UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE MATEMÁTICA

CÓDIGOS CÍCLICOS
CON UNA APLICACIÓN A LA CORRECCIÓN DE ERRORES DE RÁFAGA

Proyecto de grado

PRESENTADO PARA OPTAR AL GRADO DE LICENCIADO EN MATEMÁTICA

Postulante: Vladimir Mamani Mamani

Tutor: Lic. Ronnald Álvaro Silva Guzmán

La Paz - Bolivia

2019

Dedicatoria

A mis padres por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo.
Tambien a toda mi familia por el apoyo y la paciencia en mi formación.
Finalmente a mi hija Mileva por ser mi inspiración y la razón de superación en mi vida.

Agradecimiento

A la Universidad Mayor de San Andrés que me acogió en el trascurso de mi formación profesional, a los docentes, administrativos, amigos y familiares que me apoyaron y dieron su apoyo incondicional.

Así mismo a mi tutor al Lic. Ronnald Álvaro Silva Guzmán por guiarme y apoyarme en todo momento del desarrollo del trabajo, tambien agradecer a los tribunales Lic. Ramiro Choque Canaza y M. Sc. Roberto Carlos Huaranca Ampa por la paciencia, las correcciones y la disponibilidad de tiempo de los mismos, un agradecimiento muy especial a mis compañeros de la Carrera de Matemática, a los Docentes y a la Administración de la misma.

Finalmente un agradecimiento a toda la Comunidad Matemática de la Facultad de Ciencias Puras y Naturales, quién me formo en todo este tiempo.

Índice general

Capítulo 1

Introducción y Planteamiento del problema

1.1. Introducción

En pleno siglo XXI se utilizan códigos que facilitan el intercambio de información, ya que se vive en una era digital, es así que en todo sistema digital, ya sea de comunicaciones, almacenamiento de datos, la información se ve afectada por diversos fenómenos, generando gran área de trabajo que busca obtener mejores resultados en la transmisión de la información, para lo cual se han desarrollado toda una teoría de codificación y decodificación, los cuales en general se han aplicado primordialmente con tres grandes objetivos, como el de desarrollar y aplicar los algoritmos y códigos que corrijan errores de ráfaga, detectar-corregir posibles errores aleatorios y codificar-decodificar la variedad de palabras enviadas y recibidas, con la ayuda de la teoría de códigos lineales y cíclicos.

En otras palabras, hacer la transmisión rápida, fiable y segura. En este trabajo se enfocará a corregir esos errores el cual son ocacionados por diversas circunstancias.

1.2. Antecedentes

El estudio de los códigos cíclicos surgen de los códigos lineales, los cuales tienen estructura de espacio vectorial. Las estructuras algebraicas simplifican el estudio de códigos lineales y cíclicos. Por ejemplo un Código Lineal puede ser descrito por su matriz generadora.

En este trabajo, me enfocaré en los códigos cíclicos, presentando su parte teórica y algunas propiedades importantes, para la construcción de los mismos presentando su polinomio generador.

Los códigos cíclicos fueron estudiados por primera vez por Prange en 1957. Desde entonces, teóricos de códigos han hecho gran progreso en el estudio de códigos cíclicos para la corrección de errores de ráfaga. Muchas clases importantes de códigos están entre códigos cíclicos, como códigos de Hamming, códigos Golay y otros.

Primeramente, definimos los códigos cíclicos y luego se discutirá su estructura algebraica y otras propiedades. Caracterizamos a dichos códigos mediante un polinomio el cual sera el generador del código.

Con la teoría necesaria y las propiedades de los Códigos Ciclicos veremos la aplicación de los mismos con los algoritmos para la corrección de errores de ráfaga.

1.3. Planteamiento del problema

En el presente trabajo se plantea establecer los fundamentos algebraicos, con los antecedentes ya formulados anteriormente, surge la siguiente interrogante:

1.4. Formulación del problema

¿Cuál es la interpretación de la aplicación del algoritmo de decodificación para los códigos ciclicos que faciliten la corrección de errores de ráfaga?.
¿Cómo detectar y corregir los posibles errores aleatorios en las palabras enviadas y recibidas para códigos cíclicos?.

1.5. Conocimientos previos

El trabajo a realizar se basa en la teoría de números, anillos, anillos de polinomios, algebra lineal y teoría de campos finitos.

1.6. Objetivos

1.6.1. Objetivo General

Aplicar los algoritmos y códigos que corrigen errores de ráfaga en un Código Cíclico determinado

1.6.2. Objetivos Específicos

✓Conceptuar los códigos lineales, los códigos cíclicos y códigos que corrigen errores de ráfaga.

✓Codificar y decodificar la variedad de palabras enviadas y recibidas, con la ayuda de la teoría de códigos lineales y cíclicos.

✓Detectar y corregir posibles errores aleatorios en las palabras enviadas y recibidas, para hacer el uso del teorema del algoritmo de decodificación para códigos cíclicos el cual facilitará la comprensión de los Códigos Lineales y Ciclicos.

1.7. Alcances y limitaciones

Los alcances de este trabajo, es dar una introducción a la teoría algebraica de Códigos Lineales, el cual estará enfocado en los Códigos Cíclicos y su respectiva definición y algunas propiedades, para luego aplicar esta teoría para encontrar los pasos para la decodificación algorítmica de los códigos ciclicos aplicados a los errores de ráfaga. Por su puesto que la teoría de códigos ofrece una gran variedad como los códigos de Hamming, de Golay o de Huffmman en otros, estudiados sobre anillos, sobre curvas algebraicas, en este trabajo no se desarrollaran ninguno de ellos. El objetivo de la misma es dar una información sobre otras aplicaciones del álgebra abstracta, y marcar una línea de investigación para trabajos posteriores.

1.8. Metodología

La metodología a ser utilizado en la elaboración de este proyecto de grado sera la estándar para este tipo de investigación, está enmarcada a la resolución de problemas no resueltos en la malla curricular actual y el planteamiento de problemas específicos dados por el tutor, el cual se pretende obtener el objetivo señalado. Las reuniones con el tutor son desde anteriores gestiones, pero en esta gestión los seminarios con el tutor son semanales los días jueves y viernes en el cual se discuten las observaciones y los problemas resueltos para luego proceder a la redacción de los resultados obtenidos.

1.9. Medios

Se utilizará la bibliografía afín que se encuentre en la biblioteca de la carrera de Matemática, artículos relacionados con el tema, algunos libros provistos por el tutor y vía internet.

Capítulo 2

Tópicos de Álgebra

2.1. Producto Interno Hermitiano

Sea $\langle , \rangle_H : \mathbb{F}_{q^2}^n \times \mathbb{F}_{q^2}^n \longrightarrow \mathbb{F}_{q^2}$ se define como

$$\langle \mathbf{u}, \mathbf{v} \rangle_H = \sum_{i=1}^{n} u_i v_i^q,$$

donde $\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^2}^n$.

Teorema 2.1.1 $\langle , \rangle_H$ es un producto interno en $\mathbb{F}_{q^2}^n$.

Nota: Este producto interno se llama Hermitiano.

Para un código lineal C sobre $\mathbb{F}_{q^2}$, su dual Hermitiano se define como

$$C^{\perp_H} = \{\mathbf{v} \in \mathbb{F}_{q^2}^n : \langle \mathbf{v}, \mathbf{c} \rangle_H = 0 \text{ para todo } \mathbf{c} \in C\}.$$

Si $C = C^{\perp_H}$, entonces decimos que C es auto-dual con respecto al producto interno Hermitiano.

Demostración. Para que $\langle , \rangle_H$ sea un producto interno debe satisfacer las siguientes condiciones: para todo $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{F}_{q^2}^n$

(a) $\langle \mathbf{u}+\mathbf{v}, \mathbf{w}\rangle_H = \langle \mathbf{u}, \mathbf{w}\rangle_H + \langle \mathbf{v}, \mathbf{w}\rangle_H$;

(b) $\langle \mathbf{u}, \mathbf{v}+\mathbf{w}\rangle_H = \langle \mathbf{u}, \mathbf{v}\rangle_H + \langle \mathbf{u}, \mathbf{w}\rangle_H$;

(c) $\langle \mathbf{u}, \mathbf{v}\rangle_H = 0$ para todo $\mathbf{u} \in \mathbb{F}_{q^2}^n$ si y sólo si $\mathbf{v} = 0$;

(d) $\langle \mathbf{u}, \mathbf{v}\rangle_H = 0$ para todo $\mathbf{v} \in \mathbb{F}_{q^2}^n$ si y sólo si $\mathbf{u} = 0$;

Antes se desglozará la definición:

$$\langle \mathbf{u}, \mathbf{v}\rangle_H = \sum_{i=1}^{n} u_i v_i^q = u_1 v_1^q + u_2 v_2^q + \cdots + u_n v_n^q$$

(a) Sea

$$\begin{aligned}
\langle \mathbf{u}, \mathbf{w}\rangle_H + \langle \mathbf{v}, \mathbf{w}\rangle_H &= \sum_{i=1}^{n} u_i w_i^q + \sum_{i=1}^{n} v_i w_i^q \\
&= u_1 w_1^q + u_2 w_2^q + \cdots + u_n w_n^q + v_1 w_1^q + v_2 w_2^q + \cdots + v_n w_n^q \\
&= u_1 w_1^q + v_1 w_1^q + u_2 w_2^q + v_2 w_2^q + \cdots + u_n w_n^q + v_n w_n^q \\
&= (u_1 + v_1) w_1^q + (u_2 + v_2) w_2^q + \cdots + (u_n + v_n) w_n^q \\
&= \sum_{i=1}^{n} (u_i + v_i) w_i^q \\
&= \langle \mathbf{u} + \mathbf{v}, \mathbf{w}\rangle_H
\end{aligned}$$

(b) Sea

$$\begin{aligned}
\langle \mathbf{u}, \mathbf{v}\rangle_H + \langle \mathbf{u}, \mathbf{w}\rangle_H &= \sum_{i=1}^{n} u_i v_i^q + \sum_{i=1}^{n} u_i w_i^q \\
&= u_1 v_1^q + u_2 v_2^q + \cdots + u_n v_n^q + u_1 w_1^q + u_2 w_2^q + \cdots + u_n w_n^q \\
&= u_1 v_1^q + u_1 w_1^q + u_2 v_2^q + u_2 w_2^q + \cdots + u_n v_n^q + u_n w_n^q \\
&= u_1 (v_1^q + w_1^q) + u_2 (v_2^q + w_2^q) + \cdots + u_n (v_n^q + w_n^q) \\
&= \sum_{i=1}^{n} u_i (v_i^q + w_i^q) \\
&= \sum_{i=1}^{n} u_i (v_i + w_i)^q \\
&= \langle \mathbf{u}, \mathbf{v} + \mathbf{w}\rangle_H
\end{aligned}$$

(c) Si $\mathbf{v} = 0$ entonces para todo $\mathbf{u} \in \mathbb{F}_{q^2}^n$, $\langle \mathbf{u}, \mathbf{v} \rangle_H = 0$; Sea

$$\begin{aligned}\langle \mathbf{u}, \mathbf{v} \rangle_H &= \sum_{i=1}^{n} u_i v_i^q \\ &= u_1 v_1^q + u_2 v_2^q + \cdots + u_n v_n^q \\ &= u_1 0^q + u_2 0^q + \cdots + u_n 0^q \\ &= 0\end{aligned}$$

La recíproca es análoga tomando el caso $\mathbf{u} \neq 0$.

(d) Si $\mathbf{u} = 0$ entonces para todo $\mathbf{v} \in \mathbb{F}_{q^2}^n$, $\langle \mathbf{u}, \mathbf{v} \rangle_H = 0$; Sea

$$\begin{aligned}\langle \mathbf{u}, \mathbf{v} \rangle_H &= \sum_{i=1}^{n} u_i v_i^q \\ &= u_1 v_1^q + u_2 v_2^q + \cdots + u_n v_n^q \\ &= 0 v_1^q + 0 v_2^q + \cdots + 0 v_n^q \\ &= 0\end{aligned}$$

La recíproca es análoga tomando el caso $\mathbf{v} \neq 0$. □

Teorema 2.1.2 Sea C un código lineal sobre $\mathbb{F}_q$ con la matriz generadora $(I_n|A)$, donde I_n es la matriz identidad $n \times n$ y A es una matriz $n \times n$ que satisface $A = A^T$.

(i) Mostrar que C es auto-dual con respecto al producto interno simpléctico $\langle , \rangle_S$, es decir, $C = C^{\perp_S}$, donde

$$C^{\perp_S} = \{\mathbf{v} \in \mathbb{F}_q^{2n} : \langle \mathbf{v}, \mathbf{c} \rangle_S = 0 \text{ para todo } \mathbf{c} \in C\}.$$

(ii) Mostrar que C es equivalente a $C^{\perp}$, su dual bajo el producto interno usual euclidiano.

2.2. Distancia de Hamming

Definición 2.2.3 Sean $\mathbf{x}, \mathbf{y}$ palabras de longitud n sobre un alfabeto A. La distancia (Hamming) de $\mathbf{x}$ a $\mathbf{y}$ denotada por $d(\mathbf{x}, \mathbf{y})$, se define como el número de lugares en los cuales la palabra $\mathbf{x}$ y la palabra $\mathbf{y}$ difieren.

Sí $\mathbf{x} = x_1 \cdots x_n$, $\mathbf{y} = y_1 \cdots y_n$ entonces

$$d(\mathbf{x}, \mathbf{y}) = d(x_1, y_1) + d(x_2, y_2) + \cdots + d(x_n, y_n) \tag{0.1}$$

donde las palabras x_i, y_i se consideran como palabras de longitud 1, y

$$d(x, y) = \begin{cases} 1 & \text{sí } x \neq y \\ 0 & \text{sí } x = y \end{cases}$$

Ejemplo 2.2.4 Sean $A = \{0, 1\}$ y $\mathbf{x} = 01010$, $\mathbf{y} = 01101$, $\mathbf{z} = 11101$, entonces

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}) &= d(01010, 01101) \\ &= d(0, 0) + d(1, 1) + d(0, 1) + d(1, 0) + d(0, 1) \\ &= 0 + 0 + 1 + 1 + 1 = 3 \end{aligned}$$

2.3. MLD (Decodificación de Máxima Probabilidad)

Supongamos que los códigos palabra de un código C se envían a través de un canal de comunicación. Si se recibe una palabra $\mathbf{x}$, podemos calcular las probabilidades de canal directo

$$P(\mathbf{x} \text{ recibido} | \mathbf{c} \text{ enviado})$$

para todos los códigos palabra $\mathbf{c} \in C$. La decodificación de máxima probabilidad (MLD) concluirá que $\mathbf{c_x}$ es el código palabra más probable transmitido sí $\mathbf{c_x}$ maximiza las probabilidades del canal directo; es decir,

$$P(\mathbf{x} \text{ recibido} | \mathbf{c_x} \text{ enviado}) = \max_{\mathbf{c} \in C} P(\mathbf{x} \text{ recibido} | \mathbf{c} \text{ enviado})$$

Hay dos tipos de MLD:

(i) Decodificación completa de máxima probabilidad (CMLD). Sí se recibe una palabra $\mathbf{x}$, encuentre el código palabra más probable transmitido. Sí hay más de una de estas palabras clave, seleccione una de ellas arbitrariamente.

(ii) Decodificación incompleta de máxima probabilidad (IMLD). Sí se recibe una palabra $\mathbf{x}$, encuentre el código palabra más probable transmitido. Sí hay más de una de estas palabras clave, solicite una retransmisión.

Teorema 2.3.5 Sea $C \subseteq \mathbb{F}_q^n$ un código lineal con distancia d. Demuestre que una palabra $\mathbf{x} \in \mathbb{F}_q^n$ es el líder de clase único de $\mathbf{x} + C$ si $wt(x) \leq \lfloor (d-1)/2 \rfloor$.

Teorema 2.3.6 Sea α un elemento primitivo de $\mathbb{F}_{q^m}$. Entonces el polinomio mínimo de α^i con respecto a $\mathbb{F}_q$ es

$$M^{(i)}(x) := \prod_{j \in C_i} (x - \alpha^j),$$

donde C_i es la única clase ciclotómica de q módulo $q^m - 1$ que contiene i.

Demostración. Paso 1: Está claro que α^i es una raíz de $M^{(i)}(x)$ como $i \in C_i$.
Paso 2: Sea $M^{(i)}(x) = a_0 + a_1 x + \ldots + a_r x^r$, donde $a_k \in \mathbb{F}_{q^m}$ y $r = |C_i|$.
Elevando cada coeficiente a su potencia qth, obtenemos

$$a_0^q + a_1^q x + \ldots + a_r^q x^r = \prod_{j \in C_i} (x - \alpha^{qj}) = \prod_{j \in C_{qi}} (x - \alpha^j) = \prod_{j \in C_i} (x - \alpha^j) = M^{(i)}(x).$$

Tengamos en cuenta que utilizamos el hecho de que $C_i = C_{qi}$ en la fórmula anterior. Por lo tanto, $a_k = a_k^q$ para todo $0 \leq k \leq r$; es decir, a_k son elementos de $\mathbb{F}_q$. Esto significa que $M^{(i)}(x)$ es un polinomio sobre $\mathbb{F}_q$.
Paso 3: Como α es un elemento primitivo, tenemos $\alpha^j \neq \alpha^k$ para dos elementos distintos j, k de C_i. Por lo tanto, $M^{(i)}(x)$ no tiene múltiples raíces. Ahora sea $f(x) \in \mathbb{F}_q[x]$ y $f(\alpha^i) = 0$. Pongamos

$$f(x) = f_0 + f_1 x + \ldots + f_n x^n$$

para algunos $f_k \in \mathbb{F}_q$. Entonces, para cualquier $j \in C_i$, existe un entero l tal que

$j \equiv iq^l \pmod{q^m - 1}$. Por lo tanto,

$$f(\alpha^j) = f(\alpha^{iq^l}) = f_0 + f_1\alpha^{iq^l} + \ldots + f_n\alpha^{niq^l} = f_0^{q^l} + f_1^{q^l}\alpha^{iq^l} + \ldots + f_n^{q^l}\alpha^{niq^l}$$
$$= (f_0 + f_1\alpha^i + \ldots + f_n\alpha^{ni})^{q^l} = f(\alpha^i)^{q^l} = 0.$$

Esto implica que $M^{(i)}(x)$ es un divisor de $f(x)$.

Los tres pasos anteriores muestran que $M^{(i)}(x)$ es el polinomio mínimo de α^i. □

Observación 2.3.7

(i) El grado del polinomio mínimo de α^i es igual al tamaño de la clase ciclotómica que contiene i.

(ii) Por el teorema 2.3.6, sabemos que α^i y α^k tienen el mismo polinomio mínimo sí y solo si i, k están en la misma clase ciclotómica.

Ejemplo 2.3.8 Sea α una raíz de $2 + x + x^2 \in \mathbb{F}_3[x]$; es decir,

$$2 + \alpha + \alpha^2 = 0. \tag{0.2}$$

Entonces, el polinomio mínimo de α tanto como α^3 es $2 + x + x^2$. El polinomio mínimo de α^2 es

$$M^{(2)}(x) = \prod_{j \in C_2} (x - \alpha^j) = (x - \alpha^2)(x - \alpha^6) = \alpha^8 - (\alpha^2 + \alpha^6)x + x^2.$$

Sabemos que $\alpha^8 = 1$ como $\alpha \in \mathbb{F}_9$. Para encontrar $M^{(2)}(x)$, tenemos que simplificar $\alpha^2 + \alpha^6$.

Usamos la relación (0.2) para obtener

$$\alpha^2 + \alpha^6 = (1 - \alpha) + (1 - \alpha)^3 = 2 - \alpha - \alpha^3$$
$$= 2 - \alpha - \alpha(1 - \alpha) = 2 - 2\alpha + \alpha^2 = 0.$$

Por lo tanto, el polinomio mínimo de α^2 es $1 + x^2$. De la misma manera, podemos obtener el polinomio mínimo $2 + 2x + x^2$ de α^5.

