**MARCO COMPUTACIONAL PARA EL TRATAMIENTO ARMÓNICO DE REPRESENTACIONES BIDIMENSIONALES**

Por

Juan Pablo Soto Quirós

Tesis sometida en cumplimiento parcial de los requerimientos para el grado de

MAESTRÍA EN CIENCIAS

en

MATEMÁTICA APLICADA

UNIVERSIDAD DE PUERTO RICO
RECINTO UNIVERSITARIO DE MAYAGÜEZ

Noviembre, 2011

Aprobada por:

| | |
|---|---|
| Paul Castillo, Ph.D<br>Miembro, Comité Graduado | Fecha |
| Pedro Vásquez Urbano, D. Sc.<br>Miembro, Comité Graduado | Fecha |
| Domingo Rodríguez, Ph.D<br>Presidente, Comité Graduado | Fecha |
| Néstor Rodríguez, Ph.D<br>Representante de Estudios Graduados | Fecha |
| Omar Colón, Ph.D<br>Director del Departamento | Fecha |

Resumen de Disertación Presentado a Escuela Graduada
de la Universidad de Puerto Rico como requisito parcial de los
Requerimientos para el grado de Maestría en Ciencias

**MARCO COMPUTACIONAL PARA EL TRATAMIENTO ARMÓNICO DE REPRESENTACIONES BIDIMENSIONALES**

Por

Juan Pablo Soto Quirós

Noviembre 2011

Consejero: Domingo Rodríguez, Ph.D
Departamento: Ciencias Matemáticas

A través de los años, el análisis armónico aplicado y numérico ha sido relevante en el área de ingeniería eléctrica, para el estudio y el comportamiento de señales bidimensionales en tiempo y frecuencia, específicamente en el área de procesamiento digital de señales. Las señales en tiempo y frecuencia son representaciones (o funciones) bidimensionales que aparecen en muchas áreas de ciencia e ingeniería, como por ejemplo la transformada discreta de Fourier de tiempo corto, la función discreta ambigüedad, y la distribución discreta de Wigner.

El concepto de representación bidimensional en tiempo y frecuencia es muy propio de la ingeniería eléctrica. Pero también ha sido un gran campo de estudio para matemáticos, que contribuyen con nuevos conocimientos en diversas áreas de la matemática, como por ejemplo el análisis armónico. Pero tales estudios no han profundizado en el espacio de matrices.

En este trabajo se desarrollará un marco computacional de las representaciones en tiempo y frecuencias desarrolladas a partir la función discreta de ambigüedad. El

marco o arquetipo computacional se basará en estructuras matriciales, que se elaboraran a partir de las representaciones algebraicas de las funciones bidimensionales. Además, se desarrolla el concepto de un espacio de matrices de arreglos, para el estudio de la transformada discreta de Fourier de valores vectoriales y la función de ambigüedad de valores vectoriales, con el fin de desarrollar un marco computacional para estos dos conceptos.

Abstract of Dissertation Presented to the Graduate School
of the University of Puerto Rico in Partial Fulfillment of the
Requirements for the Degree of Master of Sciences

**COMPUTATIONAL FRAMEWORK FOR HARMONIC TREATMENT OF TWO-DIMENSIONAL REPRESENTATIONS**

By

Juan Pablo Soto Quirós

November 2011

Chair: Domingo Rodríguez, Ph.D
Major Department: Mathematical Sciences

Over the years, applied and numerical harmonic analysis has been important on electrical engineering for the study and performance of two-dimensional signals in time and frequency, specifically in the area of digital signal processing. Time-frequency signals are two-dimensional representations (or functions) that appear in many areas of science and engineering, for example the discrete Fourier transform short time, the discrete ambiguity function and discrete Wigner distribution.

The concept of two-dimensional representation in time-frequency is very typical of electrical engineering, and used for various applications. But it has also been a major field of study for mathematicians, who contribute new knowledge in different areas of mathematics, such as harmonic analysis. But such studies have not delved into the matrix space.

In this job we develop a computational framework of time-frequency representations developed from discrete ambiguity function. The computational framework is based on matrix structures, which develop from the algebraic representations of two-dimensional functions. In addition, it develops the concept of a matrix array for the

study of the discrete Fourier transform and vector-valued function of vector-valued ambiguity, in order to develop a computational framework for these two concepts.

Copyright © 2011

por

Juan Pablo Soto Quirós

DEDICATORIA

A Dios, por la oportunidad de esta etapa en mi vida. A Mayela, Ronald, Diego y Laura, por su apoyo y fortaleza.

AGRADECIMIENTOS

A mis padres, Ronald y Mayela por su apoyo en esta etapa de mi vida. A mis hermanos, Diego y Laura por estar siempre pendientes de mi.

A mi asesor Domingo, por darme la oportunidad de trabajar con él. Al personal administrativo y docente del Departamento de Ciencias Matemáticas de la UPRM, por brindarme la oportunidad de realizar mis estudios.

A mis compañeros y amigos, estudiantes de maestría en el Departamento de Ciencias Matemáticas e Ingeniería Eléctrica y Computadores.

TABLA DE CONTENIDO

página

RESUMEN EN ESPAÑOL . . . . . ii

ABSTRACT ENGLISH . . . . . iv

LISTA DE TABLAS . . . . . xii

LISTA DE FIGURAS . . . . . xiii

LISTA DE ABREVIATURAS . . . . . xiv

LISTA DE SÍMBOLOS . . . . . xv

1 INTRODUCCIÓN . . . . . 1

2 PRELIMINARES . . . . . 5

2.1 Productos Kronecker y Hadamard & Suma Directa . . . . . 5
2.2 Operadores . . . . . 8
2.2.1 Operadores Unitarios . . . . . 8
2.2.2 Otros Operadores . . . . . 13
2.3 Transformada Discreta de Fourier . . . . . 15
2.3.1 Transformada Rápida de Fourier . . . . . 17
2.3.2 Transformada Discreta de Fourier en 2 Dimensiones . . . . 19
2.4 Matrices Circulantes . . . . . 20

3 REPRESENTACIONES DISCRETAS BIDIMENSIONALES . . . . . 22

3.1 Función Discreta de Ambigüedad . . . . . 23
3.1.1 Definición y propiedades . . . . . 23
3.1.2 Representación Matricial . . . . . 26
3.2 Un método para computar la inversa de la DAF . . . . . 28
3.2.1 Formulación del problema de la inversa de la DAF . . . . . 28
3.2.2 Utilizando una fila de la matriz DAF . . . . . 28
3.2.3 Utilizando una columna de la matriz DAF . . . . . 30
3.3 Función Discreta de Ambigüedad como ente generadora de distribuciones bidimensionales . . . . . 33
3.3.1 Transformada Discreta de Fourier en Tiempo Corto . . . . 33
3.3.2 Transformada Discreta de Zak . . . . . 35
3.3.3 Distribución Discreta de Cohen . . . . . 38

4 FUNCIÓN DE AMBIGÜEDAD DE VALORES VECTORIALES . . . . 42

4.1 Álgebra de matrices de arreglos $\mathbb{C}^{D*(M\times N)}$ . . . . . 42
4.1.1 Productos Kronecker, Hadamard & Suma Directa . . . . . 49
4.2 Transformada Discreta de Fourier de valores vectoriales . . . . . 51
4.2.1 Marcos y Vectores Complejos Armónicos . . . . . 51
4.2.2 Definición . . . . . 53
4.2.3 Propiedades . . . . . 56
4.2.4 Transforma 2D de Fourier de valores vectoriales . . . . . 59
4.2.5 Transformada Rápida de Fourier de Valores Vectoriales . . 59
4.3 Función Discreta de Ambigüedad de Valores Vectoriales . . . . . 66
4.3.1 Marco Computacional . . . . . 69
4.4 Grupo de Heisenberg . . . . . 71
4.5 Proceso de Decimación . . . . . 75

5 APLICACIONES . . . . . 79

5.1 Secuencias CAZAC . . . . . 79
5.1.1 Ejemplos de Secuencias CAZAC en $\mathbb{C}^N$ . . . . . 80
5.1.2 Secuencias CAZAC en $\mathbb{C}^{D*N}$ . . . . . 80
5.1.3 Resultados Numéricos . . . . . 81
5.2 Función Discreta de Ambigüedad y Criptografía . . . . . 83
5.2.1 Definición . . . . . 83
5.2.2 Método para encriptar . . . . . 84
5.2.3 Método para recuperar . . . . . 85
5.3 Matrices Circulantes en $\mathbb{C}^{D*(N\times N)}$ . . . . . 87
5.3.1 Definición . . . . . 87
5.3.2 Matrices de Arreglos de Circulantes por Bloques . . . . . 90
5.3.3 Matrices de Arreglos de Bloques Circulantes . . . . . 92
5.3.4 Matrices de Arreglos Circulante por Bloques con Bloques Circulantes . . . . . 94

6 CONCLUSIONES Y TRABAJOS FUTUROS . . . . . 97

LISTA DE TABLAS

Tabla página

3–1 Representación Kronecker de la matrices DAF's . . . . . 27

3–2 Representación matricial del método inverso . . . . . 29

3–3 Tabla para recuperar la función $y$ . . . . . 32

3–4 Funciones ventanas . . . . . 34

3–5 Funciones núcleo . . . . . 39

4–1 Representación Kronecker de la matrices VV DAF . . . . . 71

LISTA DE FIGURAS

Figura página

5–1 Representación matricial y gráfica de DAF T-0 de una secuencia Wiener, donde $N = 7$ . . . . . 81

5–2 DAF T-0 de una secuencia de Chu para $N = 153$ y $\alpha = 2$ . . . . . 82

5–3 DAF T-0 de una secuencia de Wiener para $N = 64$ . . . . . 82

5–4 DAF T-0 de una secuencia de Björck para $N = 101$ . . . . . 83

5–5 VV DAF T-0 de una secuencia Wiener para $N = 93$ y $D = 45$, con norma 2 . . . . . 83

## LISTA DE ABREVIATURAS

| | |
|---|---|
| DFT | Discrete Fourier Transform. |
| IDFT | Inverse Discrete Fourier Transform. |
| DAF | Discrete Ambiguity Function. |
| DSTFT | Discrete Short Time Fourier Transform. |
| DZT | Discrete Zak Transform. |
| DCD | Discrete Cohen Distribution. |
| VV DFT | Vector-Valued Discrete Fourier Transform. |
| VV DAF | Vector-Valued Discrete Ambiguity Function. |

# LISTA DE SÍMBOLOS

| | |
|---|---|
| $\mathbb{Z}_N$ | Conjunto residuo modulo $N$. |
| $\mathbb{U}_N$ | $\{1, 2, ..., N-1\}$ |
| $\mathbb{C}^N$ | Espacio vectorial de números complejos de orden $N$. |
| $l^2(\mathbb{Z}_N)$ | Espacios de funciones de entradas complejas y de orden $N$. |
| $\mathbb{C}^{M\times N}$ | Espacio de matrices de valores complejos de orden $M$ por $N$. |
| $\otimes$ | Producto Kronecker en $\mathbb{C}^{M\times N}$ |
| $\odot$ | Producto Hadamard en $\mathbb{C}^{M\times N}$ |
| $\oplus$ | Suma directa en $\mathbb{C}^{M\times N}$ |
| $\mathcal{F}_x$ | Transformada discreta de Fourier de $x$. |
| $\mathcal{A}^l_{x,y}$ | Función discreta de ambigüedad Tipo-$l$ de $x, y$ |
| $C_v$ | . Matriz circulante con respecto al vector $v$. |
| $\mathbb{C}^{D*N}$ | Espacio vectorial de orden $N$ de arreglos de dimensión $D$ de número complejos. |
| $\mathbb{C}^{D*(M\times N)}$ | Espacio de matrices de orden $M$ por $N$ de arreglos de dimensión $D$ de número complejos. |
| $\boxtimes$ | Producto Kronecker en $\mathbb{C}^{D*(M\times N)}$ |
| $\boxdot$ | Producto Hadamard en $\mathbb{C}^{D*(M\times N)}$ |
| $\boxplus$ | Suma directa en $\mathbb{C}^{D*(M\times N)}$ |
| $\mathscr{F}_{\mathbf{x}}$ | Transformada discreta de Fourier de valores vectoriales de $\mathbf{x}$. |
| $\mathscr{A}^l_{\mathbf{x},\mathbf{y}}$ | Función discreta de ambigüedad de valores vectoriales Tipo-$l$ de $\mathbf{x}, \mathbf{y}$ |
| $\mathbf{C}_{\mathbf{v}}$ | Matriz de arreglos circulante con respecto a $\mathbf{v}$. |

# CAPÍTULO 1
# INTRODUCCIÓN

Las representaciones en tiempo y frecuencia aparecen en muchas áreas de ciencia e ingeniería, tales como el procesamiento de señales del habla, de señales sísmicas, imágenes, señales biomédicas, el procesamiento de señales a partir de sonares (radares) entre otros. Durante muchos años, representaciones bidimensionales en tiempo y frecuencia como la transformada discreta de Fourier de tiempo corto (DSTFT, de sus siglas en inglés), la función discreta ambigüedad (DAF, de sus siglas en inglés), y la distribución discreta de Wigner (DCD, de sus siglas en inglés) - las cuales son generadas a partir de la transformada discreta de Fourier - han sido utilizadas con éxito en el procesamiento de señales. El término representación bidimensional se refiere a cualquier función, distribución o transformada cuyo dominio sea de dos dimensiones. Por ejemplo, la DSTFT, DAF y DCD son representaciones bidimensionales cuyo dominio representa el tiempo y la frecuencia

El concepto representación bidimensional en tiempo y frecuencia es muy propio de la ingeniería eléctrica, y utilizado para diversas aplicaciones ingenieriles [1–10]. Pero también ha sido un gran campo de estudio para matemáticos, que contribuyen con nuevos conocimientos en diversas áreas de la matemática: análisis armónico, teoría de grupos, algoritmia, entre otros [11–16], pero tales estudios no han profundizado en el álgebra de matrices, a pesar de la estructura bidimensional que presentan estas funciones.

Como explican D. Rodriguez, J. Seguel y E. Cruz [17], todas las formulaciones matemáticas de los algoritmos se consideran pertenecientes a un entorno denominado

*ambiente matemático computacional* (AMC). El AMC está esencialmente constituido por un conjunto de entrada, un conjunto de salida, un conjunto de operadores matemáticos, y un conjunto de normas para estos operadores. El AMC es definido como un entorno para el desarrollo de software basado en subgrupos especiales llamado *marco computacional matemático* (MCM). Un MCM es un conjunto formado por una formulación matemática de un algoritmo, presentado en lo que se denomina su forma canónica o estándar, y todas las variantes posible. Una formulación matemática se conoce como una variante de una formulación canónica, si esta variante se puede obtener de la canónica.

Además, en [17] explican que la idea de realizar estos algoritmos es para poder implementarlos en una máquina determinada. Se utilizará el concepto de estructura de hardware computacional (EHC) para referirse a cualquier máquina arbitraria. El AMC pueden ayudar a esta implementación de la siguiente manera: la información sobre los atributos inherentes a la EHC, como la configuración de la memoria principal, el tamaño de la memoria, el número de unidades de procesamiento, los tipos de unidades de procesamiento, el tamaño de la memoria, las especificaciones del compilador, los lenguajes de programación, entre otros, pueden ser adquiridos en la forma adquirida por el AMC, algunos de ellos en forma de parámetros. Un MCM permite la elaboración de un algoritmo y algunas de sus variantes se formulan utilizando la información obtenida de la EHC. Una variante será elegida mejor, mientras se ajuste a estos criterios de desempeño.

En esta tesis se desarrollará un marco computacional matemático de las representaciones en tiempo y frecuencias desarrolladas a partir de la función discreta de ambigüedad, utilizando cuatro definiciones diferentes de la función discreta de ambigüedad, pero que son iguales en módulos. La función discreta de ambigüedad será el ente generador de las demás representaciones en tiempo y frecuencias estudiadas en este documento. Se entenderá como marco computacional, un esquema

para el desarrollo y/o la implementación de una aplicación. El marco o arquetipo computacional se basará en estructuras matriciales, que se elaboraran a partir de las representaciones algebraicas de las funciones bidimensionales. Tales estructuras matriciales, se elaboraran utilizando productos de Kronecker y Hadamard, además de operadores que se emplean sobre los espacios $\mathbb{C}^N$ y $\mathbb{C}^{M\times N}$, lo cuál permiten su implementación utilizando cómputo en paralelo. Por ser de dimensión finita y utilizar operadores en $\mathbb{C}^N$ y $\mathbb{C}^{M\times N}$, las representaciones algebraicas y estructuras matriciales se interpretaran como algoritmos para el cálculo de tales funciones bidimensionales. Un algoritmo se puede definir, de manera informal, como un procedimiento de cálculo formulado, con un número finito de pasos, que actúa sobre los elementos de un conjunto llamado conjunto de entrada para producir una salida que pertenece a un conjunto de salida. Además, en el desarrollo del documento, se presentan nuevos resultados que se clasifican en Teoremas, Lemas, Proposiciones y Corolarios. Cada nuevo resultado tiene su respectiva demostración, y cada demostración fue realizada por el autor de la tesis. Algunos resultados y demostraciones son totalmente nuevas, los otros son extensiones de otros trabajos, los cuales se explican en el documento.

La tesis está organizada como sigue: en el Capítulo 2 se discuten algunos conceptos preliminares - Productos Kronecker y Hadamard, operadores, transformada discreta de Fourier y matrices circulantes-; en el Capítulo 3 se elabora un arquetipo computacional para la función discreta de ambigüedad y de una clase de funciones bilineales de tiempo y frecuencia, generadas a partir de la función discreta de ambigüedad. En el Capítulo 4 se desarrolla un marco computacional para la transformada de Fourier de valores vectoriales y la función discreta de ambigüedad de valores vectoriales a partir del concepto del espacio de matrices de arreglos. En el Capítulo 5 se explican algunas aplicaciones de la función discreta de ambigüedad y del espacio de matrices de arreglos. Por último, se presentan algunas conclusiones en la Capítulo 6.

Además, los algoritmos desarrollados en este trabajo fueron implementados utilizando MATLAB y utilizando dos toolbox que permiten el cómputo en paralelo: "pMatlab Toolbox" ©, desarrollado por el Laboratorio Lincoln del Instituto Tecnológico de Massachusetts, y "Parallel Computing Toolbox" ©, diseñado por Mathworks.

# CAPÍTULO 2
# PRELIMINARES

## 2.1 Productos Kronecker y Hadamard & Suma Directa

El producto Hadamard, también conocido como producto de entradas o producto Schur, y el producto Kronecker, también conocido como producto directo o producto tensorial, son conceptos que tienen sus orígenes en la teoría de grupos y tienen gran importancia en el desarrollo computacional de la ingeniería eléctrica, especialmente en el campo del procesamiento digital de señales. Estos productos difieren de la forma ordinaria del producto de matrices.

**Definición 1** (**Producto Hadamard).** *El producto Hadamard de dos matrices* $A, B \in \mathbb{C}^{M\times N}$ *se define como la matriz* $A \odot B \in \mathbb{C}^{N\times N}$ *tal que* $(A \odot B)_{m,n} = a_{m,n} \cdot b_{m,n}$. *De forma general, sea* $\{A_n\}_{n\in\mathbb{Z}_N}$ *un conjunto ordenado de matrices tal que cada* $A_n \in \mathbb{C}^{N\times N}$, *entonces el producto Hadamard del conjunto de este conjunto de matrices representa*

$$A = \bigodot_{n\in\mathbb{Z}_N} A_n = A_0 \odot A_1 \odot ... \odot A_{N-1}$$

*y* $A \in \mathbb{C}^{N\times N}$. *Una propiedad del producto Hadamard es la conmutatividad.*

Para definir el producto Kronecker, primero definiremos el álgebra de señales de productos Kronecker (ASK). El ASK es una manera compacta y práctica de expresar algoritmos del álgebra lineal que son esparcidos, utilizando el producto Kronecker.

**Definición 2 (Producto Kronecker).** *El producto Kronecker de dos matrices* $A \in \mathbb{C}^{M\times N}$ *y* $B \in \mathbb{C}^{P\times Q}$ *se define como la matriz* $A \otimes B \in \mathbb{C}^{MP\times NQ}$ *tal que*

$$A \otimes B = \begin{pmatrix} a_{0,0}B & a_{0,1}B & \cdots & a_{0,(N-1)}B \\ a_{1,0}B & a_{1,1}B & \cdots & a_{1,(N-1)}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{(M-1),0}B & a_{(M-1),1}B & \cdots & a_{(M-1),(N-1)}B \end{pmatrix}$$

*De forma general, sea* $\{B_n\}_{n\in\mathbb{Z}_N}$ *un conjunto de matrices tal que* $B_n \in \mathbb{C}^{M_n\times N_n}$, *entonces el producto Kronecker de este conjunto de matrices se representa*

$$B = \bigotimes_{n\in\mathbb{Z}_N} B_n = B_0 \otimes B_1 \otimes ... \otimes B_{N-1}$$

*y* $B \in \mathbb{C}^{M\times N}$, *donde* $M = \prod_{n\in\mathbb{Z}_N} M_n$ *y* $N = \prod_{n\in\mathbb{Z}_N} N_n$.

Es fácil verificar que el producto Kronecker no es conmutativo. Una ventaja del ASK, es que contribuye al análisis, diseño e implementación de algoritmos en paralelo.

**Ejemplo.** *Sea* $A \in \mathbb{C}^{R\times M}$ *y* $x \in \mathbb{C}^{MN}$. *Consideremos la operación* $(I_N \otimes A)x$:

$$(I_N \otimes A)x = \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix} = \begin{pmatrix} Ax_0 \\ Ax_1 \\ \vdots \\ A_{N-1} \end{pmatrix},$$

*donde* $x_m \in \mathbb{C}^M$. *La operación* $(I_N \otimes A)x$ *tiene una complejidad computacional de* $O(MRN^2)$. *Pero, debido a la estructura de la operación al utilizar productos Kronecker, la operación se puede dividir en* $N$ *operaciones* $Ax_m$, *para* $m \in \mathbb{Z}_N$, *por lo que la complejidad computacional pasaría a ser* $O(RMN)$. *Además, la estructura de* $(I_N \otimes A)x$ *permite su implementación utilizando computo en paralelo.*

El cómputo $I_N \otimes A$ se denomina *operación paralela* [14]. El **Algoritmo 1** muestra la implementación del ejemplo anterior.

**Algoritmo 1** Cómputo operación $(I_N \otimes A)x$

**Entrada:** $x \in \mathbb{C}^{MN}$ y $A \in \mathbb{C}^{R\times M}$
**Salida:** $S \in \mathbb{C}^{RN}$
1: **para** $n \leftarrow 0 : N-1$ **hacer**
2: $\quad S[nR : (n+1)R-1] \leftarrow A \cdot x[nM : (n+1)M-1]$
3: **fin para**

**Ejemplo.** *Considere los datos del Ejemplo 2.1 entonces*

$$(A \otimes I_N)x = \begin{pmatrix} \sum_{m\in\mathbb{Z}_M} a_{0,m}x_m \\ \sum_{m\in\mathbb{Z}_M} a_{1,m}x_m \\ \vdots \\ \sum_{m\in\mathbb{Z}_M} a_{R-1,m}x_m \end{pmatrix} \tag{2.1}$$

*Además*

$$\mathcal{R}_{N,R}\{(A \otimes I_N)x\} = \mathcal{R}_{N,M}\{x\}A^T \tag{2.2}$$

*donde $\mathcal{R}$ es el operador reshape (ver* **Sección 2.2.2** *para más detalles de $\mathcal{R}$).*

El cómputo de la operación $A \otimes I_N$ se denomina como *operación vectorial* [14]. El siguiente teorema presenta algunas de las propiedades más importantes del producto Kronecker. Estas propiedades se utilizan a través del presente trabajo. El lector puede verificar los detalles de las demostraciones en [14, 18–21].

**Teorema 1.** *Sea $A \in \mathbb{C}^{M\times N}$, $B \in \mathbb{C}^{R\times S}$, $C \in \mathbb{C}^{N\times P}$ y $D \in \mathbb{C}^{S\times T}$. Entonces*

- $(A \otimes B) \otimes C = A \otimes (B \otimes C)$.
- $(A \otimes B)^T = A^T \otimes B^T$.
- $(A \otimes B)(C \otimes D) = AC \otimes BD$.
- $A \otimes B = (A \otimes I_S)(I_N \otimes B)$.
- $I_R \otimes I_S = I_{RS}$.

**Definición 3 (Suma Directa).** *La suma directa de dos matrices* $A \in \mathbb{C}^{M\times N}$ *y* $B \in \mathbb{C}^{P\times Q}$ *se define como la matriz* $A \oplus B \in \mathbb{C}^{(M+P)\times(N+Q)}$ *tal que*

$$A \oplus B = \begin{pmatrix} A & \\ & B \end{pmatrix}$$

*De forma general, sea* $\{C_n\}_{n\in\mathbb{Z}_N}$ *un conjunto ordenado de matrices tal que* $C_n \in \mathbb{C}^{M_n\times N_n}$*, entonces la suma directa de este conjunto de matrices se representa*

$$C = \bigoplus_{n\in\mathbb{Z}_N} C_n = C_0 \oplus C_1 \oplus ... \oplus C_{N-1}$$

*y* $C \in \mathbb{C}^{M\times N}$*, donde* $M = \sum_{n\in\mathbb{Z}_N} M_n$ *y* $N = \sum_{n\in\mathbb{Z}_N} N_n$*.*

Una propiedad importante de la suma directa, y que se utilizará en el presente trabajo se menciona en el siguiente lema.

**Lema 1.** *Sean* $A \in \mathbb{C}^{M\times N}$ *y* $B \in \mathbb{C}^{N\times R}$*, entonces* $1 \oplus (AB) = (1 \oplus A)(1 \oplus B)$.

## 2.2 Operadores

Sea $V$ y $W$ dos conjuntos. El mapeo $\mathcal{O}$ del conjunto $V$ al conjunto $W$, $\mathcal{O} : V \to W$, se llama un *operador*. En este trabajo se utilizarán operadores sobre los conjuntos $\mathbb{C}^N$ y $\mathbb{C}^{M\times N}$.

### 2.2.1 Operadores Unitarios

**Definición 4 (Operadores Lineales y Unitarios).**

1. $\mathcal{O} : \mathbb{C}^N \to \mathbb{C}^N$ *es un operador lineal si* $\mathcal{O}(\alpha v_1 + v_2) = \alpha\mathcal{O}(v_1) + \mathcal{O}(v_2)$*, donde* $v_1, v_2 \in \mathbb{C}^N$ *y* $\alpha \in \mathbb{C}$*.*
2. *Un operador* $\mathcal{U} : \mathbb{C}^N \to \mathbb{C}^N$ *es un operador unitario si es lineal y* $\mathcal{U}\mathcal{U}^* = \mathcal{I}$*, donde* $\mathcal{U}^*$ *es el operador adjunto de* $\mathcal{U}$ *y* $\mathcal{I}$ *es el operador identidad.*

Todo operador unitario en $\mathbb{C}^N$ tiene una representación matricial. Por ejemplo, $I_N$ es la representación matricial del operador identidad $\mathcal{I}$. Un ejemplo de operador unitario es el operador de permutación. El operador de permutación, $\mathcal{L} : \mathbb{C}^N \to \mathbb{C}^N$, es un operador que realiza un re-acomodo de las entradas de un vector en $\mathbb{C}^N$.

La representación matricial del operador de permutación, o simplemente matriz de permutación, es una matriz binaria cuadrada de orden $N$ que tiene exactamente una entrada con el valor de 1 en cada fila y columna y el valor de 0 en las otras entradas. En este trabajo, la matriz de permutación se define como $L \in \mathbb{C}^{N\times N}$.

**Ejemplo.** *Sea $v \in \mathbb{C}^4$, entonces un ejemplo de permutación para $\mathbb{C}^4$ es $\mathcal{L}\{v\} = (v_0, v_2, v_1, v_3)^T$. La representación matricial de $\mathcal{L}$ es la matriz $L \in \mathbb{C}^{4\times 4}$, tal que*

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

Los operadores de permutación también pueden actuar sobre $\mathbb{C}^{M\times N}$, realizando permutaciones a las columnas. Cuatro ejemplos de operadores de permutación son el operador de permutación de orden $N$ y paso $R$, el operador de traslación, el operador de reflexión y el operador de orden exponencial.

**Operador de Permutación de Orden $N$ y Paso $R$**: Sea $N = RS$. El operador de permutación de orden $N$ y paso $R$, $\mathcal{L}_R^N$, es el operador de permutación que esta definido por la regla $\mathcal{L}_R^N\{v \otimes w\} = w \otimes v$, para $v \in \mathbb{C}^R$ y $w \in \mathbb{C}^S$. La matriz de permutación de orden $N$ y paso $R$ se representará como $L_N^R \in \mathbb{C}^{N\times N}$. Además

$$L_R^N L_S^N = I_N \tag{2.3}$$

Como se explicó en la sección anterior, el producto Kronecker no es conmutativo, pero este tipo de matrices de permutación tratan de dar una noción de conmutatividad, el cual se explica en el siguiente teorema [14].

**Teorema 2 (Conmutación de productos de Kronecker).** *Sea $N = RS$, $A \in \mathbb{C}^{M\times M}$ y $B \in \mathbb{C}^{N\times N}$. Entonces $A \otimes B = L_R^N(B \otimes A)L_S^N$.*

La implementación de este operador se puede hacer de forma lineal. El **Algoritmo 2** muestra tal implementación.

**Algoritmo 2** Permutación de Orden $N$ y Paso $R$

**Entrada:** $x \in \mathbb{C}^N$
**Salida:** $y \in \mathbb{C}^N$
1: **para** $r \leftarrow 0 : R-1$ **hacer**
2: **para** $s \leftarrow 0 : S-1$ **hacer**
3: $y[r+Rs+1] \leftarrow x[Sr+s+1]$
4: **fin para**
5: **fin para**

**Operador de Traslación**: Sea $m \in \mathbb{Z}_N$. El operador de traslación, $\mathcal{S}_m$, es el operador de permutación que esta definido por la regla $\mathcal{S}_m\{v\}[n] = v[\langle n-m\rangle_N]$, para $v \in \mathbb{C}^N$ y donde $\langle a\rangle_N = a \bmod N$. La constante $m$ se denonina *constante de traslación*. La constante de traslación debe ser un número en el conjunto $\mathbb{Z}_N$, entonces cuando se utilice $\mathcal{S}_{-m}$, el valor $-m$ es una representación a nivel de módulo $N$, es decir, $\mathcal{S}_{-m} = \mathcal{S}_{\langle -m\rangle_N}$. Además, si $m \in \mathbb{Z}_N$, entonces $\mathcal{S}_{-m} = \mathcal{S}_{N-m}$, donde $N-m \in \mathbb{Z}_N$ . La matriz de traslación se definirá como $S_m \in \mathbb{C}^{N\times N}$. La implementación de este operador se puede hacer de forma lineal. El **Algoritmo 3** muestra tal implementación.

**Algoritmo 3** Permutación de Traslación con constante $m$

**Entrada:** $x \in \mathbb{C}^N$
**Salida:** $y \in \mathbb{C}^N$
1: **para** $n \leftarrow 0 : N-1$ **hacer**
2: $y[n] \leftarrow x[\langle n-m\rangle_N]$
3: **fin para**

**Operador de Reflexión**: El operador de reflexión $\mathcal{L}_r$ es el operador de permutación que está definido por la regla $\mathcal{L}_r\{v\}[n] = v[\langle -n\rangle_N]$, para $v \in \mathbb{C}^N$. La matriz de traslación se definirá $L_r \in \mathbb{C}^{N\times N}$. La matriz $L_r$ se define como

$$(L_r)_{i,j} = \begin{cases} 1 & \text{si } i=j=1 \text{ y } i+j=N+2 \\ 0 & \text{en otro caso} \end{cases} \tag{2.4}$$

La implementación de este operador se puede hacer de forma lineal. El **Algoritmo 4** muestra tal implementación.

**Algoritmo 4** Permutación de Reflexión

**Entrada:** $x \in \mathbb{C}^N$
**Salida:** $y \in \mathbb{C}^N$
1: **para** $n \leftarrow 0 : N-1$ **hacer**
2: $\quad y[n] \leftarrow x[\langle -n \rangle_N]$
3: **fin para**

**Operador de Orden Exponencial**: El operador de orden exponencial, viene definido solo para elementos de $\mathbb{C}^N$, donde $N$ un número primo. Sea $\mathbb{U}_N = \{1, 2, ..., N-1\}$. Si $N$ es un número primo, entonces existe $a \in \mathbb{U}_N$ tal que genera exponencialmente a todos los elementos de $\mathbb{U}_N$ [14], es decir, el conjunto $\{1, a^1, \langle a^2 \rangle_N, ...\langle a^{N-2} \rangle_N\}$ es una permutación de los elementos de $\mathbb{U}_N$. Considere el conjunto

$$\pi_a = \{0, 1, a, \langle a^2 \rangle_N, .., \langle a^{N-2} \rangle_N\}.$$

El conjunto $\pi_a$ es una permutación del conjunto $\mathbb{Z}_N$. Por lo tanto, si $N$ es un número primo y $a$ es un generador de $\mathbb{U}_N$ el *operador de orden generador* $\mathcal{L}_a$ es el operador de permutación que está definido por la regla

$$\mathcal{L}_a\{v\}[n] = \begin{cases} v[0] & \text{si } n = 0 \\ v[a^{n-1}] & \text{si } n \in \mathbb{U}_N \end{cases}$$

para $v \in \mathbb{C}^N$.

La matriz del operador de orden exponencial se definirá como $L_a \in \mathbb{C}^{N \times N}$. La implementación de este operador se puede hacer de forma lineal. El **Algoritmo 5** muestra tal implementación.

Otros ejemplos de operadores unitarios son los operadores de *modulación* y *rotación*. Sean $v \in \mathbb{C}^N$, $m, k \in \mathbb{Z}_N$ and $\lambda \in \mathbb{C}$, tal que $|\lambda| = 1$.

