MISCELANEA MATEMÁTICA 23 (1996), 39–54 SMM

Funciones theta:una aplicación a teoría de códigos

H. Tapia-Recillas * C. Rentería †

1 Introducción

El carácter de esta nota es de tipo expositorio y se trata de presentar una conexión entre un tema que en los últimos años ha tenido un gran desarrollo y relevancia en problemas prácticos en teoría de la información, por lo que ha llamado la atención de investigadores en varias disciplinas, y un tema que por más de un siglo ha sido (y seguirá siendo) objeto de estudio: **Códigos Lineales Detectores-Correctores de Errores, y Funciones Theta**. Más concretamente, se expresará la Identidad de MacWilliams para el Polinomio Exacto Enumerador de Pesos (PEEP) de un código lineal en términos de funciones theta con características. La conexión entre ambas partes se hace a través de una transformada finita de Fourier sobre campos finitos.

Las funciones theta tienen una larga historia en la Matemática y han sido por mucho tiempo tema de estudio. Su influencia en el desarrollo de la Matemática es de gran importancia ya que ha dado origen a diversos y variados temas en áreas como Análisis Complejo, Geometría Algebraica, Teoría de Números, etc.,([10, 11, 12]), así como en Física en relación a la ecuación del calor.

El área de estudio de códigos lineales detectores-correctores de errores, muy usados en la transmisión de información, es relativamente "nueva", ya que se empezó a trabajar en forma sistemática a partir de la década de los años 50 ([17, 7, 8]). Las herramientas matemáticas,

*Dpto.Matemáticas, U.A. Metropolitana-I, Apartado Postal 55-534, México 09340, D.F., MÉXICO

†E. Superior de Física y Matemáticas, I.P.N., MÉXICO. Parcialmente apoyado por COFAA

computacionales y de ingeniería, entre otras, han permitido desarrollar e implementar novedosos sistemas de codificación y decodificación para la transmisión de información por cualquier medio o canal, de tal manera que están siendo usados en una gran variedad de problemas en diversas disciplinas como la Medicina (tomografía), Astronomía (fotografías de cuerpos celestes), Robótica (sistemas de control), Economía y Finanzas (trasacciones comerciales y financieras), Política y Administración (decisiones estratégicas), uso doméstico y comercial (sistemas de grabación y reproducción de imágenes y sonido), etc.

Como se menciona en el párrafo anterior, los códigos detectores-correctores de errores tienen una gran aplicación en la vida cotidiana, sin embargo en los últimos años se han descubierto varias conexiones interesantes entre la Teoría de Códigos y alguas partes "teóricas" de diversas áreas de la Matemática (ver por ejemplo [2]). La conexión entre estos temas nos ha parecido interesante y consideramos adecuado presentar una de ellas, y así saber de un lugar más donde el fascinante mundo de las funciones theta tiene cabida.

Los temas y resultados que aquí se mencionan se han tomado de varias fuentes: para la parte clásica de funciones theta se ha consultado la excelente referencia [10]; para la parte básica de Códigos Lineales se han seguido de cerca las referencias [3] y [9]. La Transformada Finita de Fourier se puede consultar con mas detalle en [3, 11, 12, 19]. Para dar la conexión entre todos estos temas se han seguido los artículos [12] y [19].

Esta nota está organizada de la siguiente manera: en la sección 2 se introducirá el concepto de Código Lineal Detector-Corrector de Errores con algunos ejemplos y se darán sus principales parámetros. En la sección 3 se introducirá el Polinomio Enumerador de Pesos de Hamming (PEPH) y el Polinomio Exacto Enumerador de Pesos (PEEP) de un código lineal. También se recordará la Identidad de MacWilliams para estos polinomios. En la sección 4 se introducirá la Transformada Finita de Fourier (TFF), en la sección 5 se recordarán la definición de funciones theta con característica y algunas de sus propiedades; y en la última sección se describirá la Identidad de MacWilliams para el Polinomio Exacto Enumerador de Pesos de un código lineal en términos de funciones theta con características. Como esta nota es de carácter expositorio, no se darán demostraciones de los resultados que se mencionan, el lector interesado puede consultar las referencias [12] y [19] para mayores detalles.

