Revista Integración
Escuela de Matemáticas
Universidad Industrial de Santander
Vol. 23, No. 2, 2005, pág. 15–39

La estructura algebraica del espacio de señales unidimensionales

Marlio Paredes* Domingo Rodríguez**
Jorge Villamizar–Morales**

Resumen. En este trabajo se describe la estructura matemática del espacio de señales unidimensionales usado en el procesamiento de señales. Se muestra cómo este espacio admite estructura de álgebra y se presentan varios de los operadores que actúan sobre el espacio que son usados en el procesamiento de señales. Particularmente se muestra que las matrices de todos estos operadores son matrices circulantes.

1. Introducción

La idea de este trabajo es dar una formulación inicial de un marco teórico de álgebra de señales, en el caso de señales unidimensionales, para el modelamiento y simulación del procesamiento de las mismas.

Uno de los propósitos al formular dicho ambiente algebraico es poder traducirlo fácilmente en un ambiente computacional que permita plantear nuevas metodologías para el estudio de algunas aplicaciones tales como el fenómeno de la interferometría (ver [4]).

Existen varios antecedentes para este tipo de trabajo, por ejemplo D'Alotto, Giardina y Luo en [1] presentan un moderno enfoque para el procesamiento de señales basado en una fuerte formulación matemática. Ritter y Wilson en [11] desarrollan el álgebra de imágenes como una teoría matemática referida a la transformación y análisis de imágenes. En el libro de Rodríguez [12] se hace una presentación matemática de las señales, presentando conceptos y teoremas sobre señales muy interesantes. El

Palabras y frases claves: espacio de señales, convolución cíclica, correlación cíclica, matrices circulantes.

MSC2000: Primaria: 94A12. Secundaria: 94A08, 94A15.

* Escuela de Matemáticas, Universidad Industrial de Santander, Bucaramanga, Colombia, A.A. 678, *e-mail*: marlio@ciencias.uis.edu.co. Parcialmente financiado por la Vicerrectoría de Investigaciones de la Universidad Industrial de Santander.

** Automated Information Processing Laboratory, Electrical and Computer Engineering Department, University of Puerto Rico at Mayagüez, Mayagüez, PR 00681–9042, USA, *e-mail*: domingo@ece.uprm.edu, jorge.villamizar@ece.uprm.edu. Parcialmente financiado por NSF Grant No. CNS0424546.

presente trabajo está inspirado en el libro de Rodríguez y busca construir una teoría matemática del espacio de señales unidimensionales que pueda ser usada posteriormente para aplicaciones prácticas. En trabajos posteriores estudiaremos el espacio de señales bidimensionales, así como señales con dimensiones superiores.

Se muestra aquí que el espacio de señales es un álgebra con las operaciones binarias de la convolución cíclica y el producto de Hadamard. El principal resultado de este artículo establece que la transformada de Fourier discreta es un isomorfismo de álgebras entre $(l^2(\mathbb{Z}_N), \circledast_N)$, el álgebra de señales unidimensionales con la convolución cíclica, y el mismo espacio de señales unidimensionales con el producto de Hadamard $(l^2(\mathbb{Z}_N), \odot_N)$.

Inicialmente presentamos algunos preliminares matemáticos que podrían ser considerados muy elementales, pero con los cuales pretendemos que el artículo sea autocontenido; esperamos que este trabajo sirva como documento de estudio para estudiantes interesados en estos temas.

2. Preliminares

Esta sección tiene por objeto presentar algunos conceptos matemáticos básicos para el entendimiento de este trabajo.

2.1. Señales

Definición 2.1. Una función cuyo dominio sea un conjunto discreto será llamada una función discreta. En este trabajo llamaremos señal discreta a toda función discreta.

Ejemplo 2.2. El conjunto de los números enteros $\mathbb{Z}$ es un conjunto discreto. Definimos la señal coseno discreta como

$$\begin{array}{rccl} x: & \mathbb{Z} & \longrightarrow & \mathbb{R} \\ & n & \longmapsto & x[n] = \cos\left[2\pi f_0 n T_s\right], \end{array} \tag{1}$$

donde $f_0 \in \mathbb{R}$ es la frecuencia fundamental de la señal y $T_s \in \mathbb{R}$ es la región o periodo fundamental de la señal. Se acostumbra usar paréntesis cuadrados para encerrar los valores del dominio de una señal discreta.

El conjunto

$$\mathbb{Z}_N = \{0, 1, 2, \ldots, N-1\} \tag{2}$$

será llamado conjunto finito de indexación.

Definición 2.3. Una función cuyo codominio sea un conjunto finito discreto será llamada una señal digital.

Ejemplo 2.4. El siguiente es un ejemplo de una señal digital continua

$$\begin{array}{rccl} \mu: & \mathbb{R} & \longrightarrow & \{0,1\} \\ & t & \longmapsto & \mu[t] = \begin{cases} 1, & t \geq 0 \\ 0, & t < 0. \end{cases} \end{array} \tag{3}$$

Ejemplo 2.5. Un ejemplo de una señal digital discreta es

$$\begin{array}{rccc} y: & \mathbb{Z} & \longrightarrow & \mathbb{Z}_N \\ & k & \longmapsto & y[k] = \langle k \rangle_N , \end{array} \tag{4}$$

donde $\langle k \rangle_N$ es el resto que resulta de dividir k entre N. En algunas ocasiones, cuando se entienda qué valor de N estamos usando, escribiremos simplemente $\langle k \rangle$.

2.2. Un poco de álgebra

Definición 2.6. Se dice que un conjunto no vacío G forma un grupo si en G está definida una operación binaria $\star$ tal que se satisfacen las siguientes propiedades:

1. $a \star b \in G$, para cualesquiera $a, b \in G$.
2. $a \star (b \star c) = (a \star b) \star c$, para cualesquiera $a, b, c \in G$.
3. Existe un único elemento $e \in G$, llamado elemento identidad, tal que para todo $a \in G$, $a \star e = e \star a = a$.
4. Para cada $a \in G$, existe un único elemento $b \in G$ tal que $a \star b = b \star a = e$.

Si además, para cualesquiera $a, b \in G$ se tiene que $a \star b = b \star a$, entonces se dice que G es un grupo abeliano o conmutativo. En los ejemplos más conocidos de grupos la operación correspondiente puede ser suma o producto, caso en el cual se usan los símbolos usuales, es decir $+$ y $\cdot$ respectivamente.

Definición 2.7. Se dice que un subconjunto H de un grupo G es un subgrupo de G si con respecto a la operación en G, H mismo forma un grupo.

Ejemplo 2.8. El conjunto de los números reales $\mathbb{R}$ forma un grupo con la operación de suma usual, y en este caso el elemento identidad es el número cero. El conjunto de los números $\mathbb{R} - \{0\}$ forma un grupo con la operación de multiplicación usual y en este caso el elemento identidad es el número uno. Similarmente, el conjunto de los números complejos $\mathbb{C} - \{0\}$ es un grupo con la multiplicación usual en los números complejos; el elemento identidad en este caso es el número uno. Claramente, $\mathbb{R} - \{0\}$ es un subgrupo de $\mathbb{C} - \{0\}$.

Definición 2.9. Sea R un conjunto no vacío. Se dice que R es un anillo si en él se tienen definidas dos operaciones, denotadas por $+$ y $\cdot$, respectivamente, tales que para cualesquiera $a, b, c \in R$ se satisfacen las siguientes propiedades

1. $a + b \in R$.
2. $a + b = b + a$.
3. $(a + b) + c = a + (b + c)$.
4. Existe un único elemento $0 \in R$ tal que, para todo $a \in R$, $a + 0 = 0 + a = a$.

5. Para todo $a \in R$, existe un único elemento $(-a) \in R$ tal que $a + (-a) = 0$.

6. $a \cdot b \in R$.

7. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

8. $a \cdot (b + c) = a \cdot b + a \cdot c$ y $(a + b) \cdot c = a \cdot c + b \cdot c$.

