronesian k-arco completos en $\mathbb{P}^2(\mathbb{F}_q)$.

```
//Función para  encontrar un Veronesian k-arcos completos en PG(2,q)

function Arcg(q,k)
K<t>:=GF(q);
P<[x]>:=ProjectivePlane(K);
R<x,y,z> := PolynomialRing(K,3);
V:={P!p : p in Points(Scheme(P,[0]))};
pts:={P![1,0,0],P![0,1,0],P![0,0,1],P![1,1,1]};
D:= V diff pts;
S1:={@ e : e in Subsets(D,k-4) @};
for j in [1..#S1] do
ptss := pts join S1[j];
card1:={};
card2:={};
pplane:={};
T1:={@ {C} : C in Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p))
 : p in S]) | Degree(f) eq 1] : S in Subsets(ptss,2)]) @};
T2:={@ {C} : C in Set(&cat[[f : f in Basis(&meet[Ideal(Cluster(p))
 : p in S]) | Degree(f) eq 2] : S in Subsets(ptss,5)]) @};
for g in [1..#T1] do
pplane:=pplane join { b : b in Points(Curve(P,[l])) , l in T1[g] };
pt:={ b : b in Points(Curve(P,[l])) , l in T1[g] };
card1:= card1 join {#(pt meet ptss)};
end for;
for g in [1..#T2] do
pplane:=pplane join { b : b in Points(Curve(P,[l])) , l in T2[g] };
pc:={ b : b in Points(Curve(P,[l])) , l in T2[g] };
card2:= card2 join {#(pc meet ptss)};
end for;
if #pplane eq q^2+q+1 then
if forall(t){ t : t in card2 | t le 5 } then
if forall(t){ t : t in card1 | t le 2 } then
"El conjunto es un Veronesian Arco Completo";
"Cardinalidad ", #ptss;
"Conjunto ", ptss;
print "-----------------------" ;
end if; end if; end if; end for;
return "fin";
end function;
```

Programa 12. Hiperóvalos en $\mathbb{P}^2(\mathbb{F}_8)$.

```
q:=8;

F<w>:=GF(q);
R<x>:=PolynomialRing(F);
PS1<[Y]>:=ProjectiveSpace(F,1);
PS2<[X]>:=ProjectiveSpace(F,2);

PPS:=Points(Scheme(PS2,[0]));
PPS1:=Points(Scheme(PS1,[0]));

//Construccion Polinomios de Permutacion

PP:={};
for i in [1..#PPS] do
s:=PPS[i][1]+PPS[i][2]+PPS[i][3];
if s eq F!1  then
PF:=R![0,0,PPS[i][1],0,PPS[i][2],0,PPS[i][3]];
ImgPF:={ Evaluate(PF,k) : k in F };
if #ImgPF eq q then
PP:=PP join {PF};
for j in F do
PFj:=( Evaluate(PF,x+j) + Evaluate(PF,j) )/x;
ImgPFj:={ Evaluate(PFj,k) : k in F };
if #ImgPFj ne 8 or Evaluate(PFj,0) ne 0 then
PP:=PP diff {PF};
end if; end for; end if; end if; end for;
PP1:=[ p : p in PP ];
PP1;

//Funcion para encontrar arcos, dado el polinomio  PP1

f:=function(n);
PP1[n];
return Matrix(10,3,[ Evaluate(PP1[n],0),0,1,
Evaluate(PP1[n],1),1,1, Evaluate(PP1[n],w),w,1,
Evaluate(PP1[n],w^2),w^2,1, Evaluate(PP1[n],w^3),w^3,1,
Evaluate(PP1[n],w^4),w^4,1, Evaluate(PP1[n],w^5),w^5,1,
Evaluate(PP1[n],w^6),w^6,1,0,1,0,1,0,0]);
end function;
```