**Algoritmo 5** Permutación de Orden Exponencial, con generador $a$

**Entrada:** $x \in \mathbb{C}^N$ y $a \in \mathbb{U}_N$ (generador).
**Salida:** $y \in \mathbb{C}^N$

```
v[0] = 0
para n ← 1 : N − 1 hacer
    v[n] ← ⟨a^{n−1}⟩_N
fin para
para n ← 0 : N − 1 hacer
    y[n] ← x[v[n]]
fin para
```

**Operador de Modulación**: El operador de modulación, $\mathcal{M}_k$, es el operador definido como $\mathcal{M}_k v[n] = \omega_N^{nk} v[n]$, donde $\omega_N = e^{i\frac{2\pi}{N}}$. La constante $k$ se denonina *constante de modulación* De igual manera que se explicó para el operador de traslación, $\mathcal{M}_{-k} = \mathcal{M}_{\langle N-k \rangle_N}$ La matriz de modulación se define como $M_k \in \mathbb{C}^{N\times N}$, donde $M_k$ es una matriz diagonal de la forma $M_k = diag(1, \omega_N^k, \omega_N^{2k}, ..., \omega_N^{(N-1)k})$. La implementación de este operador se puede hacer de forma lineal. El **Algoritmo 6** muestra tal implementación.

**Algoritmo 6** Operador de Modulación, con constante $k$

**Entrada:** $x \in \mathbb{C}^N$ y $k \in \mathbb{Z}_N$
**Salida:** $y \in \mathbb{C}^N$

```
para n ← 0 : N − 1 hacer
    y[n] ← x[n]ω_N^{kn}
fin para
```

**Operador de Rotación**: El operador de rotación, $\mathcal{C}_\lambda$, es el operador definido como $\mathcal{C}_\lambda v[n] = \lambda v[n]$. La matriz de rotación se define como $C_\lambda \in \mathbb{C}^{N\times N}$, donde $C_\lambda = \lambda I_N$. La implementación de este operador se puede hacer de forma lineal. El **Algoritmo 7** muestra tal implementación.

**Algoritmo 7** Operador de Rotación, con constante $\lambda$

**Entrada:** $x \in \mathbb{C}^N$ y $\lambda \in \mathbb{C}$
**Salida:** $y \in \mathbb{C}^N$

```
para n ← 0 : N − 1 hacer
    y[n] ← λx[n]
fin para
```

### 2.2.2 Otros Operadores

P. A. Regalia y S. K. Mitra [22] desarrollan una definición generalizada del producto Kronecker[1] . Dado un conjunto ordenado de $N$ matrices $A_n \in \mathbb{C}^{M_n \times P}$, para $n \in \mathbb{Z}_N$, expresado como $\{A_n\}$, y una matriz $B \in \mathbb{C}^{N \times R}$, entonces la matriz $\{A_n\} \otimes B \in \mathbb{C}^{MN \times PR}$ es el producto definido como

$$\{A_n\} \otimes B = \begin{bmatrix} A_0 \otimes b_0 \\ \vdots \\ A_{N-1} \otimes b_{N-1} \end{bmatrix}$$

donde $b_n$ representa la $n$-ésima fila de $B$. Note que el número de matrices en el conjunto $\{A_n\}$ coincide con el número de filas en la matriz $B$. Sea $B = \mathbf{1}_N$, donde $\mathbf{1}_N \in \mathbb{C}^N$ es el vector de unos, es decir, $\mathbf{1}_N[n] = 1$, para todo $n \in \mathbb{Z}_N$. Entonces,

$$\{A_n\} \otimes \mathbf{1}_N = \begin{bmatrix} A_0 \otimes 1 \\ \vdots \\ A_{N-1} \otimes 1 \end{bmatrix} = \begin{bmatrix} A_0 \\ \vdots \\ A_{N-1} \end{bmatrix}$$

A partir de este caso especial, se desarrolla el *operador de acumulación de matrices.*

**Operador de Acumulación de Matrices**: Sea el conjunto de $N$ matrices $\{A_n\}$, $A_n \in \mathbb{C}^{M_n \times P}$, para $n \in \mathbb{Z}_N$. El operador de acumulación de matrices, $\bigsqcup : \prod_{n \in \mathbb{Z}_N} \mathbb{C}^{M_n \times P} \to \mathbb{C}^{M \times P}$, donde $M = \sum_{n \in \mathbb{Z}_N} M_n$, es definido como

$$\bigsqcup\{\{A_n\}\} = \bigsqcup_{n \in \mathbb{Z}_N} A_n = \{A_n\} \otimes \mathbf{1}_N = \begin{bmatrix} A_0 \\ \vdots \\ A_{N-1} \end{bmatrix}$$

[1] La definición es ligeramente distinta al propuesto en este trabajo, porque P. A. Regalia y S. K. Mitra utilizan una definición modificada del producto Kronecker.

La única condición que deben tener los elementos de $\{A_n\}$ es coincidir en el número de columnas.

Otros dos operadores importantes en este trabajo son los operadores *vec* y su operador inverso [23].

**Operador Vec**: El operador *vec*, $\mathcal{V} : \mathbb{C}^{M\times N} \to \mathbb{C}^{MN}$, es un operador que actúa sobre $\mathbb{C}^{M\times N}$ y da como resultado un vector formado por la "acumulación" de las columnas de las matrices, es decir, si $B \in \mathbb{C}^{M\times N}$ y $b_i$ representa cada columna de la matriz $B$, con, $i \in \mathbb{Z}_N$, entonces

$$\mathcal{V}\{B\} = \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{N-1} \end{pmatrix}.$$

**Operador Vec Inverso**: El inverso del operador *vec*, $\mathcal{R}_{M,N} : \mathbb{C}^{MN} \to \mathbb{C}^{M\times N}$, es conocido como operator *re-shape* y es el operador que transforma un vector de dimensión $MN$ a una matriz de dimensión $M \times N$, es decir, sea $v \in \mathbb{C}^{MN}$ tal que

$$v = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{N-1} \end{pmatrix}, \quad v_n \in \mathbb{C}^M$$

entonces $\mathcal{R}_{M,N}\{v\} = (v_0\ v_1\ ...\ v_{N-1})$. El **Teorema 3** explica una relación entre el operador $\mathcal{R}_{N,N}$ y la matriz de permutación $L_N^{N^2}$.

**Teorema 3.** *Sean $v \in \mathbb{C}^{N^2}$ y $A \in \mathbb{C}^{N\times N}$. Entonces*

- $(\mathcal{R}_{N,N}\{v\})^T = \mathcal{R}_{N,N}\{L_N^{N^2} v\}$.
- $\mathcal{V}\{A^T\} = L_N^{N^2}\mathcal{V}\{A\}$.

**Prueba.** *Considere los siguientes casos*

- *Sean* $i, j \in \mathbb{Z}_N$. *Entonces* $\mathcal{R}_{N,N}\{v\} = (v_0\ v_1\ ...\ v_{N-1})$ , *con* $v_n \in \mathbb{C}^N$. *Pero*

$$(\mathcal{R}_{N,N}\{v\})_{ij} = v_j[i] \Rightarrow (\mathcal{R}_{N,N}\{v\})^T_{ij} = v_i[j].$$

*Por otro lado*

$$L_N^{N^2} v = \begin{pmatrix} v'_0 \\ v'_1 \\ \vdots \\ v'_{N-1} \end{pmatrix}$$

*donde* $v'_j[i] = v_i[j]$, *para* $i, j = 1, ..., N$. *Entonces* $(\mathcal{R}_{N,N}\{L_N^{N^2} v\})_{ij} = v'_j[i] = v_i[j]$.

- *Se sabe que si* $a = \mathcal{V}\{A\}$, *entonces* $A = \mathcal{R}_{N,N}\{a\}$ *Por el teorema anterior se obtiene* $(\mathcal{R}_{N,N}\{a\})^T = \mathcal{R}_{N,N}\{\mathcal{L}_N^{N^2} a\}$. *Aplicando el operador* $\mathcal{V}$ *a ambos lados de la ecuación anterior, se obtiene*

$$\mathcal{V}\{(\mathcal{R}_{N,N}\{a\})^T\} = \mathcal{V}\{\mathcal{R}_{N,N}\{\mathcal{L}_N^{N^2} a\}\} \Rightarrow \mathcal{V}\{A^T\} = L_N^{N^2}\mathcal{V}\{A\}$$

■

## 2.3 Transformada Discreta de Fourier

**Definición 5** (**Transformada Discreta de Fourier**). *La transformada discreta de Fourier o DFT (del inglés, discrete Fourier transform) es un operador discreto, utilizado en el análisis de Fourier. Si* $x \in \mathbb{C}^N$, *entonces la transformada discreta de Fourier de* $x$ *se define como el mapeo* $\mathcal{F}_x : l^2(\mathbb{Z}_N) \to l^2(\mathbb{Z}_N)$, *tal que*

$$\mathcal{F}_x[k] = \sum_{n \in \mathbb{Z}_N} x[n]\omega_N^{-nk}, \quad k \in \mathbb{Z}_N. \tag{2.5}$$

*donde* $\omega_N = e^{2\pi i/N}$

Dado un vector $x \in l^2(\mathbb{Z}_N) = \mathbb{C}^N$, cuyo dominio es conocido como *tiempo*, la DFT realiza un mapeo del dominio inicial $\mathbb{Z}_N$ al *dominio de la frecuencia*. El **Teorema 4** muestra la principal herramienta para la investigación de las propiedades de la DFT. En términos físicos, describe la interferencia constructiva y las propiedades de refuerzo de la DFT [24]. El lector puede ver los detalles de la demostración en [24].

**Teorema 4.** *Sea $\delta[m]$ el delta de Kronecker, es decir, $\delta[m] = 1$ si $m = 0$, y $\delta[m] = 0$ si $m \neq 0$. Entonces,*

$$\sum_{n \in \mathbb{Z}_N} \omega_N^{nm} = N\delta[m] \tag{2.6}$$

La DFT tiene una representación matricial, a partir de la matriz finita de la transformada de Fourier [15, 25]. La *matriz DFT* se define como $F_N \in \mathbb{C}^{N \times N}$ tal que $(F_N)_{i,j} = \omega_N^{-ij}$, para $i, j \in \mathbb{Z}_N$. La representación matricial de la DFT de $x$ es

$$\mathcal{F}_x = F_N x. \tag{2.7}$$

**Definición 6 (Inversa de la DFT).** *La inversa de la DFT (IDFT) es el mapeo $\mathcal{F}_x^{-1} : \mathbb{Z}_N \to \mathbb{C}^N$ tal que*

$$\mathcal{F}_x^{-1}[n] = x[n] = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} \mathcal{F}_x[k]\omega_N^{nk}, \quad n \in \mathbb{Z}_N. \tag{2.8}$$

La *matriz IDFT*, que representa a la matriz inversa de $F_N$, se define como $F_N^{-1} \in \mathbb{C}^{N \times N}$, tal que $F_N^{-1} = \frac{1}{N}\overline{F_N}$. Para propósitos de la **Sección 4.2.2**, se define y demuestra el siguiente teorema

**Teorema 5.** *Sea $N$ un número compuesto, entonces existe $D < N$ tal que*

$$F = \bigodot_{i \in \mathbb{Z}_D} F_N$$

*no es invertible.*

**Prueba.** *Como $N$ es un número compuesto, entonces $N = RS$. Sin pérdida de generalidad, seleccionar $D = R$. Ahora, sea $f_1$ y $f_{S+1}$ las filas $1$ y $S+1$ de la matriz $F$, respectivamente. Entonces, para todo $n \in \mathbb{Z}_N$*

- $f_1[n] = \omega_N^{-nR}$.
- $f_{S+1}[n] = \omega_N^{-(S+1)nR} = \omega_N^{-nN-nR} = \omega_N^{-nR}$.

*Entonces, para $D = R < N$, $F$ tiene dos filas iguales. Por lo tanto, $F$ no es invertible.*

Del teorema anterior se deduce el siguiente corolario.

**Corolario 1.** *Sea $N$ un número primo, entonces para todo $D < N$, la matriz $F$ definida en el* **Teorema 5** *es invertible*

### 2.3.1 Transformada Rápida de Fourier

J. W. Cooley y J. W. Tukey [7] fueron los primeros en desarrollar un algoritmo para realizar el cómputo de la DFT de una manera rápida. Este algoritmo es conocido como *la transformada rápida de Fourier de Cooley-Tukey* o *FFT Cooley-Tukey* (del inglés, *fast Fourier transform*). La FFT reduce significativamente el costo computacional de la DFT para señales de longitud $N$, siendo $N$ un número compuesto [14]. Sea $x \in \mathbb{C}^N$, tal que $N = RS$ un número compuesto. La FFT plantea que la DFT de $x$, de orden $N$, se puede calcular utilizando $R$ DFT's de orden $S$, es decir,

$$\mathcal{F}_x[k] = \begin{cases} \mathcal{F}_{x_0}[m] & \text{si} \quad k = Rm \\ \mathcal{F}_{x_1}[m] & \text{si} \quad k = Rm+1 \\ \vdots & \vdots \\ \mathcal{F}_{x_{R-1}}[m] & \text{si} \quad k = Rm+(R-1) \end{cases} \tag{2.9}$$

para $k \in \mathbb{Z}_N$, donde

- $\mathcal{F}_{x_r}[m] = \sum_{n \in \mathbb{Z}_S} x_r[n]\omega_M^{-nk}$
- $x_r[n] = \omega_N^{nr} \sum_{d \in \mathbb{Z}_R} x[n+dS]\omega_N^{-rSk}$

para $r \in \mathbb{Z}_R$. J. Johnson y D. Rodríguez [20], Tolimieri, An y Lu [14] desarrollan una factorización de la matriz DFT, utilizando el algoritmo FFT como referencia. El **Teorema 6** explica dicha factorización, donde utilizan el producto Kronecker, lo cuál permite su implementación en paralelo. El lector puede ver los detalles de la demostración en [14].

**Teorema 6.** *Sea $N = RS$. La matriz DFT se puede factorizar de la siguiente manera*

$$F_N = (F_S \otimes I_R) T_R^S (I_S \otimes F_R) P_S^N \tag{2.10}$$

*donde $T_R^S \in \mathbb{C}^{N \times N}$ es una matriz diagonal por bloques tal que*

$$T_R^N = \bigoplus_{s \in \mathbb{Z}_S} (D_R^N)^s$$

*donde $D_R^N = diag(1, \omega_N^{-1}, ..., \omega_N^{-(R-1)})$.*

En [14] también explican una factorización de la matriz DFT para el caso $N = 2^k$. El **Teorema 7** expone los detalles de la factorización.

**Teorema 7.** *Sea $N = 2^k$. La matriz DFT se puede factorizar de la siguiente manera*

$$F_N = \left[ \prod_{n \in \mathbb{Z}_k} A_n B_n \right] Q_N \tag{2.11}$$

*donde $A_n, B_n, Q_N \in \mathbb{C}^{N \times N}$ tal que*

- $A_n = I_{2^n} \otimes F_2 \otimes I_{2^{k-n-1}}$
- $B_n = I_{2^n} \otimes T_{2^{k-n-1}}^{2^{k-n}}$
- $Q_N = \prod_{n \in \mathbb{Z}_{k-1}} \left( I_{2^{k-n-2}} \otimes L_2^{2^{n+2}} \right)$

Otro caso desarrollado en [14] es cuando $N$ es un número primo. La idea es factorizar la matriz $F_N$ de tal manera que los factores contengan a la matriz $F_{N-1}$. Como $N$ es primo, entonces $N - 1$ es compuesto, por lo que se puede utilizar el **Teorema 6** para su cómputo. El **Teorema 8** expone los detalles de la factorización.

**Teorema 8.** *Sea $N$ un número primo y sea $a \in \mathbb{U}_N$ un generador del conjunto $\mathbb{U}_N$. La matriz DFT puede factorizarse de la siguiente manera*

$$F_N = L_a^{-1}(1 \oplus F_{N-1})(1 \oplus D)(1 \oplus F_{N-1})A\ L_a \tag{2.12}$$

*donde*

- *$L_a$ es una matriz de permutación de orden exponencial.*
- *$D \in \mathbb{C}^{(N-1)\times(N-1)}$ es una matriz diagonal tal que*

$$D = F_{N-1}^{-1} C F_{N-1}^{-1}$$

  *donde $\in \mathbb{C}^{(N-1)\times(N-1)}$ es el núcleo de Winograd.*

- *$A \in \mathbb{C}^{N\times N}$ tal que*

$$A = \begin{pmatrix} 1 & \mathbf{1}_{N-1} \\ -\mathbf{1}_{N-1} & I_{N-1} \end{pmatrix}$$

### 2.3.2 Transformada Discreta de Fourier en 2 Dimensiones

**Definición 7.** *Sea $x$ un vector bidimensional, es decir, $x : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}^N$. Entonces la transformada de Fourier en 2 dimensiones (2d DFT, del inglés) de $x$ se define como el mapeo $\mathcal{F}_f^{2d} : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}^N$ tal que*

$$\mathcal{F}_x^{2d}[m,k] = \sum_{\tau\in\mathbb{Z}_N} \sum_{\nu\in\mathbb{Z}_N} x[\tau,\nu]\omega_N^{-(m\tau+k\nu)}.$$

Por su dimensionalidad, la $2d$ DFT de $x$ puede ser interpretada como una matriz $F_x^{2D} \in \mathbb{C}^{N\times N}$ tal que $(F_x^{2d})_{m,k} = \mathcal{F}_x^{2d}[m,k]$. Tolimieri [26] y Kumhom [27] explican que la matriz $F_N^{2d}$ puede ser calculada de la siguiente forma

$$F_x^{2d} = \mathcal{R}_{N,N}\{(F_N \otimes F_N)\mathcal{V}\{X\}\} \tag{2.13}$$

donde $X \in \mathbb{C}^{N\times N}$ tal que $X_{m,k} = x[m,k]$.

## 2.4 Matrices Circulantes

**Definición 8 (Matriz Circulante).** *Sea $v \in \mathbb{C}^N$, $v = (v_0, v_1, ..., v_{N-1})^T$. Una matriz $C_v \in \mathbb{C}^{N\times N}$ se llama circulante con respecto al vector $v$, o simplemente circulante, si la fila $(c_v)_m$ de la matriz $C_v$ se representa como $(C_v)_m = \mathcal{S}_m\{x\}$, para $m \in \mathbb{Z}_N$, es decir*

$$C_v = \begin{pmatrix} v_0 & v_1 & \cdots & v_{N-1} \\ v_{N-1} & v_0 & \cdots & v_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ v_1 & v_2 & \cdots & v_0 \end{pmatrix} \tag{2.14}$$

*Además, $(C_v)_{i,j} = v[\langle j - i\rangle_N]$.*

Como menciona G. Golub y C. Van Loan [28], toda matriz circulante se puede factorizar como el producto de la matriz DFT, la matriz diagonal del vector $\mathcal{F}_v$, y la inversa de la matriz DFT, es decir,

$$C_v = \tfrac{1}{N} F_N diag(\mathcal{F}_v)\overline{F_N} \tag{2.15}$$

Además, el determinate de una matriz circulante es el producto de las entradas del vector $\mathcal{F}_v$ [29], es decir

$$det(C_v) = \prod_{n\in\mathbb{Z}_N} \mathcal{F}_v[n] \tag{2.16}$$

De la ecuación (2.16) se deduce que si algún elemento de $\mathcal{F}_v$ es 0, entonces el determinante de $C_v$ es 0.

**Lema 2.** *Sea $v \in \mathbb{C}^N$ y $C_v$ la matriz circulante respecto $v$. $C_v^{-1}$ existe si y solo si $\mathcal{F}_v[n] \neq 0$, para todo $n \in \mathbb{Z}_N$. Además $C_v^{-1}$ se expresa como*

$$C_v^{-1} = \tfrac{1}{N} F_N D\overline{F_N} \tag{2.17}$$

*donde $D \in \mathbb{C}^{N\times N}$ es una matriz diagonal, tal que $D_{n,n} = {}^1\!/_{\mathcal{F}_v[n]}$.*

La siguiente proposición expone la relación que hay entre una matriz circulante y una matriz de reflección.

**Proposición 1.** *Sea $v \in \mathbb{C}^N$, y sea la matriz $G \in \mathbb{C}^{N\times N}$ cuyas filas $g_m = \mathcal{S}_{-m}$, es decir*

$$G = \begin{pmatrix} v_0 & v_1 & \cdots & v_{N-1} \\ v_1 & v_2 & \cdots & v_0 \\ \vdots & \vdots & \ddots & \vdots \\ v_{N-1} & v_0 & \cdots & v_{N-2} \end{pmatrix}$$

*Entonces $R_N G = C_v$*

Para más detalles sobre matrices circulantes, ver el trabajo de P. J. Davis [30].

# CAPÍTULO 3
# REPRESENTACIONES DISCRETAS BIDIMENSIONALES

La búsqueda de métodos para analizar señales con el objetivo de conocer atributos relacionados con los procesos físicos que las generan, ha sido siempre tema de interés para ingenieros y matemáticos. Una de las técnicas más utilizadas ha sido representar las señales en el dominio del tiempo. Esto ha permitido asociar cambios físicos con el de los parámetros amplitud-tiempo de la señal. Posteriormente, el dominio de la frecuencia vino a complementar esta información. Sin embargo, si las señales no son estacionarias o están inmersas en ruido, entonces ni la representación temporal ni la representación frecuencial arrojarán información satisfactoria del proceso. En este caso la representación en el dominio dual tiempo-frecuencia puede producir resultados interesantes si se aseguran las condiciones que favorezcan la información relevante y minimicen el ruido. Este tipo de representaciones son bidimensionales y se ubican en el área del *análisis de tiempo-frecuencia*.

En el área de procesamiento de señales, el análisis de tiempo-frecuencia es un conjunto de técnicas y métodos utilizados para la caracterización y manipulación de señales cuyas estadísticas varían en el tiempo, tales como señales transitorias. Esto es una generalización y perfeccionamiento del análisis de Fourier. Dado que muchas señales de interés - tales como el habla, la música, imágenes y señales médicas - cambian sus características de frecuencia, las representaciones en tiempo-frecuencia tienen un alcance amplio de aplicaciones. Considerando que la técnica de la transformada de Fourier se puede ampliar para obtener el espectro de frecuencia de

cualquier señal de crecimiento lento localmente integrable, este enfoque requiere una descripción completa del comportamiento de la señal a lo largo de todos los tiempos. Para aprovechar el poder de una representación de frecuencia, sin la necesidad de una caracterización completa en el dominio del tiempo, primero se obtiene una distribución tiempo-frecuencia de la señal, lo que representa la señal en el tiempo y el dominio de la frecuencia de forma simultánea. En esta representación el dominio de la frecuencia sólo refleja el comportamiento de una versión localizada temporal de la señal. El análisis tiempo-frecuencias se puede hacer en dominos continuos y discretos. En el caso de utilizar dominios discretos, estos pueden ser finitos o infinitos.

Este capítulo empezará explicando el concepto de función discreta de ambigüedad, la cuál es una función bidimensional en tiempo y frecuencia y algunas propiedades. Además se explicarán tres casos particulares de funciones discretas bidimensionales, que se generan a partir de la función discreta de ambigüedad: la transformada discreta de Zak, la transformada de Fourier en tiempo corto y la distribución discreta de Cohen.

## 3.1 Función Discreta de Ambigüedad

### 3.1.1 Definición y propiedades

En 1953, P.M. Woodward define *función de la ambigüedad*, la cual trata de un mecanismo formulado para describir el efecto Doppler en los receptores de filtro apareados [31]. Woodward reconoció la influencia de la teoría de la comunicación de Shannon, a partir de 1948, en sus ideas, y explicó la importancia de la "ambigüedad" en el procesamiento de señales de radares, tal vez el mejor concebido en términos de una forma del principio de incertidumbre.

**Definición 9** (**Función Continua de Ambigüedad**). *Sea* $f, g \in L^2(\mathbb{R})$*, entonces la función de ambigüedad de* $f$ *y* $g$ *se define como el mapeo* $\mathcal{A}_{f,g} : \mathbb{R} \times \mathbb{R} \to L^2(\mathbb{R})$

*tal que*

$$\mathcal{A}_{f,g}(t,\theta) = \int_{\mathbb{R}} f(x)\overline{g}(x-t)e^{-2i\pi x\theta}dx \tag{3.1}$$

$\mathcal{A}_{f,g}$ recibe el nombre de *función de ambigüedad cruzada* cuando $f \neq g$. En el caso $f = g$ se conoce simplemente como función de ambigüedad. En este trabajo no se hará diferencia entra ambos casos y se definirá como función de ambigüedad para el caso $f \neq g$. Por diversos propósitos, varios autores definen la función de ambigüedad con ligeras modificaciones a la que se expresa en la ecuación (3.3.1):

- J. J. Benedetto y J. J. Donatelli [16, 32]:

$$\mathcal{A}^{i}_{f,g}(t,\theta) = \int_{\mathbb{R}} f(x+t)\overline{g}(x)e^{-2i\pi x\theta}dx. \tag{3.2}$$

- L. Cohen [33] y M. S. Richaman *et al* [12, 33]:

$$\begin{aligned}\mathcal{A}^{ii}_{f,g}(t,\theta) &= \int_{\mathbb{R}} f\left(x+\frac{t}{2}\right)\overline{g}\left(x-\frac{t}{2}\right)e^{2i\pi x\theta}dx \\ &= e^{i\pi x\theta}\int_{\mathbb{R}} f\left(x+t\right)\overline{g}\left(x\right)e^{2i\pi x\theta}dx\end{aligned} \tag{3.3}$$

- En L. Auslander y R. Tolimieri [34]

$$\mathcal{A}^{iii}_{f,g}(t,\theta) = \int_{\mathbb{R}} f(x)\overline{g}(x+t)e^{-2i\pi x\theta}dx. \tag{3.4}$$

A pesar de las diferencias, todas las representaciones de la función de ambigüedad mantienen una relación a nivel de módulo

$$|\mathcal{A}_{f,g}(t,\theta)| = |\mathcal{A}^{i}_{f,g}(t,\theta)| = |\mathcal{A}^{ii}_{f,g}(t,\theta)| = |\mathcal{A}^{iii}_{f,g}(-t,\theta)|.$$

Por lo tanto, las ecuaciones (3.2), (3.3) y (3.4) serán consideradas representaciones equivalentes de la función de ambigüedad. A nivel de implementación, la función de ambigüedad que desarrollo Woodward admite una representación con dominio discreto y finito.

**Definición 10** (**Función Discreta de Ambigüedad**). *Sean $x, y \in \mathbb{C}^N$, entonces la función discreta de ambigüedad (DAF, del inglés discrete ambiguity function) de $x$, $y$ se define como el mapeo $\mathcal{A}_{x,y} : l^2(\mathbb{Z}_N) \times l^2(\mathbb{Z}_N) \to l^2(\mathbb{Z}_N \times \mathbb{Z}_N)$ tal que*

$$\mathcal{A}^0_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[n]\overline{y}[\langle n-m\rangle_N]\omega_N^{-nk} = \sum_{n\in\mathbb{Z}_N} x[n]\overline{\mathcal{M}_k\mathcal{S}_m\{y\}}[n] \tag{3.5}$$

En este trabajo, la definición de $\mathcal{A}_{x,y}$ en la ecuación (3.5) se conocerá como *función discreta de ambigüedad Tipo 0* (DAF T-0). De forma similar al caso continuo, existen representaciones de la DAF con ligeras modificaciones a la DAF T-0.

**Definición 11** (**Representaciones Equivalentes de la DAF T-0**). *Sea $x, y \in \mathbb{C}^N$, entonces tres representaciones equivalentes de $\mathcal{A}^0_{x,y}$ se definen como:*

- *Función discreta de ambigüedad Tipo 1* (DAF T-1) *[16, 32]*

$$\mathcal{A}^1_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[\langle n+m\rangle_N]\overline{y}[n]\omega_N^{-nk} = \sum_{n\in\mathbb{Z}_N} \mathcal{M}_{-k}\mathcal{S}_{-m}\{x\}[n]\overline{y}[n] \tag{3.6}$$

- *Función discreta de ambigüedad Tipo 2* (DAF T-2) *[12]*

$$\begin{aligned}\mathcal{A}^2_{x,y}[m,k] &= \lambda_{m,k}\sum_{n\in\mathbb{Z}_N} x[\langle n+m\rangle_N]\overline{y}[n]\omega_N^{nk} \\ &= \sum_{n\in\mathbb{Z}_N} \mathcal{C}_{\lambda_{m,k}}\mathcal{M}_k\mathcal{S}_{-m}\{x\}[n]\overline{y}[n]\end{aligned} \tag{3.7}$$

*donde*

$$\lambda_{m,k}{}^{1} = \begin{cases} \omega_N^{qmk} & N \text{ impar, } 2q \equiv 1 \bmod N \\ \omega_N^{mk/2} & N \text{ par, } \langle mk\rangle_N < \frac{N}{2} \\ \omega_N^{(mk-N)/2} & N \text{ par, } \langle mk\rangle_N \geqslant \frac{N}{2} \end{cases}$$

[1] La representación en continuo - ecuación (3.7) - posse la fracción 1/2, y como 1/2 no es un elemento de $\mathbb{Z}_N$, se consideran 3 casos de la constante $e^{i\frac{2\pi}{N}\langle\frac{mk}{2}\rangle_N}$. Ver [12] para mas detalles.

- *Función discreta de ambigüedad Tipo 3* (DAF T-3) *[11, 13]*

$$\mathcal{A}^3_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[n]\overline{y}[\langle n+m\rangle_N]\omega_N^{-nk} = \sum_{n\in\mathbb{Z}_N} x[n]\overline{\mathcal{M}_k\mathcal{S}_{-m}\{y\}}[n] \tag{3.8}$$

De igual manera que en el caso continuo, los diferentes tipos de DAF's presentan una equivalencia entre modulos:

$$|\mathcal{A}^0_{x,y}[m,k]| = |\mathcal{A}^1_{x,y}[m,k]| = |\mathcal{A}^2_{x,y}[m,k]| = |\mathcal{A}^3_{x,y}[-m,k]|.$$

### 3.1.2 Representación Matricial

Al ser la DAF una función de dos dimensiones, entonces se puede aprovechar esta estructura para representarla como una matriz.

**Definición 12** (**Matriz DAF**). *Sea $x, y \in \mathbb{C}^N$. La matriz DAF T-l se define como $A^l_{x,y} \in \mathbb{C}^{N\times N}$ tal que $(A^l_{x,y})_{m,k} = \mathcal{A}^l_{x,y}[m,k]$, para $m,k \in \mathbb{Z}_N$ y $l = 0,1,2,3$.*

La matriz DAF se puede calcular utilizando computo en paralelo, mediante una estructura que utiliza el producto Kronecker y Hadamard.

**Teorema 9.** *Sea $x, y \in \mathbb{C}^N$ y $A^0_{x,y} \in \mathbb{C}^{N\times N}$ la matriz DAF T-0. Entones*

$$A^0_{x,y} = \mathcal{R}_{N,N}\{L^{N^2}_N\,[I_N \otimes F_N]\,[(\mathbf{1}_N \otimes x)\odot Y]\}, \tag{3.9}$$

*donde $Y \in \mathbb{C}^{N^2}$ tal que $Y = \bigsqcup_{m\in\mathbb{Z}_N} \mathcal{S}_m\{\overline{y}\}$.*

**Prueba.** *Sea $a_{x,y} = L^{N^2}_N\,[I_N \otimes F_N]\,[(\mathbf{1}_N \otimes x)\odot Y]$. Desarrollando el vector $a^0_{x,y}$, se obtiene*

$$a_{x,y} = L^{N^2}_N \bigsqcup_{m\in\mathbb{Z}_N} H_m, \quad H_m \in \mathbb{C}^N$$

*tal que $H_m = F_N(x \odot \mathcal{S}_m\{\overline{y}\})$. Aplicando a ambos lados de la ecuación el operador $\mathcal{R}_{N,N}$, por* **Teorema 3** *se obtiene:*

$$\mathcal{R}_{N,N}\{a_{x,y}\} = \mathcal{R}_{N,N}\left\{L^{N^2}_N \bigsqcup_{m\in\mathbb{Z}_N} H_m\right\} = \left(\mathcal{R}_{N,N}\left\{\bigsqcup_{m\in\mathbb{Z}_N} H_m\right\}\right)^T$$

*Sea* $H = \mathcal{R}_{N,N}\left\{\bigsqcup_{m\in\mathbb{Z}_N} H_m\right\}$, *con* $H \in \mathbb{C}^{N\times N}$ *y* $H = (H_0, H_1, ..., H_{N-1})$. *Si* $(H)_{m,k} = h_{m,k}$, *para* $m, k \in \mathbb{Z}_N$ *se cumple*

$$h^T_{m,k} = h_{k,m} = H_m[k] = \sum_{n\in\mathbb{Z}_N} x[n]\overline{\mathcal{M}_k\mathcal{S}_m\{y\}} = A^0_{x,y}[m,k]$$

*Por lo tanto,*

$$A^0_{x,y} = \mathcal{R}_{N,N}\{L^{N^2}_N\left[I_N \otimes F_N\right]\left[(\mathbf{1}_N \otimes x)\odot Y\right]\}$$

■

En **Algoritmo 8**, muestra la implementación de la ecuación (3.9). Los pasos 2-3 son independientes en cada iteración, lo que permite su cómputo en paralelo.

**Algoritmo 8** Matriz DAF T-0

**Entrada:** $x, y \in \mathbb{C}^N$
**Salida:** $A \in \mathbb{C}^{N\times N}$
1: **para** $n = 0 : N-1$ **hacer**
2: $\quad v_n \leftarrow x \odot \mathcal{S}_n\{\overline{y}\}$
3: $\quad A[:, n] \leftarrow \mathcal{F}_{v_n}$
4: **fin para**
5: $A \leftarrow A^T$

La Tabla 3–1 muestra la representación matricial de los cuatro tipos de DAF.