2 El concepto de Código Lineal

Muchos de nosotros hemos tenido la experiencia de que algunas veces cuando estamos hablando por teléfono no se escucha bien y decimos que "hay ruido", pudiendo ser que en el otro lado de la línea se escuche perfectamente; otro ejemplo es el caso de la radio. Hay ocasiones en que la señal es perfecta y de "repente" se escucha "ruido" (por ejemplo cuando pasa un avión cerca del lugar donde se escucha la radio). En este caso la estación emisora de radio supone que la señal que envía es la misma que reciben los radioescuchas. Un ejemplo similar es el de una estación de televisión. Este tipo de situaciones se pueden presentar cuando una señal o información es enviada de una estación emisora a otra estación receptora, donde esta última recibe la información original, pero con "ruido", es decir la información ha adquirido "errores" durante la transmisión. En algunos casos el recibir la información con errores puede ser de vital importancia (por ejemplo en Medicina cuando se usa tomografía). El tratar de detectar los errores y por supuesto corregirlos, en la transmisión de información, dio origen a lo que actualmente se conoce como la *Teoría de Códigos Detectores-Correctores de Errores.*

Para hacer una motivación más formal del concepto de Código Lineal Detector-Corrector de Errores considérese la siguiente situación. Supóngase que se desea transmitir información de una base emisora a otra receptora por cualquier canal de comunicación (teléfono, radio, satélite, etc.). Para ejemplificar, digamos que esa información es: SI y NO. Este mensaje se traduce al sistema que se emplea en el canal de trasmisión, para el propósito del ejemplo, (y en la mayoria de las aplicaciones) el sistema binario $\{0,1\}$, y se le asocia a la palabra SI, por ejemplo tres uno's: (111), y a la palabra NO, se le asocia tres ceros: (000). En este ejemplo bien se le puede asociar a cada una de las palabras otra colección de ceros y unos. Para cuestiones prácticas, la colección de ceros y unos que se le asocia a cada una de las palabras de un mensaje, depende del tipo de información que se esté manejando. Ahora se necesita *codificar* la información, y digamos que a la palabra SI se representa ahora, por ejemplo, como (1111), y la palabra NO como (0000); esta información codificada se transmite. Debido a que la transmisión se hace a través de un canal que en general es "ruidoso", la información que recibe la base receptora es la información que se envió de la base emisora más un error adquirido durante la transmisión. Supongase que en el ejemplo se recibe (1010) para la palabra SI, y (0101) para la palabra NO. Este mensaje debe ser decodificado y decidir en cada uno de los casos de qué información se trata. Esta situación se ilustra en el siguiente diagrama.

$$\boxed{\text{EMISOR}} \longrightarrow \boxed{\text{CODIFICADOR}} \xrightarrow{\text{canal}} \boxed{\text{DECODIFICADOR}} \longrightarrow \boxed{\text{RECEPTOR}}$$

En general, cuando se transmite información por cualquier medio o canal se adquiere un error, por múltiples factores que van desde humanos hasta técnicos, de tal manera que en la estación receptora se tiene que decidir donde ocurrieron esos errores y en el mejor de los casos corregirlos. La idea es presentar un modelo matemático que permita detectar esos errores y por supuesto tratar de corregirlos. De esta idea nace el concepto de Código Lineal Detector-Corrector de Errores. El siguiente ejemplo motivará este concepto.

Supongase que se desea enviar el mensaje $u_1u_2u_3u_4$, donde los u_i, llamados *bits de información*, son elementos del campo binario $GF(2) = \{0,1\}$, y que el mensaje se codifica en $x_1x_2x_3x_4x_5x_6x_7$, donde:

$$x_1 = u_1, x_2 = u_2, x_3 = u_3, x_4 = u_4$$

$$x_5 = x_1 + x_2 + x_4$$

$$x_6 = x_1 + x_3 + x_4$$

$$x_7 = x_2 + x_3 + x_4$$

La primeras cuatro coordenadas se toman igual a los bits de información, y las tres restantes como combinación lineal de estos. Las coordenadas x_5, x_6, x_7 que dependen de los bits de información se denominan *bits de redundancia.* A un elemento $(x_1, ..., x_7)$ del espacio lineal binario $GF(2)^7$ que satisface las relaciones anteriores, se le llama *palabra codificada.* Nótese que si

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

es la matriz del sistema lineal arriba mencionado, entonces $\bar{x} = (x_1, ..., x_7)$ $\in GF(2)^7$ es una palabra codificada si y sólo si $H \cdot \bar{x}^t = 0$, es decir $\bar{x}$

es un elemento del espacio C de soluciones de este sistema. Si denotamos por H también a la transformación lineal $H : GF(2)^7 \longrightarrow GF(2)^3$ determinada por esta matriz, se tiene que $\bar{x} \in GF(2)^7$ es una palabra codificada si y sólo si $\bar{x} \in C = ker(H)$

Motivados por este ejemplo, se puede dar ahora una definición mas formal de Código Lineal ([3, 9, 13]).