Teorema 2.3.9 Sea n un entero positivo con el máximo comun divisor $gcd(q, n) = 1$. Suponga que m es un entero positivo que satisface $n \mid (q^m - 1)$. Sea α un elemento primitivo de $\mathbb{F}_q^m$ y sea $M^{(j)}(x)$ el polinomio mínimo de α^j con respecto a $\mathbb{F}_q$.
Sea $s_1, ..., s_t$ un conjunto completo de representantes de clase ciclotómicos de q *modulo* n. Entonces el polinomio $x^n - 1$ tiene la factorización en polinomios irreducibles mónicos sobre $\mathbb{F}_q$:

$$x^n - 1 = \prod_{i=1}^{t} M^{((q^m-1)s_i/n)}(x)$$

.

Demostración. Colocamos $r = (q^m-1)/n$. Entonces α^r es una enésima raíz primitiva de la unidad y, por lo tanto, todas las raíces de $x^n - 1$ son $1, \alpha^r, \alpha^{2r}, \ldots, \alpha^{(n-1)r}$. Por lo tanto, según la definición del polinomio mínimo, los polinomios $M^{(ir)}(x)$ son divisores de $x^n - 1$, para todo $0 \leq i \leq n - 1$. esta claro que tenenmos

$$x^n - 1 = lcm(M^{(0)}(x), M^{(r)}(x), M^{(2r)}(x), \ldots, M^{((n-1)r)}(x)).$$

Para determinar la factorización de x^n-1, basta con determinar todos los polinomios distintos entre $M^{(0)}(x), M^{(r)}(x), M^{(2r)}(x), \ldots M^{((n-1)r)}(x)$.
En la observación 2.3.7, sabemos que $M^{ir}(x) = M^{jr}(x)$ si y sólo sí, ir y jr están en la misma clase ciclotómica de q módulo $q^m-1 = rn$; es decir, i y j están en la misma clase ciclotómica de q módulo n. Esto implica que todos los polinomios distintos entre $M^0(x), M^r(x), M^{2r}(x), \ldots, M^{((n-1)r)}(x)$ son $M^{s_1 r}(x), M^{s_2 r}(x), \ldots, M^{s_t r}(x)$. Con lo cual la prueba esta completada. □

Definición 2.3.10 Sean $f(x), g(x) \in F[x]$ dos polinomios distintos de cero. El máximo común divisor de $f(x), g(x)$, denotado por $gcd(f(x), g(x))$, es el polinomio monico del grado más alto, que es un divisor de $f(x)$ y $g(x)$. En particular, decimos que $f(x)$ es coprimo (o primo) a $g(x)$ si $gcd(f(x), g(x)) = 1$. El mínimo común múltiplo de $f(x), g(x)$, denotado por $mcm(f(x), g(x))$, es el polinomio monico del grado más bajo que es un múltiplo de ambos $f(x)$ y $g(x)$.

Observación 2.3.11

(i) Si $f(x)$ y $g(x)$ tienen las siguientes factorizaciones:

$$f(x) = a \cdot p_1(x)^{e_1} \cdots p_n(x)^{e_n}, \quad g(x) = b \cdot p_1(x)^{d_1} \cdots p_n(x)^{d_n},$$

donde $a, b \in F^*$, $e_i, d_i \geq 0$ y $p_i(x)$ son polinomios irreducibles monicos distintos (la existencia y la singularidad de tal factorización polinomial son hechos conocidos), entonces

$$gcd(f(x), g(x)) = p_1(x)^{min\{e_1,d_1\}} \ldots p_n(x)^{min\{e_n,d_n\}}$$

y

$$lcm(f(x), g(x)) = p_1(x)^{max\{e_1,d_1\}} \ldots p_n(x)^{max\{e_n,d_n\}}.$$

(ii) Sea $f(x), g(x) \in F[x]$ dos polinomios distintos de cero. Luego existen dos polinomios $u(x), v(x)$ con $deg(u(x)) < deg(g(x))$ y $deg(v(x)) < deg(f(x))$ de manera que

$$gcd(f(x), g(x)) = u(x)f(x) + v(x)g(x).$$

(iii) De (ii), se muestra fácilmente que $gcd(f(x)h(x), g(x)) = gcd(f(x), g(x))$ si $gcd(h(x), g(x)) = 1$.

Hay muchas analogías entre el anillo entero $\mathbf{Z}$ y un anillo polinomial $F[x]$. Enumeramos algunos de ellos en la Tabla 0.1.

Aparte de las analogías en la Tabla 0.1, tenemos el algoritmo de división, los máximos comunes divisores, los mínimos comunes múltiplos, etc., en ambos anillos. Dado que, para cada entero $m > 1$ de $\mathbf{Z}$, se construye el anillo $\mathbf{Z}_m = \mathbf{Z}/(m)$, podemos suponer que el anillo, denotado por $F[x]/(f(x))$, se puede construir para un determinado polinomio $f(x)$ de grado $n \geq 1$. Formamos la Tabla 0.2 para definir el anillo $F[x]/(f(x))$ y lo comparamos con $\mathbf{Z}/(m)$. Enumeramos las dos últimas afirmaciones en la segunda columna de la Tabla 0.2 como un teorema.

El anillo entero $\mathbf{Z}$	*El anillo de polinomios* F [x]
Un entero m	*Un polinomio* f(x)
Un número primo p	*Un polinomio irreducible* p(x)

Tabla 0.1 Analogías entre $\mathbf{Z}$ y $F[x]$.

$\mathbf{Z}_m = \{0, 1, \ldots m-1\}$	$F[x]/(f(x)) := \{\sum_{i=0}^{n-1} a_i x^i : a_i \in F, n \geq 1\}$
$a \oplus b := (a + b(mod\ m))$	$g(x) + h(x) := (g(x) + h(x)(mod\ f(x)))$
$a \odot b := (ab(mod\ m))$	$g(x) \odot h(x) := (g(x)h(x)(mod\ f(x)))$
$\mathbf{Z}_m$ *es un anillo*	$F[x]/(f(x))$ *es un anillo*
$\mathbf{Z}_m$ *es un campo* $\Leftrightarrow$ m *es un primo*	$F[x]/(f(x))$ *es un campo* $f(x)$ *es irreducible*

Tabla 0.2 Más analogías entre $\mathbf{Z}$ y $F[x]$.

Teorema 2.3.12 Sean $v_1, v_2, \ldots v_k$ y $u_1, u_2, \ldots u_k$ vectores en $\mathbb{F}_q^n$ y

$$A = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix} \qquad B = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_k \end{pmatrix}.$$

dos matrices $k \times n$ equivalentes i.e. B se obtiene en A mediante operaciones elementales de renglón.

Entonces, la combinación lineal

$$\mathfrak{Cl}\{v_1, v_2, \ldots v_k\} = \mathfrak{Cl}\{u_1, u_2, \ldots u_k\}$$

.

Demostración. Antes de la desmostración recordemos, al conjunto de las combinaciones lineales de $v_1, v_2, \ldots v_r$, el cual lo denotamos como:

$$\mathfrak{Cl}\{v_1, v_2, \ldots v_r\} = \{\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_r v_r / \alpha_1, \alpha_2, \ldots \alpha_r \in \mathbb{F}_q\}$$

. Tambien recordemos al espacio generado por las filas de una matriz. Si $v_1, v_2, \dots v_k$ son vectores fila en $\mathbb{F}_q^n$ y $A^t = (v_1^t, v_2^t, \dots v_k^t)$, la matriz $A_{k\times n}$ cuyas filas son los vectores v_i, i.e.

$$A = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix}.$$

se denota con $\mathfrak{F}_A$ al S.E. vectorial generado por filas de A, esto es:

$$\mathfrak{F}_A = \mathfrak{Cl}\{v_1, v_2, \dots v_k\}$$

Observe que sí $w \in \mathfrak{F}_A$, se escribe como vector columna, entonces existen escalares $x_1, x_2, \dots x_k$ tal que w=x$_1 v_1^t + x_2 v_2^t + \dots x_k v_k^t = (v_1^t, v_2^t, \dots, v_k^t) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{pmatrix} = A^t x.$

O lo que es lo mismo, existe
$x = (x_1, x_2, \dots x_k)^t \in \mathbb{F}_q^k$ t.q. $w = A^t x$, así $\mathfrak{F}_A$ puede escribirse como

$$\mathfrak{F}_A = \{b \in \mathbb{F}_q^n / b = A^t x \;\; para \;\; algún \;\; x \in \mathbb{F}_q^k\}$$

El espacio generado por las columnas de A es:

$$\mathfrak{F}_{A^t} = \{c \in \mathbb{F}_q^k / c = Ay \;\; para \;\; algún \;\; y \in \mathbb{F}_q^n\}$$

Con estas definiciones empezamos la demostraciones:
Sabemos que:

$$\mathfrak{Cl}\{v_1, v_2, \dots v_k\} = \{b \in \mathbb{F}_q^n / b = A^t x, \;\; para \;\; algún \;\; x \in \mathbb{F}_q^k\}$$

t.b.

$$\mathfrak{Cl}\{u_1, u_2, \dots u_k\} = \{c \in \mathbb{F}_q^n / c = B^t y, \;\; para \;\; algún \;\; y \in \mathbb{F}_q^k\}$$

Si P es el producto de las matrices elementales necesarias para reducir A en B, i.e. $B = PA$ y $P^{-1}B = A$ (P es una matriz $k \times k$)
Sea $b \in \mathfrak{Cl}\{v_1, v_2, \dots v_k\}$ entonces existe un $x \in \mathbb{R}^k$ t.q.

$$b = A^t x = (P^{-1}B)^t x = B^t[(P^-1)^t x] = B^t y$$

donde b es una combinación lineal de las filas de B, por lo cual $b \in \mathfrak{Cl}\{u_1, u_2, \dots, u_k\}$
Así se deduce que:

$$\mathfrak{Cl}\{v_1, v_2, \dots v_k\} \subset \mathfrak{Cl}\{u_1, u_2, \dots, u_k\}$$

Análogamente se muestra que:

$$\mathfrak{Cl}\{u_1, u_2, \dots u_k\} \subset \mathfrak{Cl}\{v_1, v_2, \dots, v_k\}$$

$$\therefore \mathfrak{Cl}\{v_1, v_2, \dots v_k\} = \mathfrak{Cl}\{u_1, u_2, \dots, u_k\}$$

□

Teorema 2.3.13 Si C es un Código Lineal no trivial $[n, k]$ sobre $\mathbb{F}_q$ con matriz generadora $G = (I_k, X)$ en la forma estándar, entonces $H = (-X^T \mid I_{n-k})$ es la matriz de control de paridad de C.

Demostración. A partir de la forma de H está claro que los $n - k$ vectores fila de H son linealmente independientes sobre $\mathbb{F}_q$. Para demostrar que H es una matriz de control de paridad de C (o por definición, H es una matriz generadora de $C^\perp$) queda por verificar que cada vector fila de H sea ortogonal a cada vector fila de G. Ahora

$$HG^T = (-X^T \mid I_{n-k}) \begin{pmatrix} I_k \\ X^T \end{pmatrix} = -X^T I_k + I_{n-k} X^T = -X^T + X^T = 0_{(n-k)\times k},$$

lo cual estaría demostrado. □

Definición 2.3.14 Una matriz $(n - k) \times n$ de control de paridad H sobre $\mathbb{F}_q$ de la forma

$$H = (B \mid I_{n-k})$$

con $(n-k) \times (n-k)$ la matriz identidad I_{n-k} sobre $\mathbb{F}_q$ y algunos $(n-k) \times k$ matriz B sobre $\mathbb{F}_q$ se dice que esta en la forma estándar.

Capítulo 3

Códigos lineales

Un código lineal de longitud n sobre el campo finito $\mathbb{F}_q$ es simplemente un subespacio del espacio vectorial $\mathbb{F}_q^n$. Dado que los códigos lineales son espacios vectoriales, sus estructuras algebraicas a menudo hacen más fáciles de describirlos.

3.1. Espacios Vectoriales sobre Campos Finitos

Recordemos algunas definiciones y propiedades sobre espacios vectoriales sobre campos finitos.

Definición 3.1.1 Sea $\mathbb{F}_q$ el campo finito de orden q. Un conjunto no vacío V, junto a la adición y multiplicación escalar por elementos de $\mathbb{F}_q$, es un espacio vectorial (o espacio lineal) sobre $\mathbb{F}_q$ sí satisface las siguientes condiciones: Para todo $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ y para todo $\lambda, \mu \in \mathbb{F}_q$

(i) $\mathbf{u} + \mathbf{v} \in V$;

(ii) $(\mathbf{u} + \mathbf{v}) + \mathbf{w} = \mathbf{u} + (\mathbf{v} + \mathbf{w})$;

(iii) hay un elemento $\mathbf{0} \in V$ con la propiedad $\mathbf{0} + \mathbf{v} = \mathbf{v} + \mathbf{0}$ para todo $\mathbf{v} \in V$;

(iv) para cada $\mathbf{u} \in V$ hay un elemento de V, $-\mathbf{u}$ tal que $\mathbf{u} + (-\mathbf{u}) = \mathbf{0} = (-\mathbf{u}) + \mathbf{u}$

(v) $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$;

(vi) $\lambda \mathbf{v} \in V$

(vii) $\lambda(\mathbf{u}+\mathbf{v}) = \lambda\mathbf{u} + \lambda\mathbf{v}$, $(\lambda+\mu)\mathbf{u} = \lambda\mathbf{u} + \mu\mathbf{u}$;

(viii) $(\lambda\mu)\mathbf{u} = \lambda(\mu\mathbf{u})$;

(ix) si 1 es la identidad multiplicativa de $\mathbb{F}_q$, entonces $1\mathbf{u} = \mathbf{u}$.

Sea $\mathbb{F}_q^n$ el conjunto de todos los vectores de longitud n con entradas en $\mathbb{F}_q$:

$$\mathbb{F}_q^n = \{(v_1, v_2, ..., v_n) : v_i \in \mathbb{F}_q\}.$$

Definimos la suma de vectores para $\mathbb{F}_q^n$ componente a componente, utilizando la adición definido sobre $\mathbb{F}_q$, es decir, si

$$\mathbf{v} = \{v_1, v_2, \ldots, v_n\} \in \mathbb{F}_q^n \quad \text{y} \quad \mathbf{w} = \{w_1, w_2, \ldots, w_n\} \in \mathbb{F}_q^n,$$

entonces

$$\mathbf{v}+\mathbf{w} = (v_1 + w_1, v_2 + w_2, \ldots, v_n + w_n) \in \mathbb{F}_q^n,$$

También definimos la multiplicación escalar de $\mathbb{F}_q^n$ componente a componente; es decir, si

$$\mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n \quad \text{y} \quad \lambda \in \mathbb{F}_q$$

entonces

$$\lambda\mathbf{v} = (\lambda v_1, \lambda v_2, \ldots, \lambda v_n) \in \mathbb{F}_q^n.$$

Sea $\mathbf{0}$ denotado como el vector cero $(0, 0, \ldots, 0) \in \mathbb{F}_q^n$

Ejemplo 3.1.2 Es fácil comprobar que los siguientes son espacios vectoriales sobre $\mathbb{F}_q$;

(i) (cualquier q) $C_1 = \mathbb{F}_q^n$ y $C_2 = \{\mathbf{0}\}$;

(ii) (cualquier q) $C_3 = \{(\lambda, \lambda, \ldots, \lambda) : \lambda \in \mathbb{F}_q\}$;

(iii) $(q = 2)$ $C_4 = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$;

(iv) $(q = 3)$ $C_5 = \{(0,0,0), (0,1,2), (0,2,1)\}$.

Observación 3.1.3 En algunos momentos se escribirá al vector $(v_1, v_2, \ldots, v_n)$ simplemente como $v_1 v_2 \ldots v_n$.

Definición 3.1.4 Un subconjunto no vacío C de un espacio vectorial V es un subespacio de V si él mismo es un espacio vectorial con la misma adición vectorial y multiplicación escalar como V.

Ejemplo 3.1.5 Utilizando la misma notación que en el ejemplo 3.1.2, es fácil ver que:

(i) (cualquier q) $C_2 = \{0\}$ es un subespacio de ambos C_3 y $C_1 = \mathbb{F}_q^n$ y C_3 es un subespacio de $C_1 = \mathbb{F}_q^n$;

(ii) $(q = 2)$ C_4 es un subespacio de $\mathbb{F}_2^4$;

(iii) $(q = 3)$ C_5 es un subespacio de $\mathbb{F}_3^3$.

Proposición 3.1.6 Un subconjunto no vacío C de un espacio vectorial V sobre $\mathbb{F}_q$ es un subespacio si y sólo sí, la siguiente condición se cumple:

$$\text{si } x, y \in C \text{ y } \lambda, \mu \in \mathbb{F}_q \text{ entonces } \lambda x + \mu y \in C$$

Tengamos en cuenta que, cuando $q = 2$, una condición necesaria y suficiente para que un subconjunto no vacío C de un espacio vectorial V sobre $\mathbb{F}_2$ a un subespacio es:

$$\text{si } x, y \in C \text{ entonces } x + y \in C$$

Definición 3.1.7 Sea V un espacio vectorial sobre $\mathbb{F}_q$. Una combinación lineal de $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r \in V$ es un vector de la forma $\lambda_1 \mathbf{v}_1 + \lambda_2 \mathbf{v}_2 + \ldots + \lambda_r \mathbf{v}_r$, donde $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{F}_q$ son escalares.

Definición 3.1.8 Sea V un espacio vectorial sobre $\mathbb{F}_q$. Un conjunto $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ en V es linealmente independiente si

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots \lambda_r\mathbf{v}_r = 0 \Rightarrow \lambda_1 = \ldots = \lambda_r = 0.$$

El conjunto es linealmente dependiente si no es linealmente independiente, es decir, si hay $\lambda_1, \ldots, \lambda_r \in \mathbb{F}_q$, no todos son cero (pero quizás algunos lo son), de tal manera que

$$\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_r\mathbf{v}_r = 0.$$

Ejemplo 3.1.9

(i) Cualquier conjunto S que contiene $\mathbf{0}$ es linealmente dependiente.

(ii) Para cualquier $\mathbb{F}_q$, $\{(0,0,0,1),(0,0,1,0),(0,1,0,0)\}$ es linealmente independiente.

(iii) Para cualquier $\mathbb{F}_q$, $\{(0,0,0,1),(1,0,0,0),(1,0,0,1)\}$ es linealmente dependiente.

Definición 3.1.10 Sea V un espacio vectorial sobre $\mathbb{F}_q$ y sea $S = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ un subconjunto no vacío de V. El espacio (lineal) de S se define como

$$< S >= \{\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots + \lambda_k\mathbf{v}_k : \lambda_i \in \mathbb{F}_q\}$$

Sí $S = \varnothing$, definimos $< S >= \{\mathbf{0}\}$. Es fácil comprobar que $< S >$ es un subespacio de V, llamado el subespacio generado por S. Dado un subespacio C en V, un subconjunto S de C se llama un grupo electrógeno (conjunto generador) de C si $C =< S >$.

Observación 3.1.11 Sí S ya es un subespacio de V, entonces $< S >= S$.

Ejemplo 3.1.12 (i) Si $q = 2$ y $S = \{0001, 0010, 0100\}$, entonces

$$< S >= \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111\}.$$

(ii) Si $q = 2$ y $S = \{0001, 1000, 1001\}$, entonces

$$< S >= \{0000, 0001, 1000, 1001\}.$$

(iii) Si $q = 3$ y $S = \{0001, 1000, 1001\}$, entonces

$$< S >= \{0000, 0001, 0002, 1000, 2000, 1001, 1002, 2001, 2002\}.$$

Definición 3.1.13 Sea V un espacio vectorial sobre $\mathbb{F}_q$. Un subconjunto no vacío $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ de V se llama una base para V si $V =< B >$ y B es linealmente independiente.

