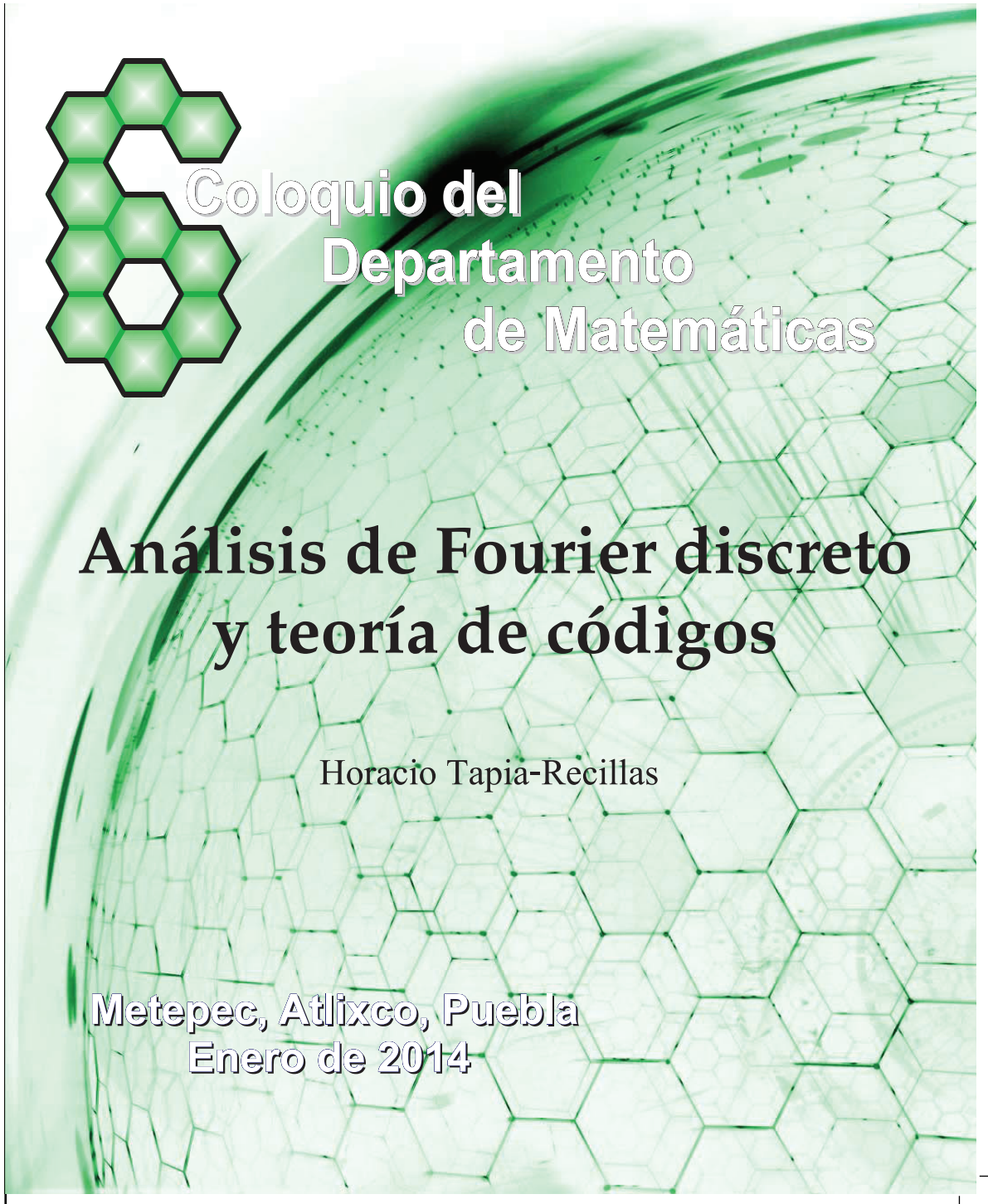
Análisis de Fourier discreto y teoría de códigos

Horacio Tapia-Recillas

Los códigos lineales detectores-correctores de errores, son usados en la transmisión de información digital por cualquier medio de comunicación susceptible de adquirir errores en su transmisión. Son varias las áreas de Matemáticas que ayudan al estudio de esos códigos, como son, entre otras, Álgebra conmutativa, Geometría algebraica, Teoría de números, Combinatoria. Otra área que provee herramientas para el mejor entendimiento de los códigos es el Análisis de Fourier discreto, particularmente sobre grupos abelianos finitos. En este curso se discutirán algunas ideas sobre este tema y se verán algunas aplicaciones a códigos lineales, particularmente en la determinación del polinomio enumerador de pesos del código. Un curso básico de Álgebra lineal es suficiente para seguir este curso.

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
Unidad Iztapalapa



6to Coloquio del Departamento de Matemáticas

Análisis de Fourier Discreto y Teoría de Códigos

Horacio Tapia-Recillas

Comité Organizador

Dr. Joaquín Delgado Fernández
Dr. Mario Pineda Ruelas
Dra. Blanca Rosa Pérez Salvador
Dr. Constancio Hernández García
M. en C. José Luis Cosme
Mat. Daniel Espinoza Pérez

Publicación del Departamento de Matemáticas de la Universidad Autonóma Metropolitana-Iztapalapa con el apoyo de la División de Ciencias Básicas e Ingeniería y Consejo Nacional de Ciencia y Tecnología (CONACYT).

Análisis de Fourier Discreto y Teoría de Códigos

Horacio Tapia-Recillas

Departamento de Matemáticas, UAM-I

Casa abierta al tiempo

Universidad Autónoma Metropolitana

Contenido

Introducción

La *teoría de códigos lineales detectores-correctores de errores* es un área que actualmente tiene una gama de aplicaciones muy extensa ya que la información digital que se transmite por cualquier medio de comunicación, debido a múltiples razones (cambio de voltaje, condiciones atmosfericas, etc.), está sujeta a adquirir errores durante su transmisión. Aplicaciones de esta área estan plasmadas, por ejemplo en comunicación satelital (GPS en particular), viajes espaciales, telefonía, comunicación inalambrica, tomografía médica, transmisión y procesamiento de imagenes digitales, entre otros. Una de las aplicaciones "cotidianas" de los códigos lineales es en los CD's y DVD's. Diversas son las áreas que intervienen en el estudio de códigos, entre las que se cuentan el Álgebra conmutativa, Teoría de números, Geometría algebraica, Combinatoria, etc. Pero no solo está la parte matemática sino que tambien interviene, sobre todo para cuestiones prácticas, la computación para implementar los algoritmos de codificación y decodificación de la información, y en última instancia la Ingeniería.

En las presentes notas se dan algunas ideas de como un concepto muy importante en varias áreas del conocimiento humano, la *Transformada Discreta de Fourier* (TDF), es útil en la teoría de códigos lineales. El estudio y aplicación de la Transformada de Fourier es tan amplio que se han escrito muchos trabajos (libros y artículos) sobre el tema. Sugerimos al lector interesado consultar algunas obras o buscar en internet sobre la aplicación de esta transformada.

Cabe mencionar que estas son notas para uno de los cursos del *Sexto Coloquio del Departamento de Matemáticas* de la Universidad Autónoma Metropolitana-Iztapalapa y que distan mucho de abarcar completamente algunos de los temas aquí mencionados, y sugerimos al lector interesado consultar la literatura especializada ([**4**]). Los errores, esperando no sean demasiados, son responsabilidad del autor.

Capítulo 1

Algo de teoría de grupos abelianos finitos

En esta Sección se recordarán conceptos básicos de Teoría de grupos, particularmente grupos abelianos (conmutativos) finitos.

Un *grupo* es una pareja $(G, \odot)$, donde G es un conjunto no vacio y "$\odot$" es una operación binaria en G,

$$\odot : G \times G \longrightarrow G,\ (g_1, g_2) \longrightarrow g_1 \odot g_2,$$

que satisface las siguientes propiedades:

(1) (asociatividad): $g_3 \odot (g_1 \odot g_2) = ((g_3 \odot g_1) \odot g_2)$ para todo elemento $g_1, g_2, g_3 \in G$.
(2) Hay un elemento $e \in G$ tal que $e \odot g = g \odot e = g$, para toda $g \in G$. Al elemento e se le llama la *identidad* de G y es único.
(3) Para todo $g \in G$ existe $\tilde{g} \in G$ tal que $g \odot \tilde{g} = \tilde{g} \odot g = e$. Al elemento $\tilde{g}$ se le llama el *inverso* de g, y es único.

Si además la operación es conmutativa, es decir, $g_1 \odot g_2 = g_2 \odot g_1$, para todo $g_1, g_2 \in G$, el grupo se dice *abeliano* o *conmutativo.* El grupo se dice finito si su cardinalidad, $|G|$, es finita y se le llama el *orden* del grupo, e infinito en otro caso.

Ejemplos. Hay muchos ejemplos de grupos y a continuación menconaremos algunos de ellos. Se deja al lector comprobar que en efecto son un grupo.

(1) El conjunto $\mathbb{Z}$ de los enteros (racionales) con la operación de suma usual de enteros.
(2) $(\mathbb{Q}, +)$, donde $\mathbb{Q}$ es el conjunto de números racionales y la operación "$+$", suma usual de fracciones.
(3) $(\mathbb{R}, +)$, donde $\mathbb{R}$ son los números reales con la suma usual de números reales.
(4) $(\mathbb{C}, +)$, donde $\mathbb{C}$ son los números complejos con la suma usual de números complejos.
(5) $(\mathbb{Q}^*, *)$, donde $\mathbb{Q}^*$ son los racionales distintos de cero y "$*$" es el producto de racionales.

(6) $(\mathbb{R}^*, *)$, donde $\mathbb{R}^*$ son los números reales distintos de cero y "$*$" es el producto de reales.
(7) $(\mathbb{C}^*, *)$, donde $\mathbb{C}^*$ son los números complejos distintos de cero y "$*$" es el producto de números complejos.
(8) Sea K alguno de los grupos de los ejemplos 1), 2), 3), 4) y sea

$$K[x] = \{f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \ : a_i \in K\}$$

el conjunto de los polinomios con coeficientes en K de cualquier grado $n \geq 0$. Entonces $(K[x], +)$ es un grupo conmutativo con la operación de suma usual de polinomios.
(9) El conjunto S_n de las funciones biyectivas sobre un conjunto de cardinalidad n con la operación de composición de funciones tiene la estructura de un grupo llamado el *grupo simétrico*. Si $n \geq 5$ este grupo no es conmutativo.