Si además existe un elemento $1 \in R$ tal que, para todo $a \in R$, $a \cdot 1 = 1 \cdot a = a$, R es llamado un anillo con elemento unitario. Si la multiplicación en R es tal que para cualesquiera $a, b \in R$ se cumple que $a \cdot b = b \cdot a$, se dice que R es un anillo conmutativo.

Ejemplo 2.10. El conjunto $\mathbb{Z}$ de los números enteros con las operaciones usuales de adición y multiplicación es un anillo conmutativo con elemento unitario.

Ejemplo 2.11. Considere el conjunto R de todos números enteros pares con las operaciones usuales de adición y multiplicación. R es un anillo conmutativo, pero sin elemento unitario.

Definición 2.12. Un campo o cuerpo es un anillo conmutativo con elemento unitario, tal que cada elemento diferente de cero tiene un inverso multiplicativo.

Los números complejos $\mathbb{C}$ y los números reales $\mathbb{R}$ son ejemplos bien conocidos de campos.

Veamos un ejemplo más interesante. Consideremos el conjunto de los números enteros y definamos la siguiente relación: "Sean m un entero positivo y $a, b \in \mathbb{Z}$. Decimos que a es congruente con b módulo m si y solo si $b - a$ es un múltiplo de m". Simbólicamente esto se escribe como

$$a \equiv b \pmod{m}. \tag{5}$$

Decir que dos números a y b son congruentes módulo m es equivalente a decir que ellos dejan el mismo residuo al dividir por m.

Llamamos clase residual de n, y la denotamos por $\underline{n}$, al conjunto formado por todos los números enteros que son congruentes con n módulo m. Por ejemplo, para $m = 4$, las clases residuales módulo 4 son:

$$\begin{array}{rcl} \underline{0} & = & \{\ldots, -8, -4, 0, 4, 8, \ldots\}, \\ \underline{1} & = & \{\ldots, -7, -3, 1, 5, 9, \ldots\}, \\ \underline{2} & = & \{\ldots, -6, -2, 2, 6, 10, \ldots\}, \\ \underline{3} & = & \{\ldots, -5, -1, 3, 7, 11, \ldots\}. \end{array}$$

Así, el conjunto de todas las clases residuales módulo 4 es $\{\underline{0}, \underline{1}, \underline{2}, \underline{3}\}$. Por ejemplo, $\underline{47} = \underline{-1} = \underline{3}$.

En general, hay m clases residuales módulo m. Denotamos el conjunto de todas las clases residuales módulo m por $\mathbb{Z}_m$:

$$\mathbb{Z}_m = \{\underline{0}, \underline{1}, \underline{2}, \ldots, \underline{m-1}\}. \tag{6}$$

Si $\underline{a}$ y $\underline{b}$ son dos clases residuales módulo m, definimos las operaciones de suma $\oplus$ y multiplicación $\otimes$ por

$$\begin{array}{rcl} \underline{a} \oplus \underline{b} & = & \underline{a+b}, \\ \underline{a} \otimes \underline{b} & = & \underline{ab}. \end{array} \tag{7}$$

Si p es un entero positivo primo, entonces con estas operaciones se puede ver que $\mathbb{Z}_p$ es un campo.

Definición 2.13. Se dice que un conjunto no vacío V es un espacio vectorial sobre un campo F si V es un grupo abeliano respecto a una operación que denotamos por $+$, y tal que para todo $\alpha \in F$ y todo $v \in V$, está definido un elemento $\alpha v \in V$ con las siguientes propiedades:

1. $\alpha(v+w) = \alpha v + \alpha w$; $\alpha \in F$ y $v, w \in V$.
2. $(\alpha+\beta)v = \alpha v + \beta v$; $\alpha, \beta \in F$ y $v \in V$.
3. $\alpha(\beta v) = (\alpha\beta)v$; $\alpha, \beta \in F$ y $v \in V$.
4. $1v = v$, $v \in V$.

El producto αv de los elementos del campo F con los elementos del espacio vectorial V es llamado producto por escalar. Los elementos de un espacio vectorial son llamados vectores.

Como un ejemplo de espacio vectorial podemos considerar el espacio F^n de todas las n-uplas con componentes en F, es decir

$$F^n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) : \alpha_i \in F, \text{ para } i = 1, 2, \ldots, n\}. \tag{8}$$

Este es un espacio vectorial sobre F y las operaciones correspondientes son

1. Suma: $(\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n)$,
2. Producto por escalar: $\alpha(\beta_1, \beta_2, \ldots, \beta_n) = (\alpha\beta_1, \alpha\beta_2, \ldots, \alpha\beta_n)$.

Los espacios vectoriales usados en este trabajo son del tipo en que el campo de escalares son los números reales o los números complejos. Estos espacios serán llamados, respectivamente, espacios vectoriales reales y espacios vectoriales complejos.

Definición 2.14. Un subconjunto W de un espacio vectorial V es llamado un subespacio vectorial de V si el mismo W también es un espacio vectorial bajo las operaciones de suma y multiplicación por escalar definidas en V.

Definición 2.15. Sea V un espacio vectorial sobre el campo F, y sean $v_0, \ldots, v_{n-1}$ vectores en V. Entonces un vector $\overline{v} \in V$ es llamado una combinación lineal de los vectores v_i si puede expresarse en la forma

$$\overline{v} = \alpha_0 v_0 + \alpha_1 v_1 + \ldots + \alpha_{n-1} v_{n-1} \; = \; \sum_{i=0}^{n-1} \alpha_i v_i, \qquad \alpha_i \in F. \tag{9}$$

Si $u_1, u_2, \ldots, u_k$ son vectores en un espacio vectorial V, entonces el conjunto formado por todas las combinaciones lineales de los u_i es un subespacio vectorial de V. Este subespacio lo denotaremos por $\text{gen}\{u_1, u_2, \ldots, u_k\}$, y lo llamaremos el subespacio generado por los vectores $u_1, u_2, \ldots, u_k$. Entonces,

$$\text{gen}\{u_1, u_2, \ldots, u_k\} = \{\alpha_1 u_1 + \ldots + \alpha_k v_k : \alpha_i \in F,\ u_i \in V,\ i = 1, 2, \ldots, k\}. \quad (10)$$

Definición 2.16. Sean $v_0, v_1, \ldots, v_{n-1}$ elementos de un espacio vectorial V sobre un campo F. Decimos que los vectores $v_0, v_1, \ldots, v_{n-1}$ son linealmente independientes, si y sólo si, la ecuación

$$\alpha_0 v_0 + \alpha_1 v_1 + \ldots + \alpha_{n-1} v_{n-1} = 0 \quad (11)$$

implica que $\alpha_i = 0$, para todo $i = 0, 1, 2, \ldots, n-1$.

Definición 2.17. Sea V un espacio vectorial y $B = \{v_0, v_1, \ldots, v_{n-1}\}$ un conjunto de vectores en V. Entonces, B es llamado una base para V si es linealmente independiente y además genera a V.

Por ejemplo, para el espacio vectorial F^n definido en la ecuación (8), una base natural que podemos considerar es el conjunto

$$\{e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)\}.$$

Esta base es llamada la base canónica para F^n.

Un hecho relativamente fácil de probar es que el número de elementos de una base de un espacio vectorial es un invariante. Es decir, que si tenemos dos bases distintas $\{v_1, v_2, \ldots, v_k\}$ y $\{u_1, u_2, \ldots, u_m\}$ de un espacio vectorial V dado, entonces $k = m$. Por esta razón, el número de elementos de una base de un espacio vectorial es llamado la dimensión del espacio. Así, por ejemplo, la dimensión del espacio F^n es n.

Definición 2.18. Sean V y W espacios vectoriales sobre un campo F. Una transformación lineal u homomorfismo de V en W es una función $T\colon V \to W$ tal que

1. $T(v_1 + v_2) = T(v_1) + T(v_2)$,
2. $T(\alpha v_1) = \alpha T(v_1)$,

para todo $v_1, v_2 \in V$ y todo $\alpha \in F$. Si T es inyectiva se dice que T es un monomorfismo; si es sobreyectiva se dice que es un epimorfismo, y si es biyectiva es llamada un isomorfismo.