Sea $K = GF(q)$ un campo finito con q elementos (q siendo potencia de un primo), y sea H una matriz con $(n - k)$ hileras y n columnas (k entero $\leq n$) con entradas en el campo K.

Definición 1 Un *código lineal* C sobre el campo finito K con *matriz de (chequeo de) paridad* H es el espacio de soluciones (sobre K) del sistema lineal homogéneo $H \cdot \bar{X}^t = 0$.

A los elementos de C se les llama *palabras* del código. El número de coordenadas de las palabras, es decir, el entero n es la *longitud* del código, y el entero k es la dimensión de C como K-espacio lineal. En este caso se dirá que C es un $[n, k]$-código lineal sobre K.

En el ejemplo anterior se tendría un $[7, 4]$-código lineal binario con matriz de paridad H.

El espacio lineal K^n tiene un producto interno natural: $\bar{x} \cdot \bar{y} = \sum_{i=1}^{n} x_i y_i$, como en el caso del espacio euclidiano $\mathbf{R}^n$. Si C es un $[n, k]$-código lineal sobre K, el subespacio lineal dual

$$C^* = \{\bar{x} \in K^n : \bar{x} \cdot \bar{c} = 0, \forall \quad \bar{c} \in C\}$$

se llama el *código dual* de C.

Es fácil ver que C^* es un $[n, n - k]$-código (lineal) sobre el campo K. Una matriz de paridad G del código dual C^* se llamará una *matriz generadora* del código C. Una relación sencilla pero útil entre una matriz de paridad H y una matriz generadora G de un lineal código C, es la siguiente:

$$H \cdot G^t = 0, \quad G \cdot H^t = 0$$

En particular, estas relaciones implican que el código lineal C está generado por las hileras de la matriz generadora G (de ahí su nombre).

Si denotamos también por G y H a las funciones lineales inducidas por las matrices respectivas, entonces se tiene que

$$C = \ker(H) = \mathrm{Im}(G^t)$$

Además de la longitud y dimensión de un código lineal C, se tiene otro parámetro muy interesante de un código lineal: la *distancia mínima.* Para definir la distancia mínima, primero recordemos que el *peso de Hamming* de una palabra $0 \neq \bar{c}$ de un código lineal C es: $p(\bar{c}) =$ número de coordenadas distintas de cero de $\bar{c}$. La distancia mínima de C se define como

$$d = \min\{p(\bar{c}) : 0 \neq \bar{c} \in C\}$$

Si un código C tiene longitud n, dimensión k y distancia mínima d, entonces se dirá que es un $[n, k, d]$-código lineal.

Una razón por la cual la distancia mínima de un código lineal es importante está dada en el siguiente resultado.

Teorema 1 *Un código lineal C con distancia mínima d puede corregir a lo más $[(d-1)/2]$ errores.*

Para una demostración de este resultado se puede consultar por ejemplo [3, 9, 13].

El peso de Hamming induce una distancia en el código en cuestión, definida de la siguiente manera:

$$d(\bar{x}, \bar{y}) = p(\bar{x} - \bar{y})$$

para $\bar{x}, \bar{y} \in C$.

Es fácil ver que esta función es en efecto una *distancia*, y que por lo tanto el código lineal C es un espacio métrico.

Veamos ahora algunos ejemplos de Códigos Lineales.

1. *Códigos binarios de Hamming.* Sea $m \geq 2$ un entero, H la matriz cuyas columnas son todos los elementos no cero del $GF(2)$-espacio lineal $GF(2)^m$, y sea $C = \ker(H)$ (vista a H como la función lineal inducida por la matriz H). Entonces C es un $[2^m - 1, 2^m - 1 - m, 3]$-código lineal binario ([3, 9, 13]). El ejemplo mencionado al

principio de esta sección es un $[7,4,3]$-código binario de Hamming, el cual puede corregir a lo más un error (de acuerdo al teorema anterior). Debido a esta restricción, los códigos de Hamming actualmente no se usan en implementaciones, sin embargo han sido fuente de generalizaciones interesantes.