Se dice que un grupo $(G, \circ)$ es *cíclico* si existe un elemento $g \in G$ tal que cualquier otro elemento $\tilde{g} \in G$ es de la forma $\tilde{g} = g \circ \cdots \circ g = g^k$ para algún entero k. Al elemento g con esta propiedad se le llama *generador* de G. Si la operación "$\circ$" es aditiva, es decir, se usa "+", la propiedad anterior se escribe como $\tilde{g} = kg = g + \cdots + g$, ($k$-veces).

Observaciones.

(1) En $\mathbb{Z}$ se tiene definida la operación de producto usual de enteros pero no forman grupo con esta opración (¿por qué?).
(2) El grupo $(\mathbb{Z}, +)$ es cíclico.
(3) Los ejemplos 1),...,8) son de grupos infinitos y S_n tiene orden $n!$.

A continuación se dará un ejemplo de un grupo finito construido a partir del grupo (aditivo) de los números enteros $\mathbb{Z}$, nos referimos a los *enteros modulares*. Para este propósito recordemos algunas propiedades de los números enteros.

(1) En $\mathbb{Z}$ se tiene el *algoritmo de la división*: dados los enteros n, m, existen enteros q, r tales que:

$$n = qm + r, \ 0 \leq r \leq m - 1.$$

(2) Se satisface el *algoritmo de Euclídes*.
(3) El *máximo común divisor*, (mcd), d de los enteros n, m es el máximo de los divisores comúnes a n y m. En algunas ocasiones se escribe $d = (n, m)$. El (mcd) de dos enteros se puede obtener aplicando repetidamente el algoritmo de la división. Mas aún, usando relaciones, de "atrás hacia adelante", obtenidas por la aplicación sucesiva del algoritmo de la división, se pueden determinar enteros a y b (no

necesariamente positivos) tales que:

$$d = an + bm,$$

es decir, el (mcd) de dos enteros se puede expresar como combinación lineal de estos enteros (Algoritmo extendido de Euclídes).

(4) Se dice que los enteros m y n son primos relativos si su máximo común divisor es igual a 1, es decir, $(n, m) = 1$. Por consiguiente: $1 = an + bm$ para algunos enteros a y b.

Ahora se definirá una relación de equivalencia en $\mathbb{Z}$. Sea $m > 1$ un entero, y se dirá que $a, b \in \mathbb{Z}$ están relacionados si:

$$a - b = mq,$$

es decir, la diferencia $a - b$ es un múltiplo de m, o equivalentemente, $a = b + mq$.

Ejercicio. Mostrar que esta relación es de equivalencia.

Si a es equivalente a b, en la literatura se acostumbra usar la notación $a \equiv b \ mod \ n$. Los elementos del conjunto que son equivalentes determinan una clase de equivalencia, y la colección de tales clases de equivalencia forman una partición del conjunto. En este ejemplo, si los enteros a y b son equivalentes se acostumbra denotar este hecho como

$$a \equiv b \bmod m,$$

y se dice que *a es congruente con b módulo m*. La clase de equivalencia del entero a es:

$$\overline{a} = \{b \in \mathbb{Z} \ : \ a \equiv b \bmod m\}$$

y se le llama la clase de congruencia de "a módulo m".

Como toda relación de equivalencia en un conjunto induce una partición (en el conjunto), en nuestro caso se tiene la partición del conjunto de los números enteros dada por las clases de congruencia módulo m. A cada elemento de una clase de equivalencia (congruencia) se le llama *representante* de la clase.

A continuación se verá como el algoritmo de la división ayuda a determinar representantes adecuados (naturales) de la clase de congruencia de un entero dado.

Dado el entero m, sea $a \in \mathbb{Z}$ cualquier entero. Usando el algoritmo de la división con los enteros m y a se tiene que

$$a = mq + r, \ 0 \leq r \leq m - 1, \qquad q \in \mathbb{Z}$$

de donde se sigue que $a - r = mq$, y de acuerdo a la definición anterior, $a \equiv r \bmod m$, es decir, a y r son congruentes módulo m y por lo tanto:

- $a \equiv r \bmod m$,
- Tanto a como r son representantes de la misma clase de congruencia, es decir, $\overline{a} = \overline{r}$

Así, dado un entero a, un representante natural de la clase de congruencia $\overline{a}$ de a, es el residuo que se obtiene de dividir al entero a por m, el cual puede tomar algúno de los valores: $\{0, 1, 2, ..., m-1\}$. Por consiguiente hay m clases de congruencia módulo m los cuales son:

$$\overline{0}, \overline{1}, ..., \overline{m-1}.$$

Denotemos por $\mathbb{Z}/m\mathbb{Z}$ al conjunto formado por las clases de congruencia módulo m, es decir,

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}.$$

A este conjunto de las clases de equivalencia módulo m se le llama de *enteros módulo m* o simplemente enteros modulares cuando no hay confusión cual es el módulo. Obsérvese que este conjunto tiene cardinalidad m.

Veamos algunos ejemplos.

(1) $m = 2$. En este caso sólo se tienen dos clases de congruencia ya que si a es cualquier entero, entonces: $a = 2q + r$ con $r = 0, 1$. Por lo tanto

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}\},$$

es decir, cualquier entero es un número par o impar.

(2) $m = 3$. En este caso, si a es cualquier entero, $a \equiv r \bmod 3$, donde $r = 0, 1, 2$. Por consiguiente:

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}.$$

(3) $m = 10$. Si $a \in \mathbb{Z}$ entonces $a \equiv r \bmod 10$ donde $r = 0, 1, 2, ..., 9$. Por lo tanto

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{9}\}.$$

En líneas anteriores se comentó que a partir del grupo (aditivo) de los número enteros el cual no es finito, se construiría un grupo finito (abeliano), y se deja como ejercicio al lector dar una demostración de la siguiente

PROPOSICIÓN 1.0.1. *El conjunto*

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{m-1}\}.$$

es un grupo (aditivo) conmutativo de orden m. A este grupo se le llama de enteros módulo m.

Ejercicio. Dar la tabla de la suma de enteros módulo $m = 2, 3, 4, 5, 6$.

Dado que en los números enteros $\mathbb{Z}$ se tienen dos operaciones, la *suma* y el *producto,* es de esperarse que en los enteros modulares también se puedan definir dos operaciones, que también se les llama *suma* y *producto*. En la demostración de la Proposición anterior se define la operación suma. De forma similar se puede definir el producto "$*$" de enteros modulares, es decir, de clases modulares. También se deja como ejercicio al lector la siguiente

PROPOSICIÓN 1.0.2. *Mostrar que la pareja*

$$((\mathbb{Z}/m\mathbb{Z})^*, *)$$

satisfacen todas excepto una de las propiedades para que se grupo con esa operación.

Recordemos que un grupo $(G, \circ)$ es *cíclico* si existe (al menos) un elemento $g \in G$ tal que cualquier otro element $\tilde{g}$ se puede expresar como $\tilde{g} = g^r$ para algún entero $r \geq 0$.

Ejemplos de grupos cíclicos incluyen: $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $(\mu_4 = \{1, i, -1, -i\}, *)$ donde $*$ es el producto de los números complejos (raices complejas cuartas de la unidad). De manera similar las raices complejas n-ésimas de la unidad, μ_n, son un grupo conmutativo finito y cíclico.

Ejercicios.

(1) Dar otros ejemplos de grupos cíclicos.
(2) Mostrar que el conjunto $(\mathbb{Z}/m\mathbb{Z})^*$ de todos los elementos de $(\mathbb{Z}/m\mathbb{Z})$ que tienen inverso bajo la operación "$*$" es un grupo, llamado el grupo de las *unidades* de $(\mathbb{Z}/m\mathbb{Z})$. ¿cual es su orden? ¿cuando es cíclico? Dar algunos ejemplos.

Ahora tenemos el siguiente resultado:

PROPOSICIÓN 1.0.3. *Con la notación anterior:*

(1) *La terna* $(\mathbb{Z}/m\mathbb{Z}, +, *)$ *es un anillo conmutativo finito con 1.*
(2) *El anillo* $(\mathbb{Z}/m\mathbb{Z}, +, *)$ *es un campo finito con* m *elementos si y sólo si* m *es primo.*

Si el módulo es un número primo p al campo $\mathbb{Z}/p\mathbb{Z}$ se acostumbra denotarlo por $\mathbb{F}_p$.

Veamos algunas de las propiedades de los campos $\mathbb{F}_p$ con diversos ejemplos. Por simplicidad, a la clase de congruencia $\overline{a}$ del entero a simplemente se denotará por a, pero sin olvidar que esta representa una clase de equivalencia.

(1) Consideremos $\mathbb{F}_3 = \{0, 1, 2\}$. Es fácil ver que bajo el producto, el inverso del 1 es el mismo y el inverso del 2 también es él mismo. Observemos que $\langle 2 \rangle = \{2^n \ : \ n \geq 0\} = \{1, 2\}$, es decir, $\mathbb{F}_3^* = \{1, 2\}$ es un grupo cíclico de orden 2 generado por el elemento 2.
(2) Sea $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. Obsérvese que en este caso tambien se tiene que $\mathbb{F}_5^* = \{1, 2, 3, 4\}$ es un grupo cíclico de orden 4 siendo 2 un generador, y es fácil ver que 3 es otro generador.
(3) En el caso de $\mathbb{F}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, 2 no es un generador del grupo cíclico $\mathbb{F}_7^*$, pues su orden es 3. Sin embargo 3 si es un generador ya que tiene orden 6. ¿hay mas generadores de este grupo cíclico?
(4) En el caso de $\mathbb{F}_{31}^*$, el elemento $\omega = 2$ tiene orden 5 por lo tanto no es un generador de este grupo, pero el elemento $\alpha = 3$ tiene orden 30 por lo cual es un generador de este grupo.