Observación 3.1.14

(i) Si $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ es una base de V, entonces cualquier vector $\mathbf{v} \in V$ se puede expresar como una única combinación lineal de vectores en B; es decir, existen únicos $\lambda_1, \lambda_2, \ldots \lambda_k \in \mathbb{F}_q$ tal que:

$$\mathbf{v} = \lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots \lambda_k\mathbf{v}_k$$

(ii) Un espacio vectorial V sobre un campo finito $\mathbb{F}_q$ puede tener muchas bases; pero todas las bases contienen el mismo número de elementos. este número es llamado la dimensión de V sobre $\mathbb{F}_q$, denotado por la $dim(V)$. En el caso en que V puede ser considerada como un espacio vectorial sobre más de un campo, la notación $dim_{\mathbb{F}_q}(V)$ se puede utilizar para evitar confusión.

Teorema 3.1.15 Sea V un espacio vectorial sobre $\mathbb{F}_q$. Si $dim(V) = k$, entonces

(i) V tiene q^k elementos;

(ii) V tiene $\frac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$ diferentes bases.

Demostración. (i) Si $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ es una base para V, entonces

$$\mathbf{V} = \{\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2 + \ldots \lambda_k\mathbf{v}_k : \lambda_1, \ldots, \lambda_k \in \mathbb{F}_q\}$$

Ya que $|\mathbb{F}_q| = q$, hay exactamente q-opciones para cada uno de $\lambda_1, \ldots, \lambda_k$; por lo tanto, V tiene exactamente q^k elementos.

(ii) Sea $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\}$ denotan una base para V. Ya que $\mathbf{v}_1 \neq 0$, existen $q^k - 1$ opciones para $\mathbf{v}_1$. Para B para ser una base, es necesaria la condición $\mathbf{v}_2 \notin < \mathbf{v}_1 >$

es necesaria la condición, por lo que hay $q^k - q$ opciones para $\mathbf{v}_2$.

Argumentando de esta manera, para cada i tal que $k \geq i \geq 2$, tenemos que $\mathbf{v}_i \notin < \mathbf{v}_1, \ldots, \mathbf{v}_{i-1} >$, así que hay $q^k - q^{i-1}$ opciones para $\mathbf{v}_i$. Por lo tanto existen

$$\prod_{i=0}^{k-1}(q^k - q^i)$$

distintas k-tuples $(\mathbf{v}_1, \ldots, \mathbf{v}_k)$ ordenadas.

Sin embargo, ya que el orden de $\mathbf{v}_1, \ldots, \mathbf{v}_k$ es irrelevante para una base, el número de bases distintas para V es

$$\frac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$$

□

Ejemplo 3.1.16 Sea $q = 2$, $S = \{0001, 0010, 0100\}$ y $V =< S >$, entonces

$$V = \{0000, 0001, 0010, 0100, 0011, 0101, 0110, 0111\}.$$

Notar que S es linealmente independiente, por lo que $dim(V) = 3$. Vemos que $|V| = 8 = 2^3$.

Por el teorema 3.1.15, el número de diferentes bases de V esta dada por

$$\frac{1}{k!}\prod_{i=0}^{k-1}(2^k - 2^i) = \frac{1}{3!}(2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 28.$$

Definición 3.1.17 Sea $\mathbf{v} = (v_1, v_2, \ldots, v_n)$, $\mathbf{w} = (w_1, w_2, \ldots, w_n) \in \mathbb{F}_q^n$.

(i) El producto escalar (también conocido como el producto euclidiano interno) de $\mathbf{v}$ y $\mathbf{w}$ se define como

$$\mathbf{v} \cdot \mathbf{w} = v_1w_1 + v_2w_2 + \ldots + v_nw_n \in \mathbb{F}_q.$$

(ii) Los dos vectores $\mathbf{v}$ y $\mathbf{w}$ se dice que son ortogonales si

$$\mathbf{v} \cdot \mathbf{w} = 0.$$

(iii) Sea S un subconjunto no vacío de $\mathbb{F}_q^n$. El complemento ortogonal $S^\perp$ de S se define como

$$S^\perp = \{\mathbf{v} \in \mathbb{F}_q^n : \mathbf{v} \cdot \mathbf{s} = 0 \text{ para todo } \mathbf{s} \in S\}.$$

Si $S = \emptyset$, entonces definimos $S^\perp = \mathbb{F}_q^n$.

Observación 3.1.18 (i) Es fácil verificar que $S^\perp$ siempre es un subespacio del vector espacio $\mathbb{F}_q^n$ para cualquier subconjunto S de $\mathbb{F}_q^n$, y que

$$< S >^\perp = S^\perp$$

. (ii) El producto escalar es un ejemplo de un producto interno en $\mathbb{F}_q^n$. Un producto interno en $\mathbb{F}_q^n$ es un emparejamiento

$$<,>= \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$$

satisface las siguientes condiciones: para todo $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{F}_q^n$,

(a) $< \mathbf{u} + \mathbf{v}, \mathbf{w} >=< \mathbf{u}, \mathbf{w} > + < \mathbf{v}, \mathbf{w} >$;

(b) $< \mathbf{u}, \mathbf{v} + \mathbf{w} >=< \mathbf{u}, \mathbf{v} > + < \mathbf{u}, \mathbf{w} >$;

(c) $< \mathbf{u}, \mathbf{v} >= 0$ para todo $\mathbf{u} \in \mathbb{F}_q^n$ si y sólo sí $\mathbf{v}$=0;

(d) $< \mathbf{u}, \mathbf{v} >= 0$ para todo $\mathbf{v} \in \mathbb{F}_q^n$ si y sólo sí $\mathbf{u}$=0.

El producto escalar de la definición 3.1.17 es a menudo llamado producto interior euclidiano. Algunos otros productos internos, tales como el producto interior Hermitiana y el producto interior simpléctico, también se utilizan en la teoría de codificación (véase capítulo 2.1.1 - 2.1.2). A lo largo de este proyecto, a menos que se especifique lo contrario, el producto interno utilizado siempre se supone que es el producto escalar, es decir, el producto interno euclidiano.

Ejemplo 3.1.19 (i) Sea $q = 2$ y sea $n = 4$. Si $\mathbf{u} = (1, 1, 1, 1)$, $\mathbf{v} = (1, 1, 1, 0)$, $\mathbf{w} = (1, 0, 0, 1)$, entonces

$$\mathbf{u} \cdot \mathbf{v} = 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 1 + 1 \cdot 0 = 1,$$

$$\mathbf{u} \cdot \mathbf{w} = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 1 \cdot 1 = 0,$$

$$\mathbf{v} \cdot \mathbf{w} = 1 \cdot 1 + 1 \cdot 0 + 1 \cdot 0 + 0 \cdot 1 = 1.$$

Por lo tanto $\mathbf{u}$ y $\mathbf{w}$ son ortogonales.
(ii) Sea $q = 2$ y sea $S = \{0100, 0101\}$. Para encontrar $S^{\perp}$, sea $\mathbf{v} = (v_1, v_2, v_3, v_4) \in S^{\perp}$. Entonces

$$\mathbf{v} \cdot (0, 1, 0, 0) = 0 \Rightarrow v_2 = 0,$$
$$\mathbf{v} \cdot (0, 1, 0, 1) = 0 \Rightarrow v_2 + v_4 = 0.$$

Por lo tanto, tenemos $v_2 = v_4 = 0$. Como v_1 y v_3 puede ser 0 o 1, podemos concluir que

$$S^{\perp} = \{0000, 0010, 1000, 1010\}.$$

Teorema 3.1.20 Sea S un subconjunto de $\mathbb{F}_q^n$, entonces tenemos

$$dim(< S >) + dim(S^{\perp}) = n.$$

Demostración. Por el teorema 3.1.20 es obviamente cierto cuando $< S >= \{0\}$.
Ahora sea $dim(< S >) = k \geq 1$ y supongamos $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ es una base de $< S >$.
Tenemos que demostrar que la $dim(S^{\perp}) = dim(< S >^{\perp}) = n - k$.
Notar que $\mathbf{x} \in S^{\perp}$ si y sólo sí

$$\mathbf{v}_1 \cdot \mathbf{x} = \ldots = \mathbf{v}_k \cdot \mathbf{x} = 0,$$

que es equivalente a decir que $\mathbf{x}$ satisface $A\mathbf{x}^T = 0$, donde A es la matriz $k \times n$ cuya i-ésima fila es $\mathbf{v}_i$.
Las filas de A son linealmente independientes, así que $A\mathbf{x}^T = 0$ es un sistema lineal de ecuaciones k linealmente independientes en n variables. Del álgebra lineal, se sabe que un sistema de este tipo admite un espacio de solución de dimensión $n - k$. □

Ejemplo 3.1.21 Sea $q = 2$, $n = 4$ y $S = \{0100, 0101\}$. Entonces

$$< S >= \{0000, 0100, 0001, 0101\}.$$

Tenga en cuenta que S es linealmente independiente, así que $dim(< S >) = 2$. Hemos calculado que (ejemplo 3.1.19)

$$S^{\perp} = \{0000, 0010, 1000, 1010\}$$

Notemos que $\{0010, 1000\}$ es una base para $S^{\perp}$, así que $dim(S^{\perp}) = 2$. Por lo tanto tenemos verificado que

$$dim(< S >) + dim(S^{\perp}) = 2 + 2 = 4 = n.$$

3.2. Códigos lineales

Ahora estamos listos para introducir los códigos lineales y discutir algunas de sus propiedades elementales.

Definición 3.2.1 Un *código lineal* C de longitud n sobre $\mathbb{F}_q$ es un subespacio de $\mathbb{F}_q^n$.

Ejemplo 3.2.2 Los siguientes son códigos lineales

(i) $C = \{(\lambda, \lambda, \ldots, \lambda) | \, \lambda \in \mathbb{F}_q\}$. Este código es con frecuencia denominado código de repetición.

(ii) $(q = 2)$ $C = \{000, 001, 010, 011\}$.

(iii) $(q = 3)$ $C = \{0000, 1100, 2200, 0001, 0002, 1101, 1102, 2201, 2202\}$.

(iv) $(q = 2)$ $C = \{000, 001, 010, 011, 100, 101, 110, 111\}$.

Definición 3.2.3 Si C es un código lineal en $\mathbb{F}_q^n$. (i) El *código dual* de C es $C^{\perp}$, el complemento ortogonal del subespacio C de $\mathbb{F}_q^n$.
(ii) La *dimensión* del código C es la dimensión de C como un espacio vectorial sobre $\mathbb{F}_q$, es decir $\dim(C)$.

Teorema 3.2.4 Sea C un código lineal de longitud n sobre $\mathbb{F}_q$. Entonces, (i) $|C| = q^{\dim(C)}$, es decir, $\dim(C) = \log_q |C|$;
(ii) $C^{\perp}$ es un código lineal y $\dim(C) + \dim(C^{\perp}) = n$;
(iii) $(C^{\perp})^{\perp} = C$.

Demostración. (i) Es una consecuencia del Teorema 3.1.15(i).

(ii) Se sigue inmediatamente de la Observación 3.1.18(i) y el Teorema 3.1.20 con $C = S$.

(iii) Usando la igualdad en (ii) y una igualdad similar con C reemplazado por $C^{\perp}$, obtenemos $\dim(C) = \dim((C^{\perp})^{\perp})$. Por lo tanto, para probar (iii), es suficiente mostrar que $C \subseteq (C^{\perp})^{\perp}$.

Sea $\mathbf{c} \in C$. Para mostrar que $\mathbf{c} \in (C^{\perp})^{\perp}$, necesitamos mostrar que $\mathbf{c} \cdot \mathbf{x} = 0$ para todo $\mathbf{x} \in C^{\perp}$. Como $\mathbf{c} \in C$ y $\mathbf{x} \in C^{\perp}$, por la definición de $C^{\perp}$, se sigue que $\mathbf{c} \cdot \mathbf{x} = 0$. Por lo tanto (iii) ha sido probado. □

Ejemplo 3.2.5 (i) ($q = 2$) Sea el código $C = \{0000, 1010, 0101, 1111\}$, entonces $\dim(C) = \log_2 |C| = \log_2 4 = 2$. Es fácil ver que $C^{\perp} = \{0000, 1010, 0101, 1111\} = C$, así $\dim(C^{\perp}) = 2$. En particular el Teorema 3.2.4 en sus incisos (ii) y (iii) se verifica.

(ii) ($q = 3$) Para el código $C = \{000, 001, 002, 010, 020, 011, 012, 021, 022\}$, se tiene $\dim(C) = \log_3 |C| = \log_3 9 = 2$. Una rápida inspección muestra que $C^{\perp} = \{000, 100, 200\}$, y así $\dim(C^{\perp}) = 1$.

Observación 3.2.6 Un código lineal C de longitud n y dimensión k sobre $\mathbb{F}_q$ es frecuentemente denominado como $[n, k]$-código q-ario o, también (n, q^k)-código o, si el contexto deja en claro el valor de q, $[n, k]$-código. Y si la distancia d de C es conocida, a veces no referiremos a él como un $[n, k, d]$-código lineal.

Definición 3.2.7 Sea C un código lineal.

(i) C es *auto-ortogonal* si $C \subseteq C^{\perp}$.

(ii) C es *auto-dual* si $C = C^{\perp}$.

Proposición 3.2.8 La dimensión de un código auto-ortogonal de longitud n debe ser $\leq n/2$ y la dimensión de un código auto-dual de longitud n es $n/2$.

Demostración. Esta proposición es una inmediata consecuencia del Teorema 3.2.4(ii) y la definición de código auto-ortogonal y código auto-dual. □

Ejemplo 3.2.9 El código en el Ejemplo 3.2.5(i) es auto-dual.

3.3. Peso de Hamming

Recuerda que la distancia de Hamming $d(\mathbf{x}, \mathbf{y})$ entre dos palabras $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ fue definida en el Capitulo 2.

Definición 3.3.1 Sea $\mathbf{x}$ una palabra en $\mathbb{F}_q^n$. El *peso* (según Hamming) de $\mathbf{x}$, denotado por $\mathrm{wt}(\mathbf{x})$, es definido como el número de coordenadas no-nulas en $\mathbf{x}$; es decir

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

donde $\mathbf{0}$ es la palabra nula.

Observación 3.3.2 Para cada elemento x de $\mathbb{F}_q$, podemos definir el peso de $\mathbf{x}$ como sigue:

$$\mathrm{wt}(x) = d(x, 0) = \begin{cases} 1 & , \text{ si } x \neq 0 \\ 0 & , \text{ si } x = 0 \end{cases}.$$

Entonces escribiendo $\mathbf{x} \in \mathbb{F}_q^n$ como $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ el peso de $\mathbf{x}$ puede ser definido equivalentemente como

$$\mathrm{wt}(\mathbf{x}) = \mathrm{wt}(x_1) + \mathrm{wt}(x_2) + \cdots + \mathrm{wt}(x_n). \tag{1.1}$$

Lema 3.3.3 Si $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, entonces $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} - \mathbf{y})$.

Demostración. Si $x, y \in \mathbb{F}_q$, entonces $d(x, y) = 0$ si, y sólo si $x = y$, que es verdad si, y sólo si $x - y = 0$ o, equivalentemente, $\mathrm{wt}(x - y) = 0$. El Lema 3.3.3 ahora se sigue de las ecuaciones (0.1) y (1.1). □

Como $a = -a$ para todo $a \in \mathbb{F}_q$ donde q es par, el siguiente Corolario es una inmediata consecuencia del Lema 3.3.3.

Corolario 3.3.4 Sea q par. Si $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, entonces $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}(\mathbf{x} + \mathbf{y})$.

Para $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ y $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ en $\mathbb{F}_q^n$, sea

$$\mathbf{x} \star \mathbf{y} = (x_1 y_1, x_2 y_2, \ldots, x_n y_n).$$

Lema 3.3.5 Si $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$, entonces

$$\mathrm{wt}\,(\mathbf{x} + \mathbf{y}) = \mathrm{wt}\,(\mathbf{x}) + \mathrm{wt}\,(\mathbf{y}) - 2\mathrm{wt}\,(\mathbf{x} \star \mathbf{y}). \tag{1.2}$$

Demostración. Por (1.1) basta con mostrar que (1.2) es verdad para $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2$. Esto se puede verificar fácilmente como en la Tabla 1.1. □

$\mathbf{x}$	$\mathbf{y}$	$\mathbf{x} \star \mathbf{y}$	$\mathrm{wt}\,(\mathbf{x}) + \mathrm{wt}\,(\mathbf{y}) - 2\mathrm{wt}\,(\mathbf{x} \star \mathbf{y})$	$\mathrm{wt}\,(\mathbf{x} + \mathbf{y})$
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	0	0

Tabla 3.1. Verificación de (1.2) para $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2$.

Claramente el Lema 3.3.5 implica que $\mathrm{wt}\,(\mathbf{x}) + \mathrm{wt}\,(\mathbf{y}) \geq \mathrm{wt}\,(\mathbf{x} + \mathbf{y})$ para $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. En efecto esta igualdad es verdad para cualquier alfabeto $\mathbb{F}_q$, y es parte del siguiente lema.

Lema 3.3.6 Para cualquier potencia prima q y $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, tenemos

$$\mathrm{wt}\,(\mathbf{x}) + \mathrm{wt}\,(\mathbf{y}) \geq \mathrm{wt}\,(\mathbf{x} + \mathbf{y}) \geq \mathrm{wt}\,(\mathbf{x}) - \mathrm{wt}\,(\mathbf{y}). \tag{1.3}$$

Definición 3.3.7 Sea C un código (no necesariamente lineal). El peso mínimo de C, denotado por $\mathrm{wt}\,(C)$, es el más pequeño de los pesos de las palabras-código no-nulas de C.

Teorema 3.3.8 Sea C un código lineal sobre $\mathbb{F}_q$. Entonces $d(C) = \mathrm{wt}\,(C)$.

Demostración. Recordemos que para cualesquiera palabras $\mathbf{x}, \mathbf{y}$ tenemos que $d(\mathbf{x}, \mathbf{y}) = \mathrm{wt}\,(\mathbf{x} - \mathbf{y})$. Por definición, existen $\mathbf{x}', \mathbf{y}' \in C$ tales que $d(\mathbf{x}', \mathbf{y}') = d(C)$, así que

$$d(C) = d(\mathbf{x}', \mathbf{y}') = \mathrm{wt}\,(\mathbf{x}' - \mathbf{y}') \geq \mathrm{wt}\,(C),$$

pues $\mathbf{x}' - \mathbf{y}' \in C$

Recíprocamente, existe un $\mathbf{z} \in C \setminus \{\mathbf{0}\}$ tal que $\mathrm{wt}(C) = \mathrm{wt}(\mathbf{z})$, con lo que

$$\mathrm{wt}(C) = \mathrm{wt}(\mathbf{z}) = d(\mathbf{z}, 0) \geq d(C).$$

De las dos ecuaciones se concluye finalmente que $d(C) = \mathrm{wt}(C)$. □

Ejemplo 3.3.9 Considerar el código lineal binario $C = \{0000, 1000, 0100, 1100\}$ vemos que

$$\mathrm{wt}(1000) = 1,$$
$$\mathrm{wt}(0100) = 1,$$
$$\mathrm{wt}(1100) = 2.$$

Por lo tanto, $d(C) = 1$.

Observación 3.3.10 (Algunas ventajas de los códigos lineales.) Las siguientes son algunas de las razones por las cuales puede ser preferible el uso de códigos lineales sobre códigos no lineales:

(i) Como un código lineal es un espacio vectorial, este puede ser descrito completamente usando una de sus bases (ver la Sección 3.4).

(ii) La distancia de un código lineal es igual al más pequeño peso de sus palabras-código no-nulas.

(iii) Los procedimientos de codificación y decodificación para un código lineal son rápidos y simples que los empleados para códigos no lineales (ver las secciones 3.7 y 3.8).

3.4. Bases para códigos lineales

Como un código lineal es un espacio vectorial, todos sus elementos pueden ser descritos en términos de una base. En esta sección, discutiremos tres algoritmos que producirán una base para un código lineal dado o una base para su dual.

Definición 3.4.1 Sea A una matriz sobre $\mathbb{F}_q$; una *operación elemental por filas* aplicada sobre A es cualquiera de las siguientes tres operaciones:

(i) intercambiando dos filas,

(ii) multiplicando una fila por un escalar no-nulo,

(iii) reemplazando una fila por su suma con el múltiplo escalar de otra fila.