2. Sea G una gráfica conexa finita, $\tilde{G}$ la matriz de incidencia de la gráfica (está matriz tiene entradas 0's y 1's) y sea C el código lineal binario con matriz generadora $\tilde{G}$.

   En el estudio de este tipo de códigos, una pregunta interesante, es cómo describir el código en términos de la estructura combinatoria de la gráfica, por ejemplo dar una base del código ([1, 14]).

3. Sea X la curva algebraica sobre el campo finito $\mathbf{F}_4 = \{0, 1, \alpha, \alpha^2\}$, (donde $\alpha^2 + \alpha + 1 = 0$) definida por la relación $x^3 + y^3 + z^3 = 0$. Esta curva es no-singular y tiene 9 puntos racionales sobre el campo $\mathbf{F}_4$: $\{P_1, ..., P_8, Q = (0,1,1)\}$. Sea $L(2Q) = \{f \in \mathbf{F}_4(X) : \operatorname{div}(f) + 2Q \geq 0\}$. Este es un $\mathbf{F}_4$-espacio lineal de dimensión 2, donde una base es: $\{1, x/(y+z)\}$. Al evaluar las funciones de esta base en los otros 8 puntos $\mathbf{F}_4$-racionales de la curva, se tiene la siguiente matriz:

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

   Sea C el código lineal con matriz generadora G. Es fácil ver que C es un [8,2,6]-código lineal sobre $\mathbf{F}_4$.

Los códigos lineales asociados a curvas algebraicas sobre campos finitos fueron introducidos por V. D. Goppa a principios de la década de los años 80 y actualmente se conocen como Códigos de Goppa o Códigos geométrico-algebraicos. Estos códigos han sido objeto de estudio desde entonces, produciendo resultados interesantes tanto en Teoría de Códigos como en Geometría Algebraica sobre campos finitos y Teoría de Números ([4, 5, 20]).

3 Polinomios Enumeradores de Pesos

En esta sección se recordará la definición del Polinomio de Hamming Enumerador de Pesos (PHEP) y del Polinomio Exacto Enumerador de

Pesos (PEEP) de un código lineal, así como la Identidad de MacWilliams para ambos polinomios ([6, 8, 9]).

Considérese el campo finito $K{=}GF(q) = \mathbf{F}_q$ con q elementos (q siendo una potencia de un primo p). Recordemos que si C es un $[n,k,d]$-código lineal sobre el campo finito K, el *peso de Hamming*, $p(c)$, de una palabra $0 \neq c \in C$, es el número de coordenadas distintas de cero de c. Sea A_r el número de palabras (elementos) de C con peso r. Obsérvese que $A_r \geq 0$ para toda r, y que si d es la distancia mínima del código C, entonces $A_r = 0$ para $0 \leq r \leq d-1$, y $\sum_{r=0}^{n} A_r = q^k = \#(C)$.

Definición 2 El *Polinomio de Hamming Enumerador de Pesos* (PHEP), de un $[n,k,d]$-código lineal C definido sobre el campo finito K, es:

$$W(x,y) = \sum_{r=0}^{n} A_r x^{n-r} y^r$$

Obsérvese que $W(x,y)$ es un polinomio homogéneo de grado n y que

$$W(x,y) = \sum_{c \in C} x^{n-p(c)} y^{p(c)}$$

Ejemplo 1 1. *Sea* $C = \{(00),(11)\}$ *el [2,1,2]-código lineal binario de repetición. Su (PHEP) es*

$$W(x,y) = x^2 + y^2$$

2. *Sea* $C = \{(000),(011),(101),(110)\}$ *un [3,2,2]-código lineal binario. Su (PHEP) es:*

$$W(x,y) = x^3 + 3xy^2$$

3. *Sea* C *el código binario de Hamming con parámetros [7,4,3] (ver ejemplo 1 de la sección anterior). En este caso es fácil ver que su (PHEP) es:*

$$W(x,y) = x^7 + 8x^4y^3 + 6x^3y^4 + y^7$$

4. *Considérese el siguiente código lineal ternario (es decir, sobre el campo* $\mathbf{Z}/(3)$*):* C*={(0000),(0121), (0212),(1022),(1110),(1201), (2011),(2102), (2220)}. Este código tiene parámetros [4,2,3] y su (PHEP) es:*

$$W(x,y) = x^4 + 8xy^3$$

Este código es un ejemplo de códigos de Hamming sobre campos no necesariamente binarios.

