Mixba'al,
Revista Metropolitana de Matemáticas.
Vol.13, No.1, páginas 95-98.
Recibido 1-06-2022. Aceptado 29-07-2022.
www.doi.org/10.24275/uami/dcbi/mix/v13n1/hotav

DIAGONALIZACIÓN DE MATRICES CIRCULANTES POR MEDIO DE LA TRANSFORMADA DISCRETA DE FOURIER SOBRE CAMPOS FINITOS

HORACIO TAPIA-RECILLAS Y ARMANDO VELAZCO-VELAZCO

Resumen. Por medio de la Transformada Discreta de Fourier (TDF) se diagonalizan matrices circulantes sobre campos finitos.

1. Introducción

La Transformada de Fourier, (TF) (y sus variantes), es una de las transformadas más usadas la cual tiene aplicaciones en varias áreas del conocimiento incluyendo comunicaciones, astronomía, geología, óptica, ingeniería médica; en diversos aspectos como son el procesamiento de señales e imágenes, diseño de antenas, teléfonos celulares, localización de reservas de hidrocarburos, procesamiento de datos, entre otras aplicaciones. Desde el punto de vista matemático también es una herramienta muy importante. Clásicamente la TF se ha tratado sobre el campo de los números complejos, pero desde hace algún tiempo ha surgido la Transformada Discreta de Fourier (TDF), particularmente por el uso de estructuras finitas como son los campos finitos. Las matrices circulantes ([2]) también tienen varias aplicaciones incluyendo teoría de gráficas (Paley), procesamiento digital de imágenes, y teoría de códigos particularmente con códigos cíclicos ([4]).
Es conocido que en el caso clásico, i.e., sobre el campo de los números complejos, las matrices circulantes se pueden diagonalizar por medio de la TDF ([1], [5]). El propósito principal de esta nota es ver que por medio de la TDF también se pueden diagonalizar las matrices circulantes sobre campos finitos. La nota se divide en 4 secciones: en la segunda sección se recordarán conceptos básicos sobre la TDF. La TDF definida sobre campos finitos se aborda en la sección 3, y en la sección 4 se da el resultado principal de esta nota (Teorema 1).

2. La Transformada de Fourier (TF)

En esta sección se recordarán resultados que aparecen en la literatura los cuales serán necesarios más adelante. Para detalles el lector puede consultar, por ejemplo, [1], [7].

Sea $\mathbb{F}$ un campo, que puede ser finito con $q = p^r$ elementos, p primo, o los números complejos $\mathbb{C}$. Sea σ la permutación actuando sobre un vector renglón moviendo las coordenadas un lugar a la derecha, i.e., $\sigma(c_1, c_2, ..., c_n) = (c_n, c_1, ..., c_{n-1})$. La permutación σ^k indica aplicar σ k veces con $0 \leq k \leq n-1$. Obsérvese que $\sigma^0 = Id = \sigma^n$.

Una matriz $n \times n$ sobre $\mathbb{F}$ es circulante ([2]) si sus renglones se obtienen del primer renglón aplicando consecutivamente la permutación σ al renglón obtenido previamente. Así una matriz circulante es:

$$M = (m, \sigma(m), \sigma^2(m), ..., \sigma^{n-1}(m))^t$$

donde m es el primer renglón de la matriz M y X^t es la matriz transpuesta.

2010 *Mathematics Subject Classification.* 42A38, 15B33, 12E20, 11T06.
Palabras clave. Transformada Discreta de Fourier, matrices circulantes, campos finitos .

Sea C el conjunto de las matrices circulantes $n \times n$ sobre $\mathbb{F}$. Es fácil ver que con la suma y producto usual de matrices y multiplicación por escalares, este conjunto es una $\mathbb{F}$-álgebra de dimensión n. Si M es una $n \times n$ matriz circulante y $(m_{11}, m_{12}, ..., m_{1n})$ es el primer renglón de M se usará la notación $M = circ(m_{11}, m_{12}, ..., m_{1n})$.