Ejercicio* Si p es un primo probar que $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ es un grupo cíclico.

Sea $\mathbb{F}_p$ un campo finito. Entonces la terna $(\mathbb{F}_p[x], +, *)$ es un anillo conmutativo el cual tiene varias de las propiedades que el anillo de los enteros (racionales) $(\mathbb{Z}, +, *)$, es decir, se satisface el algoritmo de la división, el algoritmo de Euclides, es de ideales principales, entre otras.

1.1. Conceptos básicos de campos finitos

En esta sección se recordará la construcción de campos finitos como extensiones algebraicas del campo base $\mathbb{F}_p$, donde p es un número primo, y se darán algunas de sus propiedades. Estos campos son muy usados en varias áreas de la Matemática, entre las que se cuentan la teoría de códigos detectores-correctores de errores usados en la transmisión de información por cualquier canal de comunicación; la criptografía también llamada cifrados de datos; computación, combinatoria, entre otras ([**6**]). Estos campos son también llamados de Galois ya que fue uno de los primeros matemáticos que introdujo este concepto.

La introducción de algunos conceptos sobre campos finitos se hará por medio de ejemplos, en este caso el campo finito con $2^3 = 8$ elementos.

Sea $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Es fácil ver que este polinomio es irreducible. Sea $\langle f(x) \rangle$ el ideal del anillo $\mathbb{F}_2[x]$ generado por $f(x)$ y consideremos el conjunto:

$$T = \mathbb{F}_2[x]/\langle f(x) \rangle = \{\overline{g(x)} = g(x) + \langle f(x) \rangle \ : \ g(x) \in \mathbb{F}_2[x]\}.$$

Es fácil ver que este conjunto tiene la estructura de anillo donde la suma se hereda de la suma la usual de polinomios. El producto se

realiza con representantes y se reduce módulo $f(x)$. Este anillo tiene varias de las propiedades que tiene el anillo de los enteros modulares.

Si $g(x) \in \mathbb{F}_2[x]$ es cualquier polinomio, por medio del algoritmo de la división se tiene que

$$g(x) = q(x)f(x) + r(x),\ q(x), r(x) \in \mathbb{F}_2[x]$$

donde $r(x)$, el residuo, es tal que $0 \leq gr(r) < 2$ y $g(x) - r(x) = q(x)f(x)$, es decir, $g(x) \equiv r(x) \ mod\ f(x)$. En otras palabras, la clase de $g(x)$ y $r(x)$ es la misma: $\overline{g(x)} = \overline{r(x)}$.

La condición sobre el grado de $r(x)$ implica que $r(x) = a_0 + a_1x + a_2x^2$ con $a_0, a_1, a_2 \in \mathbb{F}_2$. Por lo tanto, T consiste de las clases residuales de los siguientes polinomios,

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

Ejercicio. Dar las tablas de la suma y producto de T.

De estas tablas se puede ver que en efecto, T es un campo, en particular todo elemento distinto de cero tiene un inverso. A este campo se le donota por $\mathbb{F}_{2^3}$ o bien por $GF(2^3)$ y se le llama el campo finito o de Galois con 8 elementos.

Si α denota a la clase de x módulo $f(x)$, es decir, $\alpha = \overline{x} = x + \langle f(x) \rangle$, se pueden ver fácilmente que:

(1) El conjunto $\mathbb{F}_8^*$, de los elementos distintos de cero de $\mathbb{F}_8$, es un grupo *cíclico* de orden $2^3 - 1 = 7$ generado por α:

$$\mathbb{F}_8^* = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}.$$

A todo elemento del campo con esta propiedad se le llama *primitivo*.

(2) El campo $\mathbb{F}_8$ es un espacio vectorial sobre $\mathbb{F}_2$ de dimensión 3, siendo $\{1, \alpha, \alpha^2\}$ una base natural. Por lo tanto $\mathbb{F}_8$ es una extensión (algebraica) de $\mathbb{F}_2$.

(3) Como $\mathbb{F}_2$-espacio vectorial, $\mathbb{F}_8$ es isomorfo a $\mathbb{F}_2^3$. El isomorfismo esta dado por $\phi(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2)$. Cabe mencionar que este tipo de isomorfismo es usado en otras áreas como es la criptgrafía, donde por ejemplo, en el sistema de cifrado de llave privada AES (Advanced Encryption Standard), los ‘‘bytes", es decir los elementos del espacio vectorial $\mathbb{F}_2^8$, se identifican con los elementos del espacio vectorial del campo finito $\mathbb{F}_{2^8}$.

(4) El elemento α es una raíz del polinomio $f(x) = x^3 + x + 1$. Mas aún, las raices de $f(x)$ son $\alpha, \alpha^2, \alpha^4$ y por lo tanto $f(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)$. Como estos elementos están en $\mathbb{F}_8$, este campo es el *campo de descomposición* de $f(x)$. Dado

que este polinomio tiene como raíz un elemento primitivo, también se dice que el polinomio es *primitivo.*

(5) Sea $\tau : \mathbb{F}_8 \longrightarrow \mathbb{F}_8$ la función definida como $\tau(y) = y^2$. Es fácil ver que τ es un automorfismo (de campos) el cual es llamado de *Frobenius.* Obsérvese que las raices de $f(x)$ se pueden dar en términos de este automorfismo: $\tau^0(\alpha)$, $\tau(\alpha)$, $\tau^2(\alpha)$. Además $\tau^3 = Id$.

(6) El grupo de Galois de $\mathbb{F}_8$ sobre $\mathbb{F}_2$ es de grado 3 (el grado de la extensión) y por lo tanto cíclico. Como el automorfismo de Frobenius es un elemento de este grupo y tiene orden 3, este grupo esta generado por τ y sus elementos son Id, τ, τ^2.

(7) Si ahora se toma el polinomio $h(x) = x^3 + x^2 + 1$ el cual también es irreducible sobre $\mathbb{F}_2$, (ejercicio), de la misma manera como se procedió antes, se construye un campo R con 8 elementos. Obviamente la aritmética es distinta, sin embargo hay una relación entre estos dos campos: son isomorfos (ejercicio). Por consiguiente se dice que, módulo isomorfismo, el campo con 8 elementos es único.

Ejercicio. Construir un campo con $16, 32, 9, 25$ elementos. Determinar las propiedades equivalentes al caso del campo con 8 elementos.

Con las mismas ideas usadas para el caso anterior, se construyen campos finitos con $q = p^n$ elementos y varias de sus propiedades son básicamente las mismas que las mencionadas para el caso de $\mathbb{F}_8$ asi como los mencionados en los del ejercicio. Mayores detalles se pueden consultar en [**3**].

Capítulo 2

La Transformada Discreta de Fourier clásica (TDFc)

En este Capítulo se introducirá una de las transformaciones que ha tenido y sigue teniendo un gran impacto en diversas áreas que incluyen robótica, óptica, comunicaciones, etc. Nos referimos a la Transformada Discreta de Fourier (TDF), una derivación de la Transformada Clásica de Fourier. Existe una vasta literatura donde se puede consultar la definición, propiedades y aplicaciones de esta transformada, en estas notas se seguirán las referencias [**1**] y [**7**]. Actualmente hay varios tipos de ‘‘software" con los cuales se puede calcular esta transformada, sin embargo es importante que se tenga conocimiento de sus fundamentos matemáticos.

En un gran número de situaciones, por ejemplo, cuando se lleva a cabo un experimento o alguna observación, la información que se obtiene es un conjunto finito de datos (discretos) y en general no es fácil obtener una función que describa ese experimento a partir de esos datos. La idea es entonces, obtener mayor información sobre el problema a partir de esos datos. La (TDF) es de gran ayuda en esos casos.

Antes de dar la definición general de la (TDF) consideremos los siguientes ejemplos:

1. El elemento $\alpha = 2 \in \mathbb{F}_5$ es de orden 4, así se define la (TDF) de longitud 4 basada en α:

$$\mathcal{F}_\alpha \colon \mathbb{F}_5^4 \longrightarrow \mathbb{F}_5^4, \quad \mathcal{F}(v_0, v_1, v_2, v_3) = (V_0, V_1, V_2, V_3),$$

donde

$$V_j = \sum_{i=0}^{3} \alpha^{ij} v_i = \sum_{i=0}^{3} 2^{ij} v_i, \quad j = 0, 1, 2, 3.$$

2. El elemento $\alpha = 3 \in \mathbb{F}_7$ es de orden 3, así se define la (TDF) de longitud 3 basada en α:

$$\mathcal{F}_3 : \mathbb{F}_7^3 \longrightarrow \mathbb{F}_7^3, \quad \mathcal{F}(v_0, v_1, v_2) = (V_0, V_1, V_2),$$

donde

$$V_j = \sum_{i=0}^{2} \alpha^{ij} v_i, \quad j = 0, 1, 2.$$

3. El elemento $\beta = 3 \in \mathbb{F}_{31}$ es de orden 30, (un elemento primitivo de $\mathbb{F}_{31}$), así se define la (TDF) de longitud 30 basada en β:

$$\mathcal{F}_\beta : \mathbb{F}_{31}^{30} \longrightarrow \mathbb{F}_{31}^{30}, \quad \mathcal{F}_\beta(v_0, v_1, ..., v_{29}) = (V_0, V_1, \ldots, V_{29}),$$

donde

$$V_j = \sum_{i=0}^{29} \beta^{ij} v_i, \quad j = 0, 1, \ldots, 29.$$

Considerando estos ejemplos como antecedentes, ahora es mas natural definir la (TDF) en general sobre un campo finito $\mathbb{F}_q$. Para tal motivo sea $\alpha \in \mathbb{F}_q^*$ un elemento de orden n, $1 \leq n \leq n-1$.