Sea C un $[n, k, d]$-código lineal sobre el campo finito K, y sea C^* su código dual. El código C de dice que es *auto-dual* si $C = C^*$ (obsérvese que en este caso $k = \frac{1}{2}n$).

Ejemplo 2 1. *El código binario del ejemplo 1 mencionado anteriormente es auto-dual.*

2. *El dual del código del ejemplo 2 es* $C^* = \{(000), (111)\}$, *y su (PHEP) es:*

$$W^*(x, y) = x^3 + y^3$$

3. *El código binario C con parámetros [8,4,4] y matriz generadora*

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

es auto-dual y su (PHEP) es:

$$W(x, y) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7$$

Este es el código de Hamming extendido que se obtiene anexando una coordenada x_8 a cada palabra $\bar{c} = (x_1, ..., x_7)$ del [7,4,3]-código lineal binario de Hamming mencionado anteriormente, de tal manera que $x_1 + \cdots + x_7 + x_8 = 0$.

4 *El [4,2,3]-código del ejemplo 4 antes mencionado, también es auto-dual.*

Observemos ahora lo siguiente. Si en el (PHEP) del código del ejemplo 2 mencionado arriba, se hace el cambio de variables $x \longrightarrow x+y$, $y \longrightarrow x - y$, se tiene:

$$W(x+y, x-y) = (x+y)^3 + 3(x+y)(x-y)^3 = 4(x^3 + y^3) = 4W^*(x, y)$$

Para el caso del ejemplo 1, haciendo el mismo cambio de variables también se tiene la relación:

$$W(x + y, x - y) = 2W^*(x, y)$$

Obsérvese que en un caso el código es auto-dual y en el otro no, donde en ambos casos W^* es el (PHEP) del código dual.

Estos ejemplos motivan la siguiente pregunta: ¿ qué relación existe entre el (PHEP) de un código C y el correspondiente (PHEP) del código dual C^*?

La respuesta a esta pregunta se debe a F.J. MacWilliams, conocida como la Identidad de MacWilliams para Polinomios de Hamming Enumerador de Pesos, y es la siguiente.

Teorema 2 *Si C es un $[n,k,d]$-código lineal sobre el campo finito K con (PHEP) $W(x,y)$ y si $W^*(x,y)$ es el (PHEP) del código dual C^*, entonces:*

$$\#(C)q^{-1/2}W^*(x,y) = W(x+(q-1)y, x-y)\,.$$

Corolario 1 *Si el código C es auto-dual, entonces:*

$$\sqrt{q^n}W(x,y) = W(x+(q-1)y, x-y)\,.$$

Observación: Como el polinomio de pesos $W(x,y)$ es homogéneo de grado n, si el código es auto-dual, se tiene:

$$W(x,y) = W(\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}})$$

En relación al comportamiento del (PHEP) de un código lineal y el correspondiente del código dual, se han obtenido resultados interesantes ([18]).

Para definir el Polinomio Exacto Enumerador de Pesos, (PEEP), de un código lineal, haremos primero la siguiente identificación: a cada elemento $\underline{u} = (u(1),...,u(n)) \in K^n$ le asociamos el monomio $x^{\underline{u}} = x_{u(1)}x_{u(2)}\cdots x_{u(n)}$, en las variables (no-conmutativas) $x_0, x_1, \cdots, x_n$

EJEMPLO. Si $q=7$, al elemento $\underline{u} = (01432)$ de $GF(7)^5$ se le asocia el monomio $x^{\underline{u}} = x_0x_1x_4x_3x_2$.

Por el resto de esta nota sólo se considerarán códigos lineales definidos sobre un campo con p elementos, el cual se denotará por $K = \mathbf{F}_p$ o bien por $GF(p)$.

Definición 3 El *Polinomio Exacto Enumerador de Pesos* (PEEP) de un $[n, k, d]$-código lineal C sobre el campo finito K, es:

$$P_C = P_C(x) = \sum_{\underline{u} \in C} x^{\underline{u}} = \sum_{\underline{u} \in C} x_{u(1)} \cdots x_{u(n)}$$

donde $\underline{u} = (u(1), ..., u(n))$.