El conjunto de todos los homomorfismos entre los espacios V y W es simbolizado por $\text{Hom}(V, W)$. Este conjunto tiene estructura de espacio vectorial y las operaciones correspondientes son la suma de funciones y el producto por un escalar (elementos de F). Más precisamente, estas operaciones se definen por

1. $(T_1 + T_2)v = T_1(v) + T_2(v)$, donde $T_1, T_2 \in \text{Hom}(V, W)$ y $v \in V$.
2. $(\alpha T)v = \alpha(T(v))$, para $T \in \text{Hom}(V, W)$, $\alpha \in F$ y $v \in V$.

Definición 2.19. Un álgebra sobre un campo F es un espacio vectorial V sobre F con una operación adicional, llamada multiplicación de vectores, la cual asocia a cada par de vectores $v_0, v_1 \in V$ un vector $v_0 \cdot v_1 \in V$ llamado el producto de v_0 y v_1. Esta nueva operación en V debe cumplir las siguientes propiedades para cualesquiera $v_0, v_1, v_2 \in V$ y todo $\alpha \in F$:

1. $v_0 \cdot (v_1 \cdot v_2) = (v_0 \cdot v_1) \cdot v_2$.

2. $v_0 \cdot (v_1 + v_2) = v_0 \cdot v_1 + v_0 \cdot v_2$ y $(v_0 + v_1) \cdot v_2 = v_0 \cdot v_2 + v_1 \cdot v_2$.

3. $\alpha(v_0 \cdot v_1) = (\alpha v_0) \cdot v_1 = v_0 \cdot (\alpha v_1)$.

Sí existe un elemento 1 en V tal que $1 \cdot v_0 = v_0 \cdot 1 = v_0$, para todo vector $v_0 \in V$, entonces V es llamado un álgebra con unidad sobre F, y 1 es llamado el elemento identidad de V. Se dice que el álgebra V es conmutativa si $v_0 \cdot v_1 = v_1 \cdot v_0$, para todo $v_0, v_1 \in V$.

Un ejemplo sencillo de álgebra es el mismo campo F, el cual es un álgebra conmutativa.

El conjunto de todas las matrices $n \times n$, con entradas en un campo F, es un espacio vectorial sobre F con la operaciones de suma de matrices y multiplicación por escalar usuales. El producto de matrices usual convierte este espacio vectorial en un álgebra no conmutativa para $n \geq 2$.

El conjunto de todos los homomorfismos de un espacio vectorial V en sí mismo, $\mathrm{Hom}(V, V)$, es un álgebra con identidad, y la operación correspondiente es la composición de funciones. Más precisamente, la operación se define para cada par de elementos en $\mathrm{Hom}(V, V)$ así:

$$(T_1 \circ T_2)v = T_1(T_2(v)), \qquad T_1, T_2 \in \mathrm{Hom}(V, V).$$

El elemento identidad de esta álgebra es la transformación idéntica.

Definición 2.20. Sea F un campo y sean V y W dos álgebras sobre F. Un isomorfismo entre las álgebras V y W es una función biyectiva $T\colon V \to W$ tal que:

1. $T(\alpha_1 v_1 + \alpha_2 v_2) = \alpha_1 T(v_1) + \alpha_2 T(v_2)$,

2. $T(v_1 \cdot v_2) = T(v_1) \cdot T(v_2)$,

para cualesquiera $v_1, v_2 \in V$ y cualesquiera $\alpha_1, \alpha_2 \in F$.

Obsérvese que la primera condición nos dice que un isomorfismo de álgebras es un isomorfismo de espacios vectoriales que, adicionalmente, preserva productos.

2.3. Matrices circulantes

Definición 2.21. Una matriz circulante de orden N es una matriz $N \times N$ de la forma

$$C_N = \begin{bmatrix} C_0 & C_1 & \cdots & C_{N-1} \\ C_1 & C_2 & \cdots & C_0 \\ \vdots & \vdots & \ddots & \vdots \\ C_{N-2} & C_{N-1} & \cdots & C_{N-3} \\ C_{N-1} & C_0 & \cdots & C_{N-2} \end{bmatrix}. \tag{12}$$

Obsérvese que las entradas de cada columna son exactamente iguales a las de la columna anterior, solo que desplazadas una posición hacia arriba y además circuladas.

También puede suceder que la entradas de la matriz circulen hacia abajo; en este caso la matriz tiene la forma

$$H_N = \begin{bmatrix} H_0 & H_{N-1} & \cdots & H_1 \\ H_1 & H_0 & \cdots & H_2 \\ \vdots & \vdots & \ddots & \vdots \\ H_{N-2} & H_{N-3} & \cdots & H_{N-1} \\ H_{N-1} & H_{N-2} & \cdots & H_0 \end{bmatrix}.$$

En este trabajo también se usan matrices de bloques circulantes con bloques circulantes, las cuales representamos en la forma

$$C_N = \begin{bmatrix} C_{[0]} & C_{[1]} & \cdots & C_{[N-1]} \\ C_{[1]} & C_{[2]} & \cdots & C_{[0]} \\ \vdots & \vdots & \ddots & \vdots \\ C_{[N-2]} & C_{[N-1]} & \cdots & C_{[N-3]} \\ C_{[N-1]} & C_{[0]} & \cdots & C_{[N-2]} \end{bmatrix}, \tag{13}$$

donde cada entrada $C_{[i]}$ es una matriz circulante. Una referencia muy completa sobre matrices circulantes es el libro de Davis [2].

2.4. La transformada de Fourier discreta

Definición 2.22. Dada una sucesión finita $x[n]$, con $0 \leq n \leq N-1$, la transformada de Fourier discreta de $x[n]$ se define como la sucesión dada por

$$\widehat{x}[k] = \sum_{n=0}^{N-1} x[n] e^{-j2\pi kn/N}, \tag{14}$$

donde $0 \leq k \leq N-1$.

Es común llamar $W_N = e^{-j2\pi/N}$ y escribir la transformada de Fourier discreta de $x[n]$ como

$$\widehat{x}[k] = \sum_{n=0}^{N-1} x[n] W_N^{kn}, \quad 0 \leq k \leq N-1. \tag{15}$$

Para una sucesión finita $y[k]$, con $0 \leq k \leq N-1$, la transformada inversa de Fourier discreta de $y[k]$ está dada por

$$y^{\vee}[n] = \frac{1}{N} \sum_{k=0}^{N-1} y[k] W_N^{-kn}, \quad 0 \leq n \leq N-1. \tag{16}$$

3. El espacio de señales unidimensionales

Definición 3.1. Una señal unidimensional es una función

$$\begin{array}{rccc} x\colon & \mathbb{Z}_N & \longrightarrow & \mathbb{C} \\ & n & \longmapsto & x[n], \end{array} \tag{17}$$

tal que

$$\sum_{n=0}^{N-1} x[n] x^*[n] < \infty. \tag{18}$$

Una forma equivalente de ver una señal es como una sucesión de números complejos $x[0], x[1], \ldots, x[N-1]$. También se acostumbra escribir una señal como un vector columna

$$x = \begin{bmatrix} x[0] \\ x[1] \\ \vdots \\ x[N-1] \end{bmatrix}.$$

Denotaremos por $l^2(\mathbb{Z}_N)$ el espacio de señales unidimensionales. Claramente, este espacio tiene una estructura de espacio vectorial sobre los números complejos con las operaciones usuales de suma de funciones y mutiplicación por escalar.

Una base para el espacio de señales es el conjunto

$$\Delta_N = \{\delta_{\{k\}} : k = 0, 1, \ldots, N-1\}, \tag{19}$$

donde las funciones $\delta_{\{k\}}$ son definidas por

$$\delta_{\{k\}}[j] = \begin{cases} 1, & \text{si } j = k, \\ 0, & \text{si } j \neq k. \end{cases}$$

Esta base es llamada la base estándar para $l^2(\mathbb{Z}_N)$.