Sea $J = circ(0, 1, 0, ..., 0) \in C$ y sea $H = \langle J \rangle$ el grupo cíclico generado por J, el cual claramente es de orden n. Sea $\mathbb{F}(H)$ el álgebra de grupo generada por H sobre el campo $\mathbb{F}$, i.e,

$$\mathbb{F}(H) = \{a_0 + a_1 J + \cdots + a_{n-1} J^{n-1},\ a_i \in \mathbb{F}\}.$$

Se puede ver que el álgebra de las matrices circulantes y esta álgebra de grupo son el mismo objeto: $C = \mathbb{F}(H)$. Obsérvese que $\mathbb{F}(H)$ se puede ver como las funciones de H en $\mathbb{F}$:

$$\mathbb{F}(H) = \{f : H \longrightarrow \mathbb{F},\ f \ \text{ función}\}.$$

Sea G un grupo finito abeliano y $\hat{G} = Hom(G, \mathbb{S}^1)$, i.e., el conjunto de homomorfismos del grupo G en el círculo unitario complejo $\mathbb{S}^1$. Se puede ver que este conjunto es un grupo llamado el grupo de caractéres de G. Este grupo tiene varias propiedades entre las que se encuentran que $\hat{G}$ y G son isomorfos ([7]).

Estamos ahora en la situación de recordar la definición de la Transformada de Fourier sobre el campo de los números complejos [7]:

$$F : \mathbb{C}(G) \longrightarrow \mathbb{C}(\hat{G}),\ F_f(\chi) = \sum_{g \in G} f(g)\overline{\chi(g)},$$

donde la barra indica conjugación compleja.

3. La TDF sobre campos finitos

Antes de recordar la TDF sobre campos finitos, introduzcamos otra estructura algebraica. Sea $\mathbb{F}_q$ un campo finito con q elementos y sea

$$R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle = \{a_0 + a_1 x + \cdots + a_{n-1} x^{n-1},\ a_i \in \mathbb{F}_q\}.$$

Es decir, R_n es el conjunto de polinomios con coeficientes en $\mathbb{F}_q$ de grado a lo más n, Este conjunto con la suma usual de polinomios, el producto de polinomios usual reducido módulo $x^n - 1$ y la multiplicación natural por escalares, es también una $\mathbb{F}_q$-álgebra. Por medio de la representación polinomial se puede ver que los $\mathbb{F}_q$-espacios vectoriales $\mathbb{F}_q^n$ y R_n son isomorfos:

$$P : \mathbb{F}_q^n \longrightarrow R_n,$$

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

No es difícil ver que R_n es isomorfo al álgebra de matrices circulantes C.

Para definir la Transformada Discreta de Fourier sobre un campo finito, sea $\alpha \in \mathbb{F}_q^*$ un elemento fijo de orden n primo relativo con q y sea $\langle \alpha \rangle$ el grupo cíclico generado por α.

La Transformada Discreta de Fourier $F : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$, se define como:

$$F(a_0, a_1, ..., a_{n-1}) = ev_{\langle \alpha \rangle}(a(x)) = (a(1), a(\alpha), ..., a(\alpha^{(n-1)})),$$

donde $a(x)$ es el elemento de R_n correspondiente a $(a_0, a_1, ..., a_{n-1})$ y $a(\alpha^j) = a_0 + a_1\alpha^j + \cdots + a_{n-1}\alpha^{j(n-1)}$. Esta transformada tiene varias propiedades incluyendo

el hecho que es una transformación $\mathbb{F}_q$-lineal. La matriz asociada a F con respecto a la base canónica es:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha & \cdots & \alpha^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{n-1} & \cdots & \alpha^{(n-1)(n-1)} \end{pmatrix}$$

Esta matriz es de tipo Vandermonde, la cual en particular es invertible. Para determinar la matriz inversa se supondrá que los enteros n y q son primos relativos. La matriz inversa es:

$$\frac{1}{n}\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \alpha^{-1} & \cdots & \alpha^{-(n-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{-(n-1)} & \cdots & \alpha^{-(n-1)(n-1)} \end{pmatrix}$$

La transformación lineal asociada a esta última matriz es la inversa de la TDF:

$$F^{-1} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n,\ F^{-1}(A) = ev_{\langle \alpha^{-1} \rangle}(A(x)) = a = (a_0, a_1, ..., a_{n-1})$$

$$= \frac{1}{n}(A(1), A(\alpha^{-1}), ..., A(\alpha^{-(n-1)})),$$

donde $A(x) = A_0 + A_1 x + \cdots + A_{n-1}x^{n-1}$ y $a_j = A(\alpha^{-j}) = \frac{1}{n}\sum_{i=0}^{n-1} \alpha^{-ij} A_i$.

En teoría de códigos lineales a la TDF se le conoce como polinomio de Mattson-Solomon y es usada para estudiar el peso de Hamming de los códigos ([4]).

La discussión anterior se ilustrará con un ejemplo. Sea $q = 5$, $\alpha = 2 \in \mathbb{F}_5$. Se puede ver fácilmente que $n = 4$, i.e, $\alpha^4 = 1$, el grupo $\langle \alpha \rangle = \{1, 2, 4, 8 = 3\}$ y $\langle \alpha^{-1} \rangle = \{1, 3, 4, 2\}$.