Definición 3.4.2 Dos matrices son equivalentes por filas si una puede ser obtenida a partir de la otra por medio de una secuencia de operaciones elementales de filas.

Los siguientes son hechos bien conocidos de álgebra lineal:

(i) Cualquier matriz M sobre $\mathbb{F}_q$ puede ser colocada en la *forma escalón filas* (FEF) o la forma reducida escalón por filas (FREF) por una secuencia de operaciones elementales por filas. En otras palabras, una matriz es equivalente a una matriz en FEF o en FREF.

(ii) Para una matriz dada, su FREF es única, pero puede tener diferentes FEFs. (Recordemos que la diferencia entre FREF y FEF es que la primera entrada no-nula de una fila en la FREF es igual a 1 y es la única entrada no-nula en su columna.)

Ahora estamos listos para describir los tres algoritmos.

Algoritmo 1.1

Entrada:	Un subconjunto no vacío S que no contenga al 0 de $\mathbb{F}_q^n$.
Salida:	Una base para $C = \langle S \rangle$, el código lineal generado por S.
Descripción:	Se forma la matriz A cuyas filas son las palabras en S. Se usan operaciones elementales por filas para encontrar una FEF de A. Entonces las filas no-nulas de la FEF forman una base de C.

Ejemplo 3.4.3 Con $q = 3$, encontrar una base para $C = \langle S \rangle$, donde

$$S = \{12101, 20110, 01122, 11010\}.$$

Aplicando la descripción del Algoritmo 1.1 tenemos

$$A = \begin{pmatrix} 12101 \\ 20110 \\ 01122 \\ 11010 \end{pmatrix} \rightarrow \begin{pmatrix} 12101 \\ 02211 \\ 01122 \\ 02212 \end{pmatrix} \rightarrow \begin{pmatrix} 12101 \\ 01122 \\ 00001 \\ 00000 \end{pmatrix}.$$

La última matriz esta en FEF, entonces por el Algoritmo 1.1, $\{12101, 01122, 00001\}$ es una base para C.

Algoritmo 1.2

Entrada:	Un subconjunto no vacío S que no contenga al 0 de $\mathbb{F}_q^n$.
Salida:	Una base para $C = \langle S \rangle$, el código lineal generado por S.
Descripción:	Se forma la matriz A cuyas columnas son las palabras en S. Se usan operaciones elementales de fila para colocar A en FEF y localice el líder de las columnas en el FEF. Entonces las columnas originales de A que corresponden a las columnas principales forman una base de C.

Ejemplo 3.4.4 Con $q = 2$, encontrar una base para $C = \langle S \rangle$, donde

$$S = \{11101, 10110, 01011, 11010\}.$$

Aplicando la descripción del Algoritmo 1.2 tenemos

$$A = \begin{pmatrix} 1101 \\ 1011 \\ 1100 \\ 0111 \\ 1010 \end{pmatrix} \rightarrow \begin{pmatrix} 1101 \\ 0110 \\ 0001 \\ 0111 \\ 0111 \end{pmatrix} \rightarrow \begin{pmatrix} \mathbf{1}101 \\ 0\mathbf{1}10 \\ 000\mathbf{1} \\ 0000 \\ 0000 \end{pmatrix}.$$

Como las columnas 1, 2 y 4 de la FEF son las columnas principales, el Algoritmo 1.2 dice que las columnas 1, 2 y 4 de A forman una base de C; es decir, $\{11101, 10110, 11010\}$ es una base para C.

Observación 3.4.5 Notar que la base que el Algoritmo 1.2 provee es un subconjunto del conjunto dado S, mientras que con el Algoritmo 1.1 no pasa necesariamente lo mismo.

Algoritmo 1.3

Entrada: Un subconjunto no vacío S que no contenga al 0 de $\mathbb{F}_q^n$.

Salida: Una base para el código dual $C^\perp$ donde $C = \langle S \rangle$.

Descripción: Se forma la matriz A cuyas filas son las palabras en S. Se usan operaciones elementales de filas para colocar A en la FREF. Sea G la matriz de tamaño $k \times n$ que consta de todas las filas no-nulas de la FREF:

$$A \to \begin{pmatrix} G \\ O \end{pmatrix}.$$

(Aquí, O denota la matriz cero.) La matriz G contiene k columnas principales. Se permutan las columnas de G para formar

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

donde I_k denota la matriz identidad de tamaño $k \times k$. Formar una matriz H' como sigue:

$$H' = (-X^T | I_{n-k}),$$

donde X^T es la transpuesta de X.

Aplicar la inversa de la permutación aplicada a las columnas de G a las columnas de H' para formar H. Entonces las filas de H forman una base para $C^\perp$.

Observación 3.4.6 (i) Notar que el Algoritmo 1.3 también provee una base para C, pues el Algoritmo 1.1 esta incluido.

(ii) Una explicación de los principios tras el Algoritmo 1.3 se dará en los teoremas

2.3.13 y 3.5.9 de la preliminares y siguiente sección respectivamente.

Ejemplo 3.4.7 Con $q = 3$, encontrar una base para $C^{\perp}$ si el FREF de A es

$$G = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 2 & 0 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \end{pmatrix} \end{array}$$

Las columnas principales de G son las columnas 1, 4, 5, 7 y 9. Permutamos las columnas de G para que queden en el orden 1, 4, 5, 7, 9, 2, 3, 6, 8, 10 hasta formar la matriz.

$$G' = (I_5|X) = \begin{array}{c} \begin{matrix} 1 & 4 & 5 & 7 & 9 & 2 & 3 & 6 & 8 & 10 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} \end{array}$$

Formamos la matriz H'

$$H' = (-X^T|I_5) = \begin{array}{c} \begin{matrix} 1 & 4 & 5 & 7 & 9 & 2 & 3 & 6 & 8 & 10 \end{matrix} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 2 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Finalmente reordenamos las columnas de H' usando la permutación inversa quedan-

do H:

$$H = \begin{array}{c} \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 2 & 0 & 0 & 2 & 0 & 1 & 1 \end{pmatrix} \end{array}$$

Por el Algoritmo 1.3, las filas de H forman una base para $C^{\perp}$.

3.5. Matrices generadora y de paridad

Conocer una base para un código lineal nos permite describir sus palabras-código explícitamente. En teoría de códigos, una base para un código lineal es frecuentemente representada en la forma de una matriz, denominada matriz generadora, mientras que la matriz que representa una base para el código dual es denominada matriz paridad. Estas matrices juegan un importante papel en la teoría de códigos.

Definición 3.5.1 (i) Una *matriz generadora* para un código lineal C es una matriz G cuyas filas forman una base para C.

(ii) Una *matriz paridad* H para un código lineal C es una matriz generadora del código dual $C^{\perp}$.

Observación 3.5.2 (i) Si C es un $[n, k]$-código lineal, entonces una matriz generadora para C debe ser una matriz de $k \times n$, y una matriz paridad para C debe ser una matriz de tamaño $(n - k) \times n$.

(ii) El Algoritmo 1.3 de la Sección 3.4 puede ser usado para encontrar las matrices generadora y paridad para un código lineal.

(iii) Como el número de bases para un espacio vectorial usualmente excede a uno, el número de matrices generadoras para un código lineal usualmente también excede a uno. Además, aun cuando la base se haya fijado, una permutación (diferente de la identidad) de las filas de la matriz generadora nos provee de una matriz generadora

diferente.

(iv) Las filas de una matriz generadora son linealmente independientes. Lo mismo sucede para las filas de una matriz paridad. Para mostrar que una matriz G de tamaño $k \times n$ es en verdad la matriz generadora de un $[n, k]$-código lineal dado, es suficiente mostrar que las filas de G son palabras-código en C y que son linealmente independientes. Alternativamente, uno también puede mostrar que C esta contenido en el espacio generado por las filas de G.

Definición 3.5.3 (i) Una matriz generadora de la forma $(I_k|X)$ se dice que esta en la *forma estándar*.

(ii) Una matriz paridad de la forma $(Y|I_{n-k})$ se dice que esta en la *forma estándar*.

Lema 3.5.4 Sea C un $[n, k]$-código lineal sobre $\mathbb{F}_q$, con matriz generadora G. Entonces $\mathbf{v} \in \mathbb{F}_q^n$ pertenece a $C^\perp$ si, y sólo si $\mathbf{v}$ es ortogonal a cada fila de G; es decir,

$$\mathbf{v} \in C^\perp \quad \Leftrightarrow \quad \mathbf{v}G^T = \mathbf{0}.$$

En particular, dada una matriz H de tamaño $(n-k) \times n$, entonces H es una matriz paridad para C si, sólo si las filas de H son linealmente independientes y $HG^T = O$.

Demostración. Si $\mathbf{r}_i$ denota la i-ésima fila de G, entonces $\mathbf{r}_i \in C$ para todo $1 \leq i \leq k$, y cada $\mathbf{c} \in C$ se puede escribir como

$$\mathbf{c} = \lambda_1\mathbf{r}_1 + \lambda_2\mathbf{r}_2 + \cdots + \lambda_k\mathbf{r}_k,$$

donde $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{F}_q$.

Si $\mathbf{v} \in C^\perp$, entonces $\mathbf{v} \cdot \mathbf{c} = 0$ para todo $\mathbf{c} \in C$. En particular, $\mathbf{v}$ es ortogonal a $\mathbf{r}_i$, para todo $1 \leq i \leq k$; es decir, $\mathbf{v}G^T = \mathbf{0}$.

Recíprocamente, si $\mathbf{v} \cdot \mathbf{r}_i = 0$, para todo $1 \leq i \leq k$, entonces claramente, para cualquier $\mathbf{c} = \lambda_1\mathbf{r}_1 + \cdots + \lambda_k\mathbf{r}_k \in C$,

$$\mathbf{v} \cdot \mathbf{c} = \lambda_1(\mathbf{v} \cdot \mathbf{r}_1) + \cdots + \lambda_k(\mathbf{v} \cdot \mathbf{r}_k) = 0.$$

Para la última afirmación, si H es una matriz paridad para C, entonces las filas de

H son linealmente independientes por definición. Como las filas de H son palabras-código en $C^{\perp}$, se sigue de la anterior afirmación que $HG^T = O$.

Recíprocamente, si $HG^T = O$, entonces la anterior afirmación muestra que las filas de H, y por lo tanto el espacio generado por las filas de H están contenidos en $C^{\perp}$. Como las filas de H son linealmente independientes, el espacio generado por las filas de H tiene dimensión $n - k$, así el espacio generado por las filas de H es de veras $C^{\perp}$. En otras palabras, H es una matriz paridad para C. □

Observación 3.5.5 Una formulación alternativa pero equivalente para el Lema 3.5.4 es la siguiente:

Sea C un $[n, k]$-código lineal sobre $\mathbb{F}_q$, con matriz paridad H. Entonces $\mathbf{v} \in \mathbb{F}_q^n$ pertenece a C si, y sólo si $\mathbf{v}$ es ortogonal a cada fila de H; es decir,

$$\mathbf{v} \in C \quad \Leftrightarrow \quad \mathbf{v}H^T = \mathbf{0}.$$

En particular, dada una matriz G de tamaño $k \times n$, entonces G es una matriz generadora para C si, sólo si las filas de G son linealmente independientes y $GH^T = O$.

Una de las consecuencias del Lema 3.5.4 es el siguiente teorema que relaciona la distancia d de un código lineal C a las propiedades de una matriz paridad de C. Cuando d es pequeño, el Corolario 3.5.7 puede ser útil para determinar d.

Teorema 3.5.6 Sea C un código lineal y H una matriz paridad para C. Entonces

(i) C tiene distancia $\geq d$ si, y sólo si cualesquiera $d-1$ columnas de H son linealmente independientes, y

(ii) C tiene distancia $\leq d$ si, y sólo si H tiene d columnas que son linealmente independientes.

Demostración. Sea $\mathbf{v} = \{v_1, \ldots, v_n\} \in C$ una palabra de peso $e > 0$. Supongamos que las coordenadas no nulas se encuentran en las posiciones $i_1, \ldots, i_e$, esto es $v_j = 0$ si $j \notin \{i_1, \ldots, i_e\}$. Que $\mathbf{c}_i$ (con $1 \leq i \leq n$) denote la i-ésima columna de H.

Por el Lema 3.5.4 (o, para ser más precisos, la formulación equivalente el la Observación 3.5.5), C contiene una palabra no nula $\mathbf{v} = \{v_1, \ldots, v_n\}$ de peso e (cuyas coordenadas no nulas son $v_{i_1}, \ldots, v_{i_e}$) si, y sólo si

$$\mathbf{0} = \mathbf{v}H^T = v_{i_1}\mathbf{c}_{i_1}^T + \cdots + v_{i_e}\mathbf{c}_{i_e}^T,$$

que es verdad si, sólo si, hay e columnas de H (que llamaremos $\mathbf{c}_{i_1}, \ldots, \mathbf{c}_{i_e}$) que son linealmente independientes.

Decir que la distancia de C es $\geq d$ es equivalente a decir que C no contiene palabras no nulas de peso $\leq d-1$, que a su vez es equivalente a decir que cualesquiera $d-1$ o menos columnas de H son linealmente independientes. Esto prueba i.

De manera similar, decir que la distancia de C es $\leq d$ es equivalente a decir que C contiene una palabra no nula de peso $\leq d$, que a su vez es equivalente a decir que H tiene d o menos columnas linealmente independientes. Esto prueba ii. □

Un inmediato corolario del Teorema 3.5.6 es el siguiente resultado.

Corolario 3.5.7 Sean C un código lineal y H su matriz paridad de C. Entonces las siguientes afirmaciones son equivalentes:

(i) C tiene distancia d.

(ii) cualesquiera $d-1$ columnas de H son linealmente independientes y H tiene d columnas que son linealmente dependientes.

Ejemplo 3.5.8 Sea C un código lineal binario con matriz paridad

$$H = \begin{pmatrix} 10100 \\ 11010 \\ 01001 \end{pmatrix}.$$

Por simple inspección, se puede ver que no hay columnas nulas ni dos columnas de H que sumen $\mathbf{0}^T$, así cualesquiera dos columnas de H son linealmente independientes. Sin embargo, las columnas 1, 3 y 4 suman $\mathbf{0}^T$, y por tanto son linealmente dependientes. Por lo tanto la distancia de C es $d = 3$.

Teorema 3.5.9 Si $G = (I_k \mid X)$ es la forma estándar de la matriz generadora del $[n, k]$-código C, entonces la matriz paridad de C es $H = (-X^T \mid I_{n-k})$.

Demostración. Obviamente, la ecuación $HG^T = 0$ es satisfecha. Considerando las últimas $n - k$ coordenadas, esta claro que las filas de H son linealmente independientes. Por lo tanto, la conclusión se sigue del Lema 3.5.4. □

Observación 3.5.10 El Teorema 3.5.9 demuestra que el algoritmo 1.3 de la Sección 3.4 (que hasta ahora solo se había afirmado) es exacto y verdadero.

Ejemplo 3.5.11 Encontrar una matriz generadora y una matriz paridad para el código lineal binario $C = \langle S \rangle$, donde $S = \{11101, 10110, 01011, 11010\}$. Por el algoritmo 1.1 tenemos,

$$A = \begin{pmatrix} 11101 \\ 10110 \\ 01011 \\ 11010 \end{pmatrix} \rightarrow \begin{pmatrix} 11101 \\ 01011 \\ 00111 \\ 00000 \end{pmatrix} \rightarrow \begin{pmatrix} 10001 \\ 01011 \\ 00111 \\ 00000 \end{pmatrix},$$

que esta en FREF. Por el algoritmo 1.3 tenemos

$$G = \begin{pmatrix} 100 \mid 01 \\ 010 \mid 11 \\ 001 \mid 11 \end{pmatrix}, \quad H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Aquí, G es la matriz generadora para C y H es una matriz paridad para C. Podemos verificar que $GH^T = O = HG^T$.

Se debe notar que, no es verdad que, cada código lineal tiene una matriz generadora en la forma estándar.

Ejemplo 3.5.12 Considerar el código lineal binario

$$C = \{000, 001, 100, 101\}.$$

Como la $\dim(C) = 2$, por el Teorema 3.1.15(ii) el número de bases para C es

$$\frac{1}{2!}(2^2 - 1)(2^2 - 2) = 3.$$

Podemos enlistar todas las bases de C

$$\{001, 100\}, \quad \{001, 101\}, \quad \{100, 101\}.$$

Por lo tanto C tiene 6 matrices generadoras:

$$\begin{pmatrix} 001 \\ 100 \end{pmatrix}, \quad \begin{pmatrix} 100 \\ 001 \end{pmatrix}, \quad \begin{pmatrix} 001 \\ 101 \end{pmatrix}, \quad \begin{pmatrix} 101 \\ 001 \end{pmatrix}, \quad \begin{pmatrix} 100 \\ 101 \end{pmatrix}, \quad \begin{pmatrix} 101 \\ 100 \end{pmatrix}.$$

Notar que ninguna de estas matrices esta en la forma estándar.

3.6. Equivalencia de códigos lineales

Mientras que ciertos códigos lineales no pueden tener una matriz generadora en la forma estándar, después de una apropiada permutación de coordenadas de las palabras-código y posiblemente multiplicar ciertas coordenadas por un escalar no nulo, uno siempre puede conseguir un nuevo código que tenga una matriz generadora en la forma estándar.

Definición 3.6.1 Dos (n, M)-códigos sobre $\mathbb{F}_q$ son *equivalentes* si uno puede ser obtenido del otro por una combinación de las siguientes operaciones:

(i) permutación de los n dígitos de las palabras-código.

(ii) multiplicación de los símbolos que aparecen en una posición fija por un escalar no nulo.

Ejemplo 3.6.2 (i) Para $q = 2$ y $n = 4$, sea el código

$$C = \{0000, 0101, 0010, 0111\}.$$

Después de reordenar los bits en el orden 2, 4, 1, 3, obtenemos el código equivalente

$$C' = \{0000, 1100, 0001, 1101\}.$$

(ii) Para $q = 3$ y $n = 3$, consideremos el código ternario

$$C = \{000, 011, 022\}.$$

Permutando las primera y segunda posiciones, seguido por la multiplicación de la tercera posición por 2, obtenemos el código equivalente

$$C' = \{000, 102, 201\}.$$

Teorema 3.6.3 Cualquier código lineal C es equivalente a un código lineal C' con una matriz generadora en la forma estándar.

Demostración. Si G es una matriz generadora para C, colocando G en FREF. Reordenado las columnas de la FREF tal que las columnas principales se ubiquen para formar una matriz identidad. El resultado es una matriz G', en la forma estándar que es una matriz generadora para un código C' equivalente al código C. □

Observación 3.6.4 El Teorema 3.6.3 es esencialmente la primera parte del Algoritmo 1.3 de la Sección 3.4.

Ejemplo 3.6.5 Sea C un código lineal binario con matriz generadora

$$G = \begin{pmatrix} 1100001 \\ 0010011 \\ 0001001 \end{pmatrix}.$$

Reordenando las columnas según la permutación 1, 3, 4, 2, 5, 6, 7 se obtiene la matriz

$$G' = \begin{pmatrix} 100 \mid 1001 \\ 010 \mid 0011 \\ 001 \mid 0001 \end{pmatrix}.$$

Sea C' el código generado por G'; entonces C' es equivalente a C y C' tiene por matriz generadora a G', que está en la forma estándar.

Ejemplo 3.6.6 Dijimos en el Ejemplo 3.5.12 que el código lineal binario

$$C = \{000, 001, 100, 101\}$$

no tiene matriz generadora en la forma estándar. Sin embargo, si permutamos las segunda y tercera coordenadas, obtenemos el código lineal binario equivalente

$$C' = \{000, 010, 100, 110\}$$

y esta claro que

$$\begin{pmatrix} 100 \\ 010 \end{pmatrix}$$

es una matriz generadora de C' en la forma estándar.