Tabla 3–1: Representación Kronecker de la matrices DAF's

$$A^l_{x,y} = \mathcal{R}_{N,N}\{a_{x,y}\}$$

| $T-l$ | $a_{x,y}$ | $X-Y$ | $P$ |
|---|---|---|---|
| $T-0$ | $L^{N^2}_N\left[I_N \otimes F_N\right]\left[(\mathbf{1}_N \otimes x)\odot Y\right]$ | $\bigsqcup_{m\in\mathbb{Z}_N} \mathcal{S}_m\{\overline{y}\}$ | |
| $T-1$ | $L^{N^2}_N\left[I_N \otimes F_N\right]\left[X \odot (\mathbf{1}_N \otimes \overline{y})\right]$ | $\bigsqcup_{m\in\mathbb{Z}_N} \mathcal{S}_{-m}\{x\}$ | |
| $T-2$ | $L^{N^2}_N P\left[I_N \otimes \overline{F_N}\right]\left[X \odot (\mathbf{1}_N \otimes \overline{y})\right]$ | $\bigsqcup_{m\in\mathbb{Z}_N} \mathcal{S}_{-m}\{x\}$, | $\bigoplus_{m,k\in\mathbb{Z}_N} diag(\lambda_{m,k})$ |
| $T-3$ | $L^{N^2}_N\left[I_N \otimes F_N\right]\left[(\mathbf{1}_N \otimes x)\odot Y\right]$ | $\bigsqcup_{m\in\mathbb{Z}_N} \mathcal{S}_{-m}\{\overline{y}\}$ | |

## 3.2 Un método para computar la inversa de la DAF

### 3.2.1 Formulación del problema de la inversa de la DAF

En esta sección se desarrollará un método para resolver el siguiente problema: *Conociendo los valores de la señal $x$ y la DAF de $x, y$, ¿bajo que condiciones y con que método se puede recuperar la función $y$?.* Dicho problema consiste en obtener la inversa de DAF para la señal $y$. Para ser más específicos, se desea recuperar $y$ a partir de $x$ y de una parte de la matriz DAF, ya sea una fila o una columna de la matriz.

### 3.2.2 Utilizando una fila de la matriz DAF

Considere la DAF T-0. Sea $x \in \mathbb{C}^N$. Considere $m \in \mathbb{Z}_N$ fijo y sea $A^0_{x,y}[m,:]$ la fila $m$ de la matriz DAF T-0. Entonces,

$$A^0_{x,y}[m,k] = \sum_{n\in\mathbb{Z}_N} x[n]\overline{y}[\langle n-m\rangle_N]\omega_N^{-nk}, \quad k \in \mathbb{Z}_N$$

Utilizando la ecuación anterior, considere los siguientes pasos:

**Paso 1** Aplicar IDFT:

$$\mathcal{F}^{-1}\{A^0_{x,y}\}[n] = x[n]\overline{y}[\langle n-m\rangle_N]$$

**Paso 2** Dividir por $x[n]$, asumiendo que $x[n] \neq 0$:

$$\frac{\mathcal{F}^{-1}\{A^0_{x,y}\}[n]}{x[n]} = \overline{y}[\langle n-m\rangle_N]$$

**Paso 3** Aplicar operador de traslación $\mathcal{S}_{-m}$:

$$\mathcal{S}_{-m}\left\{\frac{\mathcal{F}^{-1}\{A^0_{x,y}\}[n]}{x[n]}\right\} = \mathcal{S}_{-m}\left\{\overline{y}[\langle n-m\rangle_N]\right\} = \overline{y}[n]$$

**Paso 4** Aplicar transpuesta:

$$\overline{\mathcal{S}_{-m}\left\{\frac{\mathcal{F}^{-1}\{A^0_{x,y}\}[n]}{x[n]}\right\}} = y[n]$$

En el **Paso 2**, es fundamental que $x[n] \neq 0$. Por lo tanto, para recuperar el vector $y$ a partir del vector $x$ y a partir de una fila de la matriz DAF T-0, una condición necesaria para $x$ es que $x[n] \neq 0$, para todo $n \in \mathbb{Z}_N$. Lo anterior prueba el siguiente teorema

**Teorema 10.** *Sean $x, y \in \mathbb{C}^N$, donde $x[n] \neq 0$, para todo $n \in \mathbb{Z}_N$, y $A^0_{x,y} \in \mathbb{C}^{N\times N}$ la matriz que representa a la DAF T-0. Entonces*

$$y = \frac{1}{N} S_{-m} M \overline{F}_N b \tag{3.10}$$

*donde $S_{-m} \in \mathbb{C}^{N\times N}$ es una matriz de traslación, $M \in \mathbb{C}^{N\times N}$ es una matriz diagonal tal que $M = diag\left(\frac{1}{x[0]}, \frac{1}{x[1]}, ..., \frac{1}{x[N-1]}\right)$ y $b \in \mathbb{C}^N$ tal que $b[n] = \overline{A^0_{x,y}}[m, n]$.*

El **Algoritmo 9** muestra la implementación de método inverso de la DAF T-0.

**Algoritmo 9** Inversa DAF T-0

**Entrada:** $m \in \mathbb{Z}_N$, $x \in \mathbb{C}^N$ y $a_m \in \mathbb{C}^N$
**Salida:** $y \in \mathbb{C}^N$
1: $v_0 \leftarrow \mathcal{F}^{-1}\{a_m\}$
2: $v_2 \leftarrow v_0 \odot v_1$, donde $v_1[n] = {}^1\!/_{x[n]}$
3: $v_3 \leftarrow \mathcal{S}_{-m}\{v_2\}$
4: $y \leftarrow \overline{v_3}$

De forma equivalente, se puede implementar este método utilizando la DAF T-1 y T-3. La Tabla 3–2 explica el procedimiento de recuperar la función $y$, utilizando cada uno de los tipos de DAF. De la DAF T-2 no se puede obtener una representación inversa, debido al valor de la constante $\lambda_{m,k}$.

Tabla 3–2: Representación matricial del método inverso

| DAF | $y$ | $b[n]$ | $M_{n,n}$ |
|---|---|---|---|
| T-0 | $\frac{1}{N} S_{-m} M \overline{F}_N b$ | $\overline{\mathcal{A}^0_{x,y}}[m, n]$ | $(x[n])^{-1}$ |
| T-1 | $\frac{1}{N} M \overline{F}_N b$ | $\overline{\mathcal{A}^1_{x,y}}[m, n]$ | $(\mathcal{S}_m\{x\}[n])^{-1}$ |
| T-3 | $\frac{1}{N} S_m M \overline{F}_N b$ | $\overline{\mathcal{A}^3_{x,y}}[m, n]$ | $(x[n])^{-1}$ |

### 3.2.3 Utilizando una columna de la matriz DAF

Considere la DAF T-1. Fijando el valor de la primera entrada ($k$) de la DAF T-1, se obtiene el siguiente sistema de ecuaciones, variando el valor de la primera entrada ($m$).

$$\begin{cases} \sum\limits_{n\in\mathbb{Z}_N} \mathcal{M}_{-k}\mathcal{S}_0\{x\}[n]\overline{y}[n] = \mathcal{A}^1_{x,y}[0,k] \\ \sum\limits_{n\in\mathbb{Z}_N} \mathcal{M}_{-k}\mathcal{S}_{-1}\{x\}[n]\overline{y}[n] = \mathcal{A}^1_{x,y}[1,k] \\ \qquad\qquad\vdots \\ \sum\limits_{n\in\mathbb{Z}_N} \mathcal{M}_{-k}\mathcal{S}_{-(N-1)}\{x\}[n]\overline{y}[n] = \mathcal{A}^1_{x,y}[N-1,k] \end{cases} \tag{3.11}$$

y la representación matricial de dicho sistema es

$$\underbrace{\begin{pmatrix} x_0 & x_1\omega_N^{-k} & \cdots & x_{N-1}\omega_N^{-(N-1)k} \\ x_1 & x_2\omega_N^{-k} & \cdots & x_0\omega_N^{-(N-1)k} \\ \vdots & \vdots & \ddots & \vdots \\ x_{N-1} & x_0\omega_N^{-k} & \cdots & x_{N-2}\omega_N^{-(N-1)k} \end{pmatrix}}_{Z} \begin{pmatrix} \overline{y_0} \\ \overline{y_1} \\ \vdots \\ \overline{y_{N-1}} \end{pmatrix} = \begin{pmatrix} \mathcal{A}^1_{x,y}[0,k] \\ \mathcal{A}^1_{x,y}[1,k] \\ \vdots \\ \mathcal{A}^1_{x,y}[N-1,k] \end{pmatrix} \tag{3.12}$$

Ahora, sea la matriz $W \in \mathbb{C}^{N\times N}$ tal que $W = diag(1, \omega_N^{-k}, ..., \omega_N^{-(N-1)k})$, entonces

$$Z = ZW^{-1}W = \underbrace{\begin{pmatrix} a_0 & a_1 & \cdots & a_{N-1} \\ a_1 & a_2 & \cdots & a_0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{N-1} & a_0 & \cdots & a_{N-2} \end{pmatrix}}_{ZW^{-1}} \underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega_N^{-k} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega_N^{-(N-1)k} \end{pmatrix}}_{W} \tag{3.13}$$

Por lo tanto, de la ecuación (3.12) se obtiene:

$$\underbrace{\begin{pmatrix} x_0 & x_1 & \cdots & x_{N-1} \\ x_1 & x_2 & \cdots & x_0 \\ \vdots & \vdots & \ddots & \vdots \\ x_{N-1} & x_0 & \cdots & x_{N-2} \end{pmatrix}}_{X} \underbrace{\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega_N^{-k} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega_N^{-(N-1)k} \end{pmatrix}}_{W} \underbrace{\begin{pmatrix} \overline{y_0} \\ \overline{y_1} \\ \vdots \\ \overline{y_{N-1}} \end{pmatrix}}_{\overline{y}} = \underbrace{\begin{pmatrix} \mathcal{A}^1_{x,y}[0,k] \\ \mathcal{A}^1_{x,y}[1,k] \\ \vdots \\ \mathcal{A}^1_{x,y}[N-1,k] \end{pmatrix}}_{c}$$

$$\Rightarrow XW\overline{y} = c \tag{3.14}$$

Sea $R_N \in \mathbb{C}^{N\times N}$ una matriz de reflexión. Aplicando la **Proposición 4** a la ecuación (3.14), se obtiene

$$R_N XW\overline{y} = R_N c \Rightarrow C_x W\overline{y} = d \tag{3.15}$$

donde $d[n] = \mathcal{A}^1_{x,y}[\langle -n\rangle_N, k]$ y $R_N X = C_x$ es la matriz circulante del vector $x$. Asumiendo que $\mathcal{F}_x[n] \neq 0$, para todo $n \in \mathbb{Z}_N$, entonces, por **Lema 2**, $C_x$ posee inversa

$$C_x^{-1} = \tfrac{1}{N} F_N D \overline{F_N} \tag{3.16}$$

donde $D$ es una matriz diagonal tal que $D = \left(\frac{1}{\mathcal{F}_x[0]}, \frac{1}{\mathcal{F}_x[1]}, ..., \frac{1}{\mathcal{F}_x[N-1]}\right)$. Por lo tanto, asumiendo que $C_x$ es invertible, entonces

$$\begin{aligned} y &= \overline{W^{-1}C_x^{-1}c} \\ &= \tfrac{1}{N} W\overline{F_N} M F_N R_N b \end{aligned}$$

donde $M \in \mathbb{C}^{N\times N}$ es una matriz diagonal tal que $M_{n,n} = \frac{1}{\overline{\mathcal{F}_x[n]}}$, $b \in \mathbb{C}^N$ tal que $b[n] = \overline{\mathcal{A}^0_{x,y}}[n,k]$, para $l = 0, 1$ y $W \in \mathbb{C}^{N\times N}$ es una matriz diagonal. Lo anterior demuestra el siguiente teorema.

**Teorema 11.** *Sean $x, y \in \mathbb{C}^N$, $\mathcal{F}_x[k] \neq 0$, para todo $k \in \mathbb{Z}_N$, y $A^1_{x,y} \in \mathbb{C}^{N\times N}$ la matriz que representa a la DAF T-1. Entonces*

$$y = \frac{1}{N} W\overline{F_N} M F_N R_N b \tag{3.17}$$

*donde*

- $M \in \mathbb{C}^{N\times N}$ *es una matriz diagonal tal que* $M_{n,n} = {}^{1}/\overline{\mathcal{F}_x}[n]$.
- $b \in \mathbb{C}^N$ *tal que* $b[n] = \overline{\mathcal{A}^1_{x,y}}[n,k]$.
- $W \in \mathbb{C}^{N\times N}$ *es una matriz diagonal tal que* $W_{n,n} = \omega_N^{-nk}$.
- $R_N \in \mathbb{C}^{N\times N}$ *es una matriz de reflexión.*

En **Algoritmo 10** se muestra la implementación de método inverso de la DAF T-0, utilizando la columna $k$ de dicha matriz.

**Algoritmo 10** Inversa DAF T-0

**Entrada:** $k \in \mathbb{Z}_N$, $x \in \mathbb{C}^N$ y $a_k \in \mathbb{C}^N$
**Salida:** $y \in \mathbb{C}^N$

1: $v_0 \leftarrow \overline{a_k}$
2: $v_1 \leftarrow \mathcal{L}_r\{v_0\}$
3: $v_2 \leftarrow \mathcal{F}_{v_1}$
4: $v_4 \leftarrow v_2 \odot v_3$, donde $v_3[n] = 1/\overline{\mathcal{F}_x}[n]$
5: $v_5 \leftarrow \mathcal{F}^{-1}_{v_4}$
6: $y \leftarrow v_5 \odot v_6$, donde $v_6[n] = \omega_N^{-nk}$

Para DAF T-1 y DAF T-3, se resuelve de forma similar. Para DAF T-2 no se puede resolver de la misma manera, utilizando matrices circulantes, ya que la matriz que se obtiene del sistema de ecuaciones no se puede descomponer de forma similar al caso DAF T-1. La Tabla 3–3 explica el procedimiento de recuperar la función $y$ para los cuatro tipos de DAF.

Tabla 3–3: Tabla para recuperar la función $y$

| DAF | $y$ | $b[n]$ | $M_{n,n}$ | $W_{n,n}$ |
|---|---|---|---|---|
| T-0 | $\frac{1}{N}\overline{F_N}S_{-k}MS_kF_MR_Nb$ | $\overline{\mathcal{A}^0_{x,y}}[n,k]$ | $\frac{1}{\overline{\mathcal{F}_x[n]}}$ | $\omega_N^{-nk}$ |
| T-1 | $\frac{1}{N}W\overline{F_N}MF_MR_Nb$ | $\overline{\mathcal{A}^1_{x,y}}[n,k]$ | $\frac{1}{\overline{\mathcal{F}_x[n]}}$ | $\omega_N^{-nk}$ |
| T-3 | $\frac{1}{N}\overline{F_N}S_{-k}MS_kF_Mb$ | $\overline{\mathcal{A}^3_{x,y}}[n,k]$ | $\frac{1}{\overline{\mathcal{F}_x[n]}}$ | $\omega_N^{-nk}$ |

## 3.3 Función Discreta de Ambigüedad como ente generadora de distribuciones bidimensionales

En esta sección se explicarán tres distribuciones discretas bidimensionales que son generadas a partir de la DAF: la transformada discreta de Fourier en tiempo corto, la transformada discreta de Zak y la distribución discreta de Cohen.

### 3.3.1 Transformada Discreta de Fourier en Tiempo Corto

#### Definición y propiedades de la transformada

En diversa aplicaciones, la funciones no tienen el espectro de la frecuencia constante, ya que este varía con respecto al tiempo [35]. Estas señales no estacionarias no deben ser analizados con transformada de Fourier convencional, porque entonces los resultados sólo producen un promedio que no están asociados a instantes de un tiempo en particular. Un enfoque para el análisis de estas señales periódicas no estacionario es utilizar la transformada de Fourier en tiempo corto, el cuál es un caso particular de la función continua de ambigüedad .

**Definición 13** (**Transformada de Fourier en Tiempo Corto).** *Sea* $f, w \in L^2(\mathbb{R})$*, tal que* $w$ *es una función ventana. La transformada de Fourier en tiempo corto (STFT, del inglés short-time Fourier transform) de* $f$ *con ventana* $w$ *se define como el mapeo* $S_{f,w} : \mathbb{R} \times \mathbb{R} \to L^2(\mathbb{R} \times \mathbb{R})$ *tal que*

$$\mathcal{ST}_{f,w}(t, \theta) = \int_{\mathbb{R}} f(x) w(x - t) e^{-j2\pi t\theta} dx \tag{3.18}$$

Una *función ventana* es una función de valor real que es cero fuera de algún conjunto $I$. El conjunto $I$ recibe el nombre de *conjunto soporte de la función* $w$, o simplemente *soporte de* $w$, y se define como

$$I = \{x : w(x) \neq 0\}.$$

Por ejemplo, una función que es constante en el interior de un conjunto $I$ y 0 afuera de $I$, se llama una *ventana rectangular*, la cuál describe la forma de la representación gráfica de la función $f$. Cuando la función $f$ se multiplica por una función ventana

$w$ con soporte $I$, el producto $fw$ también toma el valor cero fuera del intervalo $I$, es decir que el soporte de $fw$ es el mismo que el de $w$.

La transformada de Fourier en tiempo corto tiene su representación con dominio discreto y finito.

**Definición 14** (**Transformada Discreta de Fourier en Tiempo Corto).** *Sea $x \in \mathbb{C}^N$ y $w \in \mathbb{R}^M$, con $M \ll N$. Aplicando zero padding a la función $w$, entonces $w$ puede ser re-definida tal que $w \in \mathbb{C}^N$:*

$$w[n] = \begin{cases} w[n] & si \quad n \in \mathbb{Z}_M \\ 0 & si \quad n = M, M+1, ..., N-1 \end{cases}$$

*La transformada discreta de Fourier en tiempo corto (STDFT, del inglés short-time discrete Fourier transform) de $x$ con ventana $w$ se define como el mapeo $\mathcal{ST}_{x,w}$ : $l^2(\mathbb{Z}_N) \times l^2(\mathbb{Z}_N) \to l^2(\mathbb{Z}_N \times \mathbb{Z}_N)$ tal que*

$$\begin{aligned} \mathcal{ST}_{x,w}[m,k] &= \sum_{n \in \mathbb{Z}_N} x[n] w[\langle n-m \rangle_N] \omega_N^{-nk} \\ &= \sum_{n \in \mathbb{Z}_N} x[n] \mathcal{M}_{-k} \mathcal{S}_m \{w\}[n] \end{aligned} \tag{3.19}$$

La STDFT se relaciona con la DAF T-0, ya que $\mathcal{ST}_{x,w} = \mathcal{A}^0_{x,w}$. La Tabla 3–4 muestra algunos ejemplos de funciones ventanas en $\mathbb{C}^M$.

Tabla 3–4: Funciones ventanas

| **Nombre** | $w[n]$ |
|---|---|
| Rectangular | $1$ |
| Hann | $0.5\left(1 - \cos\left(\frac{2\pi n}{M-1}\right)\right)$ |
| Hamming | $0.54 - 0.46\cos\left(\frac{2\pi n}{M-1}\right)$ |
| Coseno/Seno | $\cos\left(\frac{\pi n}{M-1} - \frac{\pi}{2}\right) = \sin\left(\frac{\pi n}{M-1}\right)$ |
| Lanczos | $\frac{\sin(\pi(2n/(M-1)-1))}{\pi(2n/(M-1)-1)}$ |
| Triangular | $\frac{2}{M-1}\left(\frac{M-1}{2} - \left\lvert n - \frac{M-1}{2}\right\rvert\right)$ |
| Gausiana | $e^{-\frac{1}{2}\left(\frac{n-(M-1)/2}{\sigma(M-1)/2}\right)^2}, \quad \sigma \leqslant 0.5$ |

Por ser un caso particular de la DAF T-0, la STDFT también tiene una representación matricial.

**Definición 15** (**Matriz STDFT**). *Sea $x, w \in \mathbb{C}^N$. La matriz STDFT se define como $ST_{x,w} \in \mathbb{C}^{N\times N}$ tal que $(ST_{x,w})_{m,k} = \mathcal{ST}_{x,w}[m,k]$, para $m,k \in \mathbb{Z}_N$.*

De igual manera que la matriz DAF T-0, la matriz STDFT se puede calcular utilizando computo en paralelo, realizando una representación utilizando productos Kronecker. Como $\mathcal{ST}_{x,w} = \mathcal{A}^0_{x,w}$, entonces $(ST_{x,w})_{m,k} = (A^0_{x,w})_{m,k}$, para $m,k \in \mathbb{Z}_N$. Del **Teorema 9** se obtiene el siguiente corolario.

**Corolario 2.** *Sea $x, w \in \mathbb{C}^N$, donde $w$ es una función ventana con zero-padding, y $ST_{x,w} \in \mathbb{C}^{N\times N}$ la matriz STDFT. Entones*

$$ST_{x,w} = \mathcal{R}_{N,N}\{L^{N^2}_N\,[I_N \otimes F_N]\,[(\mathbf{1}_N \otimes x) \odot W]\},$$

*donde $W \in \mathbb{C}^{N^2}$ tal que $W = \bigsqcup_{m\in\mathbb{Z}_N} S_m\{w\}$.*

### 3.3.2 Transformada Discreta de Zak

#### Definición y propiedades de la transformada

La transformada de Zak es una función que se desarrolló originalmente para tratar problemas de la física de estado sólido y fue descubierta independientemente por varias personas en distintos ámbitos, pero se hizo muy conocido a partir de Zak [36] en 1967, quien lo utilizó para construir una representación de la mecánica cuántica para el movimiento de electrones en un campo magnético. Desde entonces se ha utilizado para resolver diversos problemas en matemáticas y física.

**Definición 16** (**Transformada de Zak**). *Sea $f \in L^2(\mathbb{R})$, entonces la transformada de Zak (TZ) [37, 38] se define como el mapeo $\mathcal{Z}_{f,a} : \mathbb{R}\times\mathbb{R} \to L^2(\mathbb{R}\times\mathbb{R})$ tal que:*

$$\mathcal{Z}_{f,a}(t,\theta) = \sum_{n\in\mathbb{Z}} f(an+t)e^{j2\pi n\theta}, \quad a \in \mathbb{Z} \tag{3.20}$$

En el campo de procesamiento de señales, la TZ se utiliza frecuentemente para calcular la frecuencia de tiempo de las representaciones incluidas las funciones de la ambigüedad [39], desarrollo de expansiones Weyl-Heisenberg [40], transformada wavelet [41], DFT filter banks y su relación con la discreta expansión de Gabor [42, 43], estimación de parametros de la función chirp, además de la detección y

eliminación de ruido [44] y decimación tiempo-frecuencia discreta de distribuciones bidimensionales [4]. Otra aplicación es el realizado por L. Auslander y R. Tolimieri [43], el cual desarrollan un algoritmo computacional para calcular los coeficientes de la expansión de Gabor cuando el dominio es discreto y continuo, usando la función continua de ambigüedad, para el caso $a = 1$. Por lo tanto, para nuestros propositios, utilizaremos el caso $a = 1$ para definir la transformada discreta de Zak de dominio discreto y finito.

**Definición 17** (**Transformada Discreta de Zak).** *La transformada discreta de Zak (DZT, del inglés discrete Zak transform) se define como el mapeo* $\mathcal{Z}_x : l^2(\mathbb{Z}_N) \times l^2(\mathbb{Z}_N) \to l^2(\mathbb{Z}_N \times \mathbb{Z}_N)$ *tal que*

$$\begin{aligned} \mathcal{Z}_x[m,k] &= \sum_{n\in\mathbb{Z}_N} x[\langle n+m\rangle_N]\omega_N^{-nk} \\ &= \sum_{n\in\mathbb{Z}_N} \mathcal{M}_{-k}\mathcal{S}_m\{x\}[n] \end{aligned} \tag{3.21}$$

La DZT es una generalización de la DFT en el sentido de que proporciona una codificación simultánea de una señal de tiempo y la información de frecuencia [45]. La DZT es cuasi-periódica, ya que

- $\mathcal{Z}_x[m+1,k] = \omega_N^{-k}\mathcal{Z}_x[m,k]$.
- $\mathcal{Z}_x[m,k+N] = \mathcal{Z}_x[m,k]$.

De lo anterior se deduce $\mathcal{Z}_x[m,k] = \omega_N^{-mk} Z_x[0,k]$. Esto implica que $\mathcal{Z}_x$ está definida en el subconjunto $\{0\} \times \mathbb{Z}_N \subset \mathbb{Z}_N \times \mathbb{Z}_N$. Además $\mathcal{Z}_x[0,k] = \mathcal{F}_x[k]$. De lo anterior, se obtiene la siguiente proposición:

**Proposición 2.** *Sea* $x \in \mathbb{C}^N$. *Entonces:*

$$\mathcal{Z}_x[m,k] = \omega_N^{-mk}\mathcal{F}_x[k] \tag{3.22}$$

Dado $\mathcal{Z}_x$, es posible recobrar el valor del vector $x$ [44], mediante la fórmula

$$x[\langle n+m\rangle_N] = \frac{1}{N}\sum_{n\in\mathbb{Z}_N} \mathcal{Z}_x[m,k]\omega_N^{-nk}$$

Si $m = 0$, entonces la función $x$ puede ser recobrada a partir de $\mathcal{Z}_x[0,k] \in \mathbb{C}^N$, $k \in \mathbb{Z}_N$, utilizando la inversa DZT (IDZT).

**Definición 18 (Inversa DZT).** *Sea $x \in \mathbb{C}^N$. La inversa de la DZT se define como*

$$\mathcal{Z}_x^{-1}[n] = x[n] = \frac{1}{N} \sum_{k \in \mathbb{Z}_N} \mathcal{Z}_x[0,k] \omega_N^{-nk} \tag{3.23}$$

Por ser un caso particular de la DAF T-1, la DZT también tiene una representación matricial.

**Definición 19 (Matriz DZT).** *La matriz DFT se define como $Z_x \in \mathbb{C}^{N \times N}$ tal que $(Z_x)_{m,k} = \mathcal{Z}_{x,y}[m,k]$, para $m,k \in \mathbb{Z}_N$.*

De forma similar a la matriz DAF, la matriz DZT se puede calcular utilizando computo en paralelo, realizando una representación utilizando productos Kronecker. Como $\mathcal{Z}_x = \mathcal{A}^1_{x,1_N}$, entonces $(Z_x)_{m,k} = (A^1_{x,1_N})_{m,k}$, para $m,k \in \mathbb{Z}_N$. De la **Tabla 3–1** se obtiene el siguiente corolario.

**Corolario 3.** *Sea $x \in \mathbb{C}^N$ y $Z_x \in \mathbb{C}^{N \times N}$ la matriz DZT. Entones*

$$Z_x = \mathcal{R}_{N,N}\{L_N^{N^2}(I_N \otimes F_N) X\},$$

*donde $X \in \mathbb{C}^{N^2}$ tal que $X = \bigsqcup_{m \in \mathbb{Z}_N} S_m\{x\}$.*

Otra forma de representar la matriz DZT es utilizando el resultado obtenido en la Proposición 2, del cuál se obtiene el siguiente lema.

**Lema 3.** *Sea $x \in \mathbb{C}^N$ y $Z_x \in \mathbb{C}^{N \times N}$ la matriz DZT. Entonces*

$$Z_x = F_N \odot (\mathbf{1}_N \otimes \mathcal{F}_x^T). \tag{3.24}$$

### Transformada Discreta de Zak y Función Discreta de Ambigüedad

La DZT se puede expresar en función de los 4 tipos de DAF:

$$\mathcal{Z}_x[m,k] = \mathcal{A}^0_{x,\mathbf{1}_N}[-m,k] = \mathcal{A}^1_{x,\mathbf{1}_N}[m,k] = \frac{1}{\lambda_{m,k}} \mathcal{A}^2_{x,\mathbf{1}_N}[m,-k] = \mathcal{A}^3_{\mathbf{1}_N,\overline{x}}[m,k].$$

Además, los 4 tipos de DAF se pueden definir en función de la DZT.

**Teorema 12.** *Sean $x, y \in \mathbb{C}^N$, $v_m, w_m, z_m \in \mathbb{C}^N$ tal que*

- $v_m[n] = \mathcal{S}_m\{x\}[n]\overline{y}[n]$.
- $w_m[n] = x[n]\overline{\mathcal{S}_m\{y\}}[n]$.
- $z_m[n] = \mathcal{S}_m\{x\}[n]\overline{\mathcal{S}_{2m}\{y\}}[n]$

*para* $n, m \in \mathbb{Z}_N$. *Entonces*

- $\mathcal{A}^0_{x,y}[m,k] = \mathcal{Z}_{v_m}[-m,k]$
- $\mathcal{A}^1_{x,y}[m,k] = \mathcal{Z}_{w_m}[m,k]$
- $\mathcal{A}^2_{x,y}[m,k] = \lambda_{m,k}\mathcal{Z}_{w_m}[m,-k]$
- $\mathcal{A}^3_{x,y}[m,k] = \mathcal{Z}_{z_m}[m,k]$

**Prueba.** *Sin pérdida de generalidad, se demostrará el primer caso. Los otros casos son similares.*

$$\begin{aligned}
\mathcal{Z}_{v_m}[-m,k] &= \sum_{n\in\mathbb{Z}_N} v_m[\langle n+m\rangle_N]\omega_N^{-nk} \\
&= \sum_{n\in\mathbb{Z}_N} x[\langle\langle n+m\rangle_N - m\rangle_N]\overline{y}[\langle\langle n+m\rangle_N - 2m\rangle_N]\omega_N^{-nk} \\
&= \sum_{n\in\mathbb{Z}_N} x[n]\overline{y}[\langle n-m\rangle_N]\omega_N^{-nk} \\
&= \mathcal{A}^0_{x,y}[m,k]
\end{aligned}$$

■

Ahora, si se consideran las funciones $x, x_+, x_- \in \mathbb{C}^N$ tal que $x_-[n] = x[n] - 1$ y $x_+[n] = x[n] + 1$, entonces

$$\mathcal{A}^1_x[m,k] + \mathcal{Z}_x[m,k] = \mathcal{A}^1_{x,x_+}[m,k] \tag{3.25}$$

$$\mathcal{A}^1_x[m,k] - \mathcal{Z}_x[m,k] = \mathcal{A}^1_{x,x_-}[m,k] \tag{3.26}$$

Restando ambas ecuaciones y despejando para $\mathcal{Z}_x[m,k]$, se obtiene la siguiente proposición.

**Proposición 3.** *Sean* $x, x_+, x_- \in \mathbb{C}^N$, *tal que* $x_+[n] = x[n] + 1$ *y* $x_-[n] = x[n] - 1$. *Entonces*

$$\mathcal{Z}_x[m,k] = \frac{\mathcal{A}^1_{x,x_+}[m,k] - \mathcal{A}^1_{x,x_-}[m,k]}{2} \tag{3.27}$$

### 3.3.3 Distribución Discreta de Cohen

#### Definición y propiedades de la distribución

Uno de los principales usos de la función de ambigüedad fue el realizado por L. Cohen en el artículo "*Generalized Phase-Space Distribution Functions*" [5] y luego profundizando en su libro "*Time-frequency analysis: theory and applications*"

[33]. Cohen desarrolló una representación general de cualquier función en tiempo-frecuencia continua, la cuál denominó *clase general*. Cohen describe que toda representación bidimensional en tiempo-frecuencia, para $f \in L^2(\mathbb{R})$, puede ser obtenida a partir del mapeo $\mathcal{CG}_f : \mathbb{R} \times \mathbb{R} \to L^2(\mathbb{R} \times \mathbb{R})$ expresado como

$$\mathcal{CG}_f(t,\theta) = \int\int \mathcal{A}_f^2(\tau,\eta)\phi(\tau,\eta)e^{-j2\pi(t\eta+\theta\tau)}\, d\eta\, d\tau, \tag{3.28}$$

donde $\mathcal{A}_f^2$ es la función de ambigüedad que se definió en la ecuación (3.3):

$$\mathcal{A}_f^{ii}(t,\theta) = e^{i\pi x\theta}\int_{\mathbb{R}} f\left(x+t\right)\overline{f}\left(x\right)e^{2i\pi x\theta}dx$$

y $\phi \in L^2(\mathbb{R}\times\mathbb{R})$ es conocido como función núcleo. En Tabla 3–5 se muestran algunos ejemplos de funciones núcleos más relevante [33].

Tabla 3–5: Funciones núcleo

| **Nombre** | $\theta(\tau,\eta)$ |
|---|---|
| Wigner | 1 |
| Margenau - Hill | $\cos\left(\pi\tau\eta\right)$ |
| Kirwood-Rihanzek | $e^{-\pi\tau\eta}$ |
| Born - Jordan | $\frac{\sin(\pi\tau\eta)}{\pi\tau\eta}$ |
| Choi - Williams | $e^{-\alpha(\pi\tau\theta/2)^2}$ |
| Zhao-Atlas-Marks | $e^{-\alpha\tau^2}\left\|\tau\right\|\frac{\sin(\alpha\pi\theta\tau/2)}{\alpha\pi\theta\tau/2}$ |

$\mathcal{CG}_f$ también recibe el nombre de *distribuciones de Cohen*, en su honor, y puede ser vista como la transformada continua de Fourier en dos dimensiones de $\mathcal{A}_f^2\phi$, considerando que los parametros del dominio están transpuestos. M. Richman, y otros [12], presentan una formulación en discreto de la expresion dada en (3.28), para el caso cuando $\theta(\tau,\eta) = 1$ (la distribución de Wigner). Basado en el trabajo de Richman, se define una representación discreta y finita de la clase general definida por Cohen, utilizando la DAF T-2, denominada *distribución discreta de Cohen*.

**Definición 20** (**Distribución Discreta de Cohen**). *Sea $x \in \mathbb{C}^N$. La distribución discreta de Cohen (DCD, del inglés discrete Cohen distribution) se define como el mapeo $\mathcal{CG}_x : l^2(\mathbb{Z}_N) \times l^2(\mathbb{Z}_N) \to l^2(\mathbb{Z}_N \times \mathbb{Z}_N)$ tal que*

$$\mathcal{CG}_x[m,k] = \sum_{\tau=0}^{N-1} \sum_{\nu=0}^{N-1} \mathcal{A}_x^2[\tau,\nu]\phi[\tau,\nu]\omega_N^{-(m\nu+k\tau)}, \tag{3.29}$$

*donde $\mathcal{A}_x^2$ es la DAF T-2 y $\phi \in \mathbb{C}^N$ es la función núcleo.*

Debido a su estructura bidimensional, la DCD $\mathcal{CG}_{x,y}$ puede ser representada como una matriz.