Definición 3.2. Definimos la operación de convolución cíclica sobre el espacio de señales unidimensionales como

$$\begin{array}{rccc} \circledast_N\colon & l^2(\mathbb{Z}_N) \times l^2(\mathbb{Z}_N) & \longrightarrow & l^2(\mathbb{Z}_N) \\ & (x, y) & \longmapsto & x \circledast_N y, \end{array} \tag{20}$$

donde $x \circledast_N y$ se define por

$$(x \circledast_N y)[n] = \sum_{k=0}^{N-1} x[k] y[\langle n-k \rangle_N]. \tag{21}$$

La primera observación que debemos hacer es que esta operación es conmutativa, es decir que

$$x \circledast_N y = y \circledast_N x, \tag{22}$$

para todo par de señales $x, y \in l^2(\mathbb{Z}_N)$. Para ver esto, llamemos $m = n - k$ en la ecuación (21); entonces, como $0 \leq n \leq N-1$ se tiene que $-k \leq n-k \leq N-1-k$. Pero como $0 \leq k \leq N-1$ y hay que reducir todo a módulo N, entonces en realidad tenemos que $0 \leq m = n-k \leq N-1$. Por tanto,

$$(x \circledast_N y)[n] = \sum_{k=0}^{N-1} x[k]y[\langle n-k\rangle_N] = \sum_{m=0}^{N-1} y[m]x[\langle n-m\rangle_N] = (y \circledast_N x)[n].$$

Veamos ahora que la convolución cíclica es una operación asociativa. Consideremos entonces tres señales $x, y, z \in l^2(\mathbb{Z}_N)$, y probemos que

$$(x \circledast_N y) \circledast_N z = x \circledast_N (y \circledast_N z). \tag{23}$$

Llamemos $s = x \circledast_N y$ y $t = y \circledast_N z$; entonces,

$$s[n] = (x \circledast_N y)[n] = \sum_{k=0}^{N-1} x[k]y[\langle n-k\rangle_N],$$

y por la conmutatividad podemos escribir

$$t[n] = (y \circledast_N z)[n] = (z \circledast_N y)[n] = \sum_{k=0}^{N-1} z[k]y[\langle n-k\rangle_N].$$

Así tenemos

$$\begin{aligned}((x \circledast_N y) \circledast_N z)[n] &= (s \circledast_N z)[n] = (z \circledast_N s)[n] = \sum_{m=0}^{N-1} z[m]s[\langle n-m\rangle_N] \\ &= \sum_{m=0}^{N-1} z[m] \sum_{k=0}^{N-1} x[k]y[\langle n-m-k\rangle_N],\end{aligned}$$

y similarmente,

$$(x \circledast_N (y \circledast_N z))[n] = (x \circledast_N t)[n] = \sum_{k=0}^{N-1} x[k] \sum_{m=0}^{N-1} z[m]y[\langle n-k-m\rangle_N].$$

Obsérvese que la única diferencia entre la última sumatoria y la anterior es el orden de sumación, y como estas sumas son finitas, podemos intercambiar los órdenes. Por tanto, concluimos que $(x \circledast_N y) \circledast_N z = x \circledast_N (y \circledast_N z)$.

Las dos siguientes propiedades son más sencillas de probar:

1. $x \circledast_N (y+z) = x \circledast_N y + x \circledast_N z$, para $x, y, z \in l^2(\mathbb{Z}_N)$.
2. $\alpha(x \circledast_N y) = (\alpha x) \circledast_N (\alpha y)$, para $\alpha \in \mathbb{C}$ y $x, y \in l^2(\mathbb{Z}_N)$.

De esta forma hemos probado el siguiente resultado:

Teorema 3.3. *El espacio $l^2(\mathbb{Z}_N)$ es un álgebra conmutativa usando la convolución cíclica como multiplicación.*

Vamos ahora a escribir la convolución cíclica en forma de operador sobre el espacio de señales $l^2(\mathbb{Z}_N)$. Consideremos $x, h \in l^2(\mathbb{Z}_N)$ y llamemos $y = x \circledast h$; entonces, si para cada n hacemos la expansión de la sumatoria,

$$y[n] = (x \circledast_N h)[n] = \sum_{k=0}^{N-1} x[k]h[\langle n-k\rangle_N],$$

obtenemos

$$\begin{aligned}
y[0] &= x[0]h[0] + x[1]h[N-1] + x[2]h[N-2] + \cdots + x[N-1]h[1],\\
y[1] &= x[0]h[1] + x[1]h[0] + x[2]h[N-1] + \cdots + x[N-1]h[2],\\
&\vdots\\
y[N-1] &= x[0]h[N-1] + x[1]h[N-2] + x[2]h[N-3] + \cdots + x[N-1]h[0].
\end{aligned}$$

Si escribimos esto matricialmente tenemos

$$\begin{bmatrix} y[0] \\ y[1] \\ \vdots \\ y[N-1] \end{bmatrix} = \begin{bmatrix} h[0] & h[N-1] & h[N-2] & \cdots & h[1] \\ h[1] & h[0] & h[N-1] & \cdots & h[2] \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ h[N-1] & h[N-2] & h[N-3] & \cdots & h[0] \end{bmatrix} \begin{bmatrix} x[0] \\ x[1] \\ \vdots \\ x[N-1] \end{bmatrix}.$$

Obsérvese que si fijamos h, podemos pensar la convolución cíclica como un operador lineal actuando sobre el espacio de señales, el cual será llamado operador de convolución cíclica. Denotaremos este operador por $\circledast_N^h$ y escribimos

$$\begin{array}{rccl} \circledast_N^h\colon & l^2(\mathbb{Z}_N) & \longrightarrow & l^2(\mathbb{Z}_N) \\ & x & \longmapsto & \circledast_N^h\{x\} = x \circledast_N h, \end{array} \tag{24}$$

y la matriz de este operador es

$$H_N = \begin{bmatrix} h[0] & h[N-1] & h[N-2] & \cdots & h[1] \\ h[1] & h[0] & h[N-1] & \cdots & h[2] \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ h[N-1] & h[N-2] & h[N-3] & \cdots & h[0] \end{bmatrix}. \tag{25}$$

De donde, inmediatamente, observamos que la matriz del operador convolución cíclica es una matriz circulante.

Estudiemos ahora otra operación importante en el espacio de señales, la correlación cíclica.

Definición 3.4. Definimos la operación de correlación cíclica sobre el espacio de señales unidimensionales como

$$\begin{array}{rccl} \circledcirc_N\colon & l^2(\mathbb{Z}_N) \times l^2(\mathbb{Z}_N) & \longrightarrow & l^2(\mathbb{Z}_N) \\ & (x, y) & \longmapsto & x \circledcirc_N y, \end{array} \tag{26}$$

donde $x \circledcirc_N y$ se define por

$$(x \circledcirc_N y)[n] = \sum_{k=0}^{N-1} x[k]y[\langle n+k \rangle_N]. \tag{27}$$

Las siguientes propiedades de la correlación cíclica son sencillas de verificar:

1. $(x \circledcirc_N y) \circledcirc_N z = x \circledcirc_N (y \circledcirc_N z)$, para $x, y, z \in l^2(\mathbb{Z}_N)$,
2. $x \circledcirc_N (y+z) = x \circledcirc_N y + x \circledcirc_N z$, para $x, y, z \in l^2(\mathbb{Z}_N)$,
3. $\alpha(x \circledcirc_N y) = (\alpha x) \circledcirc_N (\alpha y)$, para $\alpha \in \mathbb{C}$ y $x, y \in l^2(\mathbb{Z}_N)$.