3.7. Codificando con un código lineal

Sea C un $[n, k, d]$-código lineal sobre el campo finito $\mathbb{F}_q$. Cada palabra código de C puede representar una pieza de información, así C puede representar q^k piezas diferentes de información. Una vez que se fija una base $\{\mathbf{r}_1, \ldots, \mathbf{r}_k\}$ para C, cada palabra-código $\mathbf{v}$, o, equivalentemente, cada una de las q^k piezas de información, puede ser únicamente escrita como una combinación lineal,

$$\mathbf{v} = u_1\mathbf{r}_1 + \cdots + u_k\mathbf{r}_k$$

donde $u_1, \ldots, u_k \in \mathbb{F}_q$.

De manera equivalente, podemos poner G para que sea la matriz generadora de C cuya i-ésima fila es el vector $\mathbf{r}_i$ en la base elegida. Dado un vector $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$, es claro que

$$\mathbf{v} = \mathbf{u}G = u_1\mathbf{r}_1 + \cdots + u_k\mathbf{r}_k$$

es una palabra código en C. Recíprocamente, cualquier $\mathbf{v} \in C$ puede ser escrito únicamente como $\mathbf{v} = \mathbf{u}G$, donde $\mathbf{u} = (u_1, \ldots, u_k) \in \mathbb{F}_q^k$. Por tanto, cada palabra $\mathbf{u} \in \mathbb{F}_q^k$ puede ser codificado como $\mathbf{v} = \mathbf{u}G$.

El proceso de representación de elementos $\mathbf{u}$ de $\mathbb{F}_q^k$ como palabras código $\mathbf{v} = \mathbf{u}G$ en C es denominado *codificación*.

Ejemplo 3.7.1 Sea C el [5,3]-código lineal binario con la matriz generadora

$$G = \begin{pmatrix} 10110 \\ 01011 \\ 00101 \end{pmatrix};$$

entonces el mensaje $\mathbf{u} = 101$ es codificado como

$$\mathbf{v} = \mathbf{u}G = (101) \begin{pmatrix} 10110 \\ 01011 \\ 00101 \end{pmatrix} = 10011.$$

Notar que la tasa de información de C es 3/5, es decir, que por cada tres bits que salen 5 bits son usados para enviar el mensaje.

Observación 3.7.2 (Ventajas de tener G en la forma estándar.) Algunas de las ventajas de tener la matriz generadora de un código lineal en la forma estándar son las que siguen:

1. Si un código lineal C tiene una matriz generadora G en la forma estándar, $G = (I \mid X)$, entonces el Algoritmo 1.3 de la Sección 3.4 nos devuelve a

   $$H = (-X^T \mid I)$$

   como un matriz paridad para C.

2. Si un $[n, k, d]$-código lineal C tiene una matriz generadora G en la forma estándar, $G = (I \mid X)$, entonces recuperar el mensaje $\mathbf{u}$ a partir de la palabra-código $\mathbf{v} = \mathbf{u}G$ es trivial, pues

   $$\mathbf{v} = \mathbf{uG} = \mathbf{u}(I \mid X) = (\mathbf{u} \mid \mathbf{u}X);$$

   es decir, los primeros k dígitos de la palabra-código $\mathbf{v} = \mathbf{u}G$ dan el mensaje $\mathbf{u}-$; estos son llamados *dígitos-mensaje*. Los restantes $n - k$ dígitos son llamados *dígitos de verificación*. Los dígitos de verificación representan la *redundancia* que tiene que ser añadida al mensaje para protegerlo del ruido.

3.8. Decodificando un código lineal

Un código es de practico uso sólo si un eficiente esquema de decodificación puede ser aplicado en él. En ésta sección, discutiremos una simple pero elegante proceso de decodificación para códigos lineales que sigue la estrategia del vecino más cercano, tan bueno que con una pequeña modificación se puede mejorar su desempeño cuando la longitud del código es grande.

3.8.1. Clases laterales

Comenzaremos con la noción de clase lateral. Las clases laterales juegan un papel importante en los esquemas de decodificación que se discutirán en éste capítulo.

Definición 3.8.1 Sean C un codigo lineal de longitud n sobre $\mathbb{F}_q$, y $\mathbf{u} \in \mathbb{F}_q^n$ es cualquier vector de longitud n; definimos el conjunto

$$C + \mathbf{u} = \{\mathbf{v} + \mathbf{u} \mid \mathbf{v} \in C\} (= \mathbf{u} + C)$$

. como la *clase lateral* de C determinada por $\mathbf{u}$.

Observación 3.8.2 Para el lector cuyos conocimientos incluyan la Teoría de Grupos, note que, por consideración de la adición vectorial, $\mathbb{F}_q^n$ es un grupo abeliano finito, y un código lineal C sobre $\mathbb{F}_q$ de longitud n es también un subgrupo de $\mathbb{F}_q^n$. Las clases laterales de un código lineal definidas arriba coinciden con la notación usual para las clases laterales de la Teoría de Grupos.

Ejemplo 3.8.3 Sean $q = 2$ y $C = \{000, 101, 010, 111\}$. Entonces

$$C + 000 = \{000, 101, 010, 111\},$$
$$C + 001 = \{001, 100, 011, 110\},$$
$$C + 010 = \{010, 111, 000, 101\},$$
$$C + 011 = \{011, 110, 001, 100\},$$
$$C + 100 = \{100, 001, 110, 011\},$$
$$C + 101 = \{101, 000, 111, 010\},$$
$$C + 110 = \{110, 011, 100, 001\},$$
$$C + 111 = \{111, 010, 101, 000\}.$$

Notar que

$$C + 000 = C + 010 = C + 101 = C + 111 = C$$
$$C + 001 = C + 011 = C + 100 = C + 110 = \mathbb{F}_2^3 \setminus C.$$

Teorema 3.8.4 Sea C un $[n, k, d]$-código lineal sobre el campo finito $\mathbb{F}_q$. Entonces,

(i) cada vector de $\mathbb{F}_q^n$ esta contenido en alguna clase lateral de C;

(ii) para todo $\mathbf{u} \in \mathbb{F}_q^n$ se tiene, $|C + \mathbf{u}| = |C| = q^k$;

(iii) para todo $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, $\mathbf{u} \in C + \mathbf{v}$ implica que $C + \mathbf{u} = C + \mathbf{v}$;

(iv) dos clases laterales o son idénticas o tienen intersección vacía;

(v) C tiene q^{n-k} clases laterales diferentes;

(vi) para todo $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, $\mathbf{u} - \mathbf{v} \in C$ si, y sólo si, $\mathbf{u}$ y $\mathbf{v}$ están en la misma clase lateral.

Demostración. (i) El vector $\mathbf{v} \in \mathbb{F}_q^n$ esta claramente contenido en la clase lateral $C + \mathbf{v}$.

(ii) Por definición $C+\mathbf{u}$ tiene a lo más $|C| = q^k$ elementos. Claramente, dos elementos $\mathbf{c}+\mathbf{u}$ y $\mathbf{c}'+\mathbf{u}$ de $C+\mathbf{u}$ son iguales si, y sólo si, $\mathbf{c} = \mathbf{c}'$, por lo tanto $|C+\mathbf{u}| = |C| = q^k$.

(iii) se sigue de la definición de $C + \mathbf{v}$ que $C + \mathbf{u} \subseteq C + \mathbf{v}$. Entonces, por (ii), $C + \mathbf{u} = C + \mathbf{v}$.

(iv) consideremos los dos conjuntos $C+\mathbf{u}$ y $C+\mathbf{v}$ y supongamos que $x \in (C+\mathbf{u}) \cap (C+\mathbf{v})$. Como $x \in C+\mathbf{u}$, (iii) muestra que $C+\mathbf{u} = C+\mathbf{x}$. Y de manera similar, como $x \in C+\mathbf{v}$, se sigue que $C+\mathbf{v} = C+\mathbf{x}$. Por lo tanto $C+\mathbf{u} = C+\mathbf{v}$.

(v) es una consecuencia inmediata de (i), (ii) y (iv).

(vi) Si $\mathbf{u}-\mathbf{v} = \mathbf{c} \in C$, entonces $\mathbf{u} = \mathbf{c}+\mathbf{v} \in C+\mathbf{v}$, así $C+\mathbf{u} = C+\mathbf{v}$. Por la demostración de (i), $\mathbf{u} \in C+\mathbf{u}$ y $\mathbf{v} \in C+\mathbf{v}$, por lo que $\mathbf{u}$ y $\mathbf{v}$ están en la misma clase lateral.

Recíprocamente, supongamos que $\mathbf{u}$, $\mathbf{v}$ están en la clase lateral $C+\mathbf{x}$. Entonces $\mathbf{u} = \mathbf{c}+\mathbf{x}$ y $\mathbf{v} = \mathbf{c}'+\mathbf{x}$, para algunos $\mathbf{c}, \mathbf{c}' \in C$. Por lo tanto, $\mathbf{u}-\mathbf{v} = \mathbf{c}-\mathbf{c}' \in C$. □

Ejemplo 3.8.5 Las clases laterales del código lineal binario

$$C = \{0000, 1011, 0101, 1110\}$$

son las siguientes:

0000+C	0000	1011	0101	1110
0001+C	0001	1010	0100	1111
0010+C	0010	1001	0111	1100
1000+C	1000	0011	1101	0110

Observación 3.8.6 El anterior arreglo es llamado un *arreglo estándar*.

Definición 3.8.7 Una palabra de menor peso (de Hamming) en una clase lateral es llamado *lider de clase*.

Ejemplo 3.8.8 En el Ejemplo 3.8.5, el vector $\mathbf{u}$ en $\mathbf{u}+C$ de la primera columna son lideres de clase para las clases laterales respectivas. Notar que la clase lateral $0001+C$ puede también tener a 0100 como líder de clase.

3.8.2. Decodificación por el vecino más cercano para Códigos Lineales

Sea C un código lineal. Asumiendo que la palabra-código $\mathbf{v}$ es transmitida y la palabra $\mathbf{w}$ es recibida, resultando el *patrón de error* (o cadena de error)

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

Entonces $\mathbf{w} - \mathbf{e} = \mathbf{v} \in C$, así, por la parte (vi) del Teorema 3.8.4, el patrón de error $\mathbf{e}$ y la palabra recibida $\mathbf{w}$ están en la misma clase lateral.

Como los patrones de error de menor peso son los más pequeños que pueden ocurrir, la decodificación por el vecino más cercano para un código lineal C trabaja de la siguiente manera. Una vez se recibe la palabra $\mathbf{w}$, escogemos una palabra $\mathbf{e}$ de menor peso en la clase lateral $\mathbf{w} + C$ y se concluye que $\mathbf{v} = \mathbf{w} - \mathbf{e}$ tiene que ser el código transmitido.

Ejemplo 3.8.9 Con $q = 2$ y $C = \{0000, 1011, 0101, 1110\}$, decodificaremos las siguientes palabras recibidas: (i) $\mathbf{w} = 1101$; (ii) $\mathbf{w} = 1111$.

Primero escribamos el arreglo estándar de C.

0000+C	0000	1011	0101	1110
0001+C	0001	1010	0100	1111
0010+C	0010	1001	0111	1100
1000+C	1000	0011	1101	0110

(i) $\mathbf{w} = 1101$: $\mathbf{w}+C$ esta en la cuarta clase lateral (cuarta fila). La palabra de menor peso en esta clase lateral es 1000 (notar que este es el único líder de clase). Por lo tanto, $1101 - 1000 = 1101 + 1000 = 0101$ será la más probable a la palabra-código transmitida (Notar que esta es la palabra de hasta arriba de la columna donde la palabra recibida 1101 se encuentra).

(ii) $\mathbf{w} = 1111$: $\mathbf{w}+C$ esta en la segunda clase lateral (segunda fila). Hay dos palabras de menor peso, 0001 y 0100, en esta clase lateral (esto significa que hay dos opciones

para el líder de clase. En el arreglo estándar, hemos elegido a 0001 como el líder de clase. Si hubiésemos elegido a 0100 tendríamos una simple diferencia.) Cuando la clase lateral de la palabra recibida tiene un único líder, la aproximación que tomamos para decodificar depende del esquema de decodificación (es decir, completo o incompleto) usado. Si realizamos una decodificación incompleta, solicitaremos una retransmisión. Si realizamos una decodificación completa, arbitrariamente elegiremos una de las palabras de menor peso, es decir 0001 que será el patrón de error y se concluirá que $1111 - 0001 = 1111 + 0001 = 1110$ será la más parecida a la palabra-código enviada. (Nota: esto significa que elegimos a 0001 como el líder de clase, revisando el arreglo estándar observamos que la palabra más semejante a la palabra enviada es la de hasta arriba de la columna donde la palabra recibida se localiza.) ¿Y que sucedería si elegimos a 0100 como líder de clase y patrón de error?

3.8.3. Decodificación por Síndrome

El esquema de decodificación basado en el arreglo estándar trabaja razonablemente bien cuando la longitud n del código lineal es pequeño, pero puede tomar una considerable cantidad de tiempo cuando n es grande. Este inconveniente se puede a veces salvar empleando el síndrome para identificar la clase lateral a la cual pertenece la palabra recibida.

Definición 3.8.10 Sean C un $[n, k, d]$-código lineal sobre $\mathbb{F}_q$, y H una matriz paridad para C. Para cualquier $\mathbf{w} \in \mathbb{F}_q^n$, el síndrome de $\mathbf{w}$ es la palabra $S(\mathbf{w}) = \mathbf{w}H^T \in \mathbb{F}_q^{n-k}$.

Para ser precisos, como el síndrome depende de la elección de la matriz paridad H, sería más apropiado denotar el síndrome de $\mathbf{w}$ por $S_H(\mathbf{w})$, para enfatizar está dependencia. Sin embargo para simplificar la notación, el subíndice H será omitido siempre que no haya riesgo de ambigüedad.

Teorema 3.8.11 Sean C un $[n, k, d]$-código lineal y H una matriz paridad para C. Para cualesquiera $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, tenemos

(i) $S(\mathbf{u}+\mathbf{v}) = S(\mathbf{u}) + S(\mathbf{v})$;

(ii) $S(\mathbf{u}) = \mathbf{0}$ si, y sólo si, $\mathbf{u}$ es una palabra código en C;

(iii) $S(\mathbf{u}) = S(\mathbf{v})$ si, y sólo si, $\mathbf{u}$ y $\mathbf{v}$ están en la misma clase lateral de C.

Demostración. (i) Es una inmediata consecuencia de la definición de síndrome.

(ii) Por la definición de síndrome, $S(\mathbf{u}) = \mathbf{0}$ si, y sólo si, $\mathbf{u}H^T = \mathbf{0}$, lo que por la Observación 3.5.5, es equivalente a $\mathbf{u} \in C$.

(iii) Es una consecuencia de los incisos (i), (ii) y el Teorema 3.8.4(vi). □

Observación 3.8.12 (i) El Teorema 3.8.11(iii) dice que podemos identificar una clase lateral por su síndrome; recíprocamente, todas las palabras en una clase lateral dada producen el mismo síndrome, así el síndrome de una clase lateral es el síndrome de cualquier palabra en la clase lateral. En otras palabras, existe una correspondencia uno-uno entre las clases laterales y los síndromes.

(ii) Como los síndromes están en $\mathbb{F}_q^{n-k}$, hay a lo más q^{n-k} síndromes. El Teorema 3.8.4(v) dice que hay q^{n-k} clases laterales, así que hay q^{n-k} síndromes correspondientes (todos diferentes). Por lo tanto, todos los vectores en $\mathbb{F}_q^{n-k}$ aparecen como síndromes.

Definición 3.8.13 Una tabla en la que se desplieguen todos los lideres de clase con su respectivo síndrome se denominara *tabla de síndromes*.

Pasos para construir una tabla de síndromes
asumiendo una completa decodificación por el vecino más cercano

Paso 1: Formar una lista de todas las clases laterales para el código, eligiendo de cada clase la palabra de menor peso como el líder de clase $\mathbf{u}$.

Paso 2: Encontrar la matriz paridad H para el código y, el líder $\mathbf{u}$ para cada clase lateral, calculando su síndrome $S(\mathbf{u}) = \mathbf{u}H^T$.

Observación 3.8.14 Para una incompleta decodificación por el vecino más cercano, sí encontramos más de una palabra de menor peso en el Paso 1 del anterior procedimiento, se colocara el símbolo '$*$' en la entrada de la Tabla de síndromes para indicar que se requiere una retransmisión.

Líder de clase $\mathbf{u}$	Síndrome $S(\mathbf{u})$
0000	00
0001	01
0010	10
1000	11

Tabla 3.2. Tabla de síndromes para el Ejemplo 1.8.15.

Ejemplo 3.8.15 Asumamos una completa decodificación por el vecino más cercano. Para construir una tabla de síndromes para el código

$$C = \{0000, 1011, 0101, 1110\}.$$

comencemos examinando las clases laterales calculadas anteriormente, de donde elegimos las palabras 0000, 0001, 0010, y 1000 como lideres de clase. Resultando así, la matriz de paridad para C es

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

Ahora podemos construir la tabla de síndromes para C (Tabla 1.2). (Si se quiere, se pueden intercambiar las dos columnas.) Notar que cada palabra de longitud 2 aparecen exactamente como en el síndrome.

Líder de clase $\mathbf{u}$	Síndrome $S(\mathbf{u})$
0000	00
$*$	01
0010	10
1000	11

Tabla 3.3. Tabla de síndromes para el Ejemplo 1.8.16.

Ejemplo 3.8.16 Una tabla de síndromes para C, asumiendo una incompleta decodificación por el vecino más cercano, se puede apreciar en la tabla 1.3.

Observación 3.8.17 (i) Notar que un único líder de clase corresponde a un patrón de error que puede ser corregido, asumiendo una incompleta decodificación por el vecino más cercano. Un líder de clase (no necesariamente único) corresponde a un patrón de error que puede ser corregido, asumiendo una completa decodificación por el vecino más cercano.

(ii) Una rápida manera para construir una tabla de síndromes, dada la matriz paridad H y la distancia d para el código C, es el generar todos los patrones de error $\mathbf{e}$ con

$$\mathrm{wt}\,(\mathbf{e}) \leq \lfloor \frac{d-1}{2} \rfloor$$

como lideres de clase (consultando el teorema 2.3.5) y calcular el síndrome $S(\mathbf{e})$ para cada uno de ellos.

Ejemplo 3.8.18 Asumiendo una completa decodificación por el vecino más cercano, construiremos una tabla de síndromes para el código lineal binario C, con matriz paridad H, donde

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

Primero, afirmamos que la distancia de C es $d = 3$. Esto se puede ver fácilmente

aplicando el Corolario 3.5.7 y observando que no hay dos columnas de H que sean linealmente dependientes mientras que las segunda, tercera y cuarta columnas son linealmente dependientes.

Como $\lfloor (d-1)/2 \rfloor = 1$, todos los patrones de error con peso 0 o 1 serán lideres de clase. Entonces calculamos el síndrome para cada uno de ellos y obtenemos las primeras siete filas de la tabla de síndromes. Como cada palabra de longitud 3 debe aparecer como un síndrome, los restantes lideres de clase $\mathbf{u}$ tienen síndrome $\mathbf{u}H^T = 101$. Además, $\mathbf{u}$ debe tener peso ≥ 2 pues todas las palabras de peso 0 o 1 ya han sido incluidas en la tabla de síndromes. Como observamos para los lideres de clase, es razonable registrar las palabras de menor peso disponibles, es decir, 2. Haciéndolo, encontramos tres posibles lideres de clase: 000101, 001010 y 110000. Como estamos usando una completa decodificación por el vecino más cercano, podemos elegir arbitrariamente 000101 como un líder de clase y así, completar la tabla de síndromes (ver Tabla 1.4).

Líder de clase $\mathbf{u}$	Síndrome $S(\mathbf{u})$
000000	000
100000	110
010000	011
001000	111
000100	100
000010	010
000001	001
000101	101

Tabla 3.4. Tabla de síndromes para el Ejemplo 1.8.18.

Notar que, sí usamos una incompleta decodificación por el vecino más cercano, el líder de clase 000101 en la última fila de la Tabla 1.4 sería reemplazado por '$*$'.