**Definición 21** (**Matriz DCD**). *La matriz DCD se define como $CG_x \in \mathbb{C}^{N\times N}$ tal que $(CG_x)_{m,k} = \mathcal{CG}_{x,y}[m,k]$, para $m,k \in \mathbb{Z}_N$.*

De la misma forma que se explicó para el caso continuo, $\mathcal{CG}_x$ puede ser vista como la transformada discreta de Fourier en dos dimensiones de $\mathcal{A}_x^2 \cdot \phi$, considerando que los parámetros del dominio están transpuestos, es decir,

$$\mathcal{CG}_x[m,k] = \mathcal{F}^2_{\mathcal{A}_x^2,\phi}[k,m]$$

Utilizando la representación matricial de la $2D$ DFT definida en la ecuación (2.13), la matriz DCD se puede expresar

$$CG_x = \mathcal{R}_{N,N}\{(F_N \otimes F_N)\mathcal{V}\{(A_x^2 \odot \phi)^T\}\} \tag{3.30}$$

donde $\phi \in \mathbb{C}^{N\times N}$ representa a la matriz de la función núcleo.

Ahora, considere las siguientes propiedades:

- Por **Lema 2**, $\mathcal{V}\{(A_x^2 \odot \phi)^T\} = L_N^{N^2}\mathcal{V}\{(A_x^2 \odot \phi)\}$.
- Por **Teorema 1**, $F_N \otimes F_N = (I_N \otimes F_N)(F_N \otimes I_N)$.
- Por **Teorema 2**, $F_N \otimes I_N = L_N^{N^2}(I_N \otimes F_N)L_N^{N^2}$.
- De la ecuación (2.3), $L_N^{N^2}L_N^{N^2} = I_{N^2}$.

Por lo tanto, la matriz $CG_x$ se presenta como

$$CG_x = \mathcal{R}_{N,N}\{(I_N \otimes F_N)L_N^{N^2}(I_N \otimes F_N)\mathcal{V}\{(A_x^2 \odot \phi)\}\} \tag{3.31}$$

Lo anterior demuestra el **Teorema 13**.

**Teorema 13.** *Sea* $x \in \mathbb{C}^N$, $\phi \in \mathbb{C}^{N\times N}$ *la matriz que representa a la función núcleo y* $CG_{x,y} \in \mathbb{C}^{N\times N}$ *la matriz DCD. Entones*

$$CG_x = \mathcal{R}_{N,N}\{(I_N \otimes F_N)L_N^{N^2}(I_N \otimes F_N)\mathcal{V}\{(A_x^2 \odot \phi)\}\}, \tag{3.32}$$

En Algoritmo 11, muestra la implementación de la ecuación (3.32).

**Algoritmo 11** Matriz DCD

**Entrada:** $A_x^2, \phi \in \mathbb{C}^{N\times N}$.
**Salida:** $CG_x \in \mathbb{C}^{N\times N}$.

1: $CG_x \leftarrow A_x^2 \odot \phi$
2: **para** $i = 0 : N-1$ **hacer**
3: $\quad CG_x(:, i) = \mathcal{F}_{CG_x(:,i)}$.
4: **fin para**
5: $CG_x \leftarrow CG_x^T$
6: **para** $i = 0 : N-1$ **hacer**
7: $\quad CG_x(:, i) = \mathcal{F}_{CG_x(:,i)}$.
8: **fin para**

# CAPÍTULO 4
# FUNCIÓN DE AMBIGÜEDAD DE VALORES VECTORIALES

En el capítulo anterior, se definió el concepto de función de ambigüedad para $x \in \mathbb{C}^N$, donde $x[n] \in \mathbb{C}$. Ahora, considerando la importancia de las secuencias CAZAC de valores vectoriales (ver **Sección 5.1**) en la tecnologías MIMO y en los sensores vectoriales, J. J. Benedetto y J. J. Donatelli [16] elaboran el concepto de la función de ambigüedad de valores vectoriales (VV DAF, del inglés vector-valued DAF), además de la transformada discreta de Fourier de valores vectoriales (VV DFT, del inglés vector-valued DFT), donde $x[n] \in \mathbb{C}^N$ y utilizan el concepto de marcos DFT en lugar de la raiz de la unidad. El estudio de una representación matricial de esta nueva variación de DAF, no se ha realizado hasta el momento. En este capítulo se define el concepto de un espacio de matrices de arreglos, en el cual se pueda desarrollar un estudio matricial de la VV DFT y la VV DAF, similar al desarrollado en el capitulo anterior a la DAF.

Además, se extiende el concepto de VV DAF al trabajo realizado por L. Auslander y R. Tolimieri a la función de ambigüedad con el grupo de Heisenberg [46] y a la DAF T-3 sobre un método para su cómputo de decimación [11].

## 4.1 Álgebra de matrices de arreglos $\mathbb{C}^{D*(M\times N)}$

Sea $(\mathfrak{A}, \circledast, \odot)$ un anillo conmutativo. Para $M, N \in \mathbb{Z}$, entonces el conjunto $(\mathfrak{A}^{M\times N}, \circledast, \odot)$ define una matriz con elementos de $\mathfrak{A}$ [47] y forma un anillo conmutativo: Sea $A, B \in \mathfrak{A}^{M\times N}$ y $a_{m,n}$ y $b_{m,n}$ la entrada $m, n$ de $A$ y $B$ respectivamente, para $m \in \mathbb{Z}_M$ y $n \in \mathbb{Z}_N$, entonces $(A \circledast B)_{m,n} = a_{m,n} \circledast b_{m,n}$ y $(A \odot B)_{m,n} = a_{m,n} \odot b_{m,n}$.

Para el caso $\mathfrak{A} = \mathbb{C}$, donde $\circledast, \circledcirc$ son la suma y producto usual de números complejos respectivamente, entonces $\mathfrak{A}^{M\times N} = \mathbb{C}^{M\times N}$ es el anillo de matrices, con la suma usual y el producto Hadamard de matrices.

Considere el caso $\mathfrak{A} = \mathbb{C}^D$, con $\circledast = +$ (suma de vectores) y $\circledcirc = \odot$. A continuación se realizará un estudio de $\mathfrak{A}^{M\times N}$, cuya notación será $\mathbb{C}^{D*(M\times N)}$ y se conocerá como el espacio de matrices de arreglos. Además se definirán operaciones sobre este espacio, que ayudarán al desarrollo de una representación matricial del concepto de la transformada de Fourier de valores vectoriales.

**Definición 22** (**Matriz de Arreglos**). *El conjunto* $\mathbb{C}^{D*(M\times N)}$ *se define como el espacio de matrices de arreglos. Cada elemento* $\mathbf{A} \in \mathbb{C}^{D*(M\times N)}$ *tiene la forma*

$$\mathbf{A} = \begin{pmatrix} \mathbf{a}_{0,0} & \mathbf{a}_{0,1} & \cdots & \mathbf{a}_{0,N-1} \\ \mathbf{a}_{1,0} & \mathbf{a}_{1,1} & \cdots & \mathbf{a}_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{M-1,0} & \mathbf{a}_{M-1,1} & \cdots & \mathbf{a}_{M-1,N-1} \end{pmatrix} \quad \mathbf{a}_{m,n} \in \mathbb{C}^D.$$

Cada entrada de una matriz de arreglos es un vector de orden $D$. Por lo tanto, cuando $D = 1$, entonces $\mathbb{C}^{D*M\times N} = \mathbb{C}^{M\times N}$. Sean $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{D*(M\times N)}$ y $\mathbf{C} \in \mathbb{C}^{D*(N\times Q)}$. Considere las siguientes operaciones

- La suma $\mathbf{A} \boxplus \mathbf{B}$, es una matriz de arreglos en $\mathbb{C}^{D*(M\times N)}$ tal que

$$(\mathbf{A} \boxplus \mathbf{B})_{m,n} = \mathbf{a}_{m,n} + \mathbf{b}_{m,n}. \tag{4.1}$$

- Sea $\beta \in \mathbb{C}$. El producto escalar $\beta\mathbf{A}$ es una matriz de arreglos en $\mathbb{C}^{D*(M\times N)}$ tal que

$$(\beta\mathbf{A})_{m,n} = \beta\mathbf{a}_{m,n}. \tag{4.2}$$

- El producto $\mathbf{A} \cdot \mathbf{C} = \mathbf{AC}$ es una matriz de arreglos en $\mathbb{C}^{D*(M\times Q)}$ tal que

$$(\mathbf{AC})_{m,q} = \sum_{n\in\mathbb{Z}_N} \mathbf{a}_{m,n} \odot \mathbf{c}_{n,q}. \tag{4.3}$$

**Nota 1.** *No hay que confundir el concepto de matrices de arreglos de la* **Definición 22** *con el concepto de una hipermatriz y su relación con el concepto de tensores. Como define D. G. Antzoulatos y A. A. Sawchuk [48], una hipermatriz es la representación indexada de una matriz única en* $\mathbb{C}^{M\times N}$*. El concepto de matrices de arreglos considera las entradas como vectores, ya que si cada entrada de la matriz de arreglos es de dimensión* 1*, entonces la matriz de arreglos es una matriz ordinaria.*

Una matriz de arreglos en $\mathbb{C}^{D*(M\times N)}$ se puede definir a partir de un conjunto ordenado de $D$ matrices en $\mathbb{C}^{M\times N}$, que se llamará *conjunto generador*

**Definición 23** (**Conjunto Generador).** *Sea* $\{A_d\}_{d\in\mathbb{Z}_D} \subset \mathbb{C}^{M\times N}$ *un conjunto de* $D$ *matrices, llamado conjunto de matrices generadoras, o simplemente, conjunto generador. La entrada* $m, n$ *de la matriz* $A_d$ *es* $(a_d)_{m,n}$*.*

- *El operador generador se define como* $\bigvee : \prod_{d\in Z_D} \mathbb{C}^{M\times N} \to \mathbb{C}^{D*(M\times N)}$ *tal que*

$$\mathbf{A} = \bigvee \{\{A_d\}\} = \bigvee_{d\in\mathbb{Z}_D} A_d = \begin{pmatrix} \mathbf{a}_{0,0} & \mathbf{a}_{0,1} & \cdots & \mathbf{a}_{0,N-1} \\ \mathbf{a}_{1,0} & \mathbf{a}_{1,1} & \cdots & \mathbf{a}_{1,N-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{a}_{M-1,0} & \mathbf{a}_{M-1,1} & \cdots & \mathbf{a}_{M-1,N-1} \end{pmatrix}$$

  *donde* $\mathbf{a}_{m,n} = ((a_0)_{m,n}, (a_1)_{m,n}, ..., (a_{D-1})_{m,n})^T$*, para* $m \in \mathbb{Z}_M$ *y* $n \in \mathbb{Z}_N$*.*

- *El operador generador inverso se define como* $\bigvee^{-1} : \mathbb{C}^{D*(M\times N)} \to \prod_{d\in Z_d} \mathbb{C}^{M\times N}$ *tal que*

$$\bigvee{}^{-1} \{\mathbf{A}\} = \{A_d\}_{d\in\mathbb{Z}_D}$$

  *donde* $(A_d)_{m,n} = \mathbf{a}_{m,n}[d]$*.*

Cada matriz de arreglos posee un único conjunto generador y viceversa, es decir,

$$\mathbf{A} = \mathbf{B} \text{ si y solo si } A_d = B_d, \text{ para todo } d \in \mathbb{Z}_D.$$

Siguiendo la misma estructura de las ecuaciones (4.1), (4.2) y (4.3), si $\{A_d\}_{d\in\mathbb{Z}_D}$, $\{B_d\}_{d\in\mathbb{Z}_D}$ y $\{C_d\}_{d\in\mathbb{Z}_D}$ son los conjuntos de matrices generadoras de $\mathbf{A}$, $\mathbf{B}$ y $\mathbf{C}$, entonces

$$\mathbf{A}\boxplus\mathbf{B} = \bigvee_{d\in\mathbb{Z}_D}(A_d + B_d) \tag{4.4}$$

$$\beta\mathbf{A} = \bigvee_{d\in\mathbb{Z}_D}\beta A_d \tag{4.5}$$

$$\mathbf{AC} = \bigvee_{d\in\mathbb{Z}_D} A_d C_d \tag{4.6}$$

donde $\mathbf{A},\mathbf{B}\in\mathbb{C}^{D*(M\times N)}$, $\mathbf{C}\in\mathbb{C}^{D*(N\times Q)}$, $A_d, B_d\in\mathbb{C}^{M\times N}$, $C_d\in\mathbb{C}^{N\times Q}$, para $d\in\mathbb{Z}_D$. De forma similar al espacio de matrices, $\mathbb{C}^{N\times N}$, el espacio de matrices de arreglos de la **Definición 22**, $\mathbb{C}^{D*(N\times N)}$, forma un álgebra asociativa.

**Teorema 14.** $\left(\mathbb{C}^{D*(N\times N)},\boxplus,\cdot\right)$ *forma un álgebra asociativa sobre* $\mathbb{C}$.

**Prueba.** *Sean* $\alpha,\beta\in\mathbb{C}$ *y* $\mathbf{A},\mathbf{B},\mathbf{C}\in\mathbb{C}^{D*(N\times N)}$ *y* $\{A_d\}$, $\{B_d\}$ *y* $\{C_d\}$ *sus conjuntos generadores, respectivamente. Entonces hay que probar que*

**1.** $\left(\mathbb{C}^{D*(N\times N)},\boxplus\right)$ es un espacio vectorial

- *Conmutatividad:* $\mathbf{A}\boxplus\mathbf{B} = \bigvee(A_d + B_d) = \bigvee(B_d + A_d) = \mathbf{B}\boxplus\mathbf{A}$.
- *Asociatividad:* $(\mathbf{A}\boxplus\mathbf{B})\boxplus\mathbf{C} = \bigvee[(A_d + B_d) + C_d] = \bigvee[A_d + (B_d + C_d)] = \mathbf{A}\boxplus(\mathbf{B}\boxplus\mathbf{C})$.
- *Elemento Neutro:* $\widetilde{\mathbf{0}}_N\in\mathbb{C}^{D*(N\times N)}$, *cuyo conjunto generador es* $\{0_N\}$, *donde* $0_N\in\mathbb{C}^{N\times N}$ *es la matriz nula. Entonces* $\mathbf{A}\boxplus\widetilde{\mathbf{0}}_N = \bigvee(A_d + 0_N) = \bigvee A_d = \mathbf{A}$. *De forma similar,* $\widetilde{\mathbf{0}}_N\boxplus\mathbf{A} = \mathbf{A}$.
- *Elemento Inverso: Para* $\mathbf{A}\in\mathbb{C}^{D*(N\times N)}$, *el elemento inverso es* $= -\mathbf{A}\in\mathbb{C}^{D*(N\times N)}$, *cuyo conjunto generador es* $\{-A_d\}$.

  *Entonces* $\mathbf{A}\boxplus -\mathbf{A} = \bigvee(A_d + -A_d) = \bigvee 0_N = \widetilde{\mathbf{0}}_N$. *De forma similar,* $-\mathbf{A}\boxplus\mathbf{A}_N = \widetilde{\mathbf{0}}_N$.
- *Pseudo-asociativa con el producto escalar:* $\alpha(\beta\mathbf{A}) = \bigvee\alpha(\beta A_d) = \bigvee(\alpha\beta)A_d = (\alpha\beta)\mathbf{A}$.

- *Unimodular:* $1\mathbf{A} = \bigvee 1A_d = \bigvee A_d = \mathbf{A}$.
- *Distributividad:* $\alpha(\mathbf{A} \boxplus \mathbf{B}) = \bigvee \alpha(A_d + B_d) = \bigvee(\alpha A_d + \alpha B_d) = \alpha\mathbf{A} \boxplus \alpha\mathbf{B}$.

**2.** $\left(\mathbb{C}^{D*(N\times N)}, \boxplus, \cdot\right)$ cumple

- *Distributividad de* $\cdot$ *con* $\boxplus$: $\mathbf{A}(\mathbf{B} \boxplus \mathbf{C}) = \bigvee A_d(B_d + C_d) = \bigvee A_dB_d + A_dC_d = \mathbf{AB} \boxplus \mathbf{AC}$. *De forma similar se prueba* $(\mathbf{B} \boxplus \mathbf{C})\mathbf{A} = \mathbf{BA} \boxplus \mathbf{CA}$.
- *Bilinealidad:* $\mathbf{A}(\alpha\mathbf{B}) = \bigvee A_d(\alpha B_d) = \bigvee \alpha A_dB_d = \alpha\mathbf{AB}$. *De forma similar se prueba* $(\alpha\mathbf{A})\mathbf{B} = \alpha\mathbf{AB}$.
- *Asociatividad:* $(\mathbf{AB})\mathbf{C} = \bigvee(A_dB_d)C_d = \bigvee A_d(B_dC_d) = \mathbf{A}(\mathbf{BC})$.

■

**Definición 24** (**Matriz de Arreglos Transpuesta**). *La matriz de arreglos transpuesta de* $\mathbf{A} \in \mathbb{C}^{D*(M\times N)}$ *se define como* $\mathbf{A}^T \in \mathbb{C}^{D*(N\times M)}$ *tal que* $(\mathbf{A}^T)_{m,n} = \mathbf{a}_{n,m}$. *Además*

$$\mathbf{A}^T = \bigvee_{d\in\mathbb{Z}_D} A_d^T$$

**Definición 25** (**Matriz de Arreglos Conjugada**). *La matriz de arreglos conjugada de* $\mathbf{A} \in \mathbb{C}^{D*(M\times N)}$ *se define como* $\overline{\mathbf{A}} \in \mathbb{C}^{D*(N\times M)}$ *tal que* $(\overline{\mathbf{A}})_{m,n} = \overline{\mathbf{a}_{n,m}}$. *Además*

$$\overline{\mathbf{A}} = \bigvee_{d\in\mathbb{Z}_D} \overline{A_d}$$

**Definición 26** (**Matriz de Arreglos Diagonal**). *Sea* $\mathbf{x} \in \mathbb{C}^{D*N}$. *La matriz de arreglos diagonal con respecto a* $\mathbf{x}$, *es una matriz de arreglos* $\mathbf{B} \in \mathbb{C}^{D*(N\times N)}$ *tal que*

$$\mathbf{b}_{i,j} = \begin{cases} \mathbf{x}[i] & si \quad i = j \\ \mathbf{0}_D & si \quad i \neq 0 \end{cases}$$

**Definición 27** (**Matriz de arreglos identidad**). *La matriz de arreglos identidad de orden $N$ es definido como $\mathbf{I}_N \in \mathbb{C}^{D*(N\times N)}$ tal que*

$$(\mathbf{I}_N)_{i,j} = \begin{cases} \mathbf{1}_D & si \quad i = j \\ \mathbf{0}_D & si \quad i \neq j \end{cases}$$

*Además*

$$\mathbf{I}_N = \bigvee_{d\in\mathbb{Z}_D} I_N$$

**Definición 28** (**Matriz de Arreglos Inversa**). *Sea $\mathbf{A} \in \mathbb{C}^{D*N}$. La matriz de arreglos $\mathbf{A}^{-1} \in \mathbb{C}^{D*N\times N}$ es la matriz de arreglos inversa de $\mathbf{A}$ y $\mathbf{A}\mathbf{A}^{-1} = \mathbf{A}^{-1}\mathbf{A} = \mathbf{I}_N$.*

**Ejemplo.** *Sea $\mathbf{A} \in \mathbb{C}^{2*3}$ tal que*

$$\mathbf{A} = \begin{pmatrix} (1,2)^T & (3,4)^T & (1,2)^T \\ (1,2)^T & (0,0)^T & (0,1)^T \\ (3,1)^T & (1,1)^T & (1,0)^T \end{pmatrix}$$

*El conjunto generador de $\mathbf{A}$ es $\{A_0, A_1\}$, tal que*

$$A_0 = \begin{pmatrix} 1 & 3 & 1 \\ 1 & 0 & 0 \\ 3 & 1 & 1 \end{pmatrix} \quad A_1 = \begin{pmatrix} 2 & 4 & 2 \\ 2 & 4 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

*Las matrices inversa de $A_0$ y $A_1$ se definen como*

$${A_0}^{-1} = \begin{pmatrix} 0 & 1 & 0 \\ 1/2 & 1 & 1/2 \\ -1/2 & -4 & 3/2 \end{pmatrix} \quad {A_1}^{-1} = \begin{pmatrix} 1/2 & 0 & 2 \\ 1/2 & 0 & -1 \\ -1/2 & -4 & 3/2 \end{pmatrix}$$

*Ahora, considere la matriz* $B \in \mathbb{C}^{2*3}$*, tal que*

$$\mathbf{B} = \bigvee_{d\in\mathbb{Z}_2} A_d^{-1} = \begin{pmatrix} (0,1/2)^T & (1,0)^T & (0,2)^T \\ (1/2,1/2)^T & (1,0)^T & (-1/2,-1)^T \\ (-1/2,1)^T & (-4,1)^T & (3/2,-4)^T \end{pmatrix}$$

*Las matrices* $\mathbf{A}$ *y* $\mathbf{B}$ *cumplen que*

$$\mathbf{AB} = \mathbf{BA} = \mathbf{I}_3$$

*Por lo tanto,* $\mathbf{B} = \mathbf{A}^{-1}$*.*

El ejemplo anterior motiva el desarrollo del siguiente teorema.

**Teorema 15.** *Sean* $\mathbf{A} \in \mathbb{C}^{D*(N\times N)}$ *y* $\{A_d\}_{d\in\mathbb{Z}_D} \subset \mathbb{C}^{N\times N}$ *el conjunto de matrices generadas a partir de* $\mathbf{A}$*. La matriz de arreglos* $\mathbf{A}$ *posse inversa si y solo si* $A_d$ *posse inversa, para todo* $d \in \mathbb{Z}_D$*. Además,* $\mathbf{A}^{-1}$ *es única y*

$$\mathbf{A}^{-1} = \bigvee_{d\in\mathbb{Z}_D} (A_d)^{-1} \tag{4.7}$$

**Prueba.** *Sea* $\mathbf{B} = \mathbf{A}^{-1}$*.*

$$\begin{aligned} \mathbf{A} \textit{ posee inversa} &\Leftrightarrow \mathbf{AB} = \mathbf{I}_N \\ &\Leftrightarrow \bigvee A_d B_d = \bigvee I_N \\ &\Leftrightarrow A_d B_d = I_N \\ &\Leftrightarrow B_d = A_d^{-1} \\ &\Leftrightarrow A_d \textit{ posee inversa, para todo } d \in \mathbb{Z}_N \end{aligned}$$

*Lo anterior también prueba la ecuación (4.7). Además, como cada matriz de arreglos tiene un único conjunto de matrices generadoras,* $\mathbf{A}^{-1}$ *es única.*

■

### 4.1.1 Productos Kronecker, Hadamard & Suma Directa

Sea $\mathbf{v} \in \mathbb{C}^D$ y $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{D*(M\times N)}$, $\mathbf{C} \in \mathbb{C}^{D*(P\times Q)}$ con sus respectivos conjuntos generadores $\{A_d\}_{d\in\mathbb{Z}_D}$, $\{B_d\}_{d\in\mathbb{Z}_D}$ y $\{C_d\}_{d\in\mathbb{Z}_D}$.

- El *producto Hadamard* de $\mathbf{A}, \mathbf{B}$ es definida como la matriz de arreglos $\mathbf{A} \boxdot \mathbf{B} \in \mathbb{C}^{D*(N\times N)}$ tal que $(\mathbf{A} \boxdot \mathbf{B})_{m,n} = \mathbf{a}_{m,n} \odot \mathbf{b}_{m,n}$. Además,

$$\mathbf{A} \boxdot \mathbf{B} = \bigvee_{d\in\mathbb{Z}_D} A_d \odot B_d$$

- El producto *vector & matriz de arreglos* $\mathbf{v} \diamond \mathbf{A}$ se define como la matriz de arreglos $\mathbb{C}^{D*(M\times N)}$ tal que $(\mathbf{v} \diamond \mathbf{A})_{m,n} = \mathbf{v} \odot \mathbf{a}_{m,n}$. Además

$$\mathbf{v} \boxdot \mathbf{A} = \bigvee_{d\in\mathbb{Z}_D} v[d] A_d$$

- El *producto Kronecker* $\mathbf{A} \boxtimes \mathbf{C}$ se define como la matriz de arreglos $\mathbb{C}^{D*(MP\times NQ)}$ tal que

$$\mathbf{A} \boxtimes \mathbf{C} = \begin{pmatrix} \mathbf{a}_{0,0} \diamond \mathbf{C} & \cdots & \mathbf{a}_{0,N-1} \diamond \mathbf{C} \\ \vdots & \ddots & \vdots \\ \mathbf{a}_{M-1,0} \diamond \mathbf{C} & \cdots & \mathbf{a}_{M-1,N-1} \diamond \mathbf{C} \end{pmatrix}$$

Además

$$\mathbf{A} \boxtimes \mathbf{B} = \bigvee_{d\in\mathbb{Z}_D} A_d \otimes B_d$$

El **Teorema 16** muestra algunas de las propiedades de los productos de Kronecker para matrices de arreglos. Dicha proposición es una extensión del **Teorema 1** para el espacio de matrices de arreglos.

**Teorema 16.** *Sea* $\mathbf{A} \in \mathbb{C}^{D*(M\times N)}$, $\mathbf{B} \in \mathbb{C}^{D*(R\times S)}$, $\mathbf{C} \in \mathbb{C}^{D*(N\times P)}$ *y* $\mathbf{D} \in \mathbb{C}^{D*(S\times T)}$. *Entonces*

- $(\mathbf{A} \boxtimes \mathbf{B}) \boxtimes \mathbf{C} = \mathbf{A} \boxtimes (\mathbf{B} \boxtimes \mathbf{C})$.
- $\mathbf{A} \boxtimes \mathbf{B} = (\mathbf{A} \boxtimes \mathbf{I}_S)(\mathbf{I}_N \boxtimes \mathbf{B})$.
- $(\mathbf{A} \boxtimes \mathbf{B})(\mathbf{C} \boxtimes \mathbf{D}) = \mathbf{AC} \boxtimes \mathbf{BD}$.
- $\mathbf{I}_R \boxtimes \mathbf{I}_S = \mathbf{I}_{RS}$.

**Prueba.** *Se realizará la prueba de* $(\mathbf{A} \boxtimes \mathbf{B}) \boxtimes \mathbf{C} = \mathbf{A} \boxtimes (\mathbf{B} \boxtimes \mathbf{C})$. *Los otros tres casos se demuestran de forma similar, utilizando los conjuntos generadores.*

*Sean* $\{A_d\}$, $\{B_d\}$ *y* $\{C_d\}$ *los conjuntos generadores de* $\mathbf{A}$, $\mathbf{B}$ *y* $\mathbf{C}$ *respectivamente. Como* $\mathbf{A} \boxtimes \mathbf{B} = \bigvee A_d \otimes B_d$, *entonces,* $\{A_d \otimes B_d\}$ *es el conjunto generador de* $A \boxtimes B$. *Por lo tanto*

$$\begin{aligned}(\mathbf{A} \boxtimes \mathbf{B}) \boxtimes \mathbf{C} &= \bigvee (A_d \otimes B_d) \otimes C_d \\ &= \bigvee A_d \otimes (B_d \otimes C_d) \\ &= \mathbf{A} \boxtimes (\mathbf{B} \boxtimes \mathbf{C})\end{aligned}$$

*ya que* $\{B_d \otimes C_d\}$ *es el conjunto generador de* $\mathbf{B} \boxtimes \mathbf{C}$.

■

**Definición 29** (**Matriz de Arreglos de Permutación de orden** $N$ **y paso** $R$**).** *Sea* $N = RS$. *La matriz de arreglos de permutación de orden* $N$ *y paso* $R$, $\mathbf{L}_S^N \in \mathbb{C}^{D*(N \times N)}$, *es definida por la regla* $\mathbf{L}_S^N(\mathbf{a} \boxtimes \mathbf{b}) = \mathbf{b} \boxtimes \mathbf{a}$, *donde* $\mathbf{a} \in \mathbb{C}^{D*R}$ *y* $\mathbf{b} \in \mathbb{C}^{D*S}$. *Además*

$$\mathbf{L}_S^N = \bigvee_{d \in \mathbb{Z}_D} L_S^N$$

El **Teorema 17** muestra la extensión del teorema de conmutación de productos de Kronecker para el espacio de matrices de arreglos.

**Teorema 17.** *Sea* $N = RS$, $\mathbf{A} \in \mathbb{C}^{D*(R \times R)}$ *y* $\mathbf{B} \in \mathbb{C}^{D*(S \times S)}$. *Entonces*

$$\mathbf{A} \boxtimes \mathbf{B} = \mathbf{L}_R^N(\mathbf{B} \boxtimes \mathbf{A})\mathbf{L}_S^N$$

**Prueba.** *Sea* $\mathbf{x} \in \mathbb{C}^{D*N}$ *tal que* $\mathbf{x} = \mathbf{a} \boxtimes \mathbf{b}$, *donde* $\mathbf{a} \in \mathbb{C}^{D*R}$ *y* $\mathbf{b} \in \mathbb{C}^{D*S}$. *Entonces*

1. $(\mathbf{A} \boxtimes \mathbf{B})\mathbf{x} = (\mathbf{A} \boxtimes \mathbf{B})(\mathbf{a} \boxtimes \mathbf{b}) = \mathbf{Aa} \boxtimes \mathbf{Bb}$ *Por el* **Teorema 16**.
2. $$\begin{aligned}\mathbf{L}_R^N(\mathbf{B} \boxtimes \mathbf{A})\mathbf{L}_S^N x &= \mathbf{L}_R^N(\mathbf{B} \boxtimes \mathbf{A})\mathbf{L}_S^N(\mathbf{a} \boxtimes \mathbf{b}) \\ &= \mathbf{L}_R^N(\mathbf{B} \boxtimes \mathbf{A})(\mathbf{b} \boxtimes \mathbf{a}) && \text{Por definición de } \mathbf{L}_S^N \\ &= \mathbf{L}_R^N(\mathbf{Bb} \boxtimes \mathbf{Aa}) && \text{Por el } \mathbf{Teorema\ 16}. \\ &= \mathbf{Aa} \boxtimes \mathbf{Bb} && \text{Por definición de } \mathbf{L}_R^N\end{aligned}$$

■

**Definición 30** (**Suma Directa de Matrices de Arreglos**). *La suma directa de dos matrices de arreglos* $\mathbf{A} \in \mathbb{C}^{D*(M\times N)}$ *y* $\mathbf{B} \in \mathbb{C}^{D*(P\times Q)}$ *se define como la matrices* $\mathbf{A} \boxplus \mathbf{B} \in \mathbb{C}^{D*((M+P)\times(N+Q))}$ *tal que*

$$\mathbf{A} \boxplus \mathbf{B} = \begin{pmatrix} \mathbf{A} & \\ & \mathbf{B} \end{pmatrix}$$

En general, para un conjunto de matrices de arreglos $\{\mathbf{A}_p\}_{p\in\mathbb{Z}_P}$, tal que $\mathbf{A}_p \in \mathbb{C}^{D*(M_p\times N_p)}$, se define como

$$\bigboxplus_{d\in\mathbb{Z}_D} \mathbf{A}_D = \mathbf{A}_0 \boxplus \mathbf{A}_1 \boxplus ... \boxplus \mathbf{A}_{D-1}$$

Además,

$$\bigboxplus_{d\in\mathbb{Z}_D} \mathbf{A}_D = \bigvee_{d\in\mathbb{Z}_D} \bigoplus_{p\in\mathbb{Z}_P} (A_p)_d$$

donde $\{(A_p)_d\}$ representa el conjunto generador de $\mathbf{A}_p$.

**Teorema 18.** *Sean* $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{D*(N\times N)}$. *Entonces*

$$\mathbf{1}_D \boxplus AB = (\mathbf{1}_D \boxplus \mathbf{A})(\mathbf{1}_D \boxplus \mathbf{B}).$$

**Prueba.** *Sean* $\{A_d\}$ *y* $\{B_d\}$ *los conjuntos generadores de* $\mathbf{A}$ *y* $\mathbf{B}$.

$$\begin{aligned} \mathbf{1}_D \boxplus AB &= \bigvee (1 \oplus A_d B_d) \\ &= \bigvee (1 \oplus A_d)(1 \oplus B_d) \\ &= (\mathbf{1}_D \boxplus \mathbf{A})(\mathbf{1}_D \boxplus \mathbf{B}) \end{aligned}$$

■

## 4.2 Transformada Discreta de Fourier de valores vectoriales

### 4.2.1 Marcos y Vectores Complejos Armónicos

**Definición 31** (**Marco**). *Un conjunto* $F = \{f_n\}_{n\in\mathbb{Z}_N} \subset \mathbb{C}^D$ *es un marco para* $\mathbb{C}^D$ *si* $F$ *genera al espacio* $\mathbb{C}^D$.

Además, si $F$ es un marco para $\mathbb{C}^D$, entonces existen constantes $a, b > 0$, denominadas constantes del marco, tal que para todo $x \in \mathbb{C}^D$, satisface

$$a\|x\|^2 \leqslant \sum_{n\in\mathbb{Z}_N} |\langle x, f_n\rangle|^2 \leqslant a\|x\|^2.$$

Un marco $F$ se llama *marco ajustado* si se pueden seleccionar $a = b$. Si, en adición, cada $f_j$ tiene norma igual a 1, se dice que $F$ es *un marco ajustado de norma 1* y se denomina FUNTF (del inglés finite unit-norm tight frame).

Un ejemplo de FUNTF es el conjunto llamado marcos de la transformada discreta de Fourier, o simplemente, *marcos DFT*. Sea $N \geqslant D$ y considere la matriz $B \in \mathbb{C}^{N\times D}$ creada usando cualquiera $D$ columnas de la conjugada de la matriz DFT $F_N$. El conjunto formado por las filas de la matriz $B$, multiplicadas por $1/\sqrt{D}$, forma un FUNTF para $\mathbb{C}^D$.

Los marcos DFT también son conocidos como *marcos complejos armónicos* [16]. A partir del concepto de marco DFT, se elabora el concepto de *vectores complejos armónicos*, que es un caso general de los marcos DFT.

**Definición 32** (**Vectores Complejos Armónicos).** *Sea $N, D \in \mathbb{N}$. El conjunto de vectores complejos armónicos $E = \{1/\sqrt{D} \cdot e_N^n\}_{n\in\mathbb{Z}_N}$, con $E \subseteq \mathbb{C}^D$, es el conjunto de vectores tal que*

$$e_N^n = \left(\omega_N^{n\alpha_1},\ \omega_N^{n\alpha_2},\ \ldots,\ \omega_N^{n\alpha_D}\right)^T$$

*con $\alpha_k \in \mathbb{N} \cup \{0\}$ y $\alpha_k \neq \alpha_j$ if $k \neq j$. El vector $e_N^1 = e_N$ se denomina generador de los vectores complejos armónicos.*

Si $N \geqslant D$ y $max\{\alpha_k\} < N$, entonces el conjunto $E$ es un marco DFT. La siguiente proposición muestra algunas de las propiedades del generador del conjunto de vectores complejos armónicos.