La (TDF) de longitud n sobre el campo $\mathbb{F}_q$ determinada por α es la función

$$\mathcal{F}_\alpha : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n, \quad \mathcal{F}_\alpha(v_0, v_1, ..., v_{n-1}) = (V_0, V_1, \ldots, V_{n-1}),$$

donde

$$V_j = \sum_{i=0}^{n} \alpha^{ij} v_i, \quad j = 0, 1, \ldots, n-1.$$

En particular, si α es un elemento primitivo de $\mathbb{F}_q$, es decir, un generador del grupo (multiplicativo) $\mathbb{F}_q^*$, la (TDF) es de longitud $n = q - 1$.

2.1. Representación polinomial

Sea $\mathbb{F}_q$ un campo finito y $\mathbb{F}_q[x]$ el anillo de polinomios en la indeterminada x con coeficientes en $\mathbb{F}_q$. Sea $n > 1$ un entero, $\langle x^n - 1 \rangle$ el ideal de $\mathbb{F}_q[x]$ generado por $x^n - 1$ y sea

$$R_n = \mathbb{F}_q[x] / \langle x^n - 1 \rangle = \{ f(x) + \langle x^n - 1 \rangle : f(x) \in \mathbb{F}_q[x] \}.$$

Usando el algoritmo de la división, los elementos de R_n se pueden identificar con polinomios de grado a los mas $n-1$, con coeficientes en $\mathbb{F}_q$:

$$R_n = \{ a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \ : \ a_i \in \mathbb{F}_q \}.$$

La suma de elementos es la usual de polinomios y la multiplicación esta regída por la relación $x^n = 1$.

La siguiente observación será de utilidad mas adelante. Para ilustrar la idea, consideremos el caso $n = 3$:

$$R_3 = \{ a(x) = a_0 + a_1 x + a_2 x^2, \ a_i \in \mathbb{F}_q \}$$

Si $a(x) = a_0 + a_1x + a_2x^2$ y $b(x) = b_0 + b_1x + b_2x^2$ son dos elementos de R_3, tomando su producto como polinomios en $\mathbb{F}_q[x]$ se tiene:

$$a(x)b(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + (a_1b_2 + a_2b_1)x^3 + a_2b_2x^4.$$

Recordando que se esta trabajando en el anillo R_3 donde $x^3 = 1$, el producto de estos elementos se reduce a:

$$a(x)b(x) = (a_0b_0 + a_1b_2 + a_2b_1) + (a_0b_1 + a_1b_0 + a_2b_2)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2$$

Además de tener la estructura de anillo (conmutativo), R_n es un espacio vectorial sobre el campo $\mathbb{F}_q$ de dimensión n, teniendo como base (natural) $\{1, x, ..., x^{n-1}\}$. Mas aún, $\mathbb{F}_q^n$ y R_n son isomorfos como $\mathbb{F}_q$-espacios vectoriales como se puede ver por medio de la función:

$$\mathcal{P} : \mathbb{F}_q \to R_n, \quad \mathcal{P}(a_0, a_1, \ldots, a_{n-1}) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}.$$

Ejercicios

(1) Mostrar que R_n es un anillo conmutativo y determinar su cardinalidad.
(2) Mostrar que los elementos $\{1, x, ..., x^{n-1}\}$ son una base de R_n.
(3) Mostrar que $\mathcal{P}$ es un isomorfismo de $\mathbb{F}_q$-espacios vectoriales.

Al isomorfismo $\mathcal{P}$ se le llama la *representación polinomial* de $\mathbb{F}_q^n$.

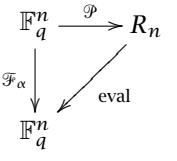
Cabe mencionar que este isomorfismo y el anillo R_n son muy usados en el estudio de códigos lineales cíclicos de longitud n que tienen como alfabeto al campo $\mathbb{F}_q$, ya que el isomorfismo $\mathcal{P}$ determina una correspondencia biyectiva entre los códigos lineales cíclicos y los ideales del anillo R_n. El anillo R_n es tambien isomorfo al anillo de matrices circulantes y al álgebra de grupo $\mathbb{C}[\mathbb{Z}_n]$, como se verá mas adelante.

Usando la representación polinomial de $\mathbb{F}_q^n$ se tiene el siguiente

TEOREMA 2.1.1. *Con la notación anterior, si* $\overline{a} = (a_0, a_1, ..., a_{n-1}) \in \mathbb{F}_q^n$ *y* $\mathcal{F}_\alpha(\overline{a}) = (A_0, A_1, \ldots, A_{n-1})$ *entonces*

$$A_j = f(\alpha^j), j = 1, 2, \ldots, n,$$

donde $\mathcal{P}(\overline{a}) = f(x)$ *es la representación polinomial del elemento* $\overline{a} \in \mathbb{F}_q^n$. *Es decir, el siguiente diagrama es conmutativo:*



donde $eval(f) = (f(1), f(\alpha), ..., f(\alpha^{n-1}))$.

Por consiguiente, determinar la (TDF) de una sucesión basta evaluar el polinomio asociado a esta sucesión.

2.2. El álgebra de grupo

A continuación se introdcirá otra estructura algebraica que permitirá ver a la (TDF) desde otro punto de vista.

Sea $\mathbb{K}$ un campo, $n > 1$ un entero y $C = \langle g \rangle$ un grupo cíclico de orden n (considerando la operación en forma multiplicativa), aunque se puede tomar a C como $\mathbb{Z}/n\mathbb{Z}$ con la operación aditiva. Sea

$$\mathbb{K}[C] = \{f : C \to \mathbb{K}, \text{ funcion}\},$$

es decir, $\mathbb{K}[C]$ es el conjunto de funciones de C en $\mathbb{K}$.

Es fácil ver que con la suma puntual de funciones, $\mathbb{K}[C]$ es un grupo conmutativo finito. Si $a \in \mathbb{K}$ y $f \in \mathbb{K}[C]$, (af) es la función definida como $(af)(h) = a(f(h))$. Con esta operación $\mathbb{K}[C]$ tiene la estructura de $\mathbb{K}$-espacio vectorial de dimensión n donde una base (natural) esta dada por las funciones

$$\delta_{g^k}(h) = 1 \text{ si } h = g^k \text{ y } \delta_{g^k}(h) = 0 \text{ si } h \neq g^k, \text{ para } k = 0, 1, ..., n-1,$$

es decir, δ_{g^k} es la función característica de g^k.

Ejercicio.

(1) Probar que el conjunto de funciones $\{\delta_{g^k},\ k = 0, 1, ..., n-1\}$ es una $\mathbb{K}$-base de $\mathbb{K}[C]$.

(2) Probar que la función

$$\phi : R_n \longrightarrow \mathbb{K}[C], \phi(x^k) = \delta_{g^k}, \phi(1) = Id,$$

es un isomorfismo de $\mathbb{K}$-espacios vectoriales.

Dado que R_n tiene estructura de anillo, es decir, se pueden multiplicar sus elementos y que es isomorfo a $\mathbb{K}[C]$ como espacios vectoriales ($\mathbb{K} = \mathbb{F}_q$), es de esperarse que también se puedan "multiplicar" los elementos de $\mathbb{K}[C]$. A continuación se definirá una operación, llamada *convolución*, denotada por "$*$", con la cual $\mathbb{K}[C]$ tiene estructura de anillo. A una estructura algebraica la cual es un grupo (finito), anillo, y espacio vectorial, se de llama un *álgebra.* Es por esta razón que a $\mathbb{K}[C]$ se le llama el *álgebra de grupo* de C sobre $\mathbb{K}$.

Como $\mathbb{K}[C]$ es un espacio vectorial, basta definir la convolución en la base $\{\delta_{g^k},\ k = 0, 1, ..., n-1\}$. Sean entonces δ_{g^j} y δ_{g^k} dos elementos de esta base, y defínase

$$\delta_{g^j} * \delta_{g^k} = \delta_{g^j g^k} = \delta_{g^{j+k}}$$

donde el exponente $j+k$ se reduce módulo n.

Si ahora $f = f_0\delta_e + f_1\delta_g + \cdots + f_{n-1}\delta_{g^{n-1}}$ y $g = g_0\delta_e + g_1\delta_g + \cdots + g_{n-1}\delta_{g^{n-1}}$, con $f_i, g_i \in \mathbb{K}$ son dos elementos de $\mathbb{K}[C]$, la convolución de estas funciones, $f * g$, se obtiene multiplicando los correspondiente elementos de la base y reduciendo los productos de acuerdo a la regla anterior.

Otra forma de definir la convolución de las funciones f y g, con notación multiplicativa del grupo, es la siguiente:

$$(f * g)(h) = \sum_{i=0}^{n-1} f(h)g(hg^{-i}),\ \forall\ h \in C.$$

En particular,

$$(\delta_{g^j} * \delta_{g^k})(h) = \sum_{i=0}^{n-1} \delta_{g^j}(h)\delta_{g^k}(hg^{-i})$$

Si el grupo tiene notación aditiva, la relación anterior queda expresada como

$$(f * g)(h) = \sum_{k=0}^{n-1} f(h)g(h-kg),\ \forall\ h \in C.$$

Ilustremos esta operación con el siguiente ejemplo. Sea $n = 3$, $C = \langle g\rangle = \{e, g, g^2\}$. Entonces,

$$\mathbb{K}[C] = \{f_0\delta_e + f_1\delta_g + f_2\delta_{g^2},\ f_i \in \mathbb{K}\}.$$

Si $f = f_0\delta_e + f_1\delta_g + f_2\delta_{g^2}$ y $h = h_0\delta_e + h_1\delta_g + h_2\delta_{g^2}$ son dos elementos de $\mathbb{K}[C]$, entonces

$$\begin{aligned} f * h = {} & f_0h_0(\delta_e * \delta_e) + (f_0h_1 + f_1h_0)(\delta_e * \delta_g) \\ & + (f_0h_2 + f_1h_1 + f_2h_0)(\delta_e * \delta_{g^2}) + (f_1h_1)(\delta_g * \delta_g) \\ & + (f_1h_2 + f_2h_1)(\delta_g * \delta_{g^2}) + (f_2h_2)(\delta_{g^2} * \delta_{g^2}). \end{aligned}$$

Tomando en cuenta la operación en el grupo C, en particular, $g^3 = e$, la relación anterior se reduce a:

$$f*h = (f_0h_0+f_1h_2+f_2h_1)\delta_e+(f_0h_1+f_1h_0+f_2h_2)\delta_g+(f_0h_2+f_1h_1+f_2h_0)\delta_{g^2}.$$

Observemos que esta operación es exactamente la misma que se describió en el caso del anillo R_3, y este hecho se cumple en el anillo R_n. Así, el producto en R_n es lo mismo que la convolución.