La identidad de MacWilliams para el Polinomio Exacto Enumerador de Pesos de un código lineal C, está dado en el siguiente resultado.

Teorema 3 **([11, 12])** *Si P_C denota el (PEEP) de un código lineal C y P^* denota el (PEEP) del código dual, entonces*

$$P_C(y) = \mid C \mid P^*(x)$$

donde $y = (y_0, \ldots, y_n)$, $y_r = \sum_{s=1}^{p-1} exp(2\phi ir \cdot s/p) x_s$.

En la última sección de esta nota se verá que la identidad de MacWilliams que relaciona el (PEEP) de un código lineal y el correspondiente de su dual, se puede expresar en términos de funciones theta con características. Para tal fin, en las siguientes secciones se recordará el concepto de transformada finita de Fourier y el de funciones theta con característica.

4 La Transformada Finita de Fourier

En esta sección se recordará la definición de la Transformada Finita de Fourier sobre campos finitos y algunas de sus propiedades básicas, el lector interesado en más detalles puede consultar por ejemplo [3, 11, 12, 19]. Los resultados de esta sección y los de la siguiente son los que prácticamente dan una relación entre las funciones theta y la Identidad de MacWilliams.

Sea $K = GF(p)$ el campo finito con p elementos. Para cada entero $g \geq 1$ sea $V_p^g = \{f : K^g \longrightarrow \mathbf{C}\}$, donde $\mathbf{C}$ es el campo de los números complejos. Es fácil ver que este conjunto es un $\mathbf{C}$-espacio lineal de dimensión p^g, y una base (natural) está dada por las funciones características $E_{\bar{v}}$, para $\bar{v} \in K^g$.

La *transformada finita de Fourier* $F_p^g : V_p^g \longrightarrow V_p^g$ se define como:

$$F_p^g(f)(\bar{y}) = \sum_{\bar{x} \in K^g} exp(2\phi i \frac{\bar{x} \cdot \bar{y}}{p})$$

donde $\bar{y} \in K^g$ y el punto denota el producto interno natural.

Sea C un $[g, k, d]$-código lineal sobre el campo K, y sea E_C su función característica, entonces se tiene el siguiente

Teorema 4 ([11, 12, 19])

$$F_p^g(E_C) = \#(C)p^{g/2}E_{C^*}.$$

Sea $V_p = \{f: K \longrightarrow \mathbf{C}\}$, y sea $T_g = \otimes_1^g V_p$. Una base del espacio T_g es $\{x^{\bar{v}} = x_{v(1)} \cdots x_{v(g)}\}$, donde $\bar{v} = (v(1), ..., v(g))$. Un cálculo directo muestra que la función $\phi(x^{\bar{v}}) = E_{\bar{v}}$ identifica a T_g con el espacio V_p^g.

Con las notaciones anteriores se tienen los siguientes resultados:

1. $\phi(P_C) = E_C$, donde P_C es el (PEEP), (ver sección anterior).

2. La función $(F_p^g)^\phi = (\phi)^{-1} \cdot F_p^g \cdot \phi$ es tal que

$$(F_p^g)^\phi(P_C) = \#(C)p^{-g/2}P_{C^*}$$

3. Si $f = \sum_{\bar{v} \in K^g} a(\bar{v})\bar{x}^{\bar{v}} \in T_g$, con $a(\bar{v})$ números complejos, entonces:

$$(F_p^g)^\phi(f) = \sum_{\bar{v} \in K^g} a(\bar{v})\bar{y}^{\bar{v}}$$

donde $\bar{y} = (y_1, ..., y_g)$ y $y_j = p^{-g/2} \sum_{k=0}^{p-1} exp(2\pi i j \cdot k/p)x^k$.

Aplicando esta última relación al (PEEP), se tiene la Identidad de MacWilliams:

$$P_C(\bar{y}) = \#(C)p^{-g/2}P_{C^*}$$

5 Funciones theta con característica

En esta sección se recordará la definición de función theta con característica y algunos de los resultados más básicos ([10]).