Procedimiento para decodificar por síndrome

Paso 1: Calcular el síndrome $S(\mathbf{w})$, para la palabra recibida $\mathbf{w}$.

Paso 2: Encontrar el líder de clase $\mathbf{u}$ asociado al síndrome $S(\mathbf{u}) = S(\mathbf{w})$ en la Tabla de síndromes.

Paso 3: Decodificar $\mathbf{w}$ como $\mathbf{v} = \mathbf{w} - \mathbf{u}$.

Ejemplo 3.8.19 Sean $q = 2$ y $C = \{0000, 1011, 0101, 1110\}$. Emplear la tabla de síndromes construida en el Ejemplo 3.8.15 para decodificar las palabras (i) $\mathbf{w} = 1101$; (ii) $\mathbf{w} = 1111$.

(i) $\mathbf{w} = 1101$. El síndrome es $S(\mathbf{w}) = \mathbf{w}H^T = 11$. En la Tabla 1.2, vemos que el líder de clase es 1000. Por lo tanto, $1101 + 1000 = 0101$ será la palabra más semejante a palabra-código enviada.

(ii) $\mathbf{w} = 1111$. El síndrome es $S(\mathbf{w}) = \mathbf{w}H^T = 01$. En la Tabla 1.2, vemos que el líder de clase es 0001. Por lo tanto, $1111 + 0001 = 1110$ será la palabra más semejante a palabra-código enviada.

Capítulo 4

Códigos Cíclicos

En los capítulos previos, nos hemos concentrado principalmente en los códigos lineales porque ellos poseen estructuras algebraicas. Estas estructuras simplifican el estudio de los códigos lineales.

Por ejemplo, un código lineal puede ser descrito por su matriz generadora o su matriz de paridad; la mínima distancia es determinada por el peso de Hamming, etc. Aun así, tenemos que introducir otras estructuras además de la linealidad con el fin de que los códigos puedan aplicarse fácilmente. Con el propósito de una fácil codificación y decodificación, naturalmente se requiere que el desplazamiento cíclico de una palabra-código en C devuelva una palabra-código en C. Este requerimiento hace aparecer una estructura combinatoria, que afortunadamente puede convertirse en una algebraica. Por otra parte, veremos que un código cíclico de longitud n es determinado totalmente por un polinomio de grado menor que n.

Los códigos cíclicos fueron estudiados por vez primera en 1957 por Prange. Desde entonces, los teóricos de los códigos algebraicos han hecho grandes progresos en el estudio de los códigos cíclicos, tanto en la corrección de errores-aleatorios como en la corrección de errores-ráfaga. Muchas clases importantes de códigos están entre los códigos cíclicos, algunos como los códigos de Hamming y los códigos de Golay.

Comenzaremos por definir que es un código cíclico, y entonces discutiremos su es-

tructura algebraica y otras propiedades. En las dos últimas secciones se estudiaran, un algoritmo de decodificación y un código corrector de errores-ráfaga.

4.1. Definiciones

Definición 4.1.1 Un subconjunto S de $\mathbb{F}_q^n$ es cíclico si $(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \in S$ siempre que $(a_0, a_1, \ldots, a_{n-1}) \in S$. Un código lineal C es llamado código cíclico si C es un conjunto cíclico.

Se dice que la palabra $(u_{n-r}, \ldots, u_{n-1}, u_0, u_1, \ldots, u_{n-r-1})$ se obtiene a partir de la palabra $(u_0, u_1, \ldots, u_{n-1}) \in \mathbb{F}_q^n$ desplazando cíclicamente r posiciones.

Es fácil verificar que el código dual de un código cíclico es también un código cíclico.

Ejemplo 4.1.2 Los conjuntos

$$\{(0,1,1,2),(2,0,1,1),(1,2,0,1),(1,1,2,0)\} \subset \mathbb{F}_3^4,$$
$$\{11111\} \subset \mathbb{F}_2^5$$

son conjuntos cíclicos, pero ellos no son códigos cíclicos pues no son espacios lineales.

Ejemplo 4.1.3 Los siguientes códigos son códigos cíclicos:

(i) los tres códigos triviales $\{\mathbf{0}\}$, $\{\lambda \cdot \mathbf{1} | \lambda \in \mathbb{F}_q\}$ y $\mathbb{F}_q^n$;

(ii) el código $[3,2,2]$−-lineal binario $\{000, 110, 101, 011\}$;

(iii) y el código simple $S(3,2) = \{0000000, 1011100, 0101110, 0010111, 1110010, 0111001, 1001011, 1100101\}$.

Con el propósito de convertir la estructura combinatoria de los códigos cíclicos en una estructura algebraica, consideraremos la siguiente correspondencia:

$$\pi : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n - 1), \tag{2.1}$$
$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots, a_{n-1}x^{n-1}$$

Entonces π es una transformación $\mathbb{F}_q$-lineal de espacios vectoriales sobre $\mathbb{F}_q$. De ahora en adelante, a veces identificaremos $\mathbb{F}_q^n$ con $\mathbb{F}_q[x]/(x^n - 1)$, y un vector $\mathbf{u} =$

$(u_0, u_1, \ldots, u_{n-1})$ con el polinomio $u(x) = u_0 + u_1 x + \cdots, u_{n-1}x^{n-1} = \sum_{i=0}^{n-1} u_i x^i$. Sabemos que $\mathbb{F}_q[x]/(x^n - 1)$ es un anillo (pero no un campo a menos que $n = 1$). De esta manera, tenemos una operación multiplicativa además de la adición en $\mathbb{F}_q^n$.

Ejemplo 4.1.4 Considerar el código cíclico $C = \{000, 110, 101, 011\}$; luego $\pi(C) = \{0, 1 + x, 1 + x^2, x + x^2\} \subset \mathbb{F}_2[x]/(x^3 - 1)$.

Ahora introducimos un importante concepto en el estudio de los códigos cíclicos.

Definición 4.1.5 Sea R un anillo. Un subconjunto I no-vacio de R es llamado *ideal* si

(i) $a + b$ y $a - b$ pertenecen a I, para todo $a, b, \in I$;

(ii) $r \cdot a$ pertenece a I, para todo $r \in R$ y $a \in I$.

Ejemplo 4.1.6 Veamos cuatro ejemplos más:

(i) En el anillo $\mathbb{Z}$ de los enteros, todos los enteros pares forman un ideal;

(ii) Para un entero positivo fijo m, todos los enteros divisibles por m forman un ideal de $\mathbb{Z}$;

(iii) En el anillo de los polinomios $\mathbb{F}_q[x]$, para un polinomio $f(x)$ no-nulo dado, todos los polinomios divisibles por $f(x)$ forman un ideal;

(iv) En el anillo $\mathbb{F}_q[x]/(x^n - 1)$, para un divisor $g(x)$ de $x^n - 1$, todos los polinomios divisibles por $g(x)$ forman un ideal.

Ejemplo 4.1.7 En el anillo $\mathbb{F}_2[x]/(x^3 - 1)$, el subconjunto

$$I = \{0, 1 + x, 1 + x^2, x + x^2\}$$

es un ideal.

Definición 4.1.8 Un ideal I de un anillo R es llamado un *ideal principal* si existe un elemento $g \in I$ tal que $I = \langle g \rangle$, donde

$$\langle g \rangle = \{gr | r \in R\}.$$

El elemento g es llamado un *generador* de I. También se dice que I es *generado* por

g. Además, un anillo R se dice que es un anillo de ideales principales si cada ideal de R es principal.

Notar que el generador de un ideal principal no puede ser único.

Ejemplo 4.1.9 En el ejemplo 4.1.7, el ideal I es principal. En efecto, $I = \langle 1 + x \rangle$. Notar que

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

Teorema 4.1.10 Los anillos $\mathbb{Z}$, $\mathbb{F}_q[x]$ y $\mathbb{F}_q[x]/(x^n - 1)$ son todos anillos de ideales principales.

Demostración. Sea I un ideal de $\mathbb{Z}$. Si $I = \{0\}$, entonces $I = \langle 0 \rangle$ es un ideal principal. Asumimos que $I \neq \{0\}$ y sea m el más pequeño entero positivo en I, y a cualquier elemento de I. Por el algoritmo de la división tenemos

$$a = qm + r \tag{2.2}$$

para algún entero q y $0 \leq r \leq m - 1$. La igualdad (2.2) implica que r también es un elemento de I pues $r = a - qm$. Esto fuerza a que $r = 0$ por la elección de m. Por lo tanto, $I = \langle m \rangle$. Esto muestra que $\mathbb{Z}$ es un anillo de ideales principales.

Empleando el mismo argumento, podemos fácilmente mostrar que $\mathbb{F}_q[x]$ es también un anillo de ideales principales.

Esencialmente el mismo método puede ser empleado para el caso $\mathbb{F}_q[x]/(x^n - 1)$. Puesto que este caso es crucial para este capítulo, repetiremos los argumentos. El ideal nulo es obviamente principal. Elijamos un polinomio no-nulo $g(x)$ de un ideal J no-nulo con el menor grado. Para cualquier polinomio $f(x) \in J$, tenemos

$$f(x) = s(x)g(x) + r(x)$$

Para algunos polinomios $s(x), r(x) \in \mathbb{F}_q[x]$ con $\deg(r(x)) < \deg(g(x))$. Esto fuerza a que $r(x) = 0$, pues $r(x) = f(x) - s(x)g(x) \in J$ y $g(x)$ tiene el menor grado entre los polinomios no-nulos de J. Por lo tanto, $J = \langle g(x) \rangle$, y el resultado deseado se sigue. □

4.2. Generadores polinomiales

La razón para definir los ideales en la sección precedente se aprecia en el siguiente resultado que relaciona ideales y códigos cíclicos.

Teorema 4.2.1 Sea π la aplicación lineal definida en (2.1). Entonces un subconjunto no-vació C de $\mathbb{F}_q^n$ es un código cíclico si, y sólo si $\pi(C)$ es un ideal de $\mathbb{F}_q[x]/(x^n - 1)$.

Demostración. Supongamos que $\pi(C)$ es un ideal de $\mathbb{F}_q[x]/(x^n - 1)$. Entonces, para cualesquiera $\alpha, \beta \in \mathbb{F}_q \subset \mathbb{F}_q[x]/(x^n - 1)$ y $\mathbf{a}, \mathbf{b} \in C$, tenemos $\alpha\pi(\mathbf{a}), \beta\pi(\mathbf{b}) \in \pi(C)$ por la Definición 4.1.5(ii). Así por la Definición 4.1.5(i) $\alpha\pi(\mathbf{a}) + \beta\pi(\mathbf{b})$ es un elemento de $\pi(C)$; es decir, $\pi(\alpha\mathbf{a} + \beta\mathbf{b}) \in \pi(C)$, por lo que $\alpha\mathbf{a} + \beta\mathbf{b}$ es una palabra-código de C. Esto muestra que C es un código lineal.

Ahora sea $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ una palabra-código de C. El polinomio

$$\pi(\mathbf{c}) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

es un elemento de $\pi(C)$. Puesto que $\pi(C)$ es un ideal, el elemento

$$\begin{aligned} x\pi(\mathbf{c}) &= c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} + c_{n-1} x^n \\ &= c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} + c_{n-1}(x^n - 1) \\ &= c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2} x^{n-1} \\ &.(\text{esto porque } x^n - 1 = 0 \text{ en } \mathbb{F}_q[x]/(x^n - 1)) \end{aligned}$$

esta en $\pi(C)$; es decir, $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ una palabra-código de C. Esto significa que C es cíclico.

Recíprocamente, supongamos que C es un código cíclico. Entonces esta claro que (i) de la Definición 4.1.5 es satisfecha por $\pi(C)$. 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 $\pi(C)$ con $(f_0, f_1, \ldots, f_{n-2}, f_{n-1}) \in C$, el polinomio

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

es también un elemento de $\pi(C)$ pues C es cíclico. Así, $x^2f(x) = x(xf(x))$ es un elemento de $\pi(C)$. Por inducción, sabemos que $x^if(x)$ pertenece a $\pi(C)$ para todo $i \geq 0$. Como C es un código lineal y π es una transformación lineal, $\pi(C)$ es un espacio lineal sobre $\mathbb{F}_q$. Por lo tanto, 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

$$g(x)f(x) = \sum_{i=0}^{n-1} g_i(x^if(x))$$

es un elemento de $\pi(C)$. Por lo tanto $\pi(C)$ es un ideal de $\mathbb{F}_q[x]/(x^n-1)$ pues (ii) de la Definición 4.1.5 también es satisfecha. □

Ejemplo 4.2.2 Ahora veamos tres ejemplos:

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

(ii) 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 $\pi^{-1}(I) = \{0000, 1010, 0101, 1111\}$;

(iii) Los códigos cíclicos triviales $\{\mathbf{0}\}$ y $\mathbb{F}_q^n$ corresponden a los ideales triviales$\{0\}$ y $\mathbb{F}_q[x]/(x^n-1)$, respectivamente.

Teorema 4.2.3 Sea I un ideal no-nulo en $\mathbb{F}_q[x]/(x^n-1)$ y sea $g(x)$ un polinomio mónico no-nulo de mínimo grado en I. Entonces $g(x)$ es un generador de I y divide a x^n-1.

Demostración. Para la primera parte, basta recordar la demostración del Teorema 4.1.10.

Considerando el algoritmo de la división tenemos que

$$x^n - 1 = s(x)g(x) + r(x)$$

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

$$r(x) = (x^n - 1) - s(x)g(x)$$

es un elemento de I (notar que $x^n - 1$ es el elemento nulo de $\mathbb{F}_q[x]/(x^n - 1)$). Esto implica que $r(x) = 0$ pues $g(x)$ tiene el mínimo grado. Por lo tanto, $g(x)$ es un divisor de $x^n - 1$. □

Ejemplo 4.2.4 En el Ejemplo 4.2.2(i), el polinomio $1 + x + x^2$ es el de menor grado, y divide a $x^3 - 1$. En el Ejemplo 4.2.2(ii), el polinomio $1 + x^2$ es el de menor grado, y divide a $x^4 - 1$. Para el código $\mathbb{F}_q^n$, el polinomio 1 es el menor grado.

Por el Teorema 4.1.10, sabemos que cada ideal en $\mathbb{F}_q[x]/(x^n - 1)$ es principal, así un código cíclico C es determinado por cualquiera de los generadores de $\pi(C)$. Usualmente, hay más de un generador para un ideal de $\mathbb{F}_q[x]/(x^n - 1)$. El siguiente resultado muestra que el generador que satisface ciertas propiedades adicionales es único.

Teorema 4.2.5 Existe un polinomio mónico único de menor grado en cada ideal I no-nulo de $\mathbb{F}_q[x]/(x^n - 1)$ (Por el Teorema 4.2.3, este es un generador de I).

Demostración. Sean $g_1(x)$, $g_2(x)$ dos generadores mónicos diferentes de menor grado en el ideal I. Entonces, un múltiplo escalar de $g_1(x) - g_2(x)$ es un polinomio mónico no-nulo de menor grado en I. Esta es una contradicción. □

A partir del resultado anterior, la siguiente definición cobra sentido.

Definición 4.2.6 El único polinomio mónico de menor grado del ideal no-nulo I de $\mathbb{F}_q[x]/(x^n - 1)$ es llamado el *polinomio generador* de I. Para un código cíclico C, el polinomio generador de $\pi(C)$ es también llamado el *polinomio generador* de C.

Ejemplo 4.2.7 (i) El generador polinomial del código cíclico $\{000, 110, 011, 101\}$ es $1 + x$.

(ii) El polinomio generador del código simple en el Ejemplo 4.1.3(iii) es $1+x^2+x^3+x^4$

Teorema 4.2.8 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 C el correspondiente código cíclico. Asumamos que $h(x)$ es el polinomio generador de 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 que $h(x)$, pues $h(x)$ tiene el menor grado y es mónico. □

A partir de los Teoremas 4.2.5 y 4.2.8, obtenemos el siguiente resultado.

Corolario 4.2.9 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 4.2.10 Los polinomios 1 y $x^n - 1$ corresponden a $\mathbb{F}_q^n$ y a $\{\mathbf{0}\}$ respectivamente.

Ejemplo 4.2.11 Con el propósito de encontrar todos los códigos cíclicos de longitud 6, factorizamos el polinomio $x^6 - 1 \in \mathbb{F}_2[x]$:

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

Y así, podemos listar todos los divisores mónicos de $x^6 - 1$:

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

Por lo tanto, existen en total nueve códigos cíclicos de longitud 6. En base a la aplicación π, podemos fácilmente escribir todos los códigos cíclicos. Por ejemplo, el código cíclico correspondiente al polinomio $(1 + x + x^2)^2$ es

$$\{000000, 101010, 010101, 111111\}.$$

A partir del ejemplo anterior, encontramos que el número de códigos cíclicos de longitud n puede ser determinado si conocemos la factorización de $x^n - 1$. Y así, tenemos el siguiente teorema.

Teorema 4.2.12 Para $x^n - 1 \in \mathbb{F}_q[x]$ tenemos 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 diferentes y $e_i \geq 1$ para todo $i = 1, 2, \ldots, r$. Entonces existen

$$\prod_{i=1}^{r}(e_i + 1)$$

códigos cíclicos de longitud n sobre $\mathbb{F}_q$.

La demostración del Teorema 4.2.12 se sigue del Corolario 4.2.9 contando el número de divisores mónicos de $x^n - 1$.

Ejemplo 4.2.13 Usando el teorema 4.3.9, podemos factorizar el polinomio $x^n - 1$, y de esta manera el numero de códigos cíclicos de longitud n puede ser determinado por el Teorema 4.2.12.

Las tablas 2.5 y 2.6 muestran la factorización de $x^n - 1$ y el número de códigos cíclicos q-arios de longitud n, para $1 \leq n \leq 10$ y $q = 2, 3$.

Como un código cíclico esta totalmente determinado por su polinomio generador, todos los parámetros de el código son también determinados por el polinomio generador. El siguiente resultado da la dimensión en términos del polinomio generador.

n	factorización de $x^n - 1$	N de códigos cíclicos
1	$1 + x$	2
2	$(1 + x)^2$	3
3	$(1 + x)(1 + x + x^2)$	4
4	$(1 + x)^4$	5
5	$(1 + x)(1 + x + x^2 + x^3 + x^4)$	4
6	$(1 + x)^2(1 + x + x^2)^2$	9
7	$(1 + x)(1 + x + x^3)(1 + x^2 + x^3)$	8
8	$(1 + x)^8$	9
9	$(1 + x)(1 + x + x^2)(1 + x^3 + x^6)$	8
10	$(1 + x)^2(1 + x + x^2 + x^3 + x^4)^2$	9

Tabla 4.5. Códigos cíclicos binarios de longitud hasta 10.

Teorema 4.2.14 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 $\deg(c_i(x)) \leq k - 1$ $(i = 1, 2)$, tenemos claramente que $g(x)c_1(x) \not\equiv g(x)c_2(x) \pmod{x^n - 1}$. Por lo tanto, el conjunto

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

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

$$a(x)g(x) = u(x)(x^n - 1) + v(x) \tag{2.3}$$

con $\deg(v(x)) < n$. Por (2.3), tenemos que $v(x) = a(x)g(x) - u(x)(x^n - 1)$. Por lo tanto, $g(x)$ divide a $v(x)$. Así que podemos escribir $v(x) = g(x)b(x)$ para algún

polinomio $b(x)$. Entonces $\deg(b(x)) < k$, por lo que $v(x)$ esta en A. Esto muestra que A es el mismo que $\langle g(x)\rangle$. Por lo tanto, la dimensión del código es $\log_q |A| = k$. □

Ejemplo 4.2.15 (i) En base a la factorización: $x^7 - 1 = (1 + x)(1 + x^2 + x^3)(1 + x + x^3) \in \mathbb{F}_2[x]$, sabemos que sólo existen dos $[7, 3]$-códigos cíclicos binarios

$$\begin{aligned}\langle(1 + x)(1 + x^2 + x^3)\rangle =&\{0000000, 1110100, 0111010, 0011101,\\ &1001110, 0100111, 1010011, 1101001\}\end{aligned}$$

y

$$\begin{aligned}\langle(1 + x)(1 + x + x^3)\rangle =&\{0000000, 1011100, 0101110, 0010111,\\ &1001011, 1100101, 1110010, 0111001\}.\end{aligned}$$

(ii) En base a la factorización: $x^7 - 1 = (2 + x)(1 + x + x^2 + x^3 + x^4 + x^5 + x^6) \in \mathbb{F}_3[x]$, podemos asegurar que no hay ningún $[7, 2]$-código cíclico ternario.

n	factorización de $x^n - 1$	Número de códigos cíclicos
1	$2 + x$	2
2	$(2 + x)(1 + x)$	4
3	$(2 + x)^3$	4
4	$(2 + x)(1 + x)(1 + x^2)$	8
5	$(2 + x)(1 + x + x^2 + x^3 + x^4)$	4
6	$(2 + x)^3(1 + x)^3$	16
7	$(2 + x)(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$	4
8	$(2 + x)(1 + x)(1 + x^2)(2 + x + x^2)(2 + 2x + x^2)$	32
9	$(2 + x)^9$	10
10	$(2 + x)(1 + x)(1 + x + x^2 + x^3 + x^4)(1 + 2x + x^2 + 2x^3 + x^4)$	16

Tabla 4.6. Códigos cíclicos ternarios de longitud hasta 10.