**Proposición 4.** *Sea $E$ un conjunto de de vectores complejos armónicos para $\mathbb{C}^D$, con generador $e_N$. Entonces*

- $e_N^{m+n} = e_N^m \odot e_N^n$.
- $e_N^0 = e_N^N = \mathbf{1}_D$.
- *Para $k \in \mathbb{Z}$ y $r \in \mathbb{Z}_N$, $e_N^{Nk+r} = e_N^r$.*
- *Si $N = LM$, entonces $e_N^{Lm} = e_M^m$.*

**Prueba.** *Se realizará la prueba de $e_N^{m+n} = e_N^m \odot e_N^n$. Los demás casos siguen siguen una estructura similar de demostración.*

$$\begin{aligned} e_N^{m+n} &= \left(\omega_N^{(m+n)\alpha_1},\ \omega_N^{(m+n)\alpha_2},\ \ldots,\ \omega_N^{(m+n)\alpha_D}\right)^T \\ &= \left(\omega_N^{m\alpha_1}\omega_N^{n\alpha_1},\ \omega_N^{m\alpha_2}\omega_N^{n\alpha_2},\ \ldots,\ \omega_N^{m\alpha_D}\omega_N^{n\alpha_D}\right)^T \\ &= \left(\omega_N^{m\alpha_1},\ \omega_N^{m\alpha_2},\ \ldots,\ \omega_N^{m\alpha_D}\right)^T \odot \left(\omega_N^{n\alpha_1},\ \omega_N^{n\alpha_2},\ \ldots,\ \omega_N^{n\alpha_D}\right)^T \\ &= e_N^m \odot e_N^n \end{aligned}$$

■

**Nota 2.** *En este trabajo se seleccionará los exponentes de los vectores armónicos complejos de la forma $\alpha_k = k$, para $k = 1, 2, ..., D$.*

### 4.2.2 Definición

J. J Benedetto y J. J. Donatelli [16] formularón una definición de la DFT para vectores en $\mathbb{C}^{D*N}$ que incluye el concepto de marcos DFT, llamado *transformada discreta de Fourier de valores vectoriales* (VV DFT, del inglés vector-valued DFT). Para esto, solo consideran los casos cuando $N \geqslant D$. En este trabajo se propone una modificación a esta definición, introduciendo el concepto de vectores armónicos complejos en lugar de los marcos DFT. Por lo tanto, la VV DFT estará definida para todo $N, D \in \mathbb{Z}$.

**Definición 33** (**Transformada de Fourier de Valores Vectoriales**). *Sean* $\mathbf{x} \in \mathbb{C}^{D*N}$ *y sea* $E$ *un conjunto de vectores complejos armónicos para* $\mathbb{C}^D$.

- *La transformada de Fourier de valores vectoriales VV DFT, por sus siglas en inglés de* $\mathbf{x}$ *se define como el mapeo* $\mathscr{F}_{\mathbf{x}} : \mathbb{Z}_N \to \mathbb{C}^D$ *tal que*

$$\mathscr{F}_{\mathbf{x}}[k] = \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot e_N^{-nk} \tag{4.8}$$

- *La matriz de arreglos VV DFT es definida como* $\mathbf{F}_N \in \mathbb{C}^{D*(N\times N)}$, *tal que* $(\mathbf{F}_N)_{m,n} = {}^1\!/\!_{\sqrt{D}} \cdot e_N^{-mn}$. *La notación matricial de la VV DFT de* $\mathbf{x}$ *es representada como*

$$\mathscr{F}_{\mathbf{x}} = \mathbf{F}_N \mathbf{x}.$$

*Además*

$$\mathbf{F}_N = \bigvee_{d \in \mathbb{Z}_D} \left( \frac{1}{\sqrt{D}} \bigodot_{n \in \mathbb{Z}_d} F_N \right)$$

**Teorema 19.** *Sea* $\mathbf{F}_N \in \mathbb{C}^{D*(N\times N)}$ *es la matriz VV DFT.*

- *Sea* $N$ *un número compuesto, y* $r$ *el menor número primo de la factorización de* $N$. *Para* $D < r$, $\mathbf{F}_N$ *posee inversa. Para* $D \geqslant r$, $\mathbf{F}_N$ *no posee inversa.*
- *Si* $N$ *es primo, entonces* $\mathbf{F}_N$ *tiene inversa.*
- *De existir, la inversa de* $\mathbf{F}_N$ *es* $\mathbf{F}_N^{-1} = \frac{D}{N}\overline{\mathbf{F}_N}$.

**Prueba.** *Por definición,* $G = \{{}^1\!/\!_{\sqrt{D}} G_d\}$, *tal que*

$$G_d = \bigodot_{n \in \mathbb{Z}_d} F_N, \qquad d \in \mathbb{Z}_D$$

*es el conjunto generador de* $\mathbf{F}_N$.

- *Sea* $N = rs$, *donde* $r$ *es el menor número primo de la factorización de* $N$. *Por el* **Teorema 5**, *existe* $m < N$ *tal que* $G_m$ *es no invertible. De la demostración de dicho teorema,* $m = r$ *cumple la condición. Ahora, hay que probar que el menor* $m$ *que cumple esa condición es* $r$. *Por contradicción, suponga que existe*

*$s < r$, tal que $G_s$ no posse inversa. Ahora, $(G_s)_{i,j} = \omega_N^{ijs}$, para $i, j \in \mathbb{Z}_N$. Considere la matriz $H_s \in \mathbb{C}^{N\times N}$ tal que $(h_s)_{ij} = \frac{1}{N}\omega_N^{-ijs}$. Entonces*

$$(G_sH_s)_{i,j} = \frac{1}{N}\sum_{n\in\mathbb{Z}_N} \omega_N^{ins}\omega_N^{-njs} = \frac{1}{N}\sum_{n\in\mathbb{Z}_N} \omega_N^{n(i-j)s}$$

*Cuando $i = j$, entonces $(G_sH_s)_{i,j} = 1$. Para $i \neq j$, se cumple*

$$i - j = -(N-1), ..., -1, 1, ...N-1.$$

*Además, como $s < r$, entonces $(i-j)s \neq 0 \ mod\ N$. Por lo tanto, para $i \neq j$, $(G_sH_s)_{i,j} = 0$. Es decir, $G_sH_s = I_N$, entonces $G_s = H_s^{-1}$, lo que contradice el hecho de que $G_s$ no es invertible. Lo supuesto es falso, por lo tanto, no existe $s < r$ tal que $G_s$ no sea invertible.*

*Ahora, la matriz inversa de $\mathbf{F}_N$ está dada por*

$$\mathbf{F}_N = \bigvee_{d\in\mathbb{Z}_D}\left(\frac{1}{\sqrt{D}}G_d\right)$$

*Por el* **Teorema 15**, *$\mathbf{F}_N$ tiene inversa si cada $G_d$ tiene inversa. Como cada elemento de $\{1/\sqrt{D}G_d\}_{d\in\mathbb{Z}_D}$ tiene inversa solamente si $D < r$, entonces $\mathbf{F}_N$ tiene inversa cuando $D < r$. Como $G_r$ no tiene inversa, entonces para $D \geqslant r$, existe algún elemento de $\{G_d\}_{d\in\mathbb{Z}_D}$ que no tiene inversa, entonces $\mathbf{F}_N$ no tiene inversa cuando $D \geqslant R$.*

- *Sea $N$ un número primo. Por* **Lema 1**, *cada elemento de $\{1/\sqrt{D}G_d\}_{d\in\mathbb{Z}_D}$ es invertible para $D < N$. Ya que $\{1/\sqrt{D}G_d\}_{d\in\mathbb{Z}_D}$ es el conjunto generador de $\mathbf{F}_N$, entonces, por el* **Teorema 15**, *$\mathbf{F}_N$ tiene inversa.*
- *De la primera parte, la inversa de $G_d$ es $G_d^{-1}$, tal que $(G_d^{-1})_{i,j} = \frac{1}{N}\omega_N^{-ijd}$. Además, $\{N/\sqrt{D}G_d^{-1}\}_{d\in\mathbb{Z}_D}$ es el conjunto generador de $\overline{\mathbf{F}_N}$. Entonces*

$$\mathbf{F}_N\mathbf{F}_N^{-1} = \frac{D}{N}\bigvee\left(\frac{1}{\sqrt{D}}G_d\frac{N}{\sqrt{D}}G_d^{-1}\right) = \bigvee I_N = \mathbf{I}_N$$

■

Del teorema anterior, se deduce que si $N$ es par, entonces, solo para $D = 1$, $\mathbf{F}_N$ posee inversa, el cual representa el caso trivial. Además, de la parte tres de teorema anterior, se deduce el siguiente corolario.

**Corolario 4.** *Sea* $\mathbf{x} \in \mathbb{C}^{D*N}$ *y* $r$ *el menor número primo de la factorización de* $N$. *Si* $D < r$ *ó* $N$ *es un número primo, entonces la función inversa de la VV DFT existe y se define como el mapeo* $\mathscr{F}_{\mathbf{x}}^{-1} : \mathbb{Z}_N \to \mathbb{C}^D$ *tal que*

$$\mathscr{F}_{\mathbf{x}}^{-1}[n] = x[n] = \frac{\sqrt{D}}{N} \sum_{k \in \mathbb{Z}_N} \mathscr{F}_{\mathbf{x}}[k] \odot e_N^{nk} \tag{4.9}$$

*Cuando* $D \geqslant r$, *no existe inversa de la VV DFT.*

### 4.2.3 Propiedades

La siguientes proposiciones prueban algunas propiedades de la VV DFT.

**Proposición 5.** *Sea* $\mathbf{x} \in \mathbb{C}^{D*N}$. *Entonces* $\|\mathscr{F}_{\mathbf{x}}[k]\|_p = \|\mathscr{F}_{\mathbf{x}}[\langle -k \rangle_N]\|_p$, *para* $p = \infty$, $p \in \mathbb{Z}^+$, *donde* $k \in \mathbb{Z}_N$.

**Prueba.** *Como* $\mathbf{x} \in \mathbb{C}^{D*N}$ , *entonces* $\mathbf{x}[n] \in \mathbb{C}^D$ *tal que* $\mathbf{x}[n] = (\mathbf{x}_0[n], ..., \mathbf{x}_{D-1}[n])^T$, *con* $\mathbf{x}_d[n] \in \mathbb{C}$.

- *Sea* $p = \infty$. *Entonces*

$$\begin{aligned}
\|\mathscr{F}_{\mathbf{x}}[k]\|_\infty &= \left\| \tfrac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot e_N^{-nk} \right\|_\infty \\
&= \max_{d \in \mathbb{Z}_D} \left\{ \left| \tfrac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}_d[n] \omega_N^{-nk(d+1)} \right| \right\} \\
&= \max_{d \in \mathbb{Z}_D} \left\{ \left| \tfrac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}_d[n] \omega_N^{(d+1)nk} \right| \right\} \\
&= \left\| \tfrac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot e_N^{nk} \right\|_\infty = \|\mathscr{F}_{\mathbf{x}}[\langle -k \rangle_N]\|_\infty
\end{aligned}$$

- *Sea* $p \in \mathbb{Z}$. *Entonces*

$$\|\mathcal{X}[k]\|_p^p = \sum_{d \in \mathbb{Z}_D} \left| \sum_{n \in \mathbb{Z}_N} x_d[n] \omega_N^{-nk(d+1)} \right|^p = \sum_{d \in \mathbb{Z}_D} \left| \sum_{n \in \mathbb{Z}_N} x_d[n] \omega_N^{nk(d+1)} \right|^p = \|\mathcal{X}[\langle -k \rangle_N]\|_p^p$$

■

**Proposición 6.** *Sea $r$ el menor número primo de la factorización de $N$ y $g_{N,k} \in \mathbb{C}^N$*

$$g_{N,k} = \sum_{n \in \mathbb{Z}_N} e_N^{nk}.$$

- *Si $k < r$ ó $N$ es un número primo, entonces $g_{N,k} = N\delta[k]$, donde*

$$\delta[k] = \begin{cases} \mathbf{1}_D & si \quad k = 0 \ mod \ N \\ \mathbf{0}_D & si \quad k \neq 0 \ mod \ N \end{cases}$$

- *Si $k \geqslant r$, entonces $g_{N,k} = Nv$, donde*

$$v[m] = \begin{cases} \mathbf{1}_D & si \quad k(m+1) = 0 \ mod \ N \\ \mathbf{0}_D & si \quad k(m+1) \neq 0 \ mod \ N \end{cases}$$

**Prueba.** *Analizando cada una de las entradas del vector $G_{N,k}$, se obtiene*

$$\sum_{n \in \mathbb{Z}_N} e_N^{nk} = \sum_{n \in \mathbb{Z}_N} \begin{pmatrix} \omega_N^{nk} \\ \omega_N^{2nk} \\ \vdots \\ \omega_N^{Dnk} \end{pmatrix} = \begin{pmatrix} \sum_{n \in \mathbb{Z}_N} \omega_N^{nk} \\ \sum_{n \in \mathbb{Z}_N} \omega_N^{2nk} \\ \vdots \\ \sum_{n \in \mathbb{Z}_N} \omega_N^{Dnk} \end{pmatrix}$$

*Entonces, $g_{n,k}[m] = \sum_{n \in \mathbb{Z}_N} \omega_N^{(m+1)nk}$. Para $m \in \mathbb{Z}_M$, si $k(m+1) = 0 \ mod \ N$, entonces $\sum_{n \in \mathbb{Z}_N} \omega_N^{nk(m+1)} = 0$, de caso contrario, $\sum_{n \in \mathbb{Z}_N} \omega_N^{nk(m+1)} = N$. Si $N$ es un número compuesto, donde $r$ el menor primo de la factorización de $N$, entonces $k(m+1) \neq 0$ para $k < r$. La condición también se cumple cuando $N$ es un número primo. En cambio, para $k \geqslant r$, existe $m+1$ tal que $k(m+1) = 0 \ mod \ N$. Por ejemplo, como $N$ es compuesto con factor $r$, entonces $N = rs$, entonces se selecciona $m = s - 1$.*

■

**Proposición 7.** *Sean* $\mathbf{x}, \mathbf{y} \in \mathbb{C}^{D*N}$*, donde* $N$ *es un número primo, o un número compuesto* $N$ *tal que* $D < r$*, donde* $r$ *es el menor número primo de la factorización de* $N$*. Entonces*

$$\sum_{n\in\mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathbf{y}}[n] = \frac{D}{N} \sum_{k\in\mathbb{Z}_N} \mathscr{F}_{\mathbf{x}}[k] \odot \overline{\mathscr{F}_{\mathbf{y}}}[k]$$

**Prueba.** *Por Corolario 4,*

$$\mathbf{x}[n] = \frac{\sqrt{D}}{N} \sum_{k\in\mathbb{Z}_N} \mathscr{F}_{\mathbf{x}}[k] \odot e_N^{-nk}, \qquad \overline{\mathbf{y}[n]} = \frac{\sqrt{D}}{N} \sum_{l\in\mathbb{Z}_N} \overline{\mathscr{F}_{\mathbf{y}}}[l] \odot e_N^{nl} \tag{4.10}$$

*Seleccionando el producto Hadamard de* $\mathbf{x}[n]$ *y* $\overline{\mathbf{y}}[n]$*, sumando con respecto a* $n$ *y utilizando la* **Proposición 6** *se obtiene*

$$\begin{aligned}
\sum_{n\in\mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathbf{y}[n]} &= \sum_{n\in\mathbb{Z}_N} \left( \frac{\sqrt{D}}{N} \sum_{k\in\mathbb{Z}_N} \mathscr{F}_{\mathbf{x}}[k] \odot e_N^{-nk} \right) \odot \left( \frac{\sqrt{D}}{N} \sum_{l\in\mathbb{Z}_N} \overline{\mathscr{F}_{\mathbf{y}}[l]} \odot e_N^{nl} \right) \\
&= \frac{D}{N^2} \sum_{k\in\mathbb{Z}_N} \sum_{l\in\mathbb{Z}_N} \mathscr{F}_{\mathbf{x}}[k] \odot \overline{\mathscr{F}_{\mathbf{y}}[l]} \odot \sum_{n\in\mathbb{Z}_N} \odot e_N^{n(l-k)} \\
&= \frac{D}{N} \sum_{k\in\mathbb{Z}_N} \mathscr{F}_{\mathbf{x}}[k] \odot \overline{\mathscr{F}_{\mathbf{y}}[k]}
\end{aligned}$$

■

**Nota 3.** *La idea de utilizar los vectores complejos armónicos en lugar de los marcos DFT en la definición de VV DFT, como originalmente lo realizó J. J. Benedetto y J. J. Donatelli, es para desarrollar algoritmos que puedan realizar su cómputo de una manera rápida, es decir, desarrollar una transformada rápida de Fourier de valores vectoriales (VV FFT). Para eso, el cálculo de la VV DFT de orden* $N$*, se puede dividir en varias VV DFT de un menor orden* $M$*, y en algunos casos sucederá que* $M < D$*, lo cuál chocaría con la definición de marcos DFT. Los diversos algoritmos de VV FFT se desarrollan en la* **Sección 4.2.5**.

### 4.2.4 Transforma 2D de Fourier de valores vectoriales

**Definición 34** (**Transformada de Fouier de Valores Vectoriales de dos Dimensiones**). *Sea* $\mathbf{X} \in \mathbb{C}^{D*(N\times N)}$ *y sea* $E$ *un conjunto de vectores complejos armónicos para* $\mathbb{C}^D$. *La transformada de Fouier de valores vectoriales de dos dimensiones VV DFT 2d de* $\mathbf{X}$ *se define como el mapeo* $\mathscr{F}^2_{\mathbf{X}} : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}^D$ *tal que*

$$\mathscr{F}^{2d}_{\mathbf{X}}[m,n] = \frac{1}{\sqrt{D}} \sum_{\alpha\in\mathbb{Z}_N} \sum_{\beta\in\mathbb{Z}_N} \mathbf{X}[\alpha,\beta] \odot E_N^{-(m\alpha+n\beta)} \tag{4.11}$$

De igual manera que en $\mathbb{C}^{N\times N}$, la VV DFT 2d de $\mathbf{X}$ puede ser vista como una matriz de arreglos. Sea $\mathbf{F}^{2d}_{\mathbf{x}} \in \mathbb{C}^{D*(N\times N)}$ la matriz de arreglos que representa a $\mathscr{F}_{\mathbf{X}}$, tal que $(\mathbf{F}^{2d}_{\mathbf{x}})_{i,j} = \mathscr{F}^{2d}_{\mathbf{X}}[i,j]$. Además

$$\mathbf{F}^{2d}_{\mathbf{X}} = \mathscr{R}_{N,N}\{(\mathbf{F_N} \otimes \mathbf{F_N})\mathscr{V}\{\mathbf{X}\}\} \tag{4.12}$$

donde:

- $\mathscr{V} : \mathbb{C}^{D*(M\times N)}) \to \mathbb{C}^{D*MN}$, es un operador que actua sobre las matrices de arreglos $\mathbb{C}^{D*(M\times N)}$ y da como resultado un vector de arreglos formado por la "acumulación" de las columnas. El análogo de este operador en $\mathbb{C}^{M\times N}$ es $\mathcal{V}$. Cuando $D = 1$, entonces $\mathscr{V} = \mathcal{V}$.
- $\mathscr{R}_{M,N} : \mathbb{C}^{D*MN} \to \mathbb{C}^{D*(M\times N)}$, es el operador que organiza un vector de arreglos en $\mathbb{C}^{D*MN}$ a una matriz de de arreglos en $\mathbb{C}^{D*(M\times N)}$. El análogo de este operador en $\mathbb{C}^{M\times N}$ es $\mathcal{R}_{M,N}$. Cuando $D = 1$, entonces $\mathscr{R}_{M,N} = \mathcal{R}_{M,N}$.

### 4.2.5 Transformada Rápida de Fourier de Valores Vectoriales

En esta sección, se desea extender los resultados sobre los diferentes tipos de factorización de la matriz DFT, $F_N \in \mathbb{C}^{N\times N}$, desarrollados en la **Sección 2.3.1**, a la matriz de arreglos $\mathbf{F}_N \in \mathbb{C}^{D*(N\times N)}$, lo que se conocería como la tranformada rápida de Fourier de valores vectoriales (VV FFT). Las demostraciones de los **Teoremas 20**, **21** y **22** tienen una estructura similar a las elaborados en [14] y [20] para la

matriz $F_N$. Por ser la matriz de arreglos VV DFT $\mathbf{F}_N$ un concepto nuevo y definido en este trabajo, se incluirá la demostración de cada teorema.

**Teorema 20.** *Si $N = RS$. Entonces*

$$\mathbf{F}_N = \sqrt{D}(\mathbf{F}_S \boxtimes \mathbf{I}_R)\mathbf{T}_R^N(\mathbf{I}_S \boxtimes \mathbf{F}_R)\mathbf{L}_S^N \tag{4.13}$$

*donde $\mathbf{T}_R^N \in \mathbb{C}^{D*(N\times N)}$ tal que*

$$\mathbf{T}_R^N = \bigoplus_{n\in\mathbb{Z}_S} (\mathbf{D}_R^N)^n$$

*donde $\mathbf{D}_R^N \in \mathbb{C}^{D*(R\times R)}$ es una matriz de arreglos diagonal por bloques tal que*

$$\mathbf{D}_R^N = diag(e_N^0,\ e_N^{-1}\ ,\ ...\ ,\ e_N^{-(R-1)})$$

**Prueba.** *Sea $\mathbf{x} \in \mathbb{C}^{D*N}$, tal que $\mathbf{x} = \mathbf{a} \boxtimes \mathbf{b}$, donde $\mathbf{a} \in \mathbb{C}^{D*R}$ y $\mathbf{b} \in \mathbb{C}^{D*S}$. Para $n \in \mathbb{Z}_N$, $r \in \mathbb{Z}_R$ y $s \in \mathbb{Z}_S$, se cumple que $\mathbf{x}[n] = \mathbf{x}[Sr + s] = \mathbf{a}[r] \odot \mathbf{b}[s]$. Entonces*

**1**. $$\begin{aligned}\mathbf{F}_N\mathbf{x} &= \sqrt{D}(\mathbf{F}_S \boxtimes \mathbf{I}_R)\mathbf{T}_R^N(\mathbf{I}_S \boxtimes \mathbf{F}_R)\mathbf{L}_S^N(\mathbf{a} \boxtimes \mathbf{b}) \\ &= \sqrt{D}(\mathbf{F}_S \boxtimes \mathbf{I}_R)\mathbf{T}_R^N(\mathbf{I}_S \boxtimes \mathbf{F}_R)(\mathbf{b} \boxtimes \mathbf{a}) \\ &= \sqrt{D}(\mathbf{F}_S \boxtimes \mathbf{I}_R)\mathbf{T}_R^N \underbrace{(\mathbf{b} \boxtimes \mathbf{F}_R\mathbf{a})}_{\mathbf{w}}\end{aligned}$$

*El vector $\mathbf{w}$ es de la forma*

$$\mathbf{w}[n] = \mathbf{w}[Rs + r] = \frac{1}{\sqrt{D}}\ \mathbf{b}[s] \odot \sum_{m\in\mathbb{Z}_R} \mathbf{a}[m] \odot e_R^{-mr}$$

**2**. $$\mathbf{F}_N\mathbf{x} = \sqrt{D}(\mathbf{F}_S \boxtimes \mathbf{I}_R)\ \underbrace{\mathbf{T}_R^N\mathbf{w}}_{\mathbf{y}}$$

*El vector $\mathbf{y}$ es de la forma*

$$\mathbf{y}[n] = \mathbf{y}[Rs + r] = \frac{1}{\sqrt{D}}\ \mathbf{b}[s] \odot e_N^{-rs} \odot \sum_{m\in\mathbb{Z}_R} \mathbf{a}[i] \odot e_R^{-mr}$$

**3**. $$\mathbf{F}_N\mathbf{x} = \sqrt{D}\ \underbrace{(\mathbf{F}_S \boxtimes \mathbf{I}_R)\mathbf{y}}_{\mathbf{z}}$$

*El vector* $\mathbf{z}$ *es de la forma*

$$\mathbf{z}[n] = \mathbf{z}[Rs + r] = \frac{1}{\sqrt{D}} \left( \frac{1}{\sqrt{D}} \sum_{c \in \mathbb{Z}_S} \mathbf{b}[c] \odot e_S^{-sc} \odot e_N^{-rc} \right) \odot \sum_{m \in \mathbb{Z}_R} \mathbf{a}[m] \odot e_R^{-mr}$$

*Re-escribiendo la última ecuación, se obtiene*

$$\mathbf{z}[n] = \mathbf{z}[Rs + r] = \frac{1}{D} \sum_{c \in \mathbb{Z}_S} \sum_{m \in \mathbb{Z}_R} \mathbf{a}[m] \odot \mathbf{b}[c] \odot e_N^{-(scR + mrS + rc)}$$

*Como* $N = RS$*, entonces* $scR + mrS + rc = scR + mrS + rc + RSms \ mod \ N$*. Además,* $scR + mrS + rc + RSms = (Sm + c)(Rs + r)$*, entonces*

$$\begin{aligned} \mathbf{z}[n] = \mathbf{z}[Rs + r] &= \frac{1}{D} \sum_{c \in \mathbb{Z}_S} \sum_{m \in \mathbb{Z}_R} \mathbf{a}[m] \odot \mathbf{b}[c] \odot e_N^{-(Sm+c)(RS+r)} \\ &= \frac{1}{D} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot e_N^{-nk} \end{aligned}$$

*Por lo tanto*

$$\mathbf{F}_N \mathbf{x}[k] = \sqrt{D} \frac{1}{D} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot e_N^{-nk} = \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot e_N^{-nk}$$

■

Del **Teorema 17**, $\mathbf{F}_S \boxtimes \mathbf{I}_R = \mathbf{L}_S^N (\mathbf{I}_R \boxtimes \mathbf{F}_S) \mathbf{L}_R^N$. Entonces la ecuación (4.13) se puede reescribir

$$\mathbf{F}_N = \sqrt{D} \mathbf{L}_S^N (\mathbf{I}_R \boxtimes \mathbf{F}_S) \mathbf{L}_R^N \mathbf{T}_R^N (\mathbf{I}_S \boxtimes \mathbf{F}_R) \mathbf{L}_S^N \tag{4.14}$$

Sea $\mathscr{L}_M^N$ el operador que representa a matriz de permutación $L_M^N$. En **Algoritmo 12**, se muestra la implementación de la ecuación (4.14).

**Algoritmo 12** VV FFT para $N = RS$

**Entrada:** $\mathbf{x} \in \mathbb{C}^{D*N}$
**Salida:** $\mathbf{y} \in \mathbb{C}^{D*N}$

$\mathbf{v}_0 \leftarrow \mathscr{L}_S^N\{\mathbf{x}\}$
**para** $s = 0 : S-1$ **hacer**
  $\mathbf{v}_1 \leftarrow \mathbf{v}_0[sR : (s+1)R-1]$
  $\mathbf{v}_2[sR : (s+1)R-1] \leftarrow \mathscr{F}_{\mathbf{v}_1}$
**fin para**
**para** $s = 0 : S-1$ **hacer**
  **para** $r = 0 : R-1$ **hacer**
    $\mathbf{v}_3[sR+r] = \mathbf{v}_2[sR+r] \odot e_N^{-rs}$
  **fin para**
**fin para**
$\mathbf{v}_4 \leftarrow \mathscr{L}_R^N\{\mathbf{v}_3\}$
**para** $r = 0 : R-1$ **hacer**
  $\mathbf{v}_5 \leftarrow \mathbf{v}_4[rS : (r+1)S-1]$
  $\mathbf{v}_6[rS : (r+1)S-1] \leftarrow \mathscr{F}_{\mathbf{v}_5}$
**fin para**
$\mathbf{v}_7 \leftarrow \mathscr{L}_S^N\{\mathbf{v}_6\}$
$\mathbf{y} \leftarrow \sqrt{D}\mathbf{v}_7$

**Teorema 21.** *Sea $N = 2^p$. Entonces*

$$\mathbf{F}_N = (\sqrt{D})^{p-1}\left[\prod_{n\in\mathbb{Z}_p} \mathbf{A}_n\mathbf{B}_n\right]\mathbf{Q}_N \tag{4.15}$$

*donde $\mathbf{A}_n, \mathbf{B}_n, \mathbf{Q}_N \in \mathbb{C}^{D*(N\times N)}$ tal que*

- $\mathbf{A}_n = \mathbf{I}_{2^n} \boxtimes \mathbf{F}_2 \boxtimes \mathbf{I}_{2^{p-n-1}}$
- $\mathbf{B}_n = \mathbf{I}_{2^n} \boxtimes \mathbf{T}^{2^{p-n}}_{2^{p-n-1}}$
- $\mathbf{Q}_N = \prod_{n\in\mathbb{Z}_{p-1}} \left(\mathbf{I}_{2^{p-n-2}} \boxtimes \mathbf{L}_2^{2^{n+2}}\right)$

**Prueba.** *La demostración se hará por inducción.*

- $p = 3$.

  *Como $N = 8 = 4 \cdot 2$, por el* **Teorema 20** *se obtiene:*

$$\mathbf{F}_8 = \sqrt{D}(\mathbf{F}_2 \boxtimes \mathbf{I}_4)\mathbf{T}_4^8(\mathbf{I}_2 \boxtimes \mathbf{F}_4)\mathbf{L}_2^8 \tag{4.16}$$

*Siguiendo la misma idea, como* $4 = 2 \cdot 2$*, por el mismo teorema se obtiene*

$$\mathbf{F}_4 = \sqrt{D}(\mathbf{F}_2 \boxtimes \mathbf{I}_2)\mathbf{T}_2^4(\mathbf{I}_2 \boxtimes \mathbf{F}_2)\mathbf{L}_2^4 \tag{4.17}$$

*Sustituyendo lo anterior en la ecuación 4.16, y aplicando los resultados obtenidos en el* **Teorema 16** *se obtiene*

$$\begin{aligned}\mathbf{F}_8 &= \sqrt{D}(\mathbf{F}_2 \boxtimes \mathbf{I}_4)\mathbf{T}_4^8(\mathbf{I}_2 \boxtimes [\sqrt{D}(\mathbf{F}_2 \boxtimes \mathbf{I}_2)\mathbf{T}_2^4(\mathbf{I}_2 \boxtimes \mathbf{F}_2)\mathbf{L}_2^4])\mathbf{L}_2^8 \\ &= D(\mathbf{F}_2 \boxtimes \mathbf{I}_4)\mathbf{T}_4^8(\mathbf{I}_2 \boxtimes \mathbf{F}_2 \boxtimes \mathbf{I}_2)(\mathbf{I}_2 \boxtimes \mathbf{T}_2^4)(\mathbf{I}_4 \boxtimes \mathbf{F}_2)(\mathbf{I}_2 \boxtimes \mathbf{L}_2^4)\mathbf{L}_2^8\end{aligned}$$

*Si*

- $\mathbf{A}_0 = \mathbf{F}_2 \boxtimes \mathbf{I}_4$
- $\mathbf{A}_1 = \mathbf{I}_2 \boxtimes \mathbf{F}_2 \boxtimes \mathbf{I}_2$
- $\mathbf{A}_2 = \mathbf{I}_4 \boxtimes \mathbf{F}_2$
- $\mathbf{B}_0 = \mathbf{T}_4^8$
- $\mathbf{B}_1 = \mathbf{I}_2 \boxtimes \mathbf{T}_2^4$
- $\mathbf{B}_2 = \mathbf{I}_8 = \mathbf{I}_4 \boxtimes \mathbf{T}_2^2$
- $\mathbf{Q}_8 = (\mathbf{I}_2 \boxtimes \mathbf{L}_2^4)\mathbf{L}_2^8$

*se cumple la ecuación (4.15) para* $N = 2^3$*.*

- *Se asume que la ecuación (4.15) se cumple para* $N = 2^k$*.*
- $N = 2^{k+1}$

  *Como* $N = 2^k \cdot 2$*, por el* **Teorema 20** *se obtiene:*

$$\mathbf{F}_N = \sqrt{D}(\mathbf{F}_2 \boxtimes \mathbf{I}_{2^k})\mathbf{T}_{2^k}^N(\mathbf{I}_2 \boxtimes \mathbf{F}_{2^k})\mathbf{L}_2^N \tag{4.18}$$

*Por hipótesis de inducción,*

$$\mathbf{F}_{2^k} = (\sqrt{D})^{k-1}\left[\prod_{n\in\mathbb{Z}_k} \mathbf{A}_n\mathbf{B}_n\right]\mathbf{Q}_{2^k} \tag{4.19}$$

*Sustituyendo lo anterior en la ecuación 4.18, y aplicando los resultados obtenidos en el* **Teorema 16** *se obtiene*

$$\begin{aligned}\mathbf{F}_N &= \sqrt{D}(\mathbf{F}_2 \boxtimes \mathbf{I}_{2^k})\mathbf{T}_{2^k}^N(\mathbf{I}_2 \boxtimes [(\sqrt{D})^{k-1}\left[\textstyle\prod_{n\in\mathbb{Z}_k} \mathbf{A}_n\mathbf{B}_n\right]\mathbf{Q}_{2^k}])\mathbf{L}_2^N \\ &= (\sqrt{D})^k(\mathbf{F}_2 \boxtimes \mathbf{I}_{2^k})\mathbf{T}_{2^k}^N(\left[\textstyle\prod_{n\in\mathbb{Z}_k}(\mathbf{I}_2 \boxtimes \mathbf{A}_n)(\mathbf{I}_2 \boxtimes \mathbf{B}_n)\right](\mathbf{I}_2 \boxtimes \mathbf{Q}_{2^k}))\mathbf{L}_2^N\end{aligned}$$

*Si*

- $\mathbf{C}_0 = \mathbf{F}_2 \boxtimes \mathbf{I}_{2^k}$
- $\mathbf{D}_0 = \mathbf{T}^N_{2^k}$
- $\mathbf{R}_N = (\mathbf{I}_2 \boxtimes \mathbf{Q}_{2^k}))\mathbf{L}^N_2$
- $\mathbf{C}_n = \mathbf{I}_2 \boxtimes \mathbf{A}_n$
- $\mathbf{D}_n = \mathbf{I}_2 \boxtimes \mathbf{B}_n$

*se cumple*

$$\mathbf{F}_N = (\sqrt{D})^k \left[ \prod_{n \in \mathbb{Z}_{k+1}} \mathbf{C}_n \mathbf{D}_n \right] \mathbf{R}_N \tag{4.20}$$

*donde* $\mathbf{C}_n, \mathbf{D}_n, \mathbf{R}_N \in \mathbb{C}^{D*(N\times N)}$ *tal que*

- $\mathbf{C}_n = \mathbf{I}_{2^n} \boxtimes \mathbf{F}_2 \boxtimes \mathbf{I}_{2^{k-n}}$
- $\mathbf{D}_n = \mathbf{I}_{2^n} \boxtimes \mathbf{T}^{2^{k-n+1}}_{2^{k-n}}$
- $\mathbf{R}_N = \prod_{n \in \mathbb{Z}_k} \left( \mathbf{I}_{2^{k-n-1}} \boxtimes \mathbf{L}^{2^{n+2}}_2 \right)$

■

**Teorema 22.** *Sea* $N$ *un número primo y sea* $a \in \mathbb{U}_N$ *un generador del conjunto* $\mathbb{U}_N$. *La matriz VV DFT puede factorizarse de la siguiente manera*

$$\mathbf{F}_N = \mathbf{L}^{-1}_a (\mathbf{1}_D \boxplus \mathbf{F})(\mathbf{1}_D \boxplus \mathbf{B})(\mathbf{1}_D \boxplus \mathbf{F})\mathbf{A}\mathbf{L}_a \tag{4.21}$$

*donde*

- $\mathbf{L}_a$ *es una matriz de arreglos de permutación de orden exponencial, tal que*

$$\mathbf{L}_a = \bigvee_{d \in \mathbb{Z}_D} L_a$$

*donde* $L_a \in \mathbb{C}^{N\times N}$ *es una matriz de permutación de orden exponencial con generador* $a$.