Esta operación de convolución tiene muchas y variadas aplicaciones, una de estas se encuentra en los llamados *códigos de convolución,* componente importante en los *turbo códigos* ampliamente usados en la detección y corrección de errores en la transmisión

de grandes cantidades de información como es el audio y video, y tratamiento de imágenes digitales, entre otros.

Volvamos con la (TDF). Con el isomorfismo ϕ mencionado entre R_n y $\mathbb{K}[C]$, veamos como se representa la (TDF) en el álgebra de grupo $\mathbb{K}[C]$. El siguiente diagrama ilustra esta situación:

$$\begin{array}{ccccc} \underline{a} & \xrightarrow{\mathcal{P}} & a(x) & \longrightarrow & f_a \\ \downarrow{\scriptstyle \mathcal{F}_\alpha} & & \downarrow{\scriptstyle \text{eval}} & & \downarrow \\ \underline{A} & \xrightarrow{\mathcal{P}} & A(x) & \longrightarrow & f_A \end{array}$$

donde $\underline{a} = (a_0, a_1, \ldots, a_{n-1})$, $\underline{A} = (A_0, A_1, \ldots, A_{n-1})$, $a(x) = a_0 + a_1 x + \cdots + a_{n-1x^{n-1}}$, $A(x) = A_0 + A_1 x + \cdots + A_{n-1}x^{n-1}$ con $A_i = \mathcal{F}_\alpha(\underline{a}) = a(\alpha^i)$, y $f_a = a_0\delta_e + a_1\delta_g + \cdots + a_{n-1\delta_{g^{n-1}}}$, $f_A = A_0\delta_e + A_1\delta_g + \cdots + A_{n-1\delta_{g^{n-1}}}$.

2.3. Ejemplos de la TDFc

Las siguientes, además de los ya mencionados al inicio del presente capítulo son ejemplos de la (TDFc).

(1) Si $\mathbb{K} = \mathbb{C}$, los números complejos y $\alpha = e^{2\pi i/n}$ es una raíz n-ésima de la unidad, se puede definir una (TDFc) de longitud n
(2) El polinomio $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$ es irreducible sobre $\mathbb{F}_2$ y se puede usar para construir el campo $\mathbb{F}_{16}$, con 16 elementos. El elemento $\alpha \in \mathbb{F}_{16}$ tal que $f(\alpha) = 0$ tiene orden 15 por lo tanto se puede definir la TDFc de longitud 15:

$$A_j = \sum_{i=0}^{14} \alpha^{ij} a_j.$$

Ejercicio. Dar otros ejemplos de la TDFc.

2.4. Propiedades de la TDFc

Las siguientes son algunas de las propiedades que poseé la (TDFc), haciendo de eśta una de las herramientas mas útiles en varias áreas del conocimiento humano.

(1) La (TDFc) es $\mathbb{K}$-lineal, es decir,

$$\mathcal{F}_\alpha(\lambda\underline{a} + \mu\underline{b}) = \lambda\mathcal{F}_\alpha(\underline{a}) + \mu\mathcal{F}_\alpha(\underline{b})$$

donde $\lambda, \mu \in \mathbb{K}$.
(2) La (TDFc) es invertible, en particular es un isomorfismo. Si $\mathbb{K}$ es un campo finito y la longitud n es primo relativo con la característica de $\mathbb{K}$. La inversa de $\mathcal{F}_\alpha$ esta dada de la siguiente manera: dado

$\underline{A} = (A_0, A_1, \ldots, A_{n-1})$, entonces, $\mathcal{F}_\alpha^{-1}(\underline{A}) = \underline{a} = (a_0, a_1, \ldots, a_{n-1})$ donde

$$a_j = \frac{1}{n} \sum_{j=0}^{n-1} \alpha^{-ij} A_j, \ i = 0, 1, ..., n-1.$$

(3) Si $0 \leq t \leq n-1$, $\underline{c} = (a_0, a_1\alpha^t, \ldots, a_r\alpha^{rt}, \ldots, a_{n-1}\alpha^{(n-1)t})$ entonces $\mathcal{F}_\alpha(\underline{c}) = (C_0, C_1, \ldots, C_{n-1})$ con:

$$C_j = C_{j+t}$$

donde el subíndice $j+t$ se reduce módulo n. A esta propiedad de la (TDFc) se le conoce como *modulación*.

(4) *Translación.*

$$\mathcal{F}_\alpha(a_{j-l}) = \alpha^{lj} A_j.$$

(5) La (TDFc) preserva la estructura de anillo de R_n, es decir

$$\mathcal{F}_\alpha(f * g) = \mathcal{F}_\alpha(f) \cdot \mathcal{F}_\alpha(g).$$

donde "$*$" es la operación de *convolución* y "$\cdot$" es el producto de funciones.

(6) *Ceros de polinomios.*
El polinomio $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ tiene un cero en α^j sí y sólo si $A_j = 0$. El polinomio $A(x) = A_0 + A_1 x + \cdots + a_{n-1}x^{n-1}$ tiene un cero en α^{-i} sí y sólo si $a_i = 0$.

(7) *Vectores recíprocos.*
El recíproco del vector $\underline{a} = (a_i)$ es el vector (a_{n-i}). La (TDFc) del recíptoco del vector $\underline{a}$ es el recíproco de su (TDFc), i.e., la "transformada del recíproco es el recíproco de la transformada".

(8) *Decimación cíclica.* Si $n = n'n''$, entonces la (TDFc) del vector $(a_{n''i'})_{i'=0,1,\ldots,n'-1}$ es el vector

$$\left(\frac{1}{n''} \sum_{j''=0}^{n''-1} A_{j'+n'j''}, \ j' = 0, 1, ..., n'-1 \right)$$

(9) *Fórmula de Poisson* Si $n = n'n''$, entonces,

$$\sum_{i'=0}^{n''-1} a_{n''i'} = \frac{1}{n''} \sum_{j''=0}^{n''-1} A_{n'j''}.$$

(10) *Permutación cíclica* Si b y n son enteros primos relativos, entonces

$$\mathcal{F}_\alpha(a_{bi}) = A_{Bj}, \text{ donde } Bb = 1 \bmod n.$$

Ejercicio. Dado que la (TDFc) es lineal, determinar la matriz correspondiente con respecto a la base natural. Determinar la matriz de la inversa de la (TDFc).

Capítulo 3

TDF sobre grupos abelianos finitos

En esta sección, despues de haber mencionado la TDF sobre espacios vectoriales (los cuales son grupos abelianos aditivos), se introducirá la Transformada Discreta de Fourier sobre grupos finitos conmutativos, así como algunas de sus propiedades. Una de las propiedades de la TDF sobre grupos es la Fórmula de Suma de Poisson, la cual se usará para dar una demostración de las relaciones de MacWilliams sobre el polinomio enumerador de pesos de un código lineal (binario) y el correspondiente del código dual.

3.1. El grupo de caractéres

Sea $(G,+)$ un grupo finito (abeliano) y sea $\mathbb{F}$ un campo (el cual puede ser finito, pero para varias situaciones se consideran el campo de los números complejos $\mathbb{C}$).

Sea

$$L^2(G) = \mathbb{F}[G] = \{f : G \longrightarrow \mathbb{F},\ \text{funcion}\},$$

el álgebra de grupo introducido anteriormente. Si $\mathbb{F} = \mathbb{C}$, se define un producto interno en $L^2(G)$: si $f, g \in \mathbb{F}[G]$,

$$\langle f, g\rangle = \sum_{x\in G} f(x)\overline{g(x)},$$

donde la barra indica conjugación compleja.

Sea S^1 el conjunto de los números complejos de magnitud igual a 1, es decir, el círculo de radio 1, y sea

$$\hat{G} = \{\chi : G \longrightarrow S^1,\ \text{homomorfismo}:\ \chi(x+y) = \chi(x)\chi(y)\}.$$

A los elementos de este conjunto se les llama *caractéres* de G y es fácil ver que es un grupo (conmutativo) bajo el producto de funciones, llamado el *grupo dual* de G.

Para ilustrar este concepto consideremos el siguiente ejemplo: sea $G = \mathbb{Z}/n\mathbb{Z}$ el grupo de enteros módulo n y $\xi = e^{2\pi i/n}$ una raíz primitiva n-ésima de la unidad, entonces:

$$\tilde{G} = \{\lambda : \mathbb{Z}/n\mathbb{Z} \longrightarrow S^1, \lambda(k) = \xi^k\}.$$

Ejercicio. Mostrar que $\hat{G} = \langle \lambda_0 \rangle$ donde $\lambda_0(1) = \xi$ y que G es isomorfo a $\hat{G}$.

Obsérvese que en el ejemplo anterior el grupo $\mathbb{Z}/n\mathbb{Z}$ es cíclico. En general se puede ver que si G es un grupo cíclico (finito) entonces G es isomorfo a su dual $\hat{G}$. Si el grupo G no es cíclico tambien es isomorfo a su dual pero la demostración no es tan natural como en el caso cíclico, de todas maneras el lector puede intentar dar una demostración.

Una propiedad interesante de los caractéres de un grupo finito (abeliano) es la siguiente:

LEMA 3.1.1. *(Ortogonalidad de caractéres) Si $\chi, \psi \in \hat{G}$, entonces*

$$\langle \chi, \psi \rangle = |G|, \ \textit{si } \chi = \psi; \ \langle \chi, \psi \rangle = 0, \ \textit{en otro caso}.$$

3.2. La TDF

Con los conceptos introducidos anteriormente, se da la definición de la Transformada Discreta de Fourier (TDF) sobre grupos abelianos finitos.