4.3. Matrices generadora y de paridad

En las secciones anteriores, mostramos que un código cíclico esta totalmente determinado por su polinomio generador. Por lo tanto, cualquier código cíclico también debería tener una matriz generadora determinada por su polinomio. De hecho, tenemos el siguiente resultado.

Teorema 4.3.1 Sea $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ el polinomio generador de un código cíclico C en $\mathbb{F}_q^n$ con $\deg(g(x)) = n - k$. Entonces la matriz de tamaño $k \times n$

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-2}g(x) \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & g_1 & g_2 & g_3 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{pmatrix}$$

es la matriz generadora de C (notar que identificamos un vector con un polinomio).

Demostración. Es suficiente mostrar que $g(x), xg(x), \ldots, x^{k-1}g(x)$ forma una base de C. Esta claro que ellos son linealmente independientes sobre $\mathbb{F}_q$. Por el Teorema 4.2.14, sabemos que $\dim(C) = k$. De donde se desprende el resultado deseado. □

Ejemplo 4.3.2 Considerar el $[7, 4]$-código cíclico binario con polinomio generador $g(x) = 1 + x^2 + x^3$. Entonces este código tiene la 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 generadora no está en la forma estándar. Si la cuarta fila es sumada a la segunda fila, y la suma de las dos últimas filas es añadida a la primera fila,

obtendremos la forma estándar de la matriz generadora, es decir:

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

Además, a partir de G' es fácil obtener la matriz de paridad aplicando el algoritmo 1.3.

Por lo visto hasta ahora, sabemos que la matriz de paridad de un código cíclico puede ser obtenida a partir de su matriz generadora empleando operaciones elementales de filas. Sin embargo, como el código dual de un código cíclico C también es cíclico, deberíamos ser capaces de encontrar una matriz de paridad a partir del polinomio generador del código dual. Entonces, solo resta encontrar el polinomio generador del código dual $C^{\perp}$.

Definición 4.3.3 Sea $h(x) = a_0 + a_1x + \cdots + a_kx^k$ un polinomio de grado k ($a_k \neq 0$) sobre $\mathbb{F}_q$. El polinomio recíproco $h_R(x)$ de $h(x)$ se define como

$$h_R(x) = x^k h\left(\frac{1}{x}\right) = \sum_{i=0}^{k} a_{k-i}x^i.$$

O de otra forma $h_R = a_k + a_{k-1}x + \cdots + a_1x^{k-1} + a_0x^k$.

Observación 4.3.4 Si $h(x)$ es un divisor de $x^n - 1$, entonces también lo será $h_R(x)$.

Ejemplo 4.3.5 (i) Para el polinomio $h(x) = 1 + 2x + 3x^5 + x^7 \in \mathbb{F}_5[x]$, el polinomio recíproco de $h(x)$ es

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

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

Ejemplo 4.3.6 Sea $g(x) = g_0 + g_1x + g_2x^2 + g_3x^3$ el polinomio generador del código cíclico C sobre $\mathbb{F}_q$ de longitud 4 y sea $h(x) = (x^4 - 1)/g(x)$. Colocando $h(x) = h_0 + h_1x + h_2x^2 + h_3x^3$, entonces $h_R(x) = (h_3 + h_2x + h_1x^2 + h_0x^3)/x^{3-k}$, donde $k = \deg(h(x))$. Considerar el producto

$$
\begin{aligned}
0 &\equiv g(x)h(x) \\
&\equiv (g_0 + g_1x + g_2x^2 + g_3x^3)(h_0 + h_1x + h_2x^2 + h_3x^3) \\
&\equiv g_0h_0 + (g_0h_1 + g_1h_0)x + (g_2h_0 + g_1h_1 + g_0h_2)x^2 + \\
&\quad + (g_3h_0 + g_2h_1 + g_1h_2 + g_0h_3)x^3 + (g_3h_1 + g_2h_2 + g_1h_3)x^4 + \\
&\quad + (g_3h_2 + g_2h_3)x^5 + g_3h_3x^6 \qquad (2.4) \\
&\equiv (g_0h_0 + g_1h_3 + g_2h_2 + g_3h_1) + (g_0h_1 + g_1h_0 + g_2h_3 + g_3h_2)x + \\
&\quad + (g_0h_2 + g_1h_1 + g_2h_0 + g_3h_3)x^2 + (g_3h_0 + g_2h_1 + g_1h_2 + g_0h_3)x^3 \pmod{x^4 - 1}.
\end{aligned}
$$

Por lo tanto, los coeficientes de cada potencia de x en el último paso de (2.4) deben ser cero. Colocando $\mathbf{b} = (h_3, h_2, h_1, h_0) \in \mathbb{F}_q^4$ y $\mathbf{g} = (g_0, g_1, g_2, g_3) \in \mathbb{F}_q^4$. Sea $\mathbf{g}_i$ el vector obtenido a partir de $\mathbf{g}$ por desplazar cíclicamente i posiciones. Al observar el coeficiente de x^3 en (2.4), obtenemos

$$\mathbf{g}_0 \cdot \mathbf{b} = \mathbf{g} \cdot \mathbf{b} = g_0h_3 + g_1h_2 + g_2h_1 + g_3h_0 = 0.$$

Al observar todos los coeficientes de las otras potencias de x en (2.4), obtenemos $\mathbf{g}_i \cdot \mathbf{b} = 0$ para todo $i = 0, 1, 2, 3$. Por lo tanto, $\mathbf{b}$ es una palabra-código de $C^\perp$ pues el conjunto $\{\mathbf{g}_0, \mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3\}$ genera C por el teorema 4.3.1.

Desplazando cíclicamente $k + 1$ posiciones el vector $\mathbf{b} = (h_3, h_2, h_1, h_0)$, obtenemos el correspondiente vector para $h_R(x)$. Esto implica que $h_R(x)$ es una palabra-código así como $C^\perp$ es un código cíclico.

Ya que $\deg(h_R(x)) = \deg(h(x)) = k$, el conjunto $\{h_R(x), xh_R(x), \ldots, x^{n-k-1}h_R(x)\}$ es una base de $C^\perp$. Por lo tanto, $C^\perp$ es generado por $h_R(x)$. Por lo tanto el polinomio mónico $h_0^{-1}h_R(x)$ es el polinomio generador de $C^\perp$ (notar que $h_0 = h(0) \neq 0$ pues $h_0g_0 = -1$).

Esta claro que el anterior ejemplo puede ser generalizado fácilmente para cualquier longitud n.

Teorema 4.3.7 Sea $g(x)$ el polinomio generador de un $[n, k]$-código cíclico q-ario C. Si se toma

$$h(x) = \frac{x^n - 1}{g(x)}.$$

Entonces $h_0^{-1} h_R(x)$ es el polinomio generador de $C^\perp$, donde h_0 es el término constante de $h(x)$.

Demostración. Sean los polinomios

$$g(x) = \sum_{i=0}^{n-1} g_i x^i \quad \text{y} \quad h(x) = \sum_{i=0}^{n-1} h_i x^i.$$

Entonces

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

donde $k = \deg(h(x))$. Considerar el producto

$$\begin{aligned} 0 &\equiv g(x)h(x) \\ &\equiv (g_0h_0 + g_1h_{n-1} + \cdots + g_{n-1}h_1) + (g_0h_1 + g_1h_0 + \cdots + g_{n-1}h_2)x + \\ &\quad + (g_0h_2 + g_1h_1 + \cdots + g_{n-1}h_3)x^2 + \cdots + \\ &\quad + (g_0h_{n-1} + g_1h_{n-2} + \cdots + g_{n-1}h_0)x^{n-1} \pmod{x^n - 1}. \end{aligned}$$

Por lo tanto la coeficiente de cada potencia de x en la última línea del desarrollo anterior debe ser cero. Observando el coeficiente de cada potencia de x, obtenemos $\mathbf{g}_i \cdot (h_{n-1}, h_{n-2}, \ldots, h_1, h_0) = 0$ para todo $i = 0, 1 \ldots, n-1$, donde $\mathbf{g}_i$ es el vector obtenido al desplazar cíclicamente i posiciones de $(g_0, g_1, \ldots, g_{n-1})$. Por lo tanto $(h_{n-1}, h_{n-2}, \ldots, h_1, h_0)$ es un código-palabra de $C^\perp$ pues $(\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1})$ genera C por el Teorema 4.3.1.

Si desplazamos cíclicamente $k+1$ posiciones en el vector $(h_{n-1}, h_{n-2}, \ldots, h_1, h_0)$, obtendremos el vector correspondiente a $h_R(x)$. Esto implica que $h_R(x)$ es una palabra-código, así como $C^\perp$ es un código cíclico.

Puesto que $\deg(h_R(x)) = \deg(h(x)) = k$, el conjunto $\{h_R(x), xh_R(x), \ldots, x^{n-k-1}h_R(x)\}$ es una base de $C^\perp$. En consecuencia, $C^\perp$ es generado por $h_R(x)$. De esta manera, el polinomio mónico $h_0^{-1}h_R(x)$ es el polinomio generador de $C^\perp$. □

Definición 4.3.8 Sea C un código cíclico q-ario de longitud n. Colocando

$$h(x) = \frac{x^n - 1}{g(x)}.$$

Entonces, $h_0^{-1}h_R(x)$ es denominado *polinomio de paridad* de C, donde h_0 es el término constante de $h(x)$.

Corolario 4.3.9 Sea C un $[n, k]$-código cíclico q-ario con polinomio generador $g(x)$. Tomando

$$h(x) = \frac{x^n - 1}{g(x)} = h_0 + h_1x + \cdots + h_kx^k.$$

Entonces la matriz

$$H = \begin{pmatrix} h_R(x) \\ xh_R(x) \\ \vdots \\ x^{k-1}h_R(x) \\ x^{n-k-1}h_R(x) \end{pmatrix} = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & h_{k-1} & h_{k-2} & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \end{pmatrix}$$

es la matriz de paridad de C.

Demostración. El resultado se sigue inmediatamente de los Teorema 4.3.1 y 4.3.7. □

Ejemplo 4.3.10 Sea C el [7,4]-código cíclico binario generado por $g(x) = 1+x^2+x^3$ como en el Ejemplo 4.3.2 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 de paridad de C. Por lo tanto,

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

es la matriz de paridad de C.

4.4. Decodificación de los códigos cíclicos

La decodificación de los códigos cíclicos consiste de los mismos tres pasos que la decodificación de los códigos lineales: calcular el síndrome; encontrar el síndrome correspondiente al patrón de error; y corregir los errores. Como la estructura de los códigos cíclicos es mas agradable, los tres pasos son usualmente más sencillos. Los códigos cíclicos tienen considerables propiedades algebraicas y geométricas. Si estas propiedades son usadas apropiadamente, se puede alcanzar una decodificación notablemente simple.

Siempre hablando de códigos cíclicos y empleando el Corolario 4.3.9, podemos fácilmente producir una matriz de paridad de la forma

$$H = (I_{n-k}|A) \tag{2.5}$$

empleando operaciones elementales de filas. Aunque las matrices de paridad para un código lineal no son únicas, la matriz de paridad de la forma (2.5) es única. Todos los síndromes considerados en esta sección son calculados con respecto a la matriz de paridad de la forma (2.5).

Teorema 4.4.1 Sea $H = (I_{n-k}|A)$ la matriz de paridad del código cíclico q-ario C y sea $g(x)$ el polinomio generador de C. Entonces el síndrome de un vector $\mathbf{w} \in \mathbb{F}_q^n$ es igual a $(w(x) \pmod{g(x)})$; es decir, el resto principal que queda al dividir $w(x)$ entre $g(x)$.

Notar que aquí identificamos un vector de $\mathbb{F}_q^n$ con un polinomio de $\mathbb{F}_q[x]/(x^n - 1)$, y así $w(x)$ es el polinomio correspondiente de $\mathbf{w}$.

Demostración. A cada vector columna de A, le asociamos un polinomio de grado a lo más $n - k - 1$ y escribimos A como

$$A = (a_0(x), a_1(x), \ldots, a_{k-1}(x)).$$

Por el algoritmo 1.3, sabemos que $G = (-A^T|I_k)$ es una matriz generadora de C. Por lo tanto, $x^{n-k+i} - a_i(x)$ es una palabra-código de C, por lo que $x^{n-k+i} - a_i(x) =$

$q_i(x)g(x)$ para algún $q_i(x) \in \mathbb{F}_q[x]/(x^n - 1)$; es decir,

$$a_i(x) = x^{n-k+i} - q_i(x)g(x) \tag{2.6}$$

Suponiendo que $w(x) = w_0 + w_1x + \cdots + w_{n-1}x^{n-1}$, para el síndrome $\mathbf{s} = \mathbf{w}H^T$ de $\mathbf{w}$, el polinomio correspondiente $s(x)$ es

$$\begin{aligned} s(x) &= w_0 + w_1x + \cdots + w_{n-k-1}x^{n-k-1} + w_{n-k}a_0(x) + \cdots + w_{n-1}a_{k-1}(x) \\ &= \sum_{i=0}^{n-k-1} w_ix^i + \sum_{j=0}^{k-1} w_{n-k+j}(x^{n-k+j} - q_j(x)g(x)) \quad \text{(por (2.6))} \\ &= \sum_{i=0}^{n-1} w_ix^i - \left(\sum_{j=0}^{k-1} w_{n-k+j}q_j(x)\right) g(x) \\ &\equiv w(x) \pmod{g(x)} \end{aligned}$$

Como el polinomio $s(x)$ tiene grado a lo más $n - k - 1$, el resultado deseado se sigue. □

Ejemplo 4.4.2 Considerar el [7,4,3]-código de Hamming binario con el polinomio generador $g(x) = 1 + x^2 + x^3$. Entonces, aplicando operaciones elementales de filas en la matriz del Ejemplo 4.3.10, obtenemos la matriz de paridad $H = (I_3|A)$, donde A es la matriz

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

Para la palabra $\mathbf{w} = 0110110$, el síndrome es $\mathbf{s} = \mathbf{w}H^T = 010$. Por otro lado,

$$w(x) = x + x^2 + x^4 + x^5 = x + x^2g(x).$$

Así, el resto ($w(x) \pmod{g(x)}$) es x, que corresponde a la palabra 010.

El Teorema 4.4.1 muestra que el síndrome de una palabra recibida $w(x)$ puede ser determinado por el resto $s(x) = (w(x) \pmod{g(x)})$. Por lo tanto, $w(x) - s(x)$ es una palabra-código.

Corolario 4.4.3 Sea $g(x)$ el polinomio generador de un código cíclico C. Para una palabra recibida $w(x)$, si el resto $s(x)$ de dividir $w(x)$ entre $g(x)$ tiene peso menor que

o igual a $\lfloor (d(C)-1)/2 \rfloor$, entonces $s(x)$ es el patrón de error de $w(x)$; es decir, $w(x)$ es decodificado como $w(x) - s(x)$ por MLD (Decodificación de Máxima Probabilidad).

Demostración. Por el Teorema 4.4.1, sabemos que $w(x)$ y $s(x)$ están en la misma clase lateral. Por otra parte, $s(x)$ es el líder de su clase por el Ejercicio 4.44 pues $\mathrm{wt}\,(s(x)) \leq \lfloor (d(C)-1)/2 \rfloor$. Que es el resultado deseado. □

Ejemplo 4.4.4 Como en el Ejemplo 4.4.2, es resto de dividir $w(x) = x+x^2+x^4+x^5$ entre $g(x) = 1 + x^2 + x^3$ es x. Por lo tanto, $w(x)$ es decodificada como $w(x) - x = x^2 + x^4 + x^5 = 0010110$. Si la palabra $w_1(x) = 1 + x^2 + x^3 + x^4$ es recibida, entonces el resto $(w_1(x) \pmod{g(x)})$ es $1 + x + x^2$. En este caso, podemos usar el síndrome de decodificación para obtener la palabra-código $w_1(x) - x^4 = 1 + x^2 + x^3 = 1011000$ pues la palabra 0000100 es el líder de la clase lateral en la que se encuentra $w_1(x)$.

En el ejemplo anterior, vimos que, algunas palabras recibidas pueden ser directamente decodificadas extrayendo el resto de las palabras. Sin embargo, para otras palabras tenemos que usar la decodificación a través del síndrome. Debido a las propiedades algebraicas y geométricas de los códigos cíclicos, podemos simplificar la decodificación por síndrome para algunas palabras recibidas. En lo que resta de esta sección, describiremos la denominada decodificación por *captura de errores*.

Lema 4.4.5 Sea C un $[n, k]$-código cíclico q-ario con polinomio generador $g(x)$. Sea $s(x) = \sum_{i=0}^{n-k-1} s_i x^i$ el síndrome de $w(x)$. Entonces el síndrome del desplazamiento cíclico $xw(x)$ es igual a $xs(x) - s_{n-k-1}g(x)$.

Demostración. Por el Teorema 4.4.1, es suficiente mostrar que $xs(x) - s_{n-k-1}g(x)$ es el resto de dividir $xw(x)$ entre $g(x)$. Si $w(x) = q(x)g(x) + s(x)$, entonces

$$\begin{aligned} xw(x) &= xq(x)g(x) + xs(x) \\ &= (xq(x) + s_{n-k-1})g(x) + (xs(x) - s_{n-k-1}g(x)). \end{aligned}$$

Que es el resultado deseado, pues $\deg(xs(x) - s_{n-k-1}g(x)) < n - k = \deg(g(x))$. □

Observación 4.4.6 El síndrome del desplazamiento cíclico $x^i w(x)$ de una palabra $w(x)$ puede ser calculado a través del síndrome del desplazamiento cíclico $x^{i-1}w(x)$. Así, los síndromes de $w(x), xw(x), x^2w(x), \ldots$ pueden ser calculados inductivamente.

Ejemplo 4.4.7 Como en el Ejemplo 4.4.2, el síndrome de $w(x) = x+x^2+x^4+x^5$ es x, por lo tanto los síndromes de $xw(x)$ y $x^2w(x)$ son $x \cdot x = x^2$ y $x \cdot x^2 - g(x) = 1+x^2$, respectivamente.

Definición 4.4.8 Un bloque cíclico de 0s de longitud l de una n-tupla, es una sucesión de l componentes ceros cíclicamente consecutivos.

Ejemplo 4.4.9 (i) La 9-tupla $\mathbf{e} = (1, 3, 0, 0, 0, 0, 0, 1, 0)$ tiene un bloque cíclico de 0s de longitud 5.

(i) La 10-tupla $\mathbf{e} = (0, 0, 1, 2, 0, 0, 0, 1, 0, 0)$ tiene un bloque cíclico de 0s de longitud 4.