- $\mathbf{F} \in \mathbb{C}^{N-1\times N-1}$ *tal que* $\mathbf{F} = \bigvee F_{N-1}$.
- $\mathbf{B} \in \mathbb{C}^{D*((N-1)\times(N-1))}$ *es una matriz de arreglos diagonal tal que*

$$B = \mathbf{F}^{-1}\mathbf{C}\mathbf{F}$$

*donde* $\mathbf{c} \in \mathbb{C}^{D*((N-1)\times(N-1))}$ *es el núcleo de Winograd.*

- $\mathbf{A} \in \mathbb{C}^{N\times N}$ *tal que*

$$A = \begin{pmatrix} \mathbf{1}_D & \boldsymbol{1}_{D*(N-1)} \\ -\boldsymbol{1}_{D*(N-1)} & \mathbf{I}_{N-1} \end{pmatrix}$$

*donde* $\boldsymbol{1}_{D*(N-1)} \in \mathbb{C}^{D*N}$ *tal que* $\boldsymbol{1}_{D*(N-1)}[n] = \mathbf{1}_D$

**Prueba.** *Sea* $\pi_a = \{0, 1, a^1, a^2, ..., a^{N-2}\}$ *el conjunto de orden exponencial, generado a partir de* $a \in \mathbb{U}_N$. $\pi_a$ *es una permutación de* $\mathbb{Z}_N$, *cuando* $N$ *es primo.* $\pi_a$ *también se define como*

$$\pi_a(n) = \begin{cases} 0 & si\ n = 0 \\ a^{n-1} & si\ n \in \mathbb{U}_N \end{cases}$$

*y satisface que* $\pi_a(i)\pi_a(j) = \pi_a(i + j - 1)$. *La matriz de arreglo VV DFT satisface* $\mathbf{F}_N = \mathbf{L}_a^{-1}\mathbf{F}_{\pi_a}\mathbf{L}_a$, *donde* $(\mathbf{F}_{\pi_a})_{ij} = e_N^{-\pi_a(i)\pi_a(j)}$, *para* $i, j \in \mathbb{Z}_N$. *Entonces*

$$(\mathbf{F}_{\pi_a})_{ij} = \begin{cases} \mathbf{1}_D & si\ i = 0\ o\ j = 0 \\ e_N^{-a^{i+j-2}} & si\ i, j \in \mathbb{U}_N \end{cases}$$

*Por lo tanto,*

$$\mathbf{F}_{\pi_a} = \begin{pmatrix} \mathbf{1}_D & \mathbf{1}_D & \cdots & \mathbf{1}_D \\ \mathbf{1}_D & & & \\ \vdots & & \mathbf{C}_N & \\ \mathbf{1}_D & & & \end{pmatrix}$$

*donde* $\mathbf{C}_N \in \mathbb{C}^{D*((N-1)\times(N-1))}$ *tal que* $(\mathbf{C}_N)_{i,j} = e_N^{-a^{i+j}}$. *Considerando la matriz de arreglos* $\mathbf{A}$, *se cumple*

$$\mathbf{F}_{\pi_a} = \begin{pmatrix} \mathbf{1}_D & \\ & \mathbf{C}_N \end{pmatrix}\mathbf{A} = (\mathbf{1}_D \boxplus \mathbf{C}_p)\mathbf{A}$$

*Además,* $\mathbf{C}_N = \mathbf{FBF}$*, donde* $\mathbf{B}$ *es una matriz diagonal. Entonces*

$$\begin{aligned}\mathbf{F}_{\pi_a} &= (\mathbf{1}_D \boxplus \mathbf{C}_p)\mathbf{A} \\ &= (\mathbf{1}_D \boxplus \mathbf{F}_{N-1}\mathbf{B}\mathbf{F}_{N-1})\mathbf{A} \\ &= (\mathbf{1}_D \boxplus \mathbf{F}_{N-1})(\mathbf{1}_D \boxplus \mathbf{B})(\mathbf{1}_D \boxplus \mathbf{F}_{N-1})\mathbf{A}\end{aligned}$$

*Por lo tanto* $\mathbf{F}_N = \mathbf{L}_a^{-1}(\mathbf{1}_D \boxplus \mathbf{F}_{N-1})(\mathbf{1}_D \boxplus \mathbf{B})(\mathbf{1}_D \boxplus \mathbf{F}_{N-1})\mathbf{A}\mathbf{L}_a$

■

Sea $\mathscr{L}_a$ el operador que representa a matriz de permutación $\mathbf{L}_a$. En **Algoritmo 13**, se muestra la implementación de la ecuación (4.21).

**Algoritmo 13** VV FFT para $N$ primo

**Entrada:** $\mathbf{x} \in \mathbb{C}^{D*N}$ y $a \in \mathbb{U}_N$ (generador)
**Salida:** $\mathbf{y} \in \mathbb{C}^{D*N}$

1: $\mathbf{v}_0 \leftarrow \mathscr{L}_a\{\mathbf{x}\}$
2: **para** $n = 0 : N-2$ **hacer**
3: $\quad \mathbf{v}_1[n] \leftarrow \mathbf{v}_0[n+1] - \mathbf{v}_0[0]$
4: **fin para**
5: $\mathbf{v}_2 \leftarrow \mathscr{F}_{\mathbf{v}_1}$
6: **para** $n = 0 : N-2$ **hacer**
7: $\quad \mathbf{v}_3[n] = \mathbf{v}_2[n] \odot \mathbf{b}[n]$ (elementos matriz diagonal $\mathbf{B}$).
8: **fin para**
9: $\mathbf{v}_4[0] = \sum_{n \in \mathbb{Z}_N} \mathbf{v}_0[n]$
10: $\mathbf{v}_4[1 : N-1] \leftarrow \mathscr{F}_{\mathbf{v}_3}$
11: $\mathbf{y} \leftarrow \mathscr{L}_a^{-1}\{\mathbf{v}_4\}$

## 4.3 Función Discreta de Ambigüedad de Valores Vectoriales

J. J. Benedetto y J. J. Donatelli también desarrollan el concepto de una *función discreta discreta de ambigüedad de valores vectoriales* (VV DAF, del inglés vector-valued DAF) [16], a partir de la DAF T-1. De forma similar a la VV DFT, se define la VV DAF utilizando los vectores complejos armónicos, a partir de los 4 tipos de DAF.

**Definición 35 (Representaciones de la Función de Ambigüedad de Valores Vectoriales).** *Sea* $\mathbf{x}, \mathbf{y} \in \mathbb{C}^{D*N}$ *y* $E$ *un conjunto de vectores complejos armónicos.*

*La VV DAF de* $\mathbf{x}, \mathbf{y}$ *tiene 4 tipos de representaciones, y se definen como los mapeos* $\mathscr{A}^l_{\mathbf{x},\mathbf{y}} : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}^D$*, para* $l = 0, 1, 2, 3$*, tal que A*

- VV DAF Tipo 0 (VV DAF T-0)

$$\mathscr{A}^0_{\mathbf{x},\mathbf{y}}[m,k] = \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathbf{y}}[\langle n-m \rangle_N] \odot e_N^{-nk}. \tag{4.22}$$

- VV DAF Tipo 1 (VV DAF T-1)[1]

$$\mathscr{A}^1_{\mathbf{x},\mathbf{y}}[m,k] = \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[\langle n+m \rangle_N] \odot \overline{\mathbf{y}[n]} \odot e_N^{-nk}. \tag{4.23}$$

- VV DAF Tipo 2 (VV DAF T-2)

$$\mathscr{A}^2_{\mathbf{x},\mathbf{y}}[m,k] = \frac{1}{\sqrt{D}} \lambda_{m,k} \odot \sum_{n \in \mathbb{Z}_N} \mathbf{x}[\langle n+m \rangle_N] \odot \overline{\mathbf{y}[n]} \odot e_N^{nk}. \tag{4.24}$$

*donde*

$$\lambda_{m,k} = \begin{cases} e_N^{qmk} & N \text{ impar, } 2q \equiv 1 \bmod N \\ e_N^{mk/2} & N \text{ par, } \langle mk \rangle_N < \frac{N}{2} \\ e_N^{(mk-N)/2} & N \text{ par, } \langle mk \rangle_N \geqslant \frac{N}{2} \end{cases}$$

- VV DAF Tipo 3 (VV DAF T-3)

$$\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[m,k] = \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathbf{y}}[\langle n+m \rangle_N] \odot e_N^{-nk}. \tag{4.25}$$

Los diferentes de tipos de VV DAF presentan una equivalencia en normas:

$$\|\mathscr{A}^0_{\mathbf{x},\mathbf{y}}[m,k]\|_p = \|\mathscr{A}^1_{\mathbf{x},\mathbf{y}}[m,k]\|_p = \|\mathscr{A}^2_{\mathbf{x},\mathbf{y}}[m,k]\|_p = \|\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[-m,k]\|_p$$

para $p \in \mathbb{Z}$ y $p = \infty$.

El **Lema 4** y **Lema 5** exponen dos propiedades de la VV DAF.

**Lema 4.** *Sean* $\mathbf{x}, \mathbf{y} \in \mathbb{C}^{D*N}$*, donde N es un número primo, o un número compuesto N tal que* $D < r$*, donde r es el menor número primo de la factorización de N.*

[1] Definida por J. J. Benedetto y J. J. Donatelli en [16], para el caso $\mathbf{x}$=$\mathbf{y}$

*Entonces*

$$\mathscr{A}^0_{\mathbf{x},\mathbf{y}}[m,k] = \frac{D}{N} e_N^{-mk} \odot \mathscr{A}^0_{\mathscr{F}_\mathbf{x},\mathscr{F}_\mathbf{y}}[k, \langle -m \rangle_N] \tag{4.26}$$

$$\mathscr{A}^1_{\mathbf{x},\mathbf{y}}[m,k] = \frac{D}{N} e_N^{mk} \odot \mathscr{A}^1_{\mathscr{F}_\mathbf{x},\mathscr{F}_\mathbf{y}}[k, \langle -m \rangle_N] \tag{4.27}$$

$$\mathscr{A}^2_{\mathbf{x},\mathbf{y}}[m,k] = \frac{D}{N} e_N^{-mk} \odot \mathscr{A}^2_{\mathscr{F}_\mathbf{x},\mathscr{F}_\mathbf{y}}[\langle -k \rangle_N, m] \tag{4.28}$$

$$\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[m,k] = \frac{D}{N} e_N^{mk} \odot \mathscr{A}^3_{\mathscr{F}_\mathbf{x},\mathscr{F}_\mathbf{y}}[k, m] \tag{4.29}$$

**Prueba.** *Se realizará la prueba para VV DAF T-0. Los otros casos son similares. La VV DFT de* $\mathbf{x}$ *es* $\mathscr{F}_\mathbf{x}$*. Ahora, sea* $\mathbf{y}^*[n] = \mathbf{y}[\langle n-m \rangle_N] \odot e_N^{nk}$*. Entonces*

$$\begin{aligned}
\mathscr{F}_{\mathbf{y}^*}[p] &= \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{y}^*[n] \odot e_N^{-np} \\
&= \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{y}[\langle n-m \rangle_N] \odot e_N^{-n(p-k)} \\
&= \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{y}[n] \odot e_N^{-(n+m)(p-k)} \\
&= \frac{1}{\sqrt{D}} e_N^{-m(p-k)} \sum_{n \in \mathbb{Z}_N} \mathbf{y}[n] \odot e_N^{-n(p-k)} \\
&= e_N^{-m(p-k)} \odot \mathscr{F}_\mathbf{y}[\langle p-k \rangle_N]
\end{aligned}$$

*De lo anterior y utilizando la* **Proposición 7** *se obtiene*

$$\begin{aligned}
\mathscr{A}^0_{\mathbf{x},\mathbf{y}}[m,k] &= \frac{1}{\sqrt{D}} \sum_{n \in \mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathbf{y}^*}[n] \\
&= \frac{1}{\sqrt{D}} \left( \frac{D}{N} \sum_{p \in \mathbb{Z}_N} \mathscr{F}_\mathbf{x}[p] \odot \overline{\mathscr{F}_{\mathbf{y}^*}}[p] \right) \\
&= \frac{D}{N} \left( \frac{1}{\sqrt{D}} e_N^{-mk} \odot \sum_{p \in \mathbb{Z}_N} \mathscr{F}_\mathbf{x}[p] \odot \overline{\mathscr{F}_\mathbf{y}}[\langle p-k \rangle_N] \odot e_N^{mp} \right) \\
&= \frac{D}{N} e_N^{-mk} \odot \mathscr{A}^0_{\mathscr{F}_\mathbf{x},\mathscr{F}_\mathbf{y}}[k, \langle -m \rangle_N]
\end{aligned}$$

■

Del lema anterior, se deduce que $\mathscr{A}^l_{\mathbf{x},\mathbf{y}}$ es proporcional a $\mathbf{A}^l_{\mathscr{F}_\mathbf{x},\mathscr{F}_\mathbf{y}}$ cuando $m, k = 0$, donde $l = 0, 1, 2, 3$. Es decir

$$\mathscr{A}^l_{\mathbf{x},\mathbf{y}}[0,0] = \frac{D}{N} \mathscr{A}^l_{\mathscr{F}_\mathbf{x},\mathscr{F}_\mathbf{y}}[0,0] \tag{4.30}$$

**Lema 5.** *Sean* $\mathbf{x} \in \mathbb{C}^{D*N}$. *Entonces*

$$\overline{\mathscr{A}^0_{\mathbf{x}}}[\langle -m\rangle_N, \langle -k\rangle_N] = e_N^{mk} \odot \mathscr{A}^0_{\mathbf{x}}[m,k] \tag{4.31}$$

$$\overline{\mathscr{A}^1_{\mathbf{x}}}[\langle -m\rangle_N, \langle -k\rangle_N] = e_N^{-mk} \odot \mathscr{A}^1_{\mathbf{x}}[m,k] \tag{4.32}$$

$$\overline{\mathscr{A}^2_{\mathbf{x}}}[\langle -m\rangle_N, \langle -k\rangle_N] = e_N^{mk} \odot \mathscr{A}^2_{\mathbf{x}}[m,k] \tag{4.33}$$

$$\overline{\mathscr{A}^2_{\mathbf{x}}}[\langle -m\rangle_N, \langle -k\rangle_N] = e_N^{-mk} \odot \mathscr{A}^3_{\mathbf{x}}[m,k] \tag{4.34}$$

**Prueba.** *Se realizará la prueba para VV DAF T-0. Los otros casos son similares.*

$$\begin{aligned}
\overline{\mathscr{A}^0_{\mathbf{x}}}[\langle -m\rangle_N, \langle -k\rangle_N] &= \overline{\frac{1}{\sqrt{D}} \sum_{n\in\mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathbf{x}}[\langle n+m\rangle_N] \odot e_N^{nk}} \\
&= \frac{1}{\sqrt{D}} \sum_{n\in\mathbb{Z}_N} \overline{\mathbf{x}}[n] \odot \mathbf{x}[\langle n+m\rangle_N] \odot e_N^{-nk} \\
&= \frac{1}{\sqrt{D}} \sum_{n\in\mathbb{Z}_N} \overline{\mathbf{x}}[\langle n-m\rangle_N] \odot \mathbf{x}[n] \odot e_N^{-(n-m)k} \\
&= \frac{1}{\sqrt{D}} e_N^{mk} \odot \sum_{n\in\mathbb{Z}_N} \overline{\mathbf{x}}[\langle n-m\rangle_N] \odot \mathbf{x}[n] \odot e_N^{-nk} \\
&= e_N^{mk} \odot \mathscr{A}^0_{\mathbf{x}}[m,k]
\end{aligned}$$

■

### 4.3.1 Marco Computacional

La VVF DAF puede representarse como una matriz de arreglos.

**Definición 36 (Matriz DAF).** *Sea* $l = 0,1,2,3$. *La matriz VV DAF T-l se define como* $\mathbf{A}^l_{\mathbf{x},\mathbf{y}} \in \mathbb{C}^{D*(N\times N)}$ *tal que* $(\mathbf{A}^l_{\mathbf{x},\mathbf{y}})_{m,k} = \mathscr{A}^l_{\mathbf{x},\mathbf{y}}[m,k]$, *para* $m,k \in \mathbb{Z}_N$.

Realizando una extensión de la **Sección 2.2.2**, para $\{\mathbf{A}_n\}_{n\in\mathbb{Z}_N}$ un conjunto de $N$ matrices de arreglos $\mathbf{A}_n \in \mathbb{C}^{D*(M_n\times P)}$, el operador $\bigsqcup$ sobre el conjunto de matrices de arreglos $\{\mathbf{A}_n\}$ se define como

$$\bigsqcup_{n\in\mathbb{Z}_N} \mathbf{A}_n = \begin{pmatrix} \mathbf{A}_0 \\ \vdots \\ \mathbf{A}_{N-1} \end{pmatrix}$$

El siguiente teorema es una extension del **Teorema 9**, para el caso de VV DAF.

**Teorema 23.** *Sea* $\mathbf{x}, \mathbf{y} \in \mathbb{C}^{D*N}$ *y* $\mathbf{A}^0_{\mathbf{x},\mathbf{y}} \in \mathbb{C}^{D*(N\times N)}$ *la matriz VV DAF T-0. Entones*

$$\mathbf{A}^0_{x,y} = \mathscr{R}_{N,N}\{\mathbf{L}^{N^2}_N[\mathbf{I}_N \boxtimes \mathbf{F}_N][(\mathbf{1}_{D*N} \boxtimes \overline{\mathbf{x}}) \boxdot \mathbf{Y}]\},$$

*donde* $\mathbf{Y} \in \mathbb{C}^{N^2}$ *tal que*

$$\mathbf{Y} = \bigsqcup_{m\in\mathbb{Z}_N} \mathscr{S}_m\{\overline{\mathbf{y}}\},$$

*donde* $\mathscr{S}_m\{\overline{\mathbf{y}}\}[n] = \overline{\mathbf{y}}[\langle n-m\rangle_N]$ *para* $n \in \mathbb{Z}_N$.

**Prueba.** *Sea* $\mathbf{a}^0_{\mathbf{x},\mathbf{y}} = \mathbf{L}^{N^2}_N[\mathbf{I}_N \boxtimes \mathbf{F}_N][(\mathbf{1}_{D*N} \boxtimes \overline{\mathbf{x}}) \boxdot \mathbf{Y}]$. *Desarrollando* $\mathbf{a}^0_{\mathbf{x},\mathbf{y}}$ *se obtiene*

$$\mathbf{a}^0_{\mathbf{x},\mathbf{y}} = \mathbf{L}^{N^2}_N \bigsqcup_{m\in\mathbb{Z}_N} \mathbf{H}_m, \quad H_m \in \mathbb{C}^N$$

*tal que* $\mathbf{H}_m = \mathbf{F}_N(\mathbf{x} \odot \mathscr{S}_m\{\overline{\mathbf{y}}\})$, *donde* $\mathscr{S}_m$ *es el operador de traslación en* $\mathbb{C}^{D*N}$ *tal que* $\mathscr{S}_m\{\overline{\mathbf{y}}\}[n] = \overline{\mathbf{y}}[\langle n-m\rangle_N]$. *Aplicando a ambos lados de la ecuación el operador* $\mathscr{R}_{N,N}$, *se obtiene*

$$\mathscr{R}_{N,N}\{\mathbf{a}^0_{\mathbf{x},\mathbf{y}}\} = \mathscr{R}_{N,N}\left\{\mathbf{L}^{N^2}_N \bigsqcup_{m\in\mathbb{Z}_N} \mathbf{H}_m\right\} = \left(\mathscr{R}_{N,N}\left\{\bigsqcup_{m\in\mathbb{Z}_N} \mathbf{H}_m\right\}\right)^T$$

*Sea* $\mathbf{H} = \mathscr{R}_{N,N}\left\{\bigsqcup_{m\in\mathbb{Z}_N} \mathbf{H}_m\right\}$, *con* $\mathbf{H} \in \mathbb{C}^{D*(N\times N)}$ *y* $\mathbf{H} = (\mathbf{H}_0, \mathbf{H}_1, ..., \mathbf{H}_{N-1})$. *Para* $m, k \in \mathbb{Z}_N$ *se cumple*

$$\mathbf{H}^T_{m,k} = \mathbf{H}_{k,m} = \mathbf{H}_m[k] = \mathscr{A}^0_{\mathbf{x},\mathbf{y}}[m,k]$$

■

En el **Algoritmo 14**, muestra la implementación de la ecuación (3.9). Los pasos 2-3 son independientes en cada iteración, lo que permite su cómputo en paralelo.

El **Teorema 23** muestra que la estructura de la matriz $DAFT-0$ en $\mathbb{C}^{N\times N}$ se mantiene para la matriz de arreglos VV DAF T-0 en el espacio $\mathbb{C}^{D*(N\times N)}$. La Tabla 4–1 muestra la representación matricial, utilizando productos de Kronecker, de los cuatro tipos de VV DAF .

**Algoritmo 14** Matriz VV DAF T-0

**Entrada:** $\mathbf{x}, \mathbf{y} \in \mathbb{C}^{D*N}$
**Salida:** $\mathbf{A} \in \mathbb{C}^{D*(N\times N)}$

1: **para** $n = 0 : N-1$ **hacer**
2: $\quad \mathbf{v} \leftarrow \mathbf{x} \boxdot \mathscr{S}_n\{\overline{\mathbf{y}}\}$
3: $\quad \mathbf{A}[:, n] \leftarrow \mathscr{F}_v$
4: **fin para**
5: $\mathbf{A} \leftarrow \mathbf{A}^T$

Tabla 4–1: Representación Kronecker de la matrices VV DAF

$$\mathscr{A}^l_{\mathbf{x},\mathbf{y}} = \mathscr{R}_{N,N}\{\mathbf{a}^l_{x,y}\}$$

| $T-l$ | $\mathbf{a}^l_{x,y}$ | $\mathbf{X}-\mathbf{Y}$ | $\mathbf{P}$ |
|---|---|---|---|
| $T-0$ | $\mathbf{L}^{N^2}_N \left[\mathbf{I}_N \boxtimes \mathbf{F}_N\right] \left[(\mathbf{1}_{D*N} \boxtimes \mathbf{x}) \boxdot \mathbf{Y}\right]$ | $\bigsqcup_{m\in\mathbb{Z}_N} \mathscr{S}_m\{\overline{\mathbf{y}}\}$ | |
| $T-1$ | $\mathbf{L}^{N^2}_N \left[\mathbf{I}_N \boxtimes \mathbf{F}_N\right] \left[\mathbf{X} \boxdot (\mathbf{1}_{D*N} \boxtimes \overline{\mathbf{y}})\right]$ | $\bigsqcup_{m\in\mathbb{Z}_N} \mathscr{S}_{-m}\{\mathbf{x}\}$ | |
| $T-2$ | $\mathbf{L}^{N^2}_N \mathbf{P} \left[\mathbf{I}_N \boxtimes \overline{\mathbf{F}_N}\right] \left[\mathbf{X} \boxdot (\mathbf{1}_{D*N} \boxtimes \overline{\mathbf{y}})\right]$ | $\bigsqcup_{m\in\mathbb{Z}_N} \mathscr{S}_{-m}\{\mathbf{x}\}$ | $\bigboxplus_{m,k\in\mathbb{Z}_N} diag(\lambda_{m,k})$ |
| $T-3$ | $\mathbf{L}^{N^2}_N \left[\mathbf{I}_N \boxtimes \mathbf{F}_N\right] \left[(\mathbf{1}_{D*N} \boxtimes \mathbf{x}) \boxdot \mathbf{Y}\right]$ | $\bigsqcup_{m\in\mathbb{Z}_N} \mathscr{S}_{-m}\{\overline{\mathbf{y}}\}$ | |

## 4.4 Grupo de Heisenberg

L. Auslander y R. Tolimieri [34] desarrolló una relación entre la función de ambigüedad y el grupo de Heisenberg. En esta sección se elabora una extensión de este trabajo, aplicado a las 4 representaciones de la VV DAF.

Para eso, primero se define lo que es un operador unitario en el espacio de las matrices de arreglos

**Definición 37 (Operador Unitario en $\mathbb{C}^{D*N}$).** *Un operador unitario en $\mathbb{C}^{D*N}$ es un mapeo lineal $\mathscr{U}$ de $\mathbb{C}^{D*N}$ que satisface*

$$\mathscr{U}\overline{\mathscr{U}} = \mathscr{I}$$

*donde $\overline{\mathscr{U}}$ es conocido como el operador adjunto y $\mathscr{I}$ es el operador identidad.*

En el caso de los operadores unitarios, el operador adjunto también es conocido como *operador inverso*, el cuál es también un operador unitario.. La colección de

todos los operadores unitarios $\mathscr{U}$ en $\mathbb{C}^{D*N}$ forman un grupo bajo la composición. Este grupo se denota con el símbolo $\mathfrak{U}$.

Todo operador unitario tiene una representación matricial. Sea $\mathbf{I}_N \in \mathbb{C}^{D*(N\times N)}$ la representación del operador identidad $\mathscr{I}$. Ejemplos de operadores unitarios en $\mathbb{C}^{D*N}$ son el operador de translación, modulación y rotación.

**Definición 38 (Operadores de Traslación, Modulación y Rotación en $\mathbb{C}^{D*N}$).** *Sea* $\mathbf{x} \in \mathbb{C}^{D*N}$, $m, k \in \mathbb{Z}_N$ *y* $\lambda \in \mathbb{C}^D$, *con* $|\lambda[n]| = 1$.

1. $\mathscr{S}_m$ *es el operador de traslación,* $S : \mathbb{Z}_N \to \mathcal{U}$ *tal que*

$$\mathscr{S}_m\{\mathbf{x}\}[n] = \mathbf{x}[\langle n - m\rangle_N].$$

*La representación matricial de* $\mathscr{S}_m$ *es* $\mathbf{S}_m \in \mathbb{C}^{D*(N\times N)}$ *tal que*

$$\mathbf{S}_m = \bigvee_{d\in\mathbb{Z}_D} S_m$$

2. $\mathscr{M}_k$ *es el operador de modulación,* $M : \mathbb{Z}_N \to \mathcal{U}$ *tal que*

$$\mathscr{M}_k\{\mathbf{x}\}[n] = e_N^{nk} \odot \mathbf{x}[n].$$

*La representación matricial de* $\mathscr{M}_k$ *es* $\mathbf{M}_k \in \mathbb{C}^{D*(N\times N)}$ *tal que*

$$\mathbf{M}_k = \bigvee_{d\in\mathbb{Z}_D} (M_k)^{d+1}$$

3. $\mathscr{C}_\lambda$ *es el operador de rotación, tal que*

$$\mathscr{C}_\lambda\{\mathbf{x}\}[n] = \lambda \odot \mathbf{x}[n].$$

*La representación matricial de* $\mathscr{C}_\lambda$ *es* $\mathbf{C}_\lambda \in \mathbb{C}^{D*(N\times N)}$ *tal que* $\mathbf{C}_\lambda = \lambda \diamond \mathbf{I}_N$

Los operadores adjuntos de $\mathscr{S}_m$, $\mathscr{M}_k$ y $\mathscr{C}_\lambda$ son $\mathscr{S}_{-m}$, $\mathscr{M}_{-k}$ y $\mathscr{C}_{1/\lambda}$ respectivamente.

**Lema 6.** $\mathscr{S}_m$ *y* $\mathscr{M}_k$ *son isomorfismos de* $\mathbb{Z}_N$ *en* $\mathcal{U}$.

**Prueba.** *Los operadores unitarios $\mathscr{S}_m$, $\mathscr{M}_k$, $\mathscr{S}_{-m}$, $\mathscr{M}_{-k}$ son homomorfismos de $\mathbb{Z}_N$ en $\mathcal{U}$, por lo tanto, se cumple el Lemma.*

Como se explicó anteriormente, la colección de todos los operadores unitarios $\mathscr{U}$ en $\mathbb{C}^{D*N}$ forman un grupo bajo la composición. Pero este grupo no es conmutativo.

**Ejemplo.** *Sea $\mathbf{x} \in \mathbb{C}^{D*N}$, entonces:*

- $(\mathscr{M}_k \circ \mathscr{S}_m)\{\mathbf{x}\}[n] = e_N^{nk} \odot \mathscr{S}_m\{\mathbf{x}\}[n] = e_N^{nk} \odot \mathbf{x}[n-m]$.
- $(\mathscr{S}_m \circ \mathscr{M}_k)\{\mathbf{x}\}[n] = \mathscr{M}_k\{\mathbf{x}\}[n-m] = e_N^{(n-m)k} \odot \mathbf{x}[n-m]$

*Por lo tanto, $\mathscr{M}_k$ y $\mathscr{S}_m$ no son conmutativos. La relación que se tiene entre ambos operadores es*

$$\mathscr{M}_k \circ \mathscr{S}_m = e_N^{mk} \odot (\mathscr{S}_m \circ \mathscr{M}_k).$$

Considere el conjunto $\mathcal{H} \subset \mathfrak{U}$, tal que

$$\mathcal{H} = \{\mathscr{D} \in \mathcal{U} : \mathscr{D} = \mathscr{C}_\lambda \circ \mathscr{M}_k \circ \mathscr{S}_M, \lambda \in \mathbb{C}^D, |\lambda[n]| = 1, m, k \in \mathbb{Z}_N\} \tag{4.35}$$

Un caso especial, es cuando $\lambda = e_N^{c-mk}$, lo que ayuda a introducir el grupo discreto de Heisenberg. El *grupo discreto de Heisenberg* se define como el el conjunto $\mathbb{H}_N$ tal que

$$\mathbb{H}_N = \{\mathbf{v} = (v_1, v_2, v_3) : v_i \in \mathbb{Z}_N\} \tag{4.36}$$

$\mathbb{H}_N$ es un grupo bajo la operación $\mathbf{v} \cdot \mathbf{w} = (v_1 + w_1, v_2 + w_2, v_3 + w_3 + v_1 w_2)$ [12, 49]. Sea $\mathbf{v} = (v_1, v_2, v_3)$ en $\mathbb{H}_N$. Ahora, considere $\mathcal{H}_{\lambda_v} \subset \mathcal{H}$, tal que

$$\mathcal{H}_{\lambda_v} = \{\mathscr{D}_\mathbf{v} \in \mathcal{U} : \mathscr{D}_\mathbf{v} = \mathscr{C}_{\lambda_v} \circ \mathscr{M}_k \circ \mathscr{S}_M, \lambda_\mathbf{v} = e_N^{v_3 - v_1 v_2} \in \mathbb{C}^D, m, k \in \mathbb{Z}_N\} \tag{4.37}$$

$\mathscr{D}_\mathbf{v}$ está relacionado con el grupo de Heisenberg.