Sea G un grupo abeliano finito y $\hat{G}$ su grupo dual. La Transformada Discreta de Fourier (TDF) es:

$$\mathcal{F} : \mathbb{C}[G] \longrightarrow \mathbb{C}[\hat{G}], \quad \mathcal{F}_f(\chi) = \hat{f}(\chi) = \sum_{g \in G} f(g)\overline{\chi(g)}, \ f \in \mathbb{C}[G], \chi \in \hat{G}.$$

Veamos un ejemplo.

Sea $G = \mathbb{Z}/n\mathbb{Z}$ el grupo (cíclico aditivo) de enteros módulo n. Como se mencionó anteriormente, $\hat{G} = \{\chi : G \longrightarrow S^1, \ \chi(k) = \xi^k\}$ donde $\xi = e^{2\pi i/n}$ es una raíz (primitiva) n-ésima de la unidad. Sea $f \in \mathbb{C}[G]$, entonces,

$$\mathcal{F}_f(\chi) = \hat{f}(\chi) = \sum_{j=0}^{n-1} f(j)\overline{\chi(j)} = \sum_{j=0}^{n-1} f(j)\overline{\xi^j} = \sum_{j=0}^{n-1} e^{-2\pi i j/n} f(j).$$

3.3. Aplicaciones de la TDF

Las aplicaciones de la TDF cubren una amplia gama en diversos campos del conocimiento. A continuación mencionaremos algunas de ellas.

Ejemplo 1. Recordemos que una sucesión de longitud m se puede identificar como una función sobre el grupo de enteros módulo m. Sea $x_n, \ n = 0, 1, ..., m-1$ una sucesión (finita) de números reales o complejos (por ejemplo una muestra de observaciones de

un experimento). La TDF de esta sucesión es otra sucesión $\{y_k\}$ (de la misma longitud) donde:

$$y_k = \sum_{j=0}^{m-1} x_j e^{-2\pi i k j/m}, k = 0, 1, ..., m-1.$$

Ejemplo 2. La TDF tiene varias generalizaciones de las cuales una de ellas es muy útil en la teoría de códigos y criptogrfía, y que ahora recordamos su definición.

Sea $\mathbb{F}_2 = \{0, 1\}$ el campo (finito) de los números binarios. Así como en el caso (clásico) de $\mathbb{C}$ donde se consideró una raíz n-ésima de la unidad (caractéres de $\mathbb{Z}/n\mathbb{Z}$), en este caso se considera la raíz cuadrada de la unidad $\xi = -1$.

Sea $\mathbb{F}_2^n$ el espacio euclideano de dimensión n sobre $\mathbb{F}_2$, $\mathbb{F}_2[\mathbb{F}_2^n] = \{f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2,\ f \text{ funcion}\}$, el álgebra de grupo de $\mathbb{F}_2^n$ sobre $\mathbb{F}_2$. Sea $f \in \mathbb{F}_2[\mathbb{F}_2^n]$ y considerese la función $\zeta_f = (-1)^f$, es decir, $\zeta_f(\underline{x}) = (-1)^{f(\underline{x})}$, $\underline{x} \in \mathbb{F}_2^n$. La TDF de f, tambien llamada de Hadamard, es la función:

$$\hat{\zeta_f}(\underline{a}) = \sum_{\underline{x} \in \mathbb{F}_2^n} \zeta(\underline{x})(-1)^{\underline{x}\cdot\underline{a}} = \sum_{\underline{x} \in \mathbb{F}_2^n} (-1)^{f(\underline{x})+\underline{x}\cdot\underline{a}}.$$

donde $() \cdot ()$ denota el producto interno (natural) en $\mathbb{F}_2^n$.

Sea n un entero par. Una función $f \in \mathbb{F}_2[\mathbb{F}_2^n]$ se llama *bent* si:

$$\hat{\zeta_f}(\underline{a}) = \pm 2^{\frac{n}{2}}.$$

Las funciones bent, así como otras relacionadas a esta (casi-bent, perfectamente no-lineales, etc.) son objeto de un estudio amplio debido a que sus propiedades son importantes en el diseño de sistemas de cifrado de llave privada (DES, AES, etc.), compartición de secretos, esquemas de autenticación, entre otras aplicaciones.

3.4. La operación de convolución discreta

Sea $(G, +)$ un grupo abeliano finito. La operación de *convolución* de $f, g \in \mathbb{F}[G]$, denotada por $f * g$, es un elemento de $\mathbb{F}[G]$ definido como:

$$(f * g)(x) = \sum_{y \in G} f(y)g(x - y),\ x \in G.$$

Veamos algunos ejemplos de esta operación.

3.4.1. La convolución en sucesiones. La convolución de dos sucesiones se introdujo anteriormente pero veamos que con la definición de convolución recien mencionada, se recupera la definición anterior.

Recordemos que una sucesión $\underline{a} = (a_0, a_1, ..., a_{n-1})$ de longitud n se puede describir como una función sobre el grupo de enteros módulo n con valores en $\mathbb{F}$:

$$f : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{F},\ f(i) = a_i.$$

Sean $\underline{a} = (a_0, a_1, ..., a_{n-1})$ y $\underline{b} = (b_0, b_1, ..., b_{n-1})$ dos sucesiones de longitud n determinadas por las funciones f y g respectivamente. Entonces $f * g : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{F}$ es la función tal que:

$$(f * g)(i) = \sum_{j=0}^{n-1} f(i)g(i-j),\ i \in \mathbb{Z}/n\mathbb{Z}.$$

Haciendo el cambio de notación de $f(i)$ por a_i, y de manera similar para g, se tiene que

$$(f * g)(i) = \sum_{j=0}^{n-1} a_i b_{i-j},$$

la cual es la convolución de dos sucesiones.

Para ilustrar este caso consideremos el siguiente ejemplo.

Sea $\underline{a} = (a_0.a_1, a_2)$ y $\underline{b} = (b_0.b_1, b_2, b_3)$ dos sucesiones de longitud 3 y 4 respectivamente. Entonces,

$$\underline{a} * \underline{b} = (c_0.c_1, ..., c_7),$$

donde

$$c_0 = a_0b_0, \qquad c_1 = c_0b_1 + a_1b_0, \qquad c_2 = a_0b_2 + a_1b_1 + a_2b_0,$$
$$c_3 = a_1b_2 + a_2b_0, \qquad c_4 = a_1b_3 + a_2b_2, \qquad c_5 = a_2b_3.$$

3.4.2. Producto de polinomios. Recordemos que existe una relación biunívoca entre las sucesiones de longitud finita, digamos n con entradas en $\mathbb{F}$ y los polinomios de grado $n-1$ con coeficientes en $\mathbb{F}$ dada por la representación polinomial de $\mathbb{F}^n$:

$$\underline{a} = (a_0, a_1, \ldots, a_{n-1}) \longrightarrow a(x) = a_0 + a_1x + \cdots a_{n-1}x^{n-1}.$$

Es directo ver que las coordenadas de la sucesión $\underline{a} * \underline{b}$ son precisamente los coeficientes del polinomio $a(x)b(x)$, producto de los polinomios correspondientes a las sucesiones.

Observación. La operación de convolución de dos sucesiones o equivalentemente de dos polinomios se puede expresar en términos matriciales. El siguiente ejemplo ilustra la idea.

Sean $\underline{a} = (a_0, a_1.a_2)$ y $\underline{b} = (b_0, b_1, b_2, b_3)$ dos sucesiones (de diferente longitud), y consideremos el siguiente producto de matrices:

$$\begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix} \begin{pmatrix} b_0 & b_1 & b_2 & b_3 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 & b_3 \end{pmatrix} =$$

$$(a_0b_0 \quad a_0b_1 + a_1b_0 \quad a_0b_2 + a_1b_1 + a_2b_0 \quad a_0b_3 + a_1b_2 + a_2b_1 \quad a_1b_3 + a_2b_2 \; a_2b_3).$$

Las entradas de ésta última matrix (vector) son precisamente las coordenadas de la convolución de las sucesiones $\underline{a} = (a_0, a_1, a_2)$ y $\underline{b} = (b_0, b_1, b_2, b_3)$. Obsérvese que si se consideran los polinomios $A(x)$ y $B(x)$ asociados a las respectivas sucesiones, estas entradas son los coeficientes del polinomio $A(x)B(x)$.

Como el producto de polinomios (o de la convolución) es conmutativo, si se invierten los papeles de las sucesiones $\underline{a}$ y $\underline{b}$ se tiene el producto $B(x)A(x)$.

3.4.3. Códigos de convolución. Los *turbo códigos* son una alternativa a los códigos de bloques para la detección y corrección de errores en la transmisión de información y son usados en una gran variedad de situaciones donde se manejan grandes volumenes de información, las cuales incluyen audio y video, entre otras. Una de las principales componentes de estos códigos son los *códigos de convolución*. Estos códigos reciben ese nombre debido a que su principal operación es la convolución entre la sucesión del mensaje a codificar y la correspondiente a un polinomio el cual esta asociado a un bit de redundancia (polinomio generdor). Hay tantos polinomios generadores como bits de redundancia se requieren, los cuales constituyen la información que se transmitirá por el canal de comunicación ([**2**]).

3.4.4. Procesamiento de imágenes digitales. En el procesamiento de imágenes digitales que incluyen médicas, atmosféricas, astronómicas, etc. una de las principales operaciones, por ejemplo para contruir filtros que resalten alguna característica de la imagen bajo consideración, es la convolución (en una o dos dimensiones). Detalles sobre el el tratamiento de imágenes digitales se puede consultar en cualquier texto sobre el tema, por ejemplo, ([**5**]).

3.5. Propiedades de la TDF

A continuación se mencionarán algunas propiedades básicas de la TDF sobre grupos abelianos finitos las cuales son similares a las mencionadas en la Sección de la TDF clásica, pero vale la pena recordarlas en un contexto relacionado con Teoría de Grupos.

(1) (**Linealidad.**) $\mathcal{F} : \mathbb{C}[G] \longrightarrow \mathbb{C}[\hat{G}]$ es una función lineal biyectiva.