Programa 13. Hiperóvalos en $\mathbb{P}^2(\mathbb{F}_{16})$.

```
q:=16;

F<w>:=GF(q);
R<x>:=PolynomialRing(F);

PP:={};

//Construcción de Polinomios de Permutacion

for i1,i2,i3,i4,i5,i6,i7 in F do
s:=i1+i2+i3+i4+i5+i6+i7;
if s eq F!1  then
PF:=R![0,0,i1,0,i2,0,i3,0,i4,0,i5,0,i6,0,i7];
ImgPF:={ Evaluate(PF,k) : k in F };
if #ImgPF eq q then
PP:=PP join {PF};
for j in F do
PFj:=( Evaluate(PF,x+j) + Evaluate(PF,j) )/x;
ImgPFj:={ Evaluate(PFj,k) : k in F };
if #ImgPFj ne q or Evaluate(PFj,0) ne 0 then
PP:=PP diff {PF};
end if; end for; end if; end if; end for;
PP1:=[ p : p in PP ];
PP1;

//Funcion para encontrar arcos, dado el polinomio  PP1

f:=function(n);
PP1[n];
return Matrix(10,3,[ Evaluate(PP1[n],0),0,1,
Evaluate(PP1[n],1),1,1, Evaluate(PP1[n],w),w,1,
Evaluate(PP1[n],w^2),w^2,1, Evaluate(PP1[n],w^3),w^3,1,
Evaluate(PP1[n],w^4),w^4,1, Evaluate(PP1[n],w^5),w^5,1,
Evaluate(PP1[n],w^7),w^7,1, Evaluate(PP1[n],w^8),w^8,1,
Evaluate(PP1[n],w^9),w^9,1, Evaluate(PP1[n],w^10),w^10,1,
Evaluate(PP1[n],w^11),w^11,1, Evaluate(PP1[n],w^12),w^12,1,
Evaluate(PP1[n],w^13),w^13,1, Evaluate(PP1[n],w^14),w^14,1,0,1,0,1,0,0]);
end function;
```

Bibliografía

[1] Ball, S. On small complete arcs in a finite plane. *Discrete Mathematics* 174, 1-3 (1997), 29–34.

[2] Bartoli, D., Davydov, A., Faina, G., Marcugini, S., and Pambianco, F. New upper bounds on the smallest size of a complete arc in a finite desarguesian projective plane. *Journal of Geometry* 104, 1 (2013), 11–43.

[3] Berlekamp, E. *Algebraic Coding Theory.* McGraw-Hill, 1968.

[4] Bose, R. C. Mathematical theory of the symmetrical factorial design. *Sankhyā: The Indian Journal of Statistics* 8 (1947), 107–166.

[5] Boucher, D., Sole, P., and Ulmer, F. Skew constacyclic codes over galois rings. *Advances in Mathematics of Communications* 2 (2008), 273–292.

[6] Boucher, D., and Ulmer, F. Codes as modules over skew polynomial rings. *Cryptography and coding, Lecture Notes in Comput. Sci. 5921* (2009), 38–55.

[7] Boucher, D., and Ulmer, F. A note on the dual codes of module skew codes. *Crystography and Coding* 7089 (2011), 230–243.

[8] Boucher, D., and Ulmer, F. Linear codes using skew polynomials with automorphisms and derivations. *Designs, Codes and Cryptography* 70, 3 (2014), 405–431.

[9] Boucher, D., Ulmer, F., and W.Geiselmann. Skew-cyclic codes. *Applicable Algebra in Engineering, Communication and Computing* 18 (2007), 379–389.

[10] Coolsaet, K., and Sticker, H. The complete k-arcs of PG$(2, 27)$ and PG$(2, 29)$. *Journal of Combinatorial Designs* 19 (2011), 111–130.

[11] Edgar, T. Finite projective geometries and linear codes, 2004.

[12] Fogarty, N., and Gluesing-Luerssen, H. A circulant approach to skew-constacyclic codes. *Finite Fields Appl. 35* (2015), 92–114.

[13] Glynn, D. G. *Two new sequences of ovals in finite Desarguesian planes of even order*, vol. 1036. Combinatorial Mathematics X, Lecture Notes in Mathematics, L. R. A. Casse, 1983, pp. 217–229.

[14] Grassl, M. Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de`, 2007. Accessed on 2016-03-31.

[15] Harris, J. *Algebraic Geometry: A First Course*. Graduate Texts in Mathematics. Springer, 1992.