**Teorema 24.** *$\mathscr{D}_\mathbf{v}$ es un homomorfismo de $\mathbb{H}$ en $\mathcal{U}$. Además*

- *$ker(\mathscr{D}_\mathbf{v}) = \{(0,0,0)\}$.*
- *$im(\mathscr{D}_\mathbf{v}) = \mathcal{H}_{\lambda_v}$.*

**Prueba.** *Sea* $\mathbf{x} \in \mathbb{C}^{D*N}$ *y* $\mathbf{v}, \mathbf{w} \in \mathbb{H}$. *Hay que demostrar que*

$$\mathscr{D}_{\mathbf{v}\cdot\mathbf{w}}\{\mathbf{x}\}[n] = (\mathscr{D}_{\mathbf{v}} \circ \mathscr{D}_{\mathbf{w}})\{\mathbf{x}\}[n].$$

- *Caso 1:* $\mathscr{D}_{\mathbf{v}\cdot\mathbf{w}}[n]$. *Se conoce que* $\mathbf{v}\cdot\mathbf{w} = (v_1 + w_1, v_2 + w_2, v_3 + w_3 + v_1 w_2)$. *Entonces*

$$\begin{aligned}\mathscr{D}_{\mathbf{v}\cdot\mathbf{w}}\{\mathbf{x}\}[n] &= (\mathscr{C}_{\lambda_{\mathbf{v}\cdot\mathbf{w}}} \circ \mathscr{M}_{v_1+w_1} \circ \mathscr{S}_{v_2+w_2})\{\mathbf{x}\}[n] \\ &= e_N^{v_3+w_3-v_1w_1-v_2w_1-w_1w_2} \odot e_N^{(v_1+w_1)n} \odot \mathbf{x}[n-(v_2+w_2)]\end{aligned}$$

- *Caso 2:* $(\mathscr{D}_{\mathbf{v}} \circ \mathscr{D}_{\mathbf{w}})\{\mathbf{x}\}[n]$. *Entonces*

$$\begin{aligned}(\mathscr{D}_{\mathbf{v}} \circ \mathscr{D}_{\mathbf{w}})\{\mathbf{x}\}[n] &= ((\mathscr{C}_{\lambda_{\mathbf{v}}} \circ \mathscr{M}_{v_1} \circ \mathscr{S}_{v_2}) \circ (\mathscr{C}_{\lambda_{\mathbf{w}}} \circ \mathscr{M}_{w_1} \circ \mathscr{S}_{w_2}))\{\mathbf{x}\}[n] \\ &= e_N^{v_3-v_1v_2} \odot e_N^{v_1 n} \odot (\mathscr{C}_{\lambda_{\mathbf{w}}} \circ \mathscr{M}_{w_1} \circ \mathscr{S}_{w_2})\{\mathbf{x}\}[n-v_2] \\ &= e_N^{v_3-v_1v_2} \odot e_N^{v_1 n} \odot e_N^{w_3-w_1w_2} \odot e_N^{w_1(n-v_2)} \odot \mathbf{x}[n-v_2-w_2] \\ &= e_N^{v_3+w_3-v_1w_1-v_2w_1-w_1w_2} \odot e_N^{(v_1+w_1)n} \odot \mathbf{x}[n-(v_2+w_2)]\end{aligned}$$

*Es claro que solo* $\mathbf{v} = (0,0,0)$ *cumple que* $\mathscr{D}_{\mathbf{v}} = \mathscr{I}$ *y por definición de* $\mathcal{H}_{\lambda_v}$ *(ecuación (4.37)),* $im(\mathscr{D}_{\mathbf{v}}) = \mathcal{H}_{\lambda_v}$.

■

Sea $\mathbf{x}, \mathbf{y} \in \mathbb{C}^{D*N}$, $\mathbf{u} \in \mathbb{H}$, donde $\mathbf{u} = (k, m, c)$. Re-escribiendo los diferentes tipos de VV DAF de la Definición 35, se obtiene

$$\mathscr{A}^0_{\mathbf{x},\mathbf{y}}[m,k] = \frac{1}{\sqrt{D}}\, e_N^{c-mk} \odot \sum_{n\in\mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathscr{D}_{\mathbf{v}}\{\mathbf{y}\}}[n]. \tag{4.38}$$

$$\mathscr{A}^1_{\mathbf{x},\mathbf{y}}[m,k] = \frac{1}{\sqrt{D}}\, e_N^{c} \odot \sum_{n\in\mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathscr{D}_{\mathbf{v}}\{\mathbf{y}\}}[n]. \tag{4.39}$$

$$\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[-m,k] = \frac{1}{\sqrt{D}}\, e_N^{c-mk} \odot \sum_{n\in\mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathscr{D}_{\mathbf{v}}\{\mathbf{y}\}}[n]. \tag{4.40}$$

Por lo tanto, VV FDA T-0, VV FDA T-1 y VV FDA T-3 están relacionadas con el grupo de Heisenberg. Para el caso VV FDA T-2, bajo la estructura que propone Richman [12] de FDA T-2, no se puede relacionar con el grupo de Heisenberg de la manera que se desarrolló anteriormente.

## 4.5 Proceso de Decimación

En está sección, se expone un método de decimanción para la VV DAF T-2, basado en el trabajo realizado por Auslander y Tolimieri para la DAF T-2 [11], ya que el método explicado por Auslander y Tolimieri mantiene la misma estructura para elementos en $\mathbb{C}^{D*N^2}$, cuando $N$ es un número primo.

De la ecuación (4.25), VV DAF T-2 es definida como

$$\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[m,k] = \frac{1}{\sqrt{D}} \sum_{n\in\mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathbf{y}}[\langle n+m\rangle_N] \odot e_N^{-nk}$$

Definiendo el operador unitario $\mathscr{G}_{m,k} \in \mathfrak{U}$, tal que $\mathscr{G}_{m,k} = \mathscr{M}_k \circ \mathscr{S}_{-m}$, entonces VV DAF T-2 se puede definir como

$$\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[m,k] = \frac{1}{\sqrt{D}} \sum_{n\in\mathbb{Z}_N} \mathbf{x}[n] \odot \overline{\mathscr{G}_{m,k}\{y\}}[n]$$

Ahora, considerando el espacio $\mathbb{C}^{D*N^2}$, donde $N$ es un número primo, existen ciertas relaciones entre $\mathscr{G}_{m,k}\{y\}$ y $\mathbf{y}$ que pueden dar ventajas para el desarrollo del método. Sea $\mathbf{z} \in \mathbb{C}^{D*N^2}$, el operador $\mathscr{U}_z : \mathbb{Z}_N \times \mathbb{Z}_N \to \mathbb{C}^{D*N^2}$ se define como

$$\mathscr{U}_z[\alpha,\beta] = \sum_{\delta\in\mathbb{Z}_N} \mathbf{z}[\alpha+\delta N] \odot e_N^{\beta\delta}$$

Sea $\mathbf{x},\mathbf{y} \in \mathbb{C}^{D*N^2}$. Aplicando el operador $\mathcal{U}$ a $\mathbf{x}$ y $\mathscr{G}_{m,k}\{y\} = \mathbf{y}[n+m] \odot E_{N^2}^{nk}$ se obtiene:

$$\mathscr{U}_x[\alpha,\beta] = \sum_{\delta_1\in\mathbb{Z}_N} \mathbf{x}[\alpha+\delta_1 N] \odot e_N^{\beta\delta_1}, \tag{4.41}$$

$$\mathscr{U}_{\mathscr{G}_{m,k}\{y\}}[\alpha,\beta] = \sum_{\delta_2\in\mathbb{Z}_N} \mathscr{G}_{m,k}\{y\}[\alpha+\delta_2 N] \odot e_N^{\beta\delta_2}, \tag{4.42}$$

Ahora, se opera a $\mathscr{U}_{\mathscr{G}_{m,k}\{y\}}$ y $\mathscr{U}_x$ de la siguiente manera

$$
\begin{aligned}
&\frac{1}{N}\sum_{\alpha\in\mathbb{Z}_N}\sum_{\beta\in\mathbb{Z}_N}\mathscr{U}_x[\alpha,\beta]\odot\overline{\mathscr{U}_{\mathscr{G}_{m,k}\{y\}}}[\alpha,\beta]\\
&\quad=\frac{1}{N}\sum_{\alpha\in\mathbb{Z}_N}\sum_{\beta\in\mathbb{Z}_N}\left\{\left[\sum_{\delta_1\in\mathbb{Z}_N}\mathbf{x}[\alpha+\delta_1N]\odot e_N^{\beta\delta_1}\right]\odot\right.\\
&\qquad\qquad\left.\overline{\left[\sum_{\delta_2\in\mathbb{Z}_N}\mathscr{G}_{m,k}\{y\}[\alpha+\delta_2N]\odot e_N^{\beta\delta_2}\right]}\right\}\\
&\quad=\frac{1}{N}\sum_{\alpha\in\mathbb{Z}_N}\sum_{\delta_1\in\mathbb{Z}_N}\sum_{\delta_2\in\mathbb{Z}_N}\mathbf{x}[\alpha+\delta_1N]\odot\overline{\mathscr{G}_{m,k}\{y\}}[\alpha+\delta_2N]\odot\underbrace{\sum_{\beta\in\mathbb{Z}_N}e_N^{(\delta_1-\delta_2)\beta}}_{N\cdot\mathbf{1}_D\text{ si }\delta_1=\delta_2\,(*)}\\
&\quad=\sum_{\alpha\in\mathbb{Z}_N}\sum_{\delta_1\in\mathbb{Z}_N}\mathbf{x}[\alpha+\delta_1N]\odot\overline{\mathscr{G}_{m,k}\{y\}}[\alpha+\delta_1N]\\
&\quad=\sum_{n\in\mathbb{Z}_{N^2}}\mathbf{x}[n]\odot\overline{\mathscr{G}_{m,k}\{y\}}[n]\\
&\quad=\frac{1}{\sqrt{D}}\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[m,k]
\end{aligned}
$$

Por lo tanto

$$
\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[m,k]=\frac{1}{N\sqrt{(D)}}\sum_{\alpha\in\mathbb{Z}_N}\sum_{\beta\in\mathbb{Z}_N}\mathscr{U}_{\mathbf{x}}[\alpha,\beta]\odot\overline{\mathscr{U}_{\mathscr{G}_{m,k}\{y\}}}[\alpha,\beta]\tag{4.43}
$$

La importancia de seleccionar $N$ como número primo es para que se cumpla $(*)$. Seleccionado $m=\theta N$ y $k=\tau N$ se obtiene

$$
\begin{aligned}
\mathscr{U}_{\mathscr{G}_{\theta N,\tau N}\{y\}}[\alpha,\beta]&=\sum_{\delta_2\in\mathbb{Z}_N}\mathbf{y}[\theta N+\alpha+\delta_2N]\odot e_{N^2}^{(\alpha+\delta_2N)\tau N}\odot e_N^{\beta\delta_2}\\
&=\sum_{\substack{\delta_2\in\mathbb{Z}_N\\ N-1+\theta}}\mathbf{y}[\alpha+(\theta+\delta_2)N]\odot e_N^{\alpha\tau}\odot\overbrace{e_N^{\delta_2N\tau}}^{\mathbf{1}_D}\odot e_N^{\beta\delta_2}\\
&=\sum_{\delta_2=\theta}\mathbf{y}[\alpha+\delta_2N]\odot e_N^{\alpha\tau}\odot e_N^{\beta(\delta_2-\theta)}\\
&=E_N^{\alpha\tau-\beta\theta}\odot\sum_{\delta_2\in\mathbb{Z}_N}\mathbf{y}[\alpha+\delta_2N]\odot e_N^{\beta\delta_2}\\
&=e_N^{\alpha\tau-\beta\theta}\odot\mathscr{U}_{\mathbf{y}}[\alpha,\beta]
\end{aligned}
$$

Entonces

$$
\mathscr{U}_{\mathscr{G}_{\theta N,\tau N}\{y\}}[\alpha,\beta]=\mathscr{U}_{\mathbf{y}}[\alpha,\beta]\odot e_N^{\alpha\tau-\beta\theta}\tag{4.44}
$$

Por lo tanto, de las ecuaciones (4.43) y (4.44), se obtiene

$$\begin{aligned}\mathscr{A}^3_{x,y}[\theta N, \tau N] &= \frac{1}{N}\sum_{\alpha\in\mathbb{Z}_N}\sum_{\beta\in\mathbb{Z}_N}\mathscr{U}_{\mathbf{x}}[\alpha,\beta]\odot\overline{\mathscr{U}_{\mathbf{y}}}[\alpha,\beta]\odot e_N^{-(\alpha\tau-\beta\theta)} \\ &= \mathscr{F}^{2d}_{\mathbf{H}}[\tau,-\theta]\end{aligned} \tag{4.45}$$

donde $\mathbf{H}\in\mathbb{C}^{D*(N\times N)}$, tal que $\mathbf{H}[\alpha,\beta] = \mathscr{U}_{\mathbf{x}}[\alpha,\beta]\odot\overline{\mathscr{U}_{\mathbf{y}}}[\alpha,\beta]$. Por lo tanto, lo anterior demuestra que el cálculo de $\mathscr{A}^3_{\mathbf{x},\mathbf{y}}$ en el subconjunto $\mathbb{F}\subseteq\mathbb{Z}_{N^2}\times\mathbb{Z}_{N^2}$, con $\mathbb{F} = \{(\theta N,\tau N) : \theta,\tau\in\mathbb{Z}_N\}$, se obtiene apartir de la VV DFT $2D$ de $\mathbf{H}$

Ahora, considere el conjunto $\mathbb{H}\subseteq\mathbb{Z}_{N^2}\times\mathbb{Z}_{N^2}$, tal que $\mathbb{H} = \{(\lambda+\theta N,\mu+\tau N) : \theta,\tau,\lambda,\mu\in\mathbb{Z}_N\}$. Ahora, se mostrará que el cálculo de $\mathscr{A}^3_{\mathbf{x},\mathbf{y}}$ en el conjunto $\mathbb{H}$ es equivalente a realizar el cálculo en el conjunto $\mathbb{H}$. Sabiendo que

- $\mathscr{G}_{\lambda,\mu}\{\mathbf{y}\}[n+\theta N] = e_N^{\theta\mu}\odot\mathbf{y}[n+\theta N+\lambda]\odot e_{N^2}^{n\mu}$.
- $\mathbf{y}[n+\theta N+\lambda]\odot E_{N^2}^{n\mu} = e_N^{-\theta\mu}\odot\mathscr{G}_{\lambda,\mu}\{\mathbf{y}\}[n+\theta N]$.

obtenemos:

$$\begin{aligned}\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[\lambda+\theta N,\mu+\tau N] &= \sum_{n\in\mathbb{Z}_{N^2}}\mathbf{x}[n]\odot\overline{\mathbf{y}[n+\lambda+\theta N]\odot e_{N^2}^{\mu n}}\odot e_{N^2}^{-\tau N n} \\ &= \sum_{n\in\mathbb{Z}_{N^2}}\mathbf{x}[n]\odot\overline{e_N^{-\theta\mu}\odot\mathscr{G}_{\lambda,\mu}\{\mathbf{y}\}[n+\theta N]}\odot e_{N^2}^{-\tau N n} \\ &= e_N^{\theta\mu}\odot\sum_{n\in\mathbb{Z}_{N^2}}\mathbf{x}[n]\odot\overline{\mathscr{G}_{\lambda,\mu}\{\mathbf{y}\}}[n+\theta N]\odot e_{N^2}^{-\tau N n} \\ &= E_N^{\theta\mu}\odot\mathscr{A}^2_{\mathbf{x},\mathscr{G}_{\lambda,\mu}\{\mathbf{y}\}}[\theta N,\tau N]\end{aligned}$$

Entonces

$$\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[\lambda+\theta N,\mu+\tau N] = e_N^{\theta\mu}\odot\mathscr{A}^3_{\mathbf{x},\mathscr{G}_{\lambda,\mu}\{\mathbf{y}\}}[\theta N,\tau N] \tag{4.46}$$

Por lo tanto, el cómputo de $\mathscr{A}^2_{\mathbf{x},\mathbf{y}}$ en el espacio $\mathbb{H}$, se obtiene de realizar el cómputo de $\mathscr{A}^2_{\mathbf{x},\mathscr{G}_{\lambda,\mu}\{\mathbf{y}\}}$ en el espacio $\mathbb{F}$.

En resumen, sea $\mathbf{x}\in\mathbb{C}^{D*N^2}$, donde $N$ es primo o $N$ es un número compuesto, y $r$ el menor número primo de la factorización de $N$ y $D<r$. Entonces:

- El cómputo de $\mathscr{A}^3_{x,y}$ en el conjunto $\mathbb{F} = \{(\theta N, \tau N) : \theta, \tau \in \mathbb{Z}_N\}$ se obtiene a partir de

$$\mathscr{A}^3_{x,y}[\theta N, \tau N] = \mathscr{F}^{2d}_{\mathbf{H}}[\tau, -\theta]$$

donde $\mathbf{H} \in \mathbb{C}^{D*(N\times N)}$, tal que $\mathbf{H}[\alpha, \beta] = \mathscr{U}_{\mathbf{x}}[\alpha, \beta] \odot \overline{\mathscr{U}_{\mathbf{y}}}[\alpha, \beta]$

- El cómputo de $\mathscr{A}^3_{x,y}$ en el conjunto $\mathbb{H} = \{(\lambda + \theta N, \mu + \tau N) : \theta, \tau, \lambda, \mu \in \mathbb{Z}_N\}$ se obtiene a partir de

$$\mathscr{A}^3_{\mathbf{x},\mathbf{y}}[\lambda + \theta N, \mu + \tau N] = e^{\theta\mu}_N \odot \mathscr{A}^3_{\mathbf{x},\mathscr{G}_{\lambda,\mu}\{\mathbf{y}\}}[\theta N, \tau N]$$

# CAPÍTULO 5
# APLICACIONES

En esta sección se explicará dos aplicaciones de la DAF y VV DAF. La primera es en el modelamiento de secuencias discretas de constante amplitud y cero autocorrelación, conocidas como secuencias CAZAC (del inglés, constant amplitude zero-autocorrelation) y, una nueva aplicación propuesta por el autor, que es en el campo de la criptografía. Además, se desarrolla el concepto de matrices arreglos circulantes, utilizando el álgebra de matrices de arreglos.

## 5.1 Secuencias CAZAC

El área de diseño de ondas (del inglés, waveform design) cuenta con una atención constante debido a los avances en el hardware, algoritmos y sistemas de codificación aplicado a radares, utilizando la función de ambigüedad. Estos avances han tenido un impacto creativo y sinérgico en el diseño de ondas de radar, proporcionando mejoras a la función de ambigüedad y a las propiedades de detección de objetos [32]. Un ejemplo específico de diseño de ondas son las secuencias de amplitud constante y cero autocorrelación, conocidas como secuencias CAZAC.

**Definición 39** (**Secuencia CAZAC).** *Sea $x \in \mathbb{C}^N$. Entonces $x$ es una secuencia CAZAC (del inglés, constant amplitude zero-autocorrelation) si*

- *Para todo $n \in \mathbb{Z}_N$, $|x[n]| = 1$, (CA-amplitud constante)*
- *Para todo $m \in \mathbb{U}_N$, (ZAC- Cero autocorrelación)*

$$C_x[m] = \frac{1}{N} \sum_{n \in \mathbb{Z}_N} x[\langle n+m \rangle_N] \overline{x}[n] = 0$$

Las secuencias CAZAC son importantes en el diseño de ondas por su transmisión eficiente y sus propiedades en la localización del tiempo. Cierta clase de secuencias CAZAC son utilizadas en radares, criptografía y comunicaciones [10].

### 5.1.1 Ejemplos de Secuencias CAZAC en $\mathbb{C}^N$

A continuación se definen algunos ejemplos de secuencias CAZAC. En [10, 15, 32] el lector puede encontrar mas detalles del tema.

**Definición 40** (**Secuencia de Fase Cuadrática**). *Una secuencia de fase cuadrática se define como* $u_1 \in \mathbb{C}^N$, *tal que* $u_1[n] = e^{i\pi P(n)/N}$ *donde* $P(n)$ *es un polinomio cuadrático. Algunos ejemplos son*

- *Secuencias Chu* $P(n) = \alpha n(n-1)$, *para* $n \in \mathbb{Z}_N$, *donde* $N$ *es impar y* $\alpha \in \mathbb{U}_N$.
- *Secuencias P4* $P(n) = \alpha n(n-N)$ *y* $\alpha \in \mathbb{U}_N$.

**Definición 41** (**Secuencia de Wiener**). *Sea* $M = N$, *si* $N$ *impar, ó* $M = 2N$, *si* $N$ *es par. Una secuencia de Wiener se define como* $u_2\mathbb{C}^N$ *tal que* $u_2[n] = e^{2i\pi k n^2/M}$, *donde* $k$ *y* $M$ *son primos relativos.*

**Definición 42** (**Secuencia de Björck**). *Sea* $N$ *un número primo tal que* $N = 1 \ mod\ 4$. *Una secuencia de Björck se define como* $u_3\mathbb{C}^N$ *tal que* $u_3[n] = e^{2i\pi\theta\left(\frac{n}{N}\right)}$ *donde*

- $\theta = \arccos\left(\frac{1}{1+\sqrt{N}}\right)$.
- $\left(\frac{n}{P}\right)$ *es el símbolo de Legendre:*

$$\left(\frac{n}{N}\right) = \begin{cases} 0 & si\ m = 0\ mod\ N \\ 1 & si\ m\ es\ un\ cuadrado\ mod\ N \\ -1 & si\ m\ no\ es\ un\ cuadrado\ mod\ N \end{cases}$$

### 5.1.2 Secuencias CAZAC en $\mathbb{C}^{D*N}$

Las secuencias CAZAC mencionadas en la sección anterior son vectores en el espacio $\mathbb{C}^N$ y son utilizadas para cualquiera de los cuatros tipos de DAF, explicado a lo largo de este trabajo.

En [15], J. J. Benedetto y J. J. Donatelli extienden el concepto de secuencias CAZAC al espacio de vectores de arreglos $\mathbb{C}^{D*N}$, mediante el siguiente teorema.

**Teorema 25.** *Sea* $u \in \mathbb{C}^N$ *una secuencia CAZAC y* $D$ *un número entero positivo tal que* $D < N$. *Ahora considere* $\mathbf{u} \in \mathbb{C}^{D*N}$, *tal que:*

$$\mathbf{u}[n] = \frac{1}{\sqrt{D}} \left(u[n], u[\langle n+1 \rangle_N], ..., u[\langle n+D-1 \rangle_N]\right)^T$$

*Entonces* $\mathbf{u}$ *es una secuencia CAZAC en* $\mathbb{C}^{D*N}$ *y, además, un FUNTF con constante de marco* $\frac{N}{D}$.

### 5.1.3 Resultados Numéricos

Una gráfica que represente a la DAF se obtienen a partir del módulo de cada una de las entradas de la matriz DAF. Para elementos en $\mathbb{C}^{D*N}$ se utiliza una norma vectorial en lugar de módulo. En la **Figura 5–1** se presenta un ejemplo de como se realiza la gráfica de la DAF T-0 para secuencia Wiener de longitud $N = 7$ para .

$$A_x^0 = \begin{pmatrix} 7 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1.8+0.86i & 4.5-2.16i & -1.8+0.86i & -1.8+0.86i & -1.8+0.86i & -1.8+0.86i & -1.8+0.86i \\ 1.55+1.94i & -0.8+3.51i & -0.66-2.92i & 2.24+2.81i & 2.24+1.08i & 0.89 & -1.8+0.38i \\ 0.35-1.56i & 0.69+0.86i & 4.49 & -0.62+0.78i & -1-4.38i & -1-0.48i & 1.44-0.69i \\ 0.35+1.56i & -1.6 & -0.24+1.08i & -4.04-1.94i & -0.62+0.78i & 2.8+3.51i & -1+0.48i \\ 1.55-1.94i & 0.55-0.69i & -0.8-0.38i & 0.55-2.43i & 3.60 & -0.66-2.92i & -3.24+1.56i \\ -1.80-0.86i & -0.44-1.94i & 1.24-1.56i & 2 & 1.24+1.56i & -0.44-1.94i & 4.5-2.16i \end{pmatrix}$$

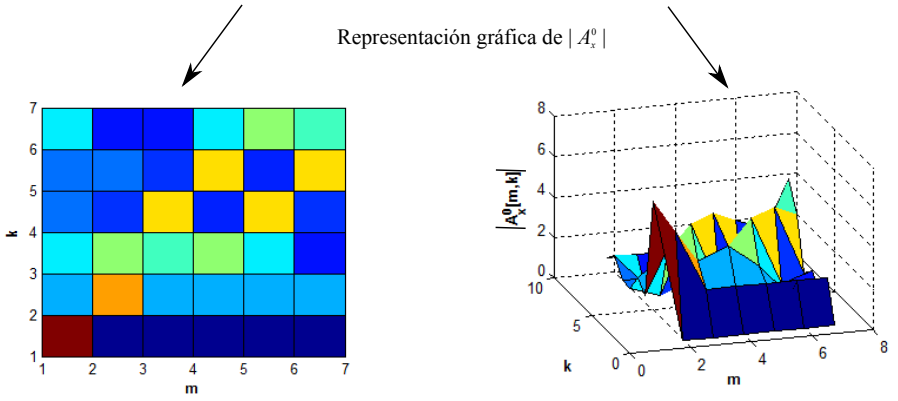


Figura 5–1: Representación matricial y gráfica de DAF T-0 de una secuencia Wiener, donde $N = 7$

A continuación se presentan algunas gráficas de las secuencias CAZAC explicadas anteriormente.

1. La **Figura 5–2** muestra la DAF T-0 de una secuencia Chu, para $N = 153$ y $\alpha = 2$.

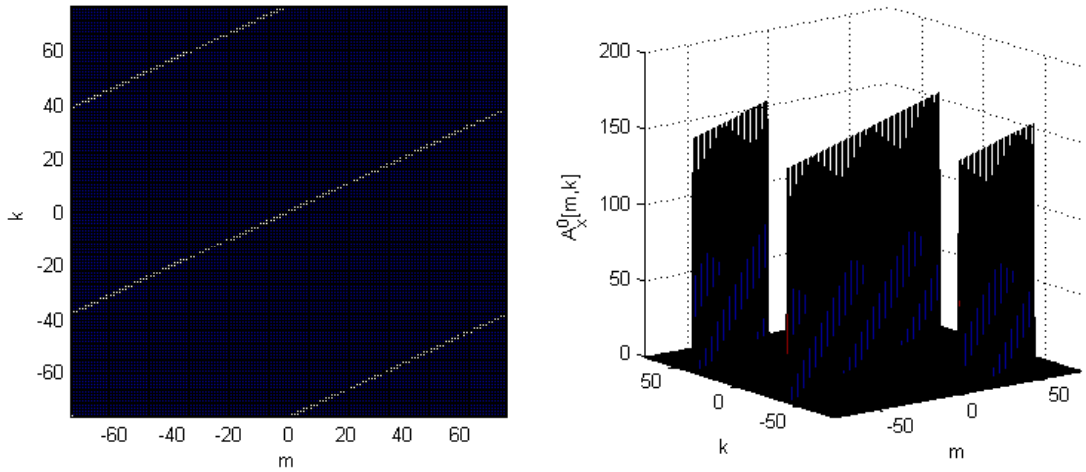


Figura 5–2: DAF T-0 de una secuencia de Chu para $N = 153$ y $\alpha = 2$

2. La **Figura 5–3** muestra la DAF T-0 de una secuencia de Wiener, para $N = 64$.

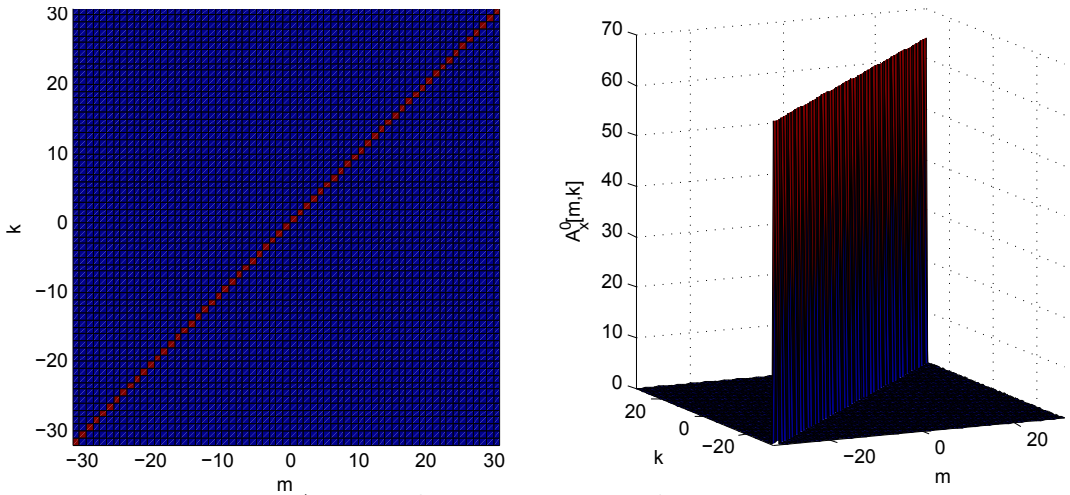


Figura 5–3: DAF T-0 de una secuencia de Wiener para $N = 64$

3. La **Figura 5–4** muestra la DAF T-0 de una secuencia de Björk, para $N = 101$.

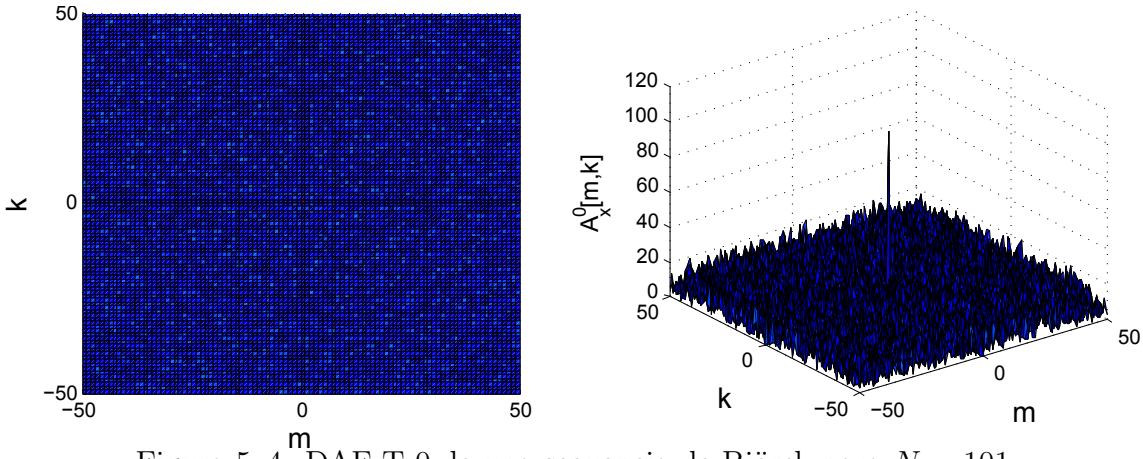


Figura 5–4: DAF T-0 de una secuencia de Björck para $N = 101$

4. La **Figura 5–5** muestra la VV DAF T-0 de una secuencia de Wiener, para $N = 93$ y $D = 45$.

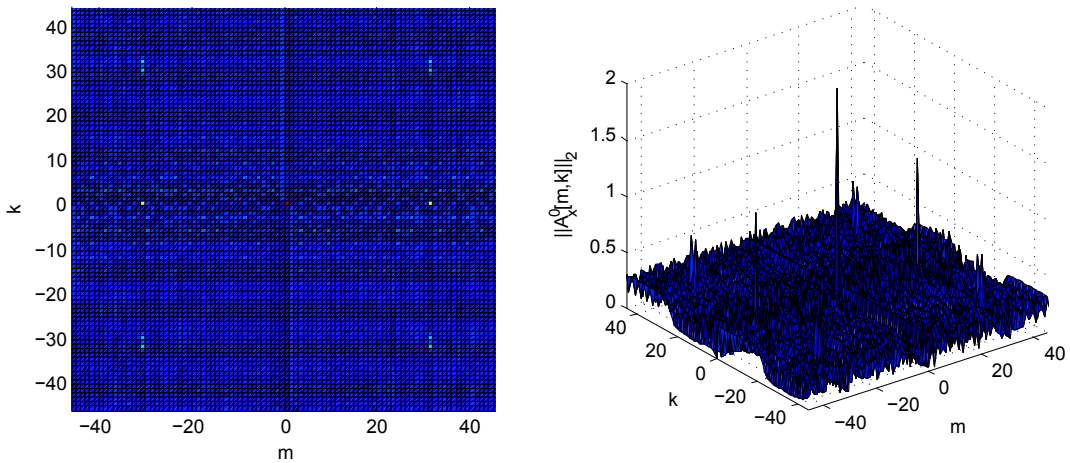


Figura 5–5: VV DAF T-0 de una secuencia Wiener para $N = 93$ y $D = 45$, con norma 2

## 5.2 Función Discreta de Ambigüedad y Criptografía

### 5.2.1 Definición

La palabra criptografía es un término genérico que describe todas las técnicas que permiten cifrar mensajes o hacerlos ininteligibles sin recurrir a una acción específica. En esencia la criptografía trata de enmascarar las representaciones caligráficas de una lengua, de forma discreta.

La criptografía se basa en la aritmética: En el caso de un texto, consiste en transformar las letras que conforman el mensaje en una serie de números y luego realizar cálculos con estos números para:

- modificarlos y hacerlos incomprensibles. El resultado de esta modificación (el mensaje cifrado) se llama texto cifrado, en contraste con el mensaje inicial, llamado texto simple.
- asegurarse de que el receptor pueda descifrarlos. El hecho de codificar un mensaje para que sea secreto se llama cifrado. El método inverso, que consiste en recuperar el mensaje original, se llama descifrado.

El cifrado normalmente se realiza mediante una clave de cifrado y el descifrado requiere una clave de descifrado. Las claves generalmente se dividen en dos tipos

- Las claves simétricas: son las claves que se usan tanto para el cifrado como para el descifrado. En este caso hablamos de cifrado simétrico o cifrado con clave secreta.
- Las claves asimétricas: son las claves que se usan en el caso del cifrado asimétrico (también llamado cifrado con clave pública). En este caso, se usa una clave para el cifrado y otra para el descifrado.

Utilizando la matriz DAF, se puede implementar dos métodos criptográficos de un mensaje numérico, que utilice claves asimétricas, utilizando ya sea una fila o una columna de la matriz DAF. Sin perdida de generalidad, se utiizará la matriz DAF T-0 como referencia.

### 5.2.2 Método para encriptar

Para el proceso de encriptado, se necesitará el siguiente resultado.

**Proposición 8.** *Sea* $x \in \mathbb{C}^N$ *tal que* $x[n] > 0$ *y* $x[n] \neq x[m]$*, para todo* $n, m \in \mathbb{Z}_N$*. Entonces* $\mathcal{F}_x[k] \neq 0$*, para todo* $k \in \mathbb{C}^N$*.*

Sea $\mathbb{Z}_+^N$ el conjunto que representa todos los vectores de orden $N$, tal que los valores en cada entrada es un número entero positivo. Si $x \in \mathbb{Z}_+^N$, entonces $z \in \mathbb{C}^N$,

tal que $z[n] = x[n]e^n$, cumple que $\mathcal{F}_z[k] \neq 0$, para todo $k \in \mathbb{Z}_N$, lo cuál es muy importante para el desarrollo del método de encriptación y recuperación del mensaje.