(2) (**Convolución**.)

$$\mathcal{F}_{f*g}(\chi) = \mathcal{F}_f \cdot \mathcal{F}_g,\ \chi \in \hat{G}.$$

es decir, $\mathcal{F}$ es un homomorfismo con las operaciones de convolución y producto de funciones.

(3) (**Inversa**.) Dado que $\mathcal{F}$ es lineal biyectiva, su inversa esta dada por:

$$f(x) = \frac{1}{|G|}\sum_{\chi\in\hat{G}} \mathcal{F}_f(\chi)\chi(x) = \frac{1}{|G|}\sum_{a\in G}\langle f,\chi\rangle\chi(a)$$

(4) (**Igualdad de Parseval**.)

$$\langle f, f\rangle = \frac{1}{|G|}\langle \mathcal{F}_f, \mathcal{F}_f\rangle$$

(5) (**Translación**.) Si $x \in G$ sea $f^s(x) = f(s+x)$. Entonces,

$$\mathcal{F}_{f^s}(\chi) = \chi(s)\mathcal{F}_f(x).$$

3.6. La fórmula de Poisson

En esta sección se recuerda un resultado el cual es fundamental para dar la identidad de MacWilliams que relacionan el polinomio enumerador de pesos de un código lineal binario y el correspondiente de su código dual.

TEOREMA 3.6.1. *(Fórmula de Poisson) Sea G un grupo finito abeliano y H un subgrupo de G. Si $f \in \mathbb{C}[G]$, sea $\mathcal{F}_f$ la TDF de f y $g \in G$, entonces:*

$$\frac{1}{|H|}\sum_{h\in H} f(gh) = \frac{1}{|G|}\sum_{\chi\in H^*}\mathcal{F}_f(\chi)\chi(g),$$

donde $H^* = \{\chi \in \hat{G} :\ \chi(h) = 1\ \forall\ h \in H\}$.

El siguiente corolario del teorema anterior es el que realmente se usará para demostrar la relación de MacWilliams.

COROLARIO 3.6.2. *Con la notación anterior, si $g = 1$, entonces*

$$\frac{1}{|H|}\sum_{h\in H} f(h) = \frac{1}{|G|}\sum_{\chi\in H^*}\mathcal{F}_f(\chi)\chi(g).$$

Capítulo 4

Conceptos básicos de códigos lineales

Se presentarán conceptos básicos de códigos lineales (de bloque) y se aplicará el Teorema de Poisson para determinar la relación de MacWilliams entre el polinomio enumerador de pesos de un código lineal binario y el de su dual. Mayores detalles se pueden consultar en ([**4**], [**1**]).

Sea $\mathbb{F}_q$ un campo finito con $q = p^r$ elementos, donde p es un primo y $r > 0$ un entero. Un $[n, k]$-código lineal C sobre $\mathbb{F}_q$ es un subespacio lineal de $\mathbb{F}_q^n$ de dimensión k.

4.1. Matriz generadora y de paridad

Hay varias maneras de determinar un $[n, k]$-código lineal, una de ellas es por medio de una matriz generadora, y otra, por su matriz de paridad.

Sea $\{\mathbf{v_1}, \ldots, \mathbf{v_k}\}$ una base de C (sobre $\mathbb{F}_q$). Cada $\mathbf{v_i}$, siendo un elemento de $\mathbb{F}_q^n$, tiene n coordenadas (elementos del campo). Con esos elementos de puede formar la matriz

$$G = (\mathbf{v_1}, \ldots, \mathbf{v_k})^t$$

de tamaño $k \times n$. Es obvio que el código C esta generado por los renglones de esta matriz, es decir,

$$C = \langle \mathbf{v_1}, \ldots, \mathbf{v_k} \rangle_{\mathbb{F}_q} = \{\sum_{i=1}^{k} a_i \mathbf{v_i}, a_i \in \mathbb{F}_q\}.$$

A una matriz con estas características se le llama una matriz *generadora* de C. Como es natural, hay tantas matrices generadoras de un código como bases tenga este espacio vectorial.

Dado que una matriz determina una transformación lineal, si G es una matriz generadora de un código C, sea $T_G : \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$, $T_G(\mathbf{u}) = \mathbf{u}G$ la transformación lineal determinada por la matriz G. Es fácil ver que

$$C = Im(T_G).$$

Otra manera de determinar los elementos de un código (espacio) lineal es por medio de una matriz de paridad. Sea H una matriz $n \times t$ con entradas en el campo $\mathbb{F}_q$ y sea D el conjunto de soluciones del sistema homogéneo

$$HX^t = 0.$$

Es bien conocido que este conjunto es un subespacio lineal de $\mathbb{F}_q^n$, por lo tanto define un $[n, k]$-código lineal sobre $\mathbb{F}_q$, donde k es su dimensión. A una matriz H con la propiedad anterior se le llama una matriz de *paridad* del código D.

Si H es una matriz de paridad de un código D y T_H es la transformación lineal determinada por H, entonces

$$D = ker(T_H).$$

Existe una relación importante entre una matriz generadora G de un código lineal C y su matriz de paridad. Por medio de transformaciones elementales (cambio de renglones/columnas, multiplicación de un renglón/columna por una constante no-cero, suma de renglones/columnas, etc.) siempre es posible llevar una matriz de rango k a la forma (A, I_{n-k}), donde I_{n-k} es la matriz identidad $(n-k) \times (n-k)$. Una matriz que tiene esta forma se dice que esta en *forma estándard*.

Sea H una matriz de paridad de un código $C = ker(T_H)$ la cual, por la observación anterior podemos suponer que está en la forma estándar (A, I_{n-k}). Si $\mathbf{v} \in C$ entonces una matriz generadora del código C es ([**4**]):

$$G = \left(I_k, A^t\right)$$

Otro parámetro importante de un código lineal es su *distancia mínima*. El peso de *Hamming*, $p_H(\mathbf{v})$, de $\mathbf{v} \in \mathbb{F}_{\mathbf{q}}^{\mathbf{n}}$, se define como el número de coordenadas distintas de cero de $\mathbf{v}$. La *distancia* de Hamming entre los elementos $\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, es

$$d_H(\mathbf{u}, \mathbf{v}) = p_H(\mathbf{u} - \mathbf{v}).$$

La distancia *mínima*, d, de un código lineal C es

$$d = \min\{p_H(\mathbf{c}) : o \neq \mathbf{c} \in C\}.$$

Así, un código lineal sobre un campo finito $\mathbb{F}_q$ que tiene longitud n, dimensión k y distancia mínima d, decimos que es un $[n, k, d]$-código sobre $\mathbb{F}_q$.

4.2. Ejemplos

Para ilustrar los conceptos anteriores se presentan algunos ejemplos.

Ejemplo 1. (El código binario $[7, 4, 3]$ de Hamming). Sea H la matriz 3×7 cuyas columnas son los elementos distintos de cero del espacio lineal $\mathbb{F}_2^3$. Usando las transformaciones elementales podemos suponer que H tiene la forma estándar:

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

Como la matriz H tiene rango 3, el espacio C de soluciones del sistema homogéneo $HX^t = 0$ tiene dimensión 4 $(= 7 - 3)$, y por lo tanto C tiene 16 elementos (se deja como ejercicio al lector dar explícitamente estos elementos). Una vez teniendo esos elementos se puede ver que la distancia mínima de este código es 3 (de hecho hay mas de un elemento en C con peso de Hamming igual a 3). Mas aún, se tiene que hay: 1 elemento de peso igual a 0, 0 elementos de peso 1, 0 elementos de peso 2, 7 elementos de peso 3, 7 elementos de peso 4, y 1 elemento de peso 7.

Ejercicio. Determinar todos los elementos y una matriz generadora del código anterior.

Este ejemplo se puede generalizar. Sea $k \geq 2$ un entero y sea H_k la matriz de tamaño $k \times (2^k - 1)$ cuyas columnas son los elementos no-cero del espacio lineal $\mathbb{F}_2^k$. El código binario de Hamming se define como

$$\mathcal{H}_k = \{\mathbf{c} \in \mathbb{F}_2^{2^k-1} : H_k \mathbf{c}^t = 0\}.$$

Es fácil ver que la longitud de este código es $2^k - 1$ y dimensión $2^k - 1 - k$. Como ejercicio se deja al lector ver que la distancia mínima es igual a 3.

Ejercicio. Determinar una matriz generadora del código de Hamming $\mathcal{H}_k$.

Ejemplo 2. (El código de Reed-Solomon). A continuación se presenta uno de los códigos lineales que tiene una amplia gama de aplicaciones, entre ellas se encuentra los lectores de CD's ([**8**]). Para ilustrar las ideas se presenta un código de Reed-Solomon sobre el campo con 8 elementos.

Sea $\mathbb{F}_8$ el campo finito con 8 elementos, $n = 2^3 - 1 = 7$ y k entero tal que $1 \leq k \leq 7$, digamos $k = 5$. Sea

$$\mathcal{P}_5 = \{g(x) \in \mathbb{F}_8[x],\ t.q.\ gr(g) < 5\}.$$

Este conjunto es un $\mathbb{F}_8$- espacio vectorial de dimensión 5. Una base (natural) es $\{1, x, x^2, x^3, x^4\}$.

Consideremos la función (evaluación):

$$ev_{\mathbb{F}_8^*} : \mathcal{P}_5 \longrightarrow \mathbb{F}_8^7, \quad ev_{\mathbb{F}_8^*}(g) = (g(1), g(\alpha), ..., g(\alpha^6)).$$

donde α es un elemento primitivo de $\mathbb{F}_8$. Esta función es $\mathbb{F}_8$-lineal inyectiva, por lo tanto su imágen, $ev_{\mathbb{F}_8^*}(\mathcal{P}_5)$, es un subespacio lineal de $\mathbb{F}_8^7$ de dimensión 5.

A este subespacio de le denota por $RS(8,5)$ y se le llama el *código de Reed-Solomon* de orden 5 sobre $\mathbb{F}_8$.

Los parámetros de este código son: longitud $n = 7$, dimensión $k = 5$.