Sea $g \geq 1$ un entero, H_g={matrices Ω (g x g): $Im(\Omega) \geq 0$} el semiplano-superior de Siegel. Si $\Omega \in H_g$, sea $L_\Omega = \mathbf{Z}^g + \Omega\mathbf{Z}^g$ la latice (algunos autores le llaman red) generada por Ω, y sea $R_p^g(\Omega) = \{f : \mathbf{C} \longrightarrow \mathbf{C} : f$ es L_Ω-cuasi periódica $\}$, es decir satisface las relaciones siguientes:

$$f(\bar{z} + \bar{m}) = f(\bar{z})$$

$$f(\bar{z} + \Omega\bar{m}) = exp(-\pi i\bar{m}^t\Omega\bar{m} + 2\pi ip\bar{z}^t\bar{m})f(\bar{z})$$

El conjunto $R_p^g(\Omega)$ es un $\mathbf{C}$-espacio lineal de dimensión p^g. A continuación se darán dos bases naturales de este espacio.

Sea $\mathbf{Q}$ el campo de los números racionales. Si $\Omega \in H_g$, la *función theta con características* $\bar{r}, \bar{s} \in \mathbf{Q}^g$, se define como:

$$\theta\begin{pmatrix} \bar{r} \\ \bar{s} \end{pmatrix}(\bar{z}, \Omega) = \sum_{\bar{n}\in\mathbf{Z}^g} exp(\pi i(\bar{n} + \bar{r})^t\Omega(\bar{n} + \bar{r}) + 2\pi i(\bar{n} + \bar{r})^t \cdot (\bar{z} + \bar{s})$$

Una base del espacio $R_p^g(\Omega)$ es el conjunto de funciones:

$$f_{\bar{a}}(\bar{z}) = \theta\begin{pmatrix} \bar{a}/p \\ \bar{0} \end{pmatrix}(p\bar{z}, \Omega)$$

donde $\bar{a} \in K^g$

Otra base del espacio $R_p^g(\Omega)$ es el siguiente conjunto de funciones:

$$g_{\bar{b}}(\bar{z}) = \theta\begin{pmatrix} \bar{0} \\ \bar{b}/p \end{pmatrix}(\bar{z}, p^{-1}\Omega)$$

donde $\bar{b} \in K^g$

Estas dos bases están relacionadas de la siguiente manera ([10]):

$$g_{\bar{b}}(\bar{z}) = \sum_{\bar{a}\in\mathbf{F}_p^g} exp(2\pi i\bar{a}^t \cdot \bar{b}/p)f_{\bar{a}}(\bar{z})$$

6 Funciones theta e Identidad de MacWilliams

Haciendo uso de los resultados de la sección 4 y los mencionados en la sección anterior sobre funciones theta, se tienen las siguientes observaciones:

1. La función $\phi : V_p^g \longrightarrow R_p^g(\Omega)$ definida como $\phi(E_{\bar{a}}) = f_{\bar{a}}$ es un isomorfismo entre esos dos espacios.

2. La transformada finita de Fourier $F_p^g : V_p^g \longrightarrow V_p^g$ introducida en la sección 4, induce la función $F_p^g(\Omega)$: $R_p^g(\Omega) \longrightarrow R_p^g(\Omega)$ tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} V_p^g & \xrightarrow{F_p^g} & V_p^g \\ \phi \downarrow & & \downarrow \phi \\ R_p^g(\Omega) & \xrightarrow{F_p^g(\Omega)} & R_p^g(\Omega) \end{array}$$

3. Se tienen las siguientes identificaciones:

$$\begin{array}{ccccccc} F_p^g & \leftrightarrow & T^g & \overset{\varphi}{\leftrightarrow} & V_p^g & \overset{\phi}{\leftrightarrow} & R_p^g(\Omega) \\ \bar{v} & \leftrightarrow & x^{\bar{v}} & \leftrightarrow & E_{\bar{v}} & \leftrightarrow & f_{\bar{v}} \end{array}$$

4. Una de las observaciones que servirá directamente a nuestro propósito es la siguiente (la relación entre las dos bases del espacio $R_p^g(\Omega)$ a través de la función inducida por la transformada finita de Fourier):

$$g_{\bar{b}} = F_p^g(\Omega)(f_{\bar{b}})$$

Ahora se está en la posición de interpretar la Identidad de MacWilliams para el Polinomio Exacto Enumerador de Pesos de un código lineal C, en términos de funciones theta con característica.