Sea $y \in \mathbb{C}^N$ el mensaje a encriptar. Primero generamos un vector de orden $N$, cuyos valores de $w$ son enteros positivos. Este vector será parte de la clave privada. Ahora, se necesita generar un vector cuyos elementos de la DFT sean no nulos. Entonces para eso, se construye el vector $z \in \mathbb{C}^N$ tal que $z[n] = w[n]e^n$, $n \in \mathbb{Z}_N$. Por la **Proposición 8**, la construcción de $z$ garantizan que $\mathcal{F}_z[k] \neq 0$, para todo $k \in \mathbb{Z}_N$. Posteriormente, se calcula la matriz DAF T-0 de $z, y$. Luego, se selecciona aleatoriamente un entero $m \in \mathbb{Z}_N$ para escoger la columna o fila $m$ de la matriz DAF T-0, que representará la clave pública. La clave privada sera el vector $x \in \mathbb{C}^{N+1}$ tal que $x[0] = m$ y $x[n] = w[n-1]$, para $n \in \mathbb{U}_{N+1}$.

El **Algoritmo 15** muestra la implementación de lo explicado anteriormente. Dicho algoritmo genera la clave pública y privada del mensaje $y$ a encriptar.

**Algoritmo 15** Encriptación DAF T-0 del vector $y$

**Entrada:** $y \in \mathbb{C}^N$.
**Salida:** $x \in \mathbb{C}^{N+1}$ y $v_m \in \mathbb{C}^N$.

1: $v_0 \leftarrow \text{rand}(\mathbb{Z}_+^N)$
2: $v_2 \leftarrow v_0 \odot v_1$, donde $v_1[n] = e^n$
3: $A \leftarrow A_{z,y}^0$
4: $\alpha \leftarrow \text{rand}(\mathbb{Z}_N)$
5: **si** almacena columna **entonces**
6: $\quad v_m \leftarrow A[:, m]$
7: **si no**, **si** almacena una fila **entonces**
8: $\quad v_m \leftarrow A[m, :]^T$
9: **fin si**
10: $x[0] \leftarrow \alpha$
11: $x[1 : N] \leftarrow w$.

### 5.2.3 Método para recuperar

El proceso de recuperar la señal original, a partir de la clave privada $x \in \mathbb{C}^{N+1}$ y la clave pública $v \in \mathbb{C}^N$ depende de si el vector $x$ representa los valores de la fila o la columna de la matriz DAF T-0.

**Utilizando la fila de la matriz DAF como clave privada**

Sea $x \in \mathbb{C}^{N+1}$ la clave privada y $v \in \mathbb{C}^N$ la clave pública. El proceso de recuperación a partir de una columna de la matriz DAF T-0 es relativamente sencillo, para eso se utiliza el **Teorema 10** desarrollado en la **Seccion 3.2.2** el cuál consiste en recuperar el vector $y$, conociendo el vector $x$ y la fila $m$ de la matriz DAF T-0, que es representada por el vector $a_m$.

El **Algoritmo 16** muestra la implementación de lo explicado anteriormente.

**Algoritmo 16** Inversa DAF T-0

**Entrada:** $x \in \mathbb{C}^{N+1}$ y $v_m \in \mathbb{C}^N$
**Salida:** $y \in \mathbb{C}^N$
1: $v_1 \leftarrow \mathcal{F}^{-1}\{v_m\}$
2: $v_2 \leftarrow x[1:N]$
3: $v_3 \leftarrow v_1 \odot v_2$, donde $v_1[n] = {}^{1}/_{v_2[n]}$
4: $v_4 \leftarrow \mathcal{S}_{-x[0]}\{v_3\}$
5: $y \leftarrow \overline{v_4}$

Este método de encriptación utilizó la DAF T-0. Los otros tipos de DAF tienen una estructura similar, por lo tanto se puede hacer el mismo método criptográfico explicado anteriormente, utilizando la DAF T-1 y T-3, con los datos de la Tabla 3–2, para poder recuperar la señal.

**Utilizando la columna de la matriz DAF como clave privada**

El proceso de recuperar la señal original, a partir de la clave privada $x \in \mathbb{C}^{N+1}$ y la clave pública $v \in \mathbb{C}^N$, se basa en el **Teorema 11** desarrollado en la **Sección 3.2.3**, el cuál consiste en recuperar el vector $y$, conociendo el vector $x$ y la columna $m$ de la matriz DAF T-1, que es representada por el vector $v$.

El **Algoritmo 17** muestra la implementación de lo explicado anteriormente. Dicho algoritmo recupera el mensaje $y$ a partir de las clave pública y privada.

Este método de encriptación utilizó la DAF T-1. Los otros tipos de DAF tienen una estructura similar, por lo tanto se puede hacer el mismo método criptográfico

**Algoritmo 17** Recuperarción del mensaje $y$

**Entrada:** $x \in \mathbb{C}^{N+1}$ (clave privada) y $v \in \mathbb{C}^N$ (clave pública)
**Salida:** $y \in \mathbb{C}^N$

1: $v_0 \leftarrow \overline{v}$
2: $v_1 \leftarrow \mathcal{L}_r\{v_0\}$
3: $z \leftarrow x[1:N]$
4: $v_2 \leftarrow \mathcal{F}_z$
5: $v_3 \leftarrow v_1 \odot v_4$, donde $v_4[n] = {}^{1}\!/\!_{\overline{v_2[n]}}$
6: $v_5 \leftarrow \mathcal{F}^{-1}\{a_4\}$
7: $y \leftarrow v_6 \odot v_5$, donde $v_6[n] = \omega_N^{-n\left(x[0]+\frac{1}{N}\right)}$

explicado anteriormente, utilizando la DAF T-0 y T-3, con los datos de la Tabla 3–3, para poder recuperar la señal.

## 5.3 Matrices Circulantes en $\mathbb{C}^{D*(N\times N)}$

Esta sección explica el concepto de matrices de arreglos de circulantes para el espacio $\mathbb{C}^{D*(N\times N)}$, basados en el trabajo de P. J. Davis para el espacio $\mathbb{C}^{N\times N}$ [30].

### 5.3.1 Definición

**Definición 43** (**Matriz de Arreglos Circulante**). *Sea* $\mathbf{v} \in \mathbb{C}^{D*N}$, $\mathbf{v} = (\mathbf{v}_0, \mathbf{v}_1, ..., \mathbf{v}_{N-1})^T$. *Una matriz de arreglos* $\mathbf{C}_\mathbf{v} \in \mathbb{C}^{D*(N\times N)}$ *se llama circulante con respecto a* $\mathbf{v}$, *si la fila* $m$ *de* $\mathbf{C}_\mathbf{v}$ *se representa como* $\mathscr{S}_m\{\mathbf{v}\}$, *para* $m \in \mathbb{Z}_N$, *es decir*

$$\mathbf{C}_\mathbf{x} = \begin{pmatrix} \mathbf{v}_0 & \mathbf{v}_1 & \cdots & \mathbf{v}_{N-1} \\ \mathbf{v}_{N-1} & \mathbf{v}_0 & \cdots & \mathbf{v}_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{v}_1 & \mathbf{v}_2 & \cdots & \mathbf{v}_0 \end{pmatrix} \tag{5.1}$$

Cada entrada de una matriz de arreglos circulante es un elemento de $\mathbf{v}$, y $(\mathbf{C}_\mathbf{v})_{mn} = \mathbf{v}[\langle n-m\rangle_N]$. Como se explicó en la **Sección 4.1**, cuando $D = 1$, entonces $\mathbb{C}^{D*N\times N} = \mathbb{C}^{N\times N}$. Por lo tanto, para el caso $D = 1$, $\mathbf{C}_\mathbf{v}$ representa una matriz circulante en $\mathbb{C}^{N\times N}$, como se desarrolló en la **Sección** 2.4. El **Teorema 26**

muestra una factorización de una matriz de arreglos circulante utilizando la matriz VV DFT, utilizando los resultados ya desarrollados para la matriz VV DFT.

**Teorema 26.** *Sea* $\mathbf{v} \in \mathbb{C}^{D*N}$*, donde* $N$ *es un número primo, ó* $N$ *es un número compuesto tal que* $D < r$*, donde* $r$ *es el menor primo de la factorización de* $N$*. Entonces la matriz de arreglos circulante con respecto a* $\mathbf{v}$*,* $\mathbf{C_v} \in \mathbb{C}^{D*(N\times N)}$*, presenta la siguiente factorización*

$$\mathbf{C_v} = \frac{D\sqrt{D}}{N}\mathbf{F}_N\mathbf{M}\overline{\mathbf{F}_N}$$

*donde* $\mathbf{M} \in \mathbb{C}^{D*(N\times N)}$ *es una matriz de arreglos diagonal tal que*

$$\mathbf{M} = diag(\mathscr{F}_{\mathbf{v}}[0], \mathscr{F}_{\mathbf{v}}[1], ..., \mathscr{F}_{\mathbf{v}}[N-1])$$

**Prueba.** *Sea* $\mathbf{H} = \mathbf{M}\overline{\mathbf{F}_N}$*, entonces para* $i, j \in \mathbb{Z}_N$

$$\mathbf{H}_{i,j} = \sum_{n\in\mathbb{Z}_N} \mathbf{M}_{in} \odot (\overline{\mathbf{F}_N})_{nj} = \frac{1}{\sqrt{D}}\mathscr{F}_{\mathbf{v}}[i] \odot e_N^{ij} = \frac{1}{D}\sum_{k\in\mathbb{Z}_N} \mathbf{v}[n] \odot e_N^{i(j-k)}$$

*Ahora, considere la multiplicación* $\mathbf{F}_N\mathbf{H}$*, entonces para* $i, j \in \mathbb{Z}_N$

$$\begin{aligned}(\mathbf{F}_N\mathbf{H})_{i,j} &= \sum_{n\in\mathbb{Z}_N} (\mathbf{F}_N)_{in} \odot (\mathbf{H})_{nj} \\ &= \tfrac{1}{D\sqrt{D}} \sum_{k\in\mathbb{Z}_N} \mathbf{v}[n] \odot \sum_{n\in\mathbb{Z}_N} e_N^{(j-i-k)n} \\ &= \tfrac{N}{D\sqrt{D}}\mathbf{v}[\langle j-i\rangle_N]\end{aligned}$$

*Entonces,* $\frac{D\sqrt{D}}{N}(\mathbf{F}_N\mathbf{M}\overline{\mathbf{F}_N})_{i,j} = \mathbf{x}[\langle j-i\rangle_N]$*, lo cuál indica la entrada de la matriz de arreglos circurlante* $\mathbf{C_v}$*.*

■

Ahora, si $\mathbf{B}$ es una matriz de arreglos diagonal, entonces su conjunto generador $\{B_d\}$ está formado por matrices diagonales. Sabiendo por una matriz diagonal tiene inversa si los elementos de la diagonal son no nulos, entonces $\mathbf{B}$ *posee inversa si ninguna de las matrices de su conjunto generador posee elementos nulos en su*

*diagonal*. Lo explicado anteriormente, y

$$\mathbf{F}_N\overline{\mathbf{F}_N} = \overline{\mathbf{F}_N}\mathbf{F}_N = \frac{D}{N}\mathbf{I}_N$$

prueban el siguiente lema, el cuál explica una factorización de la inversa de una matriz de arreglos circulante, bajo las hipótesis del **Teorema 26**.

**Lema 7.** *Sea* $\mathbf{v} \in \mathbb{C}^{D*N}$*, tal que* $\mathscr{F}_{\mathbf{v}}[n]$ *no posee entradas nulas, para* $n \in \mathbb{Z}_N$*, para* $N$ *primo, ó* $N$ *compuesto tal que* $D < r$*, donde* $r$ *es el menor primo de la factorización de* $N$*. Entonces existe la matriz de arreglos inversa de* $\mathbf{C}_{\mathbf{v}}$*, y se puede factorizar como*

$$\mathbf{C}_{\mathbf{v}} = \frac{\sqrt{D}}{N}\mathbf{F}_N\mathbf{B}\overline{\mathbf{F}_N}$$

*donde* $\mathbf{B} \in \mathbb{C}^{D*(N\times N)}$ *es una matriz de arreglos diagonal tal que*

$$\mathbf{B} = diag\left(\mathbf{1}_D \oslash \mathscr{F}_{\mathbf{v}}[0], \mathbf{1}_D \oslash \mathscr{F}_{\mathbf{v}}[1], ..., \mathbf{1}_D \oslash \mathscr{F}_{\mathbf{v}}[N-1]\right),$$

*donde* $\oslash$ *representa la división puntual.*

El conjunto generador de una matriz de arreglos circulante está formada por matrices circulantes. Sea $\{C_{v_d}\}$ es el conjunto generador de la matriz de arreglos circulante $\mathbf{C}_v$, donde $C_{v_d}$ representa la matriz circulante del vector $v_d$, para todo $d \in \mathbb{Z}_D$. Por **Lemma 2** y **Teorema 15**, la matriz de arreglos circulante tiene inversa si $\mathcal{F}_{v_d}[n] \neq 0$, para todo $d \in \mathbb{Z}_D$ y $n \in \mathbb{Z}_N$. Entonces, si $G_d = diag(1/\mathcal{F}_{v_d}[0], ..., 1/\mathcal{F}_{v_d}[N-1])$, para $d \in \mathbb{Z}_D$, entonces

$$\begin{aligned}\mathbf{C}_v &= \bigvee_{d\in\mathbb{Z}_D} C_{v_d} \\ &= \bigvee_{d\in\mathbb{Z}_D} \frac{1}{N} F_N G_d \overline{F_N} \\ &= \mathbf{PGQ}\end{aligned}$$

donde

- $\mathbf{P} = \bigvee_{d\in\mathbb{Z}_D} F_N$
- $\mathbf{G} = \bigvee_{d\in\mathbb{Z}_D} G_d$
- $\mathbf{Q} = \bigvee_{d\in\mathbb{Z}_D} \frac{1}{N}\overline{F_N}$

### 5.3.2 Matrices de Arreglos de Circulantes por Bloques

**Definición 44** (**Matriz de Arreglos Circulante por bloques**). *Sea* $\{\mathbf{A}_m\}_{m\in\mathbb{Z}_M}$ *tal que* $\mathbf{A}_m \in \mathbb{C}^{D*(N\times N)}$. *Una matriz de arreglos circulante por bloques (del inglés,* **block circulant***), es una matriz de arreglos* $\mathbf{BC}_{\{\mathbf{A}_m\}} \in \mathbb{C}^{D*(MN\times MN)}$ *tal que*

$$\mathbf{BC}_{\{\mathbf{A}_m\}} = \begin{pmatrix} \mathbf{A}_0 & \mathbf{A}_1 & \cdots & \mathbf{A}_{N-1} \\ \mathbf{A}_{N-1} & \mathbf{A}_0 & \cdots & \mathbf{A}_{N-2} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_1 & \mathbf{A}_2 & \cdots & \mathbf{A}_0 \end{pmatrix} \tag{5.2}$$

El espacio de las matrices de arreglos circulantes por bloques en $\mathbb{C}^{D*(MN\times MN)}$ se designa como $\mathbb{BC}^{D(M,N)}$. Si $N = 1$, entonces se obtiene una matriz de arreglos circulante. Una observación importante es que una matriz circulante por bloques no necesariamente tiene que ser una matriz circulante.

Una matrices de arreglos circulantes por bloques tiene una relación con el producto de Kronecker, bajo la siguiente igualdad

$$\mathbf{BC}_{\{\mathbf{A}_m\}} = \sum_{m\in\mathbb{Z}_M} \mathbf{S}_{M-m-1} \boxtimes \mathbf{A}_m \tag{5.3}$$

donde $\mathbf{S}_{N-m-1} \in \mathbb{C}^{D*(M\times M)}$ es la matriz de arreglos que representa al operador de traslación $\mathscr{S}_{M-m-1}$.

**Teorema 27.** *Sea* $\{\mathbf{A}_m\}_{m\in\mathbb{Z}_M}$ *tal que* $\mathbf{A}_m \in \mathbb{C}^{D*(N\times N)}$, *para* $N$ *primo ó* $N$ *compuesto que satisface* $D < r$, *donde* $r$ *es el menor primo de la factorización de* $N$. *Entonces*

$$\mathbf{BC}_{\{\mathbf{A}_m\}} = \frac{1}{MN}(\mathbf{F}_M \boxtimes \mathbf{F}_N)\mathbf{B}(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N}) \tag{5.4}$$

*donde* $\mathbf{B} \in \mathbb{C}^{D*(MN\times MN)}$ *es una matriz de arreglos diagonal por bloques.*

**Prueba.** *Utilizando la ecuación (5.3) se obtiene*

$$\mathbf{BC}_{\{\mathbf{A}_m\}} = \sum_{m\in\mathbb{Z}_M} \mathbf{S}_{M-m-1} \boxtimes \mathbf{A}_m$$

*Ahora considere:*

- $\mathbf{S}_{M-m-1}$ *es una matriz de arreglos circulante tal que* $\mathbf{S}_{N-m-1} = \mathbf{C}_{\mathbf{w}_{M-m-1}}$, *donde* $\mathbf{w}_{M-m-1} = \mathscr{S}_{M-m-1}\{(\mathbf{1}_D, \mathbf{0}_D, ..., \mathbf{0}_D)^T\}$. *Por lo tanto,*

$$\mathbf{S}_{M-m-1} = \frac{D\sqrt{D}}{M}\mathbf{F}_M\mathbf{Q}_{M-m-1}\overline{\mathbf{F}_M},$$

*donde* $\mathbf{Q}_{M-m-1} \in \mathbb{C}^{D*(M\times M)}$ *tal que* $(\mathbf{Q}_{M-m-1})_{k,k} = \mathscr{F}_{\mathbf{w}_{M-m-1}}[k]$, *para* $k \in \mathbb{Z}_M$.

- *Para cada* $\mathbf{A}_m$, *se cumple,*

$$\mathbf{A}_m = \frac{N^2}{D^2}\mathbf{F}_N(\overline{\mathbf{F}_N}\mathbf{A}_m\mathbf{F}_N)\overline{\mathbf{F}_N}.$$

*Sea* $\mathbf{E}_m = \overline{\mathbf{F}_N}\mathbf{A}_m\mathbf{F}_N$

*Entonces, utilizando propiedades del producto Kronecker de matrices de arreglos se cumple*

$$\begin{aligned}
\mathbf{BC}_{\{\mathbf{A}_m\}} &= \sum_{m\in\mathbb{Z}_M} \mathbf{S}_{M-m-1} \boxtimes \mathbf{A}_m \\
&= \sum_{m\in\mathbb{Z}_M} \left(\tfrac{D\sqrt{D}}{M}\mathbf{F}_M\mathbf{Q}_{N-m-1}\overline{\mathbf{F}_M}\right) \boxtimes \left(\tfrac{N^2}{D^2}\mathbf{F}_N\mathbf{E}_m\overline{\mathbf{F}_N}\right) \\
&= \tfrac{N^2}{M\sqrt{D}} \sum_{m\in\mathbb{Z}_M} (\mathbf{F}_M \boxtimes \mathbf{F}_N)\,(\mathbf{Q}_{M-m-1} \boxtimes \mathbf{E}_m)\,\left(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N}\right) \\
&= \tfrac{N^2}{M\sqrt{D}}\,(\mathbf{F}_M \boxtimes \mathbf{F}_N) \left[\sum_{m\in\mathbb{Z}_M} \mathbf{Q}_{M-m-1} \boxtimes \mathbf{E}_m\right] \left(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N}\right)
\end{aligned}$$

*Ahora,* $\mathbf{Q}_{M-m-1}$ *es una matriz de arreglos diagonal, entonces* $\mathbf{Q}_{N-m-1} \boxtimes \mathbf{E}_m$ *es una matriz de arreglos diagonal por bloques. Además, la suma finita de matrices diagonal por bloques, cuyos bloques son del mismo tamaño, es otra matriz diagonal por bloques. Entonces* $\mathbf{B} = \sum_{m\in\mathbb{Z}_M} \mathbf{Q}_{N-m-1} \boxtimes \mathbf{A}_m$ *es una matriz diagonal por bloques.*

*Por lo tanto,*

$$\mathbf{BC}_{\{\mathbf{A}_m\}} = \frac{1}{MN}(\mathbf{F}_M \boxtimes \mathbf{F}_N)\mathbf{B}(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N})$$

*donde $B$ es una matriz de arreglos diagonal por bloques.*

■

### 5.3.3 Matrices de Arreglos de Bloques Circulantes

**Definición 45 (Matriz de Arreglos de Bloques Circulantes).** *Una matriz de arreglos de bloques circulantes (del inglés,* **circulant blocks***) es una matriz de arreglos* $\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} \in \mathbb{C}^{D*(MN\times MN)}$ *tal que*

$$\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} = \begin{pmatrix} \mathbf{C}_{\mathbf{v}_{0,0}} & \mathbf{C}_{\mathbf{v}_{0,1}} & \cdots & \mathbf{C}_{\mathbf{v}_{0,M-1}} \\ \mathbf{C}_{\mathbf{v}_{1,0}} & \mathbf{C}_{\mathbf{v}_{1,1}} & \cdots & \mathbf{C}_{\mathbf{v}_{1,M-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{C}_{\mathbf{v}_{M-1,0}} & \mathbf{C}_{\mathbf{v}_{M-1,1}} & \cdots & \mathbf{C}_{\mathbf{v}_{M-1,M-1}} \end{pmatrix} \tag{5.5}$$

*donde* $\mathbf{C}_{\mathbf{v}_{i,j}} \in \mathbb{C}^{D*(N\times N)}$ *es una matriz de arreglos circulante respecto a* $\mathbf{v}_{i,j} \in \mathbb{C}^{D*N}$*, para* $i, j \in \mathbb{Z}_M$*.*

Una matriz de arreglos de bloques circulantes se puede expresar utilizando productos de Kronecker:

- Si $\mathbf{A}_m \in \mathbb{C}^{D*(M\times M)}$, tal que $(\mathbf{A}_m)_{i,j} = \mathbf{v}_{i,j}[k]$, para $i, j \in \mathbb{Z}_M$ y $k \in \mathbb{Z}_N$, entonces

$$\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} = \sum_{m\in\mathbb{Z}_M} \mathbf{A}_m \boxtimes \mathbf{S}_{N-m-1} \tag{5.6}$$

- Si $N$ es primo ó $N$ es compuesto que satisface $D < r$, donde $r$ es el menor primo de la factorización de $N$, entonces como $\mathbf{C}_{\mathbf{v}_{i,j}}$ es una matriz de arreglos circulante, $\mathbf{C}_{\mathbf{v}_{i,j}} = \frac{D\sqrt{D}}{N}\mathbf{F}_N\mathbf{G}_{\mathbf{v}_{i,j}}\overline{\mathbf{F}_N}$, donde $\mathbf{G}_{\mathbf{v}_{i,j}}$ es una matriz diagonal que

contiene los valores de la VV DFT de $\mathbf{v}_{i,j}$. Por lo tanto:

$$\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} = \frac{D\sqrt{D}}{N}\begin{pmatrix} \mathbf{F}_N\mathbf{G}_{\mathbf{v}_{0,0}}\overline{\mathbf{F}_N} & \cdots & \mathbf{F}_N\mathbf{G}_{\mathbf{v}_{0,M-1}}\overline{\mathbf{F}_N} \\ \vdots & \ddots & \vdots \\ \mathbf{F}_N\mathbf{G}_{\mathbf{v}_{M-1,0}}\overline{\mathbf{F}_N} & \cdots & \mathbf{F}_N\mathbf{G}_{\mathbf{v}_{M-1,M-1}}\overline{\mathbf{F}_N} \end{pmatrix}$$

$$= \frac{D\sqrt{D}}{N}(\mathbf{I}_M \boxtimes \mathbf{F}_N)\underbrace{\begin{pmatrix} \mathbf{G}_{\mathbf{v}_{0,0}} & \cdots & \mathbf{G}_{\mathbf{v}_{0,M-1}} \\ \vdots & \ddots & \vdots \\ \mathbf{G}_{\mathbf{v}_{M-1,0}} & \cdots & \mathbf{G}_{\mathbf{v}_{M-1,M-1}} \end{pmatrix}}_{\mathbf{G}}(\mathbf{I}_M \boxtimes \overline{\mathbf{F}_N})$$

Por lo tanto,

$$\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} = \frac{D\sqrt{D}}{N}(\mathbf{I}_M \boxtimes \mathbf{F}_N)\mathbf{G}(\mathbf{I}_M \boxtimes \overline{\mathbf{F}_N}) \tag{5.7}$$

donde $\mathbf{G}$ es una matriz de arreglos por bloques, cuyos bloques son matrices diagonales.

**Teorema 28.** *Sea* $\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}}$ *un conjunto de matrices de arreglos de bloques circulantes, tal que* $\mathbf{C}_{\mathbf{v}_{i,j}} \in \mathbb{C}^{D*(N\times N)}$*, para* $N$ *primo ó* $N$ *compuesto que satisface* $D < r$*, donde* $r$ *es el menor primo de la factorización de* $N$*. Entonces*

$$\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} = \frac{M}{\sqrt{D}}(\mathbf{F}_M \boxtimes \mathbf{F}_N)\mathbf{B}(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N}) \tag{5.8}$$

*donde* $\mathbf{B} \in \mathbb{C}^{D*(MN\times MN)}$ *es una matriz de arreglos por bloques, cuyos bloques son matrices diagonales.*

**Prueba.** *De la ecuación (5.7) se obtiene*

$$\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} = \frac{D\sqrt{D}}{N}(\mathbf{I}_M \boxtimes \mathbf{F}_N)\mathbf{G}(\mathbf{I}_M \boxtimes \overline{\mathbf{F}_N})$$

*Propiedades del producto Kronecker de matrices de arreglos, se obtiene*

- $\mathbf{I}_M \boxtimes \mathbf{F}_N = \frac{N}{D}(\mathbf{F}_M \boxtimes \mathbf{F}_N)(\overline{\mathbf{F}_M} \boxtimes \mathbf{I}_N)$
- $\mathbf{I}_M \boxtimes \overline{\mathbf{F}_N} = \frac{M}{D}(\mathbf{F}_M \boxtimes \mathbf{I}_N)(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N})$

*Por lo tanto*

$$\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} = \frac{M}{\sqrt{D}}(\mathbf{F}_M \boxtimes \mathbf{F}_N)(\overline{\mathbf{F}_M} \boxtimes \mathbf{I}_N)\mathbf{G}(\mathbf{F}_M \boxtimes \mathbf{I}_N)(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N})$$

*Como* $\overline{\mathbf{F}_M} \boxtimes \mathbf{I}_N$, $\mathbf{G}$ *y* $\mathbf{F}_M \boxtimes \mathbf{I}_N$ *son matrices de arreglos por bloques, cuyos bloques son matrices de arreglos diagonales y del mismo tamaño, entonces* $(\overline{\mathbf{F}_M} \boxtimes \mathbf{I}_N)\mathbf{G}(\mathbf{F}_M \boxtimes \mathbf{I}_N)$ *es también una matriz de arreglos por bloques, y cada bloque es una matriz de arreglos diagonal. Sea*

$$\mathbf{B} = (\overline{\mathbf{F}_M} \boxtimes \mathbf{I}_N)\mathbf{G}(\mathbf{F}_M \boxtimes \mathbf{I}_N).$$

*Por lo tanto*

$$\mathbf{CB}_{\{\mathbf{C}_{\mathbf{v}_{i,j}}\}} = \frac{M}{\sqrt{D}}(\mathbf{F}_M \boxtimes \mathbf{F}_N)\mathbf{B}(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N})$$

*donde* $\mathbf{B} \in \mathbb{C}^{D*(MN\times MN)}$ *es una matriz de arreglos por bloques, cuyos bloques son matrices diagonales.*

■

### 5.3.4 Matrices de Arreglos Circulante por Bloques con Bloques Circulantes

**Definición 46** (Matriz de Arreglos Circulante por Bloques de Bloques Circulantes)**.** *Sea* $\{\mathbf{C}_{\mathbf{v}_m}\}_{m\in\mathbb{Z}_M}$ *tal que* $\mathbf{C}_{\mathbf{v}_m} \in \mathbb{C}^{D*(N\times N)}$ *es un conjunto de matrices de arreglos circulantes con respecto a* $\mathbf{v}_m \in \mathbb{C}^{D*N}$*. Una matriz de arreglos circulante por bloques de bloques circulantes (del inglés,* **block circulant of circulant blocks***), es una matriz de arreglos* $\mathbf{BCCB}_{\{\mathbf{C}_{v_m}\}} \in \mathbb{C}^{D*(MN\times MN)}$ *tal que*

$$\mathbf{BCCB}_{\{\mathbf{C}_{\mathbf{v}_m}\}} = \begin{pmatrix} \mathbf{C}_{\mathbf{v}_0} & \mathbf{C}_{\mathbf{v}_1} & \cdots & \mathbf{C}_{\mathbf{v}_{N-1}} \\ \mathbf{C}_{\mathbf{v}_{N-1}} & \mathbf{C}_{\mathbf{v}_0} & \cdots & \mathbf{C}_{\mathbf{v}_{N-2}} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{C}_{\mathbf{v}_1} & \mathbf{C}_{\mathbf{v}_2} & \cdots & \mathbf{C}_{\mathbf{v}_0} \end{pmatrix} \tag{5.9}$$

**Teorema 29.** *Sea* $\{\mathbf{C}_{\mathbf{v}_m}\}_{m\in\mathbb{Z}_M}$ *tal que* $\mathbf{C}_{\mathbf{v}_m} \in \mathbb{C}^{D*(N\times N)}$ *es un conjunto de matrices de arreglos circulantes con respecto a* $\mathbf{v}_m \in \mathbb{C}^{D*N}$*, para* $N$ *primo, ó* $N$ *compuesto tal que* $D < r$*, donde* $r$ *es el menor primo de la factorización de* $N$*. Entonces*

$$\mathbf{BCCB}_{\{\mathbf{C}_{\mathbf{v}_m}\}} = \frac{D^3}{MN}\left(\mathbf{F}_M \boxtimes \mathbf{F}_N\right)\mathbf{B}\left(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N}\right)$$

*donde* $\mathbf{B} \in \mathbb{C}^{D*(MN\times MN)}$ *es una matriz de arreglos diagonal.*

**Prueba.** *Como es una matriz circulante por bloques, entonces, por la ecuación (5.3), se obtiene*

$$\sum_{m\in\mathbb{Z}_M} \mathbf{S}_{M-m-1} \boxtimes \mathbf{C}_{\mathbf{v}_m}$$

*Ahora considere*

- *Del* **Teorema 27** *se obtiene que*

$$\mathbf{S}_{M-m-1} = \frac{D\sqrt{D}}{M}\mathbf{F}_M\mathbf{Q}_{M-m-1}\overline{\mathbf{F}_M},$$

*donde* $\mathbf{Q}_{M-m-1} \in \mathbb{C}^{D*(M\times M)}$ *es una matriz de arreglos diagonal.*

- *Como* $\mathbf{C}_{\mathbf{v}_m}$ *es una matriz de arreglos circulante, del* **Teorema 26** *se obtiene*

$$\mathbf{C}_{\mathbf{v}_m} = \frac{D\sqrt{D}}{N}\mathbf{F}_N\mathbf{G}_{\mathbf{v}_m}\overline{\mathbf{F}_N},$$

*donde* $\mathbf{G}_{\mathbf{v}_m} \in \mathbb{C}^{D*(N\times N)}$ *es una matriz de arreglos diagonal.*

*Por lo tanto*

$$\begin{aligned}
\mathbf{BCCB}_{\{\mathbf{C}_m\}} &= \sum_{m\in\mathbb{Z}_M} \mathbf{S}_{M-m-1} \boxtimes \mathbf{C}_{\mathbf{v}_m} \\
&= \sum_{m\in\mathbb{Z}_M} \left(\frac{D\sqrt{D}}{M}\mathbf{F}_M\mathbf{Q}_k\overline{\mathbf{F}_M}\right) \boxtimes \left(\frac{D\sqrt{D}}{N}\mathbf{F}_N\mathbf{G}_m\overline{\mathbf{F}_N}\right) \\
&= \frac{D^3}{MN}\sum_{m\in\mathbb{Z}_M} \left(\mathbf{F}_M \boxtimes \mathbf{F}_N\right)\left(\mathbf{Q}_{M-m-1} \boxtimes \mathbf{G}_m\right)\left(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N}\right) \\
&= \frac{D^3}{MN}\left(\mathbf{F}_M \boxtimes \mathbf{F}_N\right)\underbrace{\left[\sum_{m\in\mathbb{Z}_M} \mathbf{Q}_{M-m-1} \boxtimes \mathbf{G}_m\right]}_{\mathbf{B}}\left(\overline{\mathbf{F}_M} \boxtimes \overline{\mathbf{F}_N}\right)
\end{aligned}$$

*donde* $\mathbf{B} \in \mathbb{C}^{D*(MN\times MN)}$. *Como* $\mathbf{Q}_{M-m-1}$ *y* $\mathbf{G}_m$ *son matricies de arreglos diagonales, entonces* $\mathbf{Q}_{M-m-1} \boxtimes \mathbf{G}_m$ *tambien es una matriz de arreglos diagonal por bloques. Además, la suma finita de matrices de arreglos diagonales es una matriz de arreglos diagonales. Por lo tanto,* $\mathbf{B}$ *es una matriz de arreglos diagonal.*

# CAPÍTULO 6
# CONCLUSIONES Y TRABAJOS FUTUROS

En general, en esta tesis se desarrolló un marco computacional de las representaciones en tiempo y frecuencias las cuales fueron desarrolladas a partir la función discreta de ambigüedad. En detalle, se obtuvieron las siguientes conclusiones:

1. Se trabajó con 4 definiciones equivalentes en módulo de la función discreta de ambigüedad (DAF).
2. Se formuló y se demostró una representación matricial de los 4 tipos de DAF, que permite su implementación en paralelo.
3. Se desarrolló y se demostró un método para calcular la inversa de la DAF.
4. Se trabajó con la transformada discreta de Fourier de valores vectoriales, un caso particular de la DAF-T0. Además se formuló una representación matricial que permite su cómputo en paralelo.
5. Se trabajó con la transformada discreta de Zak (DZT), un caso particular de la DAF-T1 y se formuló una representación matricial. Además se obtienen nuevos resultados para la DZT, con sus respectivas demostraciones.
6. Se trabajó con la distribución discreta de Cohen (DCD), la cuál utiliza la DAF-T2 para su formulación. Se define y se demuestra una representación matricial para la DCD.
7. Se definió el concepto de matrices de arreglos, el cual representan matrices cuyas entradas son vectores. Se obtienen