Matrix generadora.
Dado que $\mathcal{P}_5 = \langle 1, x, x^2, x^3, x^4 \rangle$ y la función $ev_{\mathbb{F}_8^*}$ es inyectiva, una matriz generadora de $RS(8,5)$ es:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$$

Distancia mínima.
Uno de los parámetros de un código lineal que en general no es fácil determinar, es la *distancia mínima*. En el caso de los códigos RS, ésta esta dada por

$$d = n - k + 1$$

que en este caso $d = 3$. En general se tiene que $d \leq n - k + 1$ (Cota Singleton). Cuando se tiene la igualdad se dice que el código es MDS (Maximum Distance Separable). Así el código RS es MDS.

Otro ejemplo del código de Reed-Solomon es el $RS(8,2)$ que se obtiene usando el mapeo evaluación sobre el espacio vectorial $\mathcal{P}_2 = \langle 1, x \rangle_{\mathbb{F}_8}$. En este caso la matriz generadora es:

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{pmatrix}$$

Se puede ver que este código tiene una palabra de peso cero, 49 palabras de peso 6, 14 palabras de peso 7, haciendo un total de $8^2 = |RS(8,2)|$ palabras del código. Los códigos de Reed-Solomon además de ser MDS son *cíclicos* ([**4**]).

4.3. El código dual

En el espacio lineal $\mathbb{F}_2^k$ se define un producto interno en la forma usual, igual que en $\mathbb{R}^k$: si $\mathbf{c} = (c_0, c_1, ..., c_{k-1}), \mathbf{d} = (d_0, d_1, ..., d_{k-1}) \in \mathbb{F}_2^k$,

$$\mathbf{c} \cdot \mathbf{d} = c_0 d_0 + \cdots + c_{k-1} d_{k-1}.$$

Con este producto interno se puede decir cuando dos vectores son ortogonales:

$$\mathbf{c} \perp \mathbf{c} \iff \mathbf{c} \cdot \mathbf{d} = 0$$

Si C es un $[n, m, d]$-código binario su *código dual* se define como:

$$C^\perp = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \cdot \mathbf{c} = 0 \ \forall \ \mathbf{c} \in C\}.$$

Es fácil ver, $C^\perp$ es un código lineal (binario) de longitud n y dimensión $n - m$. La distancia mínima, de igual manera que en otros códigos, en general no es fácil determinarla.

Si G es una matriz generadora de C y H una matriz de paridad, entonces G es la matriz de paridad del código dual $C^\perp$ y H su matriz generadora.

Ejemplo 1. (El código binario Simplex). Sea $\mathcal{H}_3$ el $[7, 4, 3]$-código de Hamming. Al código dual $\mathcal{H}_3^\perp$ se le llama *código simplex* y se denota por $\mathcal{S}_3$.

Ejercicio. Determinar los parámetros del código simplex $\mathcal{S}_3$, todos sus elementos y el número de palabras de distintos pesos. Como consecuencia se sigue este código tiene 7 elementos de peso 4 y un elemento de peso cero. Hacer lo mismo para el código de Reed-Solomon $RS(8, 2)$.

4.4. La relación de MacWilliams

Una pregunta interesante en Teoría de códigos lineales es la siguiente: ¿si se conoce la distribución de pesos de un código C será posible determinar la distribución de pesos de su código dual $C^\perp$? Esto es importante porque en algunas ocasiones es mas fácil determinar la distribución de pesos del código dual y se desa conocer la distribución de pesos del código.

En esta sección se usará la Fórmula de Poisson (Teorema 6) para dar una relación entre el polinomio enumerador de pesos de un código lineal binario y el correspondiente de su dual.

Si C es un $[n, k, d]$-código lineal (binario) su *polinomio enumerador de pesos*, $P_C(X, Y)$, se define de la siguiente manera: para $0 \leq i \leq n$ sea

A_i el número de palabras de C que tienen peso i, entonces su polinomio enumerador de pesos es:

$$P_C(X,Y) = \sum_{i=0}^{n} A_i X^{n-i} Y^i.$$

Observe que este polinomio es homogéneo de grado n, la potencia de Y indica el peso de las palabras (en algunos casos en la literatura los papeles de X y Y se invierten). Además, el término X^n siempre aparece ya que la palabra cero es un elemento de un código lineal, pero no siempre aparece el término Y^n ya que la palabra que tiene 1 en cada una de sus coordenadas no siempre es un elemento del código.

En la sección anterior se presentó el $[7,4,3]$-código binario de Hamming $\mathcal{H}_3$ el cual se vió que tiene: una palabra de peso cero, cero palabras de peso 1, cero palabras de peso 2, 7 palabras de peso 3, 7 palabras de peso 4, 0 palabras de peso 5, 0 palabras de peso 6 y una palabra de peso 7. Con estos valores el *polinomio enumerador* de pesos del código es:

$$P_{\mathcal{H}_3}(X,Y) = X^7 + 7X^4Y^3 + 7X^3Y^4 + Y^7.$$

La distribución de pesos del código $C = RS(8,2)$ introducido anteriormente es:

$$P_C(X,Y) = X^7 + 49XY^6 + 14Y^7.$$

Recordemos que el código simplex $\mathcal{S}_3$, el dual del código $\mathcal{H}_3$, es tal que todas sus palabras distintas de cero tienen peso igual a 4, por lo tanto es un código de peso constante (igual a 4), y su polinomio enumerador de pesos es:

$$P_{\mathcal{S}_3}(X,Y) = X^7 + 7X^3\mathcal{Y}^4.$$

Dado que en este ejemplo el polinomio enumerador de pesos de $\mathcal{S}_3$ es mas sencillo que el correspondiente polinomio de $\mathcal{H}_3$ y $\mathcal{S}_3$ es el dual de $\mathcal{H}_3$, ¿será posible obtener $P_{\mathcal{H}_3}(X,Y)$ a partir de $P_{\mathcal{S}_3}(X,Y)$? Este ejemplo ilustra el siguiente hecho general:

TEOREMA 4.4.1 (Identidades de MacWilliams). *Sea C un $[n,k,d]$-código lineal binario y $C^\perp$ su código dual. Entonces:*

$$P_{C^\perp}(X,Y) = \frac{1}{|C|} P_C(X+Y, X-Y)$$

A continuación se dará una demostración de este resultado usando el material introducido anteriormente sobre la Transformada Discreta de Fourier (TDF) y particularmente la *Fórmula de Poisson*.

Se aplicará la Fórmula de Poisson al caso $(G,+) = (\mathbb{F}_2^n,+)$ y $H = C$, el código lineal. Entonces,

$$C^* = \{\chi : \mathbb{F}_2^n \longrightarrow T : \chi(\mathbf{c}) = 1 \ \forall \ \mathbf{c} \in C\}$$

Recordemos que $\chi = \chi_{\mathbf{c}}$ para alguna $\mathbf{c} \in C$ y que $\chi_{\mathbf{c}}(\mathbf{x}) = (-1)^{\mathbf{c}\cdot\mathbf{x}}$. Por lo tanto,

$$C^* = \{\chi_{\mathbf{a}} : \mathbf{a} \in \mathbb{F}_2^n \ y \ \mathbf{a}\cdot\mathbf{c} = 0 \ \forall \ \mathbf{c} \in C\} = C^{\perp}.$$

Con estas identificaciones la Fórmula de Poisson toma la forma:

$$\frac{1}{|C|}\sum_{\mathbf{c}\in C} f(\mathbf{c}) = \frac{1}{2^n}\sum_{u\in C^{\perp}} \hat{f}(\chi_u),$$

donde $\hat{f}(\chi_u) = \sum_{x\in\mathbb{F}_2^n}(-1)^{u\cdot x} f(x)$.

Si ahora se substituye C por $C^{\perp}$ se tiene

$$\frac{1}{|C^*|}\sum_{\mathbf{a}\in C^{\perp}} f(\mathbf{a}) = \frac{1}{2^n}\sum_{u\in C} \hat{f}(\chi_u),$$

y como $|C^{\perp}| = |\mathbb{F}_2^n/|C| = \frac{2^n}{|C|}$, la relación anterior se reduce a

$$\sum_{\mathbf{a}\in C^{\perp}} f(\mathbf{a}) = \frac{1}{|C|}\sum_{u\in C} \hat{f}(\chi_u).$$

Considérese ahora la función $f(\mathbf{u}) = x^{n-|\mathbf{u}|}y^{|\mathbf{u}|}$, donde x, y son dos complejos fíjos. Por lo tanto la relación anterior se expresa como:

$$\sum_{\mathbf{a}\in C^{\perp}} x^{n-|\mathbf{a}|}y^{|\mathbf{a}|} = \frac{1}{|C|}\sum_{\mathbf{u}\in C} \hat{f}(\mathbf{u}).$$

Es fácil ver que

$$\hat{f}(\mathbf{u}) = \prod_{i=1}^{n}\left(\sum_{v_i=0}^{1}(-1)^{u_i v_i}x^{1-v_i}y^{v_i}\right).$$

Si $u_i = 0$, la expresión de la suma se reduce a $x + y$, y si $u_i = 0$, la suma se reduce a $x - y$, con lo cual se prueba la identidad de MacWilliams.

Bibliografía

[1] R.E. Blahut, *Algebraic Codes on Lines, Planes and Curves*, Cambridge U. Press, 2008.

[2] R. Johannesson and K. Sh. Zigangirov, *Fundamentals of Convolutional Coding*, IEEE Press, 1999.

[3] R. Lidl and H. Niederreiter, *Finite fields* , Cambridge University Press 1987.

[4] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*. New York: Elsevier/North Holland, 1977.

[5] Ch. Solomon and T. Breckon, *Fundamentals of Digital Image Processing: A Practical Approach with Exp. in Matlab*. Wiley-Blackwell, 2010, ISBN 978-0470844731.

[6] H. Tapia-Recillas, *Sobre algunas aplicaciones de los campos de Galois*, Miscelánea Matemática, 53 ,Soc. Mat. Méx., pag. 81- 100, Dic. 2011.

[7] A. Terras, *Fourier Analysis on Finite Groups and Applications*, London Math. Soc., Student Text 43, 1999.

[8] St. B. Wicker and V. Bhargava, *Reed-Solomon codes and their Applications*, IEEE Press, 1994.