Es decir que el espacio de señales unidimensionales $l^2(\mathbb{Z}_N)$ es un álgebra con la correlación cíclica como multiplicación. Pero no es cierto que la correlación cíclica sea conmutativa. Por ejemplo, si tomamos las siguientes dos señales,

$$x = \begin{bmatrix} x[0] \\ x[1] \\ x[2] \\ x[3] \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ -1 \\ 2 \end{bmatrix} \quad \text{y} \quad y = \begin{bmatrix} y[0] \\ y[1] \\ y[2] \\ y[3] \end{bmatrix} = \begin{bmatrix} -1 \\ 1 \\ 2 \\ 0 \end{bmatrix},$$

calculando directamente la correlación cíclica de estas señales obtenemos

$$x \circledcirc_N y = \begin{bmatrix} -3 \\ -1 \\ 5 \\ 3 \end{bmatrix} \quad \text{y} \quad y \circledcirc_N x = \begin{bmatrix} -3 \\ 3 \\ 5 \\ -1 \end{bmatrix}.$$

Por tanto, el espacio de señales unidimensionales $l^2(\mathbb{Z}_N)$ es un álgebra no conmutativa con la correlación cíclica como multiplicación.

Así como en el caso de la convolución cíclica, la correlación cíclica también se puede ver como un operador sobre el espacio $l^2(\mathbb{Z}_N)$. Para ver esto fijamos una señal $g \in l^2(\mathbb{Z}_N)$, y definimos el operador de correlación cíclica como

$$\begin{array}{rccc} \circledcirc_N^g: & l^2(\mathbb{Z}_N) & \longrightarrow & l^2(\mathbb{Z}_N) \\ & x & \longmapsto & \circledcirc_N^g\{x\} = x \circledcirc_N g. \end{array} \tag{28}$$

Para calcular la matriz C_N del operador correlación cíclica usamos $\Delta_N = \{\delta_{\{k\}} : k = 0, 1, \ldots, N-1\}$ la base estandar de $l^2(\mathbb{Z}_N)$. Entonces,

$$C_N = \left[\circledcirc_N^g\{\delta_{\{0\}}\} \ \circledcirc_N^g\{\delta_{\{1\}}\} \ \ldots \ \circledcirc_N^g\{\delta_{\{N-1\}}\} \right];$$

calculamos cada columna y obtenemos

$$\left(\circledcirc_N^g\{\delta_{\{k\}}\} \right)[n] = \sum_{m=0}^{N-1} \delta_{\{k\}}[m] g[\langle n+m \rangle_N] = g[\langle n+k \rangle_N].$$

Así,

$$\begin{aligned}
\left[\left(\circledcirc_N^g\{\delta_{\{0\}}\}\right)[n]\right] = [g[\langle n\rangle_N]] &= \begin{bmatrix} g[0] \\ g[1] \\ \vdots \\ g[N-2] \\ g[N-1] \end{bmatrix}, \\
\left[\left(\circledcirc_N^g\{\delta_{\{1\}}\}\right)[n]\right] = [g[\langle n+1\rangle_N]] &= \begin{bmatrix} g[1] \\ g[2] \\ \vdots \\ g[N-1] \\ g[0] \end{bmatrix}, \\
&\vdots \\
\left[\left(\circledcirc_N^g\{\delta_{\{n+N-1\}}\}\right)[n]\right] = [g[\langle N-1\rangle_N]] &= \begin{bmatrix} g[N-1] \\ g[0] \\ \vdots \\ g[N-3] \\ g[N-2] \end{bmatrix}.
\end{aligned}$$

Por tanto la matriz del operador de correlación cíclica es

$$C_N = \begin{bmatrix} g[0] & g[1] & g[2] & \cdots & g[N-1] \\ g[1] & g[2] & g[3] & \cdots & g[0] \\ g[2] & g[3] & g[4] & \cdots & g[1] \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ g[N-2] & g[N-1] & g[0] & \cdots & g[N-3] \\ g[N-1] & g[0] & g[1] & \cdots & g[N-2] \end{bmatrix}. \tag{29}$$

Obsérvese que, así como en el caso del operador de convolución cíclica, la matriz del operador de correlación cíclica también es una matriz circulante.

4. Otros operadores y propiedades

El primer operador que estudiamos en esta sección es el operador de reflexión, el cual tiene propiedades muy importantes e interesantes.

Definición 4.1. El operador de reflexión sobre el espacio de señales unidimensionales se define por

$$\begin{array}{rccc} \Re_N\colon & l^2(\mathbb{Z}_N) & \longrightarrow & l^2(\mathbb{Z}_N) \\ & x & \longmapsto & \Re_N\{x\} = x^{(-)}, \end{array} \tag{30}$$

donde

$$(\Re_N\{x\})[k] = x^{(-)}[k] = x[\langle N-k\rangle_N] = x[\langle -k\rangle_N]. \tag{31}$$

Calculemos la matriz R_N del operador de reflexión con respecto a la base estándar, esto es

$$R_N = \left[\Re_N\{\delta_{\{0\}}\} \quad \Re_N\{\delta_{\{1\}}\} \quad \cdots \quad \Re_N\{\delta_{\{N-1\}}\}\right].$$

Ahora,

$$\begin{aligned}
\left[\left(\Re_N\{\delta_{\{0\}}\}\right)[n]\right] = \left[\delta_{\{0\}}\left[\langle -n\rangle_N\right]\right] &= \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \\
\left[\left(\Re_N\{\delta_{\{1\}}\}\right)[n]\right] = \left[\delta_{\{1\}}\left[\langle -n\rangle_N\right]\right] &= \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}, \\
&\vdots \\
\left[\left(\Re_N\{\delta_{\{N-1\}}\}\right)[n]\right] = \left[\delta_{\{N-1\}}\left[\langle -n\rangle_N\right]\right] &= \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.
\end{aligned}$$

Es decir, que la matriz del operador de reflexión es

$$R_N = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \end{bmatrix}, \tag{32}$$

la cual nuevamente vemos que es circulante.

Una interesante propiedad que relaciona la convolución cíclica, la correlación cíclica y el operador de reflexión es la siguiente:

Teorema 4.2. *Si $x, y \in l^2(\mathbb{Z}_N)$, entonces*

$$x \circledcirc_N y = (\Re_N\{x\}) \circledast_N y. \tag{33}$$

Demostración.

$$(x \circledcirc_N y)[n] = \sum_{k=0}^{N-1} x[k]y[\langle n+k\rangle_N];$$

haciendo $m = n + k$ esta suma se convierte en

$$(x \circledcirc_N y)[n] = \sum_{m=n}^{N+n-1} x[m-n]y[m];$$

no escribimos $\langle\ \rangle_N$ para facilitar la escritura, pero se sobrentiende que la igualdad es módulo N. Haciendo la expansión de esta sumatoria, reordenando los términos de la misma, y reduciendo módulo N obtenemos

$$\begin{aligned}
(x \circledcirc_N y)[n] &= x[0]y[n] + x[1]y[n+1] + x[2]y[n+2] + \cdots + \\
&\quad + x[N-n-1]y[N-1] + x[N-n]y[N] + x[N-n+1]y[N+1] \\
&\quad + \cdots + x[N-2]y[N+n-2] + x[N-1]y[N+n-1], \\
&= x[0]y[n] + x[1]y[n+1] + x[2]y[n+2] + \cdots + \\
&\quad + x[N-(n+1)]y[N-1] + x[N-n]y[0] + x[N-(n-1)]y[1] \\
&\quad + \cdots + x[N-2]y[n-2] + x[N-1]y[n-1], \\
&= y[0]x[N-n] + y[1]x[N-(n-1)] + \cdots + y[n-2]x[N-2] + \\
&\quad + y[n-1]x[N-1] + y[n]x[0] + y[n+1]x[1] + y[n+2]x[2] + \\
&\quad + \cdots + y[N-1]x[N-(n+1)].
\end{aligned}$$

De aquí tenemos que

$$\begin{aligned}
(x \circledcirc_N y)[n] &= \sum_{j=0}^{N-1} y[j]x[N-(n-j)], \\
&= \sum_{j=0}^{N-1} y[j](\Re_N\{x\})[n-j], \\
&= (y \circledast_N \Re_N\{x\})[n], \\
&= ((\Re_N\{x\}) \circledast_N y)[n]. \qquad \boxdot
\end{aligned}$$