Algoritmo de decodificación para códigos cíclicos

Sea C un $[n, k, d]$-código cíclico q-ario con polinomio generador $g(x)$. Sea $w(x)$ la palabra recibida con patrón de errores $e(x)$, donde $\text{wt}\,(e(x)) \leq \lfloor (d-1)/2 \rfloor$ y $e(x)$ tiene un bloque cíclico de 0s de longitud al menos k. El objetivo es determinar $e(x)$.

Paso 1: Calcular el síndrome de $x^i w(x)$, para $i = 0, 1, 2, \ldots$, hasta que se cumpla el paso 2 y denotar por $s_i(x)$ el síndrome $(x^i w_1(x)$ (mód $g(x))$).

Paso 2: Encontrar m tal que el peso del síndrome $s_m(x)$ para $x^m w(x)$ es menor que o igual a $\lfloor (d-1)/2 \rfloor$.

Paso 3: Calcular el resto $e(x)$ de dividir $x^{n-m} s_m(x)$ entre $x^n - 1$. Decodificar $w(x)$ como $w(x) - e(x)$.

Demostración. En primer lugar, mostraremos la existencia de m en el Paso 2. Como se supuso, existe un patrón de error $e(x)$ tal que $e(x)$ tiene un bloque cíclico de 0s de longitud al menos k. Así existe un entero $m \geq 0$ tal que el desplazamiento cíclico

de m posiciones del patrón de error $e(x)$ tiene todas sus componentes no-nulas en las primera $n-k$ posiciones. El resultado de desplazar cíclicamente m posiciones del patrón de error $e(x)$ es de hecho el resto de dividir $x^m w(x) \pmod{x^n-1}$ entre $g(x)$. Colocando

$$r(x) = ((x^m w(x) \pmod{x^n-1}) \pmod{g(x)}) = (x^m w(x) \pmod{g(x)}).$$

El peso de $r(x)$ es claramente el mismo que el peso de $e(x)$, que es a lo más $\lfloor (d-1)/2 \rfloor$. Esto muestra la existencia de m.

La palabra $t(x) = (x^{n-m} s_m(x) \pmod{x^n-1})$ es un desplazamiento cíclico de $n-m$ posiciones de $(\mathbf{s}_m, \mathbf{0})$, donde $\mathbf{s}_m$ es el vector de $\mathbb{F}_q^{n-k}$ correspondiente al polinomio $s_m(x)$. Es evidente que el peso de $t(x)$ es el mismo que el peso de $s_m(x)$. Por lo tanto, $\mathrm{wt}\,(t(x)) \leq \lfloor (d-1)/2 \rfloor$. Como

$$\begin{aligned} x^m\,(w(x) - t(x)) &\equiv x^m \left(w(x) - x^{n-m} s_m(x)\right) \\ &\equiv x^m w(x) - x^n s_m(x) \\ &\equiv s_m(x) - x^n s_m(x) \\ &\equiv (1-x^n) s_m(x) \\ &\equiv 0 \pmod{g(x)} \end{aligned}$$

y x^m es coprimo a $g(x)$ (ver la Observación 2.3.11 (iii)), afirmamos que $w(x)-t(x)$ es divisible por $g(x)$; es decir, $w(x)-t(x)$ es una palabra código. Como $t(x)$ y el patrón de errores $e(x)$ están en la misma clase lateral, tenemos que $e(x) = t(x) = x^{n-m} s_m(x) \pmod{x^n-1}$. □

Ejemplo 4.4.10 Como en el Ejemplo 2.4.4, consideremos la palabra recibida

$$w_1(x) = 1011100 = 1 + x^2 + x^3 + x^4.$$

Calcular los síndromes $s_i(x)$ de $x^i w_1(x)$ hasta que $\mathrm{wt}\,(s_i(x)) \leq 1$, como se muestra en la Tabla 2.7. Y por último decodificar $w_1(x) = 1011100$ como $w_1(x) - x^4 s_3(x) = w_1(x) - x^4 = 1 + x^2 + x^3 = 1011000$.

i	$s_i(x)$
0	$1+x+x^2$
1	$1+x$
2	$x+x^2$
3	1

Tabla 4.7. Síndromes $s_i(x)$ de $x^i w_1(x)$ hasta que $\mathrm{wt}\,(s_i(x)) \leq 1$.

Ejemplo 4.4.11 Considerar el [15,7]-código cíclico binario generado por $g(x) = 1+x^4+x^6+x^7+x^8$. Podemos comprobar por medio de la matriz de paridad que la distancia mínima es 5. Un patrón de error con peso a lo más 2 debe tener un bloque cíclico de 0s de longitud al menos 7. Por lo tanto podemos corregir este patrón de error usando el algoritmo anteriormente expuesto. Considerar la palabra recibida

$$w(x) = 110011101100010 = 1+x+x^4+x^5+x^6+x^8+x^9+x^{13}.$$

Calcular los síndromes $s_i(x)$ de $x^i w_1(x)$ hasta que $\mathrm{wt}\,(s_i(x)) \leq 2$, como se muestra en la Tabla 2.8. Y por último decodificar $w(x) = 110011101100010$ como $w(x) - x^8 s_7(x) = w(x) - x^8 - x^{13} = 1+x+x^4+x^5+x^6+x^9 = 110011100100000$.

i	$s_i(x)$
0	$1+x^2+x^5+x^7$
1	$1+x+x^3+x^4+x^7$
2	$1+x+x^2+x^5+x^6+x^7$
3	$1+x+x^2+x^3+x^4$
4	$x+x^2+x^3+x^4+x^5$
5	$x^2+x^3+x^4+x^5+x^6$
6	$x^3+x^4+x^5+x^6+x^7$
7	$1+x^5$

Tabla 4.8. Síndromes $s_i(x)$ de $x^i w_1(x)$ hasta que $\mathrm{wt}\,(s_i(x)) \leq 2$.

4.5. Códigos que corrigen errores de ráfaga

Hasta ahora, nos hemos ocupado únicamente en códigos que corrigen errores aleatorios. Sin embargo, hay ciertos canales de comunicación, tales como las líneas telefónicas y sistemas de almacenamiento magnético, que son afectados por errores localizados en breves intervalos en lugar de errores aleatorios. A tal error se denomina *error de ráfaga*. En general, los códigos para corregir errores aleatorios no son eficientes para la corrección de errores de ráfaga. Por lo tanto, es deseable construir códigos específicos para la corrección de errores de ráfaga. Códigos de este tipo se denominan *códigos correctores de errores de ráfaga*.

Los códigos cíclicos son muy eficientes para corregir errores de ráfaga. Desde la década de los 70s, se han encontrado muchos códigos cíclicos eficaces en la corrección de errores de ráfaga. En esta sección, trataremos algunas propiedades de los códigos correctores de errores de ráfaga y un algoritmo para decodificarlos. Los códigos en esta sección son todos binarios.

Definición 4.5.1 Una *ráfaga* de longitud $l \geq 1$ es un vector binario cuyas componentes no-nulas se limitan a l posiciones cíclicamente consecutivas, siendo la primera y última posiciones no-nulas.

Un código se denomina *código corrector de l errores de ráfaga* si este puede corregir todos los errores de ráfaga de longitud l o menos; es decir, los patrones de error que son ráfagas de longitud l o menos.

Ejemplo 4.5.2 El vector 01000000000000100 es una ráfaga de longitud 5, mientras que, 0011010000 es una ráfaga de longitud 4.

Teorema 4.5.3 Un código lineal C es un código corrector de l errores de ráfaga si, sólo si todos los errores de ráfaga de longitud l o menos se encuentran en clases laterales diferentes de C.

Demostración. Si todos los errores de ráfaga de longitud l o menos se encuentran en clases laterales diferentes, entonces cada error de ráfaga es determinado por su

síndrome; entonces el error puede ser corregido por medio de su síndrome.

Por otro lado, supongamos que dos errores de ráfaga diferentes $\mathbf{b}_1$ y $\mathbf{b}_2$ de longitud l o menos se encuentran en la misma clase lateral de C. La diferencia $\mathbf{c} = \mathbf{b}_1 - \mathbf{b}_2$ es una palabra-código. Por lo tanto, si $\mathbf{b}_1$ es recibido, entonces $\mathbf{b}_1$ se decodificaría como $\mathbf{0}$ y $\mathbf{c}$. □

Corolario 4.5.4 Sea C un $[n, k]$-código lineal corrector de l errores de ráfaga. Entonces

(i) ninguna ráfaga no-nula de longitud $2l$ o menos puede ser una palabra-código;

(ii) (Cota de Reiger) $n - k \geq 2l$.

Demostración. (i) Supongamos que existe una palabra-código $\mathbf{c}$ que es una ráfaga de longitud $\leq 2l$. Entonces, $\mathbf{c}$ es de la forma $(\mathbf{0}, 1, \mathbf{u}, \mathbf{v}, 1, \mathbf{0})$, donde $\mathbf{u}$ y bfv son dos palabras de longitud $\leq l - 1$. Por lo tanto, las palabras $\mathbf{w} = (\mathbf{0}, 1, \mathbf{u}, \mathbf{0}, 0, \mathbf{0})$ y $\mathbf{c} - \mathbf{w} = (\mathbf{0}, 0, \mathbf{0}, \mathbf{v}, 1, \mathbf{0})$ son dos ráfagas de longitud $\leq l$; ellas están en la misma clase lateral. Esta es una contradicción al Teorema 4.5.3.

(ii) Sean $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{n-k+1}$ las primeras $n-k+1$ vectores columna de una matriz de paridad de C. Entonces, ellos se encuentran en $\mathbb{F}_2^{n-k}$ y por lo tanto son linealmente dependientes. Por lo tanto, existen $c_1, c_2, \ldots, c_{n-k+1} \in \mathbb{F}_2$, no todos nulos, tales que $c_1\mathbf{u}_1 + c_2\mathbf{u}_2 + \cdots + c_{n-k+1}\mathbf{u}_{n-k+1} = \mathbf{0}$. Esto implica que $(c_1, c_2, \ldots, c_{n-k+1}, \mathbf{0})$ es una palabra-código y esta claro que esta palabra-código es una ráfaga de longitud $\leq n - k + 1$. Por la parte (i), tenemos que $n - k + 1 > 2l$; es decir $n - k \geq 2l$. □

Un $[n, k]$-código lineal corrector de l errores de ráfaga satisface $n - k \geq 2l$; es decir,

$$l \leq \lfloor \frac{n-k}{2} \rfloor. \tag{2.7}$$

Un código lineal corrector de errores de ráfaga que alcanza la Cota de Reiger se denomina código corrector de errores de ráfaga *óptimo*.

Ejemplo 4.5.5 Sea C el código cíclico binario de longitud 15 generado por $1 + x + x^2 + x^3 + x^6$. Este es un [15,9]-código lineal. El lector puede verificar que todos

los errores de longitud 3 o menos se encuentran en distintas clases laterales de C. Por el Teorema 4.5.3, C es un código corrector de 3 errores de ráfaga. Si el lector quiere confirmar el Corolario 4.5.4(i) puede observar que no hay errores de ráfaga de longitud 6 o menor que sean palabras-código. Este código además es óptimo pues alcanza la Cota de Reiger (2.7).

Notar que una ráfaga de longitud l tiene un bloque de 0s de longitud $n-l$. Por el Corolario 4.5.4, tenemos que $k \leq n-2l \leq n-l$ para un $[n,k]$-código lineal corrector de l errores de ráfaga. Esto satisface el requerimiento del algoritmo de decodificación de la Sección 4.4 para corregir un error conteniendo un bloque cíclico de al menos k ceros. Por lo tanto, el algoritmo puede ser usado directamente para corregir errores de ráfaga. La principal diferencia es que, en el caso de la corrección de errores de ráfaga, no requerimos que el peso de un patrón de error sea $\leq \lfloor (d(C)-1)/2 \rfloor$. El algoritmo modificado para la decodificación de errores de ráfaga es el siguiente.

Algoritmo de decodificación para códigos correctores de errores de ráfaga

Sea C un $[n,k]$-código cíclico q-ario con polinomio generador $g(x)$. Sea $w(x)$ la palabra recibida con patrón de errores $e(x)$, que es una ráfaga de longitud l o menos.

Paso 1: Calcular el síndrome de $x^i w(x)$, para $i = 0, 1, 2, \ldots$ hasta que se cumpla el paso 2, y denotar por $s_i(x)$ el síndrome $x^i w(x)$.

Paso 2: Encontrar m tal que el síndrome para $x^m w(x)$ es una ráfaga de longitud l o menos.

Paso 3: Calcular el resto $e(x)$ de dividir $x^{n-m} s_m(x)$ entre $x^n - 1$. Decodificar $w(x)$ como $w(x) - e(x)$.

La demostración del algoritmo es similar al de la sección previa. Ahora usaremos el código del Ejemplo 4.5.5 para ilustrar este algoritmo.

Ejemplo 4.5.6 Considerar el [15,9]-código cíclico binario generado por $g(x) = 1 + x + x^2 + x^3 + x^6$. Podemos corregir todos los errores de longitud 3 o menos.

Supongamos que

$$w(x) = 111011101100000 = 1 + x + x^2 + x^4 + x^5 + x^6 + x^8 + x^9.$$

Calculemos el síndrome $s_i(x)$ para $x^i w(x)$ mientras $s_m(x)$ es una ráfaga de longitud 3 o menos (ver la Tabla 2.9). Decodificamos $w(x) = 111011101100000$ como $w(x) - x^6 s_9(x) = w(x) - x^6 - x^8 = 1 + x + x^2 + x^4 + x^5 + x^9 = 111011000100000$.

i	$s_i(x)$
0	$1 + x + x^4 + x^5$
1	$1 + x^3 + x^5$
2	$1 + x^2 + x^3 + x^4$
3	$x + x^3 + x^4 + x^5$
4	$1 + x + x^3 + x^4 + x^5$
5	$1 + x^3 + x^4 + x^5$
6	$1 + x^2 + x^3 + x^4 + x^5$
7	$1 + x^2 + x^4 + x^5$
8	$1 + x^2 + x^5$
9	$1 + x^2$

Tabla 4.9. Síndrome $s_i(x)$ para $x^m w(x)$ del Ejemplo 2.5.6.

Concluimos nuestra discusión con una lista de algunos códigos cíclicos óptimos.

Parámetros del código	Polinomios generadores
[7,3]	$1 + x + x^3 + x^4$
[15,9]	$1 + x + x^2 + x^3 + x^6$
[15,7]	$1 + x^4 + x^6 + x^7 + x^8$
[15,5]	$1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$

Tabla 4.10. Algunos códigos cíclicos correctores de errores de ráfaga óptimos.

Conclusiones

✓Con este trabajo se concluye que la aplicación de los algoritmos y los códigos correctores de errores de ráfaga son eficientes para corregir las palabras enviadas y recibidas, ya que los códigos lineales y códigos cíclicos son aplicados en distintos ámbitos, primero se codificaron y decodificaron las palabras enviadas y recibidas.

✓Se detectaron y corrigieron los errores aleatorios haciendo uso de algoritmos en donde la matriz generadora y la matriz de control de paridad tienen que necesariamente convertirse en FEF y FREF para encontrar la base necesaria. Así mismo cuando se encuentran dos errores se utiliza el síndrome y el patrón de errores para detectar y corregir los errores de ráfaga.

✓Existirán palabras enviadas y recibidas que necesariamente tendrán que ser codificadas y decodificadas respectivamente, para esto la teoría de códigos lineales y los códigos cíclicos nos ofrece los pasos para poder realizarlo el cual con mucho éxito se logró realizarlo y así se facilitó la coreeción de errores.

Por lo tanto, se ha comprobado que los algoritmos y los códigos correctores de ráfaga som muy eficientes al momento de corregir códigos cíclicos, ya que al utilizar este tipo de algoritmos se logra consolidar la comprensión de conceptos básicos y las carecterísticas principales de los códigos.

En este trabajo se facilito las operaciones con matrices utilizando el programa MATLAB, el cual tiene el rol de acelerar los cálculos matemáticos, específicamente las matrices, en donde introduciendo los datos las matrices se convertirán en FEF y FREF esto para encontrar la base requerida, obviamente esto dependerá del campo en donde se está trabajando.

Recomendaciones

Esta claro que existen muchos códigos en donde se pretende una correcta codificación y decodificación, es así que los códigos lineales y cíclicos no son la solución deseada para los diferentes códigos. Es por eso que surgen los códigos BCH, que son un tipo particular de códigos cíclicos, construidos a partir del método de selección de raíces, que nos permiten averiguar a priori la capacidad correctora de nuestro código. Con esta técnica es viable, conocida la tasa de errores a la que nos queremos ajustar, construir de forma eficiente un código tal que sea capaz de corregir dicha tasa de errores, dejo al lector este tema pendiente ya que es un tema interesante a desarrollar.

Las investigaciones y aplicaciones que posee el Algebra Abstracta, como ser: Los Códigos de Hamming, los Códigos BCH, los Códigos de Golay, Códigos Reed Solomon, y otros que son de relativa importancia en la decodificación de Códigos, con esto se motiva a los investigadores poder profundizar más sobre estos temas pendientes.

Bibliografía

[1] K.J. Horadam, Hadamard Matrices and Their Applications, Princeton University Press, Princeton, 2007.

[2] D. Jungnickel, Finite Fields: Structure and Arithmetics, Bibliographisches Institut, Mannheim, 1993.

[3] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam (1998).

[4] Raymond Hill, A first course in coding theory, Oxford Applied Mathematics and Computing Science Series, The Clarendon Press Oxford University Press, New York, 1986.

[5] Neal Koblitz, A course in number theory and cryptography, Graduate Texts in Mathematics, vol. 114, Springer-Verlag, New York, 1987.

[6] Simon Singh, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, Anchor, 2000.

[7] W. C. Huffman, Codes and groups, in Handbook of Coding Theory, eds. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, pp. 13451440.

[8] Munuera Gómez. Juan y Tena. Juan. Codificación de la información . Secretariado de publicaciones e intercambio científico (1997).

[9] W.C. Huffman y V. Pless, Fundamentals of Error Correcting Codes, Cambridge, 2003.

[10] V. Pless, Introduction to the Theory of Error-Correcting Codes, Wiley, 1982.

[11] V. Pless and Z. Qian, Cyclic codes and quadratic residue codes over Z4,ÏEEE Trans. Inform. Theory IT42 (1996), 15941600.

[12] O. Pretzel, Codes and Finite Fields, Clarendon, 1992.

[13] Yehuda Lindell, Ïntroduction to Coding Theory", Lecture Notes.Department of Computer Science Bar-Ilan University, Israel, January 25, 2010.

[14] Dave K. Kythe - Prem K. Kythe, .ªlgebraic and Stochastic Coding Theory", 2012.

[15] Harald Niederreiter Arne Winterhof, .ªpplied Number Theory", March 2015.

[16] Carlos Arce - William Castillo - Jorge Gonzalez - .ªlgebra Lineal", Universidad de Costa Rica Escuela de Matemática, 2003.

[17] Michael Stoll, "Linear Algebra I", Course No. 100 221, Fall 2006, December 10, 2007.

[18] Cándido López - Manuel Veiga, "Teoría de la Información y Codificación", 2002.

[19] Sarah A. Spence, Ïntroduction to Algebraic Coding Theory", Supplementary material for Math 336 Cornell University, 2001.

[20] J. Gallian, Çontemporary Abstract Algebra", D.C. Heath and Company, Lexington, MA, third ed., 1994.

[21] W. W. Peterson, .ErError-Correcting Codes", The M.I.T. Press, Cambridge, Mass., 1961.

[22] I. S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields, J. Soc. Indust. Appl. Math., 8 (1960), pp. 300-304.

[23] R. Lidl, H. Niederreiter, "Finite Fields"(Addison-Wesley, Reading, 1983). Reprint, Cambridge University Press, Cambridge, 1997.

[24] F.J. MacWilliams, N.J.A. Sloane, "The Theory of Error-Correcting Codes", North-Holland, Amsterdam, 1977.

[25] K. Mahler, .On the fractional parts of the powers of a rational number II", Mathematika 4, 122124, 1957.

[26] G. Marsaglia, Random numbers fall mainly in the planes", Proc. Natl. Acad. Sci. USA 61, 2528, 1968.