Aplicando la función ϕ a la relación $F_p^g(E_C) = \#(C)p^{-g/2}E_{C^*}$ y usando la conmutatividad del diagrama de la observación 2 de arriba, el lado izquierdo de esta relación conduce a la expresión: $\sum_{\bar{b}\in C} g_{\bar{b}}$, y el lado derecho a: $\#(C)p^{-g/2}\sum_{\bar{a}\in C^*} f_{\bar{a}}$. Por consiguiente se tiene:

$$\sum_{\bar{b}\in C} g_{\bar{b}} = \#(C)p^{-g/2}\sum_{\bar{a}\in C^*} f_{\bar{a}}$$

la cual es la Identidad de MacWilliams para el Polinomio Exacto Enumerador de Pesos de un código C.

Haciendo uso de algunas otras propiedades de las funciones theta y la transformada finita de Fourier se pueden obtener resultados en conexión con Teoría de Códigos y Variedades Abelianas. El lector interesado puede consultar la referencia [12]. Para concluir, podemos decir que las funciones theta siguen vigentes, a pesar de haber sido introducidas hace ya muchos años. Por otro lado, pocos nos podíamos imaginar una conexión entre este tema tan clásico de Variable Compleja y un tema relativamente nuevo de la Matemática Discreta como son los códigos lineales detectores-correctores de errores, usados en la transmisión de información y de gran aplicación en el mundo moderno.

Agradecemos a los revisores de este trabajo sus comentarios y sugerencias para la mejor presentación del mismo.

Referencias

[1] Babai, L., Oral, H., Phelps, K.T. *Eulerian self-dual codes* (preprint).

[2] Beth, T. *Aspects between Coding Theory,* Probability, Algebra, Combinatorics and Complex Analysis. LNM, Springer Verlag, (1983).

[3] Blahut, R. E. *Theory and practice of error control codes,* Addison-Wesley, Reading, Mass., (1983).

[4] Goppa, V.D. *Codes and Information,* Usp.Math. Nauk 39:1 (1984). Russ. Math. Surveys 39:1, 87-141, (1984).

[5] Goppa, V. D. *Geometry and codes,* Kluwer Ac. Publ., (1988).

[6] Gleason, A. *Weight polynomials of self-dual codes and the MacWilliams identities,* Actes Congrès Internat. Math., vol.3, Paris, 211-215, (1971).

[7] Hamming, R. W. *Error detecting and error correcting codes,* Bell Syst. Tech. J., 29, 147-160, (1950).

[8] MacWilliams, F. J. *A theorem on the distribution of weights in a systematic code,* Bell System Tech. J., 42, 79-84, (1963).

[9] MacWilliams F. J., Sloane N. *The theory of error correcting codes,* North-Holland, Amsterdam, (1978).

[10] Mumford, D. *Tata lectures on theta I,* Birkhäuser, Boston, (1983)

[11] Opolka, H. *The finite Fourier transform and theta functions,* Springer Lecture Notes in Computer Science, vol. 229, 156-166, (1986).

[12] Opolka, H. *Geometry of the finite Fourier transform,* Comm. in Algebra, 19(2), 427-432, (1991).

[13] Rentería, C., Tapia-Recillas, H., Vélez, W. Y. *Breve introducción a códigos detectores-correctores de errores,* Aportaciones Matemáticas, Comunicaciones 7, Soc. Mat. Mex. (1990).

[14] Rentería, C., Tapia-Recillas, H. *A class of binary codes associated with graphs*, C. Numerantium, vol.76, 231-242, (1990).

[15] Rentería, C., Tapia-Recillas, H. *A hyperelliptic code which is a lifting of a BCH code*, To appear in M. Hall Memorial Conference (Wiley Pub.).

[16] Rentería, C., Tapia-Recillas, H. *Curvas Algebraicas y Teoría de Códigos*, Reporte de Investigación, Dpto. Matemáticas, UAM-I, (1989).

[17] Shannon, C.E. *A mathematical theory of communications*, Bell Syst. Tech. J. 27, 379-423, (1948).

[18] Sloane, N. *Error-correcting codes and invariant theory*, Amer. Math. Monthly 84, 82-107, (1977).

[19] Tolimieri, R. *The algebra of the finite Fourier transform and coding theory*, AMS Transactions, 287, 253-273, (1985).

[20] van Lint, J.H., van der Geer, G. *Introduction to Coding Theory and Algebraic Geometry*, DVM Seminar Band 12, Birkhäuser Verlag, 1988.