Definición 4.3. El operador de desplazamiento cíclico sobre el espacio de señales unidimensionales se define por

$$\begin{array}{rccc} \mathscr{S}_N\colon & l^2(\mathbb{Z}_N) & \longrightarrow & l^2(\mathbb{Z}_N) \\ & x & \longmapsto & \mathscr{S}_N\{x\}, \end{array} \tag{34}$$

donde

$$(\mathscr{S}_N\{x\})[n] = x[\langle n+1\rangle_N]. \tag{35}$$

De forma similar a como hemos hecho con los otros operadores, podemos calcular la matriz S_N del operador de desplazamiento cíclico con respecto a la base estándar, y obtenemos

$$S_N = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix}. \tag{36}$$

Definición 4.4. El producto de Hadamard sobre el espacio $l^2(\mathbb{Z}_N)$ de señales unidimensionales se define como

$$\begin{array}{rccc} \odot\colon & l^2(\mathbb{Z}_N) \times l^2(\mathbb{Z}_N) & \longrightarrow & l^2(\mathbb{Z}_N) \\ & (x, y) & \longmapsto & x \odot_N y, \end{array} \tag{37}$$

donde

$$(x \odot_N y)[n] = x[n]\, y[n]. \tag{38}$$

Es decir, que si

$$x = \begin{bmatrix} x[0] \\ x[1] \\ \vdots \\ x[n] \end{bmatrix} \qquad \text{y} \quad y = \begin{bmatrix} y[0] \\ y[1] \\ \vdots \\ y[n] \end{bmatrix},$$

entonces

$$x \odot_N y = \begin{bmatrix} x[0]\, y[0] \\ x[1]\, y[1] \\ \vdots \\ x[n]\, y[n] \end{bmatrix}. \tag{39}$$

Claramente el producto de Hadamard satisface las siguientes propiedades:

1. $x \odot_N y = y \odot_N x$, para todo $x, y \in l^2(\mathbb{Z}_N)$.
2. $x \odot_N (y \odot_N z) = (x \odot_N y) \odot_N z$, para todo $x, y, z \in l^2(\mathbb{Z}_N)$.
3. $x \odot_N (y + z) = x \odot_N y + x \odot_N z$, para todo $x, y, z \in l^2(\mathbb{Z}_N)$.
4. $\alpha(x \odot_N y) = (\alpha x) \odot_N y = x \odot_N (\alpha y)$, para todo $x, y \in l^2(\mathbb{Z}_N)$ y todo $\alpha \in \mathbb{C}$.

Es decir, que el siguiente resultado es verdadero:

Teorema 4.5. *El espacio $l^2(\mathbb{Z}_N)$ de señales unidimensionales es un álgebra con el producto de Hadamard como multiplicación.*

A continuación mostramos una propiedad que relaciona la operación de convolución cíclica y el producto de Hadamard, a través de la transformada de Fourier discreta. Recordemos que si $S \in l^2(\mathbb{Z}_N)$, entonces la transformada de Fourier discreta de S, la cual denotaremos en adelante como $S\widehat{\ }$, está dada por la sucesión

$$S\widehat{\ }[k] = \sum_{n=0}^{N-1} S[n]e^{-j2\pi kn/N} = \sum_{n=0}^{N-1} S[n]W_N^{kn},$$

donde $W_N = e^{-j2\pi/N}$ y $0 \leq k \leq N-1$.

Teorema 4.6. *Si S_0 y S_1 son señales unidimensionales, entonces se cumple que*

$$(S_0 \circledast_N S_1)\widehat{\ } = (S_0)\widehat{\ } \odot_N (S_1)\widehat{\ } \tag{40}$$

Demostración.

$$\begin{aligned}
(S_0 \circledast_N S_1)\widehat{\ }[k] &= \left(\sum_{m=0}^{N-1} S_0[m]S_1[\langle n-m\rangle_N]\right)\widehat{\ }[k], \\
&= \sum_{n=0}^{N-1}\sum_{m=0}^{N-1} S_0[m]S_1[\langle n-m\rangle_N]W_N^{nk}, \\
&= \sum_{m=0}^{N-1} S_0[m] \sum_{n=0}^{N-1} S_1[\langle n-m\rangle_N]W_N^{nk}.
\end{aligned}$$

Si hacemos $p = n - m$, entonces

$$\begin{aligned}
\sum_{n=0}^{N-1} S_1\left[\langle n-m\rangle_N\right] W_N^{nk} &= \sum_{p=-m}^{N-1-m} S_1\left[\langle p\rangle_N\right] W_N^{(p+m)k}, \\
&= \sum_{p=-m}^{N-1-m} S_1\left[\langle p\rangle_N\right] W_N^{pk} W_N^{mk}, \\
&= W_N^{mk} \sum_{p=-m}^{N-1-m} S_1\left[\langle p\rangle_N\right] W_N^{pk}, \\
&= W_N^{mk} \sum_{p=0}^{N-1} S_1[p] W_N^{pk}, \\
&= W_N^{mk} S_1[k].
\end{aligned}$$

Sustituyendo arriba tenemos

$$\sum_{m=0}^{N-1} S_0[m] \sum_{n=0}^{N-1} S_1\left[\langle n-m\rangle_N\right] W_N^{nk} = \sum_{m=0}^{N-1} S_0[m] S_1\left[k\right] W_N^{mk},$$

$$= ((S_0)\widehat{\ }\odot_N (S_1)\widehat{\ })[k]. \qquad \boxtimes$$

Como consecuencia de este teorema podemos deducir que si $S_0, S_1 \in l^2(\mathbb{Z}_N)$, entonces

$$S_0 \circledast_N S_1 = \left[(S_0)\widehat{\ }\odot_N (S_1)\widehat{\ }\right]^{\vee}. \tag{41}$$

Observemos que la transformada de Fourier discreta es un homomorfismo de espacios vectoriales, o, equivalentemente, una transformación lineal del espacio de señales unidimensionales en sí mismo:

$$\begin{array}{rccc} \widehat{\ }: & l^2(\mathbb{Z}_N) & \longrightarrow & l^2(\mathbb{Z}_N) \\ & S & \longmapsto & S\widehat{\ }, \end{array} \tag{42}$$

puesto que cumple las siguientes propiedades:

1. $(S_0 + S_1)\widehat{\ } = (S_0)\widehat{\ } + (S_1)\widehat{\ }$, para todo $S_0, S_1 \in l^2(\mathbb{Z}_N)$.
2. $(\alpha S)\widehat{\ } = \alpha S\widehat{\ }$, para todo $S \in l^2(\mathbb{Z}_N)$ y todo $\alpha \in \mathbb{C}$.

Adicionalmente, la transformada discreta de Fourier es una función inyectiva, puesto que señales distintas tienen transformadas distintas, esto es,

$$S_0 \neq S_1 \Longrightarrow (S_0)\widehat{\ } \neq (S_1)\widehat{\ },$$

y como el espacio $l^2(\mathbb{Z}_N)$ es de dimensión finita, podemos concluir que la transformada discreta de Fourier en realidad es biyectiva. El teorema anterior muestra que la transformada discreta de Fourier es un homomorfismo de álgebras entre $(l^2(\mathbb{Z}_N), \circledast_N)$, el espacio de señales unidimensionales con la operación de convolución cíclica, y $(l^2(\mathbb{Z}_N), \odot_N)$, el espacio de señales unidimensionales con el producto de Hadamard. Por tanto, podemos enunciar el siguiente resultado:

Teorema 4.7. *El espacio de señales unidimensionales con la operación de convolución cíclica $(l^2(\mathbb{Z}_N), \circledast_N)$ es isomorfo como un álgebra al mismo espacio de señales unidimensionales con el producto de Hadamard $(l^2(\mathbb{Z}_N), \odot_N)$.*

Para terminar presentamos a continuación una serie de propiedades del álgebra de señales unidimensionales y sus respectivas demostraciones.