[16] Hirschfeld, J., and Korchmáros, G. On the embedding of an arc into a conic in a finite plane. *Finite Fields and Their Applications* 2, 3 (1996), 274–292.

[17] Hirschfeld, J. W. P. *Projective Geometries over Finite Field*. Oxford University Press, 1979.

[18] Hirschfeld, J. W. P. *Finite Projective Space of Three Dimensions*. Oxford University Press, 1985.

[19] Hirschfeld, J. W. P. Complete arcs. *Descrete Mathematics* 174, 1-3 (1997), 177–184.

[20] Hirschfeld, J. W. P., and Thas, J. A. Open problemas in finite projective spaces. *Finite Fields and Their Applications* 32 (2015), 44–81.

[21] Lam, T., and Leroy, A. Vandermonde and wronskian mattrices over division rings. *Journal of Algebra* 119 (1988), 308–336.

[22] Landjev, I. Linear codes over finite fields and finite projective geometries. *Discrete Mathematics* 213, 1-3 (2000), 211–244.

[23] Lefschetz, S. *Algebraic Geometry*. Princeton University Press, 2015.

[24] Leroy, A. Noncommutative polynomial maps. *Journal of Algebra and Its Aplications* 11, 4 (2012), 1250076 (16 pages).

[25] Lidl, R., and Niederreiter, H. *Introduction to Finite Fields and their applications*. Cambridge University Press, 1986.

[26] Ling, S., and Xing, C. *Coding Theory, A First Course*. Cambridge University Press, 2004.

[27] Lunelli, L., and Sce, M. Considerazioni aritmetiche e risultati sperimentali sui $\{K, n\}_q$-archi. *Istituto Lombardo, Accademia di Scienze e Lettere* 98 (1964), 3–52.

[28] MacWilliams, F., and Sloane, N. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[29] Maruta, T. A geometric approach to semi-cyclic codes. *Advances in finite geometries and designs* (1991), 311–318.

[30] Maruta, T. On the existence of cyclic and pseudo-cyclic MDS codes. *European Journal of Combinatorics* 19, 2 (1998), 159–174.

[31] Maruta, T., Shinohara, M., and Takenaka, M. Constructing linear codes from some orbits of projectivities. *Discrete Mathematics* 308, 5-6 (2008), 832–841.

[32] McDonald, B. R. *Finite Ring with Identity*. Marcel Dekker Inc., 1943.

[33] Segre, B. Ovals in a finite projective plane. *Canadian Journal of Mathematics* 7 (1955), 414–416.

[34] Segre, B. Sui k-archi nei piani finiti di caratteristica due. *Rev. Mat. Pures Appl.* 2 (1957), 289–300.

[35] Segre, B. Ovali e curve σ nei piani di galois di caratteristica due. *Atti dell' Accad. Naz. Lincei Mem.* 8 (1962), 785–790.

[36] Segre, B. Introduction to galois geometries. *Atti della Accademia Nazionale dei Lincei* 8 (1967), 133–236.

[37] Shallue, C. J. Permutation polynomials of finite fields, 2012.

[38] Shannon, C. A mathematical theory of communication. *Bell System Technical Journal* 27 (1948), 379–423.

[39] Siap, I., Abualrub, T., Aydin, N., and Seneviratne, P. Skew cyclic codes of arbitrary length. *Int. J. Inf. Coding Theory* 2, 1 (2011), 10–20.

[40] Singleton, R. Maximum distance q -nary codes. *Information Theory, IEEE Transactions on* 10, 2 (1964), 116–118.

[41] Tapia, L., and Tironi, A. Dual codes of product semi-linear codes. *Linear Algebra and its Applications* 457 (2014), 114–153.

[42] Tapia, L., and Tironi, A. Some properties of skew codes over finite fields. *arXiv:1507.02726* (2015).

[43] Thas, J. Complete arcs and algebraic curves in PG$(2, q)$. *Journal of Algebra* 106, 2 (1987), 451–464.

[44] Ueno, K., and Nomizu, K. *An Introduction to Algebraic Geometry.* American Mathematical Society, 1997.

[45] Zehendner, E. A non-existence theorem for cyclic MDS-codes. *Atti Sem. Mat. Fis. Univ. Modena* 32 (1983), 203–205.