La matriz asociada a la TDF es:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix},$$

y su inversa:

$$M^{-1} = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} \\ 1 & \alpha^{-2} & \alpha^{-4} & \alpha^{-6} \\ 1 & \alpha^{-3} & \alpha^{-6} & \alpha^{-9} \end{pmatrix}.$$

4. La TDF y matrices circulantes

En esta sección se demuestra que las matrices circulantes sobre un campo finito se pueden diagonalizar por medio de la TDF.

Recordemos que una matriz circulante $A = circ(a_0, a_1, ..., a_{n-1})$ está asociada con el elemento $a = (a_0, a_1, ..., a_{n-1}) \in \mathbb{F}_q^n$ el cual a su vez esta asociado al polinomio $a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} \in R_n$. De esta manera se puede hablar indistintamente de la matriz circulante, el vector o el polinomio asociado. Con la notación anterior se tiene el siguiente,

Teorema 1. *Sea A una matriz circulante, M la matriz asociada a la TDF y M^{-1} su inversa. Entonces,*

$$M^{-1}AM = D$$

donde D es una matriz diagonal.

Demostración. Dado que una matriz circulante A es un elemento del álgebra de grupo $\mathbb{F}_q(J)$, i.e., $A = b_0 I + b_1 J + \cdots + b_{n-1}J^{n-1}$ con $b_j \in \mathbb{F}_q$ y $J = circ(0, 1, 0, ...0)$, por linealidad es suficiente probar el resultado para $A = J$. En este caso se afirma que $M^{-1}JM = diag(1, \alpha, \alpha^2, ..., \alpha^{n-1})$. Probar esta relación es equivalente a ver que,

$$JM = Mdiag(1, \alpha, \alpha^2, ..., \alpha^{n-1}).$$

Primero obsérvese que la operación JM hace un corrimiento hacia arriba a los renglones de la matriz M y la operación $Mdiag((1, \alpha, \alpha^2, ..., \alpha^{n-1})$ también hace un corrimiento hacia arriba a los renglones de la matriz M. El último renglón $(\alpha^n, \alpha^{2n}, ..., \alpha^{(n-1)n}) = (1, 1, ..., 1)$ dado que $\alpha^n = 1$, con lo cual queda probada la afirmación. □

A continuación se ilustra este resultado con un ejemplo, para lo cual tomaremos el caso introducido anteriormente donde $\alpha = 2$. En este caso $J = circ(0, 1, 0, 0)$ y se tiene:

$$JM = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

y

$$Mdiag(1, \alpha, \alpha^2, \alpha^3) = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Tomando en cuenta que $\alpha^4 = 1$, ambas matrices son iguales.

AGRADECIMIENTOS. Los autores expresan su gratitud a CONACyT (#764803) y a la Universidad Autónoma Metropolitana-I el apoyo brindado. Agradecemos al árbitro sus sugerencias y comentarios.

Referencias

[1] Arveson W., A Short Course on Spectral Theory, Springer-Verlag (Graduate Texts in Mathematics 209), (2002)
[2] Davis P.J. *Circulant Matrices.* Wiley-Interscience, N.Y, (1979).
[3] Discrete Fourier Transform, Wikipedia.
[4] MacWilliams, F.J. and Sloane, N.J.A. *The Theory of Error-Correcting Codes.* New York: Elsevier/North Holland, 1977.
[5] Márquez-Martínez A.C. y Quezada R. El espectro de Gelfand del álgebra circulante, MIXBA'AL Rev. Met. de Mat., Vol. IX, 2018, 7-12.
[6] Tapia-Recillas, H. *Análisis de Fourier Discreto y Teoría de códigos.* 6^0 Coloquio del Departamento de Matemáticas de la UAM-I, (2014).
[7] Terras, A. *Fourier analysis on Finite groups and Applications.* London Math. Soc., Student Text 43, (1999).

Horacio Tapia Recillas,
Armando Velazco Velazco.
Universidad Autónoma Metropolitana,
Unidad Iztapalapa,
División de Ciencias Básicas e Ingeniería,
Departamento de Matemáticas.
Avenida Ferrocarril San Rafael Atlixco, número186
Colonia Leyes de Reforma 1^A Sección, Alcaldía Iztapalapa,
C.P.09340, CDMX, México.
e-mail: `htr@xanum.uam.mx, oczalevaj@gmail.com`