Teorema 4.8. *Si $S_0, S_1 \in l^2(\mathbb{Z}_N)$, entonces*

$$(S_0 \odot_N S_1)\widehat{\ } = \frac{1}{N} (S_0)\widehat{\ } \circledast_N (S_1)\widehat{\ }$$

Demostración. Por definición tenemos que

$$(S_0 \odot_N S_1)\hat{}[k] = \sum_{n=0}^{N-1} S_0[n]S_1[n]W_N^{nk}.$$

Aplicando transformada discreta de Fourier inversa tenemos

$$S_0[n] = \frac{1}{N}\sum_{r=0}^{N-1}(S_0)\hat{}[r]W^{-nr};$$

entonces, substituyendo en la ecuación inicial,

$$\begin{aligned}
(S_0 \odot_N S_1)\hat{}[k] &= \frac{1}{N}\sum_{n=0}^{N-1}\sum_{r=0}^{N-1}(S_0)\hat{}[r]S_1[n]W_N^{nk}W^{-nr}, \\
&= \frac{1}{N}\sum_{n=0}^{N-1}(S_0)\hat{}[r]\sum_{r=0}^{N-1}S_1[n]W^{(k-r)n}, \\
&= \frac{1}{N}\sum_{n=0}^{N-1}(S_0)\hat{}[r](S_1)\hat{}[k-r], \\
&= \frac{1}{N}\left((S_0)\hat{} \circledast_N (S_1)\hat{}\right)[k]. \qquad \boxtimes
\end{aligned}$$

El teorema anterior es enunciado, sin demostración, en el libro de Mitra [10]. Este resultado obviamente implica que si $S_0, S_1 \in l^2(\mathbb{Z}_N)$, entonces

$$S_0 \odot_N S_1 = \left[\frac{1}{N}(S_0)\hat{} \circledast_N (S_1)\hat{}\right]^{\vee}. \tag{43}$$

La demostración del siguiente teorema es consecuencia inmediata de los teoremas 4.2 y 4.6.

Teorema 4.9. *Si S_0 y S_1 son señales, entonces*

$$(S_0 \circledcirc_N S_1)\hat{} = (\Re_N\{S_0\})\hat{} \odot_N (S_1)\hat{}. \tag{44}$$

Esto implica que si $S_0, S_1 \in l^2(\mathbb{Z}_N)$, entonces

$$S_0 \circledcirc_N S_1 = [(\Re_N\{S_0\})\hat{} \odot_N (S_1)\hat{}]^{\vee}. \tag{45}$$

El siguiente teorema también aparece en el libro de Mitra [10] sin demostración.

Teorema 4.10. *Si $S \in l^2(\mathbb{Z}_N)$, entonces*

$$(\Re_N\{S^*\})\hat{} = (S\hat{})^*. \tag{46}$$

Demostración.

$$
\begin{aligned}
(\Re_N\{S^*\}\widehat{\ }\,) &= \sum_{n=0}^{N-1}(\Re_N\{S^*\})[n]W_N^{kn} = \sum_{n=0}^{N-1} S^*[-n]W_N^{kn} = \left(\sum_{n=0}^{N-1} S[-n]W_N^{k(-n)}\right)^* \\
&= \left(\sum_{n=0}^{N-1} S[-n+N]W_N^{k(-n+N)}\right)^* = \left(\sum_{n=0}^{N-1} S[N-n]W_N^{k(N-n)}\right)^* \\
&= \Big(S[N]W_N^{k(N)} + S[N-1]W_N^{k(N-1)} + S[N-2]W_N^{k(N-2)} + \ldots + \\
&\quad + S[N-(N-2)]W_N^{k(N-(N-2))} + S[N-(N-1)]W_N^{k(N-(N-1))}\Big)^* \\
&= \Big(S[0]W_N^{k(0)} + S[N-1]W_N^{k(N-1)} + S[N-2]W_N^{k(N-2)} + \\
&\quad + \ldots + S[2]W_N^{k(2)} + S[1]W_N^{k(1)}\Big)^* \\
&= \Big(S[0]W_N^{k(0)} + S[1]W_N^{k(1)} + S[2]W_N^{k(2)} + \\
&\quad + \ldots + S[N-2]W_N^{k(N-2)} + S[N-1]W_N^{k(N-1)}\Big)^* \\
&= \left(\sum_{m=0}^{N-1} S[m]W_N^{k(m)}\right)^* = (S\widehat{\ }[k])^* \\
&= (S\widehat{\ })^*[k]. \qquad \boxdot
\end{aligned}
$$

Teorema 4.11. *Si S_0 y S_1 son señales, entonces*

$$(S_0 \circledast_N \Re_N\{S_1^*\})\widehat{\ } = (S_0)\widehat{\ } \odot_N (S_1\widehat{\ })^*. \tag{47}$$

Demostración.

$$
\begin{aligned}
(S_0 \circledast_N \Re_N S_1^*)\widehat{\ } &= (S_0)\widehat{\ } \odot_N (\Re_N\{S_1^*\})\widehat{\ } \\
&= (S_0)\widehat{\ } \odot_N (S_1\widehat{\ })^*. \qquad \boxdot
\end{aligned}
$$

Así, aplicando transformada inversa de Fourier discreta, del teorema anterior obtenemos

$$S_0 \circledast_N \Re_N\{S_1^*\} = \left[(S_0)\widehat{\ } \odot_N (S_1\widehat{\ })^*\right]^\vee, \tag{48}$$

para $S_0, S_1 \in l^2(\mathbb{Z}_N)$.

El siguiente teorema también es enunciado en el libro de Mitra [10] sin demostración.

Teorema 4.12. *Si $S \in l^2(\mathbb{Z}_N)$, entonces*

$$(S^*)\widehat{}= \Re_N\{(S\widehat{})^*\}. \tag{49}$$

Demostración. Recordemos que

$$S\widehat{}[k] = \sum_{n=0}^{N-1} S[n]W_N^{nk};$$

tomando conjugado tenemos

$$(S\widehat{})^*[k] = (S\widehat{}[k])^* = \sum_{n=0}^{N-1} S^*[n]W_N^{-nk}.$$

Ahora, aplicando el operador de reflexión,

$$\begin{aligned}
\Re_N\{(S\widehat{})^*\}[k] &= (S\widehat{})^*[N-k] \\
&= \sum_{n=0}^{N-1} S^*[n]W_N^{-n(N-k)} \\
&= \sum_{n=0}^{N-1} S^*[n]W_N^{-nN+nk} \\
&= \sum_{n=0}^{N-1} S^*[n]W_N^{nk} \\
&= (S^*)\widehat{}[k].
\end{aligned}$$

☑

Teorema 4.13. *Si S_0 y S_1 son señales, entonces*

$$(S_0 \odot_N S_1^*)\widehat{}= \frac{1}{N}(S_1\widehat{})^* \circledcirc_N (S_0)\widehat{}. \tag{50}$$

Demostración.

$$\begin{aligned}
(S_0 \odot_N S_1^*)\widehat{}&= \frac{1}{N}(S_0)\widehat{} \circledast_N (S_1^*)\widehat{} \\
&= \frac{1}{N}(S_0)\widehat{} \circledast_N \Re_N\{(S_1\widehat{})^*\} \\
&= \frac{1}{N}\Re_N\{(S_1\widehat{})^*\} \circledast_N (S_0)\widehat{} \\
&= \frac{1}{N}(S_1\widehat{})^* \circledcirc_N (S_0)\widehat{}.
\end{aligned}$$

☑

Aplicando transformada inversa de Fourier discreta en la ecuación (50), obtenemos

$$S_0 \odot_N S_1^* = \left[\frac{1}{N}(S_0)\widehat{\ }\circledcirc_N(S_1\widehat{\ })^*\right]^\vee, \tag{51}$$

para $S_0, S_1 \in l^2(\mathbb{Z}_N)$.

El siguiente resultado muestra que la transformada de Fourier discreta y el operador de reflexión conmutan.

Teorema 4.14. *Si $S \in l^2(\mathbb{Z}_N)$, entonces*

$$(\Re_N\{S\})\widehat{\ } = \Re_N\{S\widehat{\ }\}. \tag{52}$$

Demostración.

$$\begin{aligned}
(\Re_N\{S\})\widehat{\ }[k] &= \sum_{n=0}^{N-1}(\Re_N\{S\})[n]W_N^{nk} \\
&= \sum_{n=0}^{N-1} S[N-n]W_N^{nk} \\
&= S[N]W_N^{0k} + S[N-1]W_N^{1k} + S[N-2]W_N^{2k} + \cdots + \\
&\quad + S[N-(N-2)]W_N^{(N-2)k} + S[N-(N-1)]W_N^{(N-1)k} \\
&= S[0]W_N^{0k} + S[N-1]W_N^{1k} + S[N-2]W_N^{2k} + \cdots + \\
&\quad + S[2]W_N^{(N-2)k} + S[1]W_N^{(N-1)k} \\
&= S[0]W_N^{0k} + S[1]W_N^{-k} + S[2]W_N^{-2k} + \cdots + \\
&\quad + S[N-2]W_N^{-(N-2)k} + S[N-1]W_N^{-(N-1)k} \\
&= \sum_{m=0}^{N-1} S[m]W_N^{-mk} = \sum_{m=0}^{N-1} S[m]W_N^{m(-k)} \\
&= (S\widehat{\ })[-k] = \Re_N\{S\widehat{\ }\}[k]. \qquad \boxtimes
\end{aligned}$$

Como consecuencia del anterior resultado, tenemos el siguiente

Teorema 4.15. *Si S_0 y S_1 son señales, entonces*

$$(S_0\circledcirc_N S_1^*)\widehat{\ } = \Re_N\{S_0\widehat{\ }\} \odot_N (S_1^*)\widehat{\ }. \tag{53}$$

Demostración.

$$(S_0\circledcirc_N S_1^*)\widehat{\ } = (\Re_N\{S_0\})\widehat{\ }\odot_N (S_1^*)\widehat{\ } = \Re_N\{S_0\widehat{\ }\} \odot_N (S_1^*)\widehat{\ }. \qquad \boxtimes$$

Dada $S_0 \in l^2(\mathbb{Z}_N)$, veamos que $(S_0\widehat{\ })^* = \Re_N\{(S_0^*)\widehat{\ }\}$:

$$\begin{aligned}(S_0\widehat{\ })^*[k] &= ((S_0\widehat{\ })[k])^* \\ &= \left(\sum_{n=0}^{N-1} S_0[n]W_N^{nk}\right)^* \\ &= \sum_{n=0}^{N-1} S_0^*[n]W_N^{-nk} = \sum_{n=0}^{N-1} S_0^*[n]W_N^{n(-k)} \\ &= (S_0^*)\widehat{\ }[-k] = (\Re_N\{(S_0^*)\widehat{\ }\})[k].\end{aligned}$$

Así, tenemos que

$$\begin{aligned}(S_0^* \circledcirc S_1)\widehat{\ } &= (\Re_N\{S_0^*\})\widehat{\ } \odot_N (S_1)\widehat{\ } = (S_0\widehat{\ })^* \odot_N (S_1)\widehat{\ }, \\ &= \Re_N\{(S_0^*)\widehat{\ }\} \odot_N (S_1)\widehat{\ },\end{aligned}$$

es decir que hemos probado el siguiente

Teorema 4.16. *Si $S_0, S_1 \in l^2(\mathbb{Z}_N)$, entonces*

$$(S_0^* \circledcirc S_1)\widehat{\ } = \Re_N\{(S_0^*)\widehat{\ }\} \odot_N (S_1)\widehat{\ }. \tag{54}$$

Aplicando transformada inversa de Fourier discreta obtenemos

$$S_0^* \circledcirc_N S_1 = \left[\Re_N\{(S_0^*)\widehat{\ }\} \odot_N (S_1)\widehat{\ }\right]^\vee, \tag{55}$$

para $S_0, S_1 \in l^2(\mathbb{Z}_N)$.

El siguiente resultado es presentado en el libro de Mitra [10] sin demostración.

Teorema 4.17. *Si $S_0 \in l^2(\mathbb{Z}_N)$, entonces*

$$(S_0[\langle n - n_0\rangle_N])\widehat{\ } = W_N^{kn_0} (S_0)\widehat{\ }. \tag{56}$$

Demostración.

$$(S_0[\langle n - n_0\rangle_N])\widehat{\ } = \sum_{n=0}^{N-1} S_0[\langle n - n_0\rangle_N]W_N^{kn}.$$

Haciendo $m = n - n_0$, tenemos

$$\begin{aligned}
(S_0[\langle n - n_0\rangle_N])\widehat{\ } &= \sum_{m=-n_0}^{N-1-n_0} S_0[\langle m\rangle_N] W_N^{k(m+n_0)} \\
&= \sum_{m=-n_0}^{N-1-n_0} S_0[m] W_N^{km} W_N^{kn_0} \\
&= W_N^{kn_0} \sum_{m=-n_0}^{N-1-n_0} S_0[m] W_N^{km} \\
&= W_N^{kn_0} \sum_{m=0}^{N-1} S_0[m] W_N^{km} \\
&= W_N^{kn_0} \, (S_0)\widehat{\ }. \qquad \boxtimes
\end{aligned}$$

Agradecimiento. El primer autor agradece al Departamento de Ingeniería Eléctrica y Computadoras de la Universidad de Puerto Rico en Mayagüez por la hospitalidad recibida durante la realización de este trabajo.

Referencias

[1] L. A. D'ALOTTO, C. R. GIARDINA & H. LUO. *A Unified Signal Algebra Approach to Two-Dimensional Parallel Digital Signal Processing*, Marcel Dekker, 1998.

[2] P. J. DAVIS. *Circulant Matrices*, John Wiley and Sons, 1979.

[3] A. H. DÍAZ–PÉREZ. *Análisis y diseño de algoritmos para la computación con estructuras circulantes*, Master Thesis, Electrical and Computer Engineering Department, University of Puerto Rico at Mayagüez, 2004.

[4] G. FRANCESCHETTI, R. LANARI & R. LANARI. *Synthetic Aperture Radar Processing*, Electronic Engineering Systems Series, CRC Press,1999.

[5] I. N. HERSTEIN. *Topics in Algebra*, Second Edition, Wiley & sons,1975.

[6] K. M. HOFFMAN & R. KUNZE. *Linear Algebra*, Second Edition, Prentice Hall, 1971.

[7] A. HOWARD. *Elementary Linear algebra*, Seventh Edition, Wiley & sons, 1994.

[8] T. LARA. "Matrices Circulantes", *Divulgaciones Matemáticas*, **9** (2001), no. 1, 85–102.

[9] G. Y. Mao. "Some properties of a special class of block circulant matrices with circulant blocks", *Math. Appl.* (Wuhan) **8** (1995), no. 3, 311-316.

[10] S. K. Mitra. *Digital Signal Processing: A Computer-Based Approach*, Second Edition, McGraw-Hill, 2001

[11] G. X. Ritter & J. N. Wilson. *Handbook of Computer Vision Algorithms in Image Algebra*, Second Edition, CRC Press LLC, 2000.

[12] D. Rodríguez. *Computational Signal Processing and Sensor Array Signal Algebra: A Representation Development Approach*, University of Puerto Rico at Mayaguez, 2002.

[13] J. Villamizar–Morales. *Marco teórico computacional de un álgebra de señales para el procesamiento de imágenes en aplicaciones de interferometría*, Tesis de Maestría, Electrical and Computer Engineering Department, University of Puerto Rico at Mayagüez, 2006.

[14] J. Villamizar–Morales, L. X. Bautista–Rozo & D. A. Rodriguez. "A Computational Signal Processing System for Correlated Digital Interferometry", *IEEE International MWSCAS* 05, Ohio, USA, 2005.

Marlio Paredes
Escuela de Matemáticas
Universidad Industrial de Santander
Bucaramanga, Colombia, A.A. 678
e-mail: marlio@ciencias.uis.edu.co

Domingo A. Rodríguez & Jorge Villamizar–Morales
Automated Information Processing Laboratory
Electrical and Computer Engineering Department
University of Puerto Rico at Mayagüez
Mayagüez, PR 00681–9042, USA
e-mail: domingo@ece.uprm.edu, jorge.villamizar@ece.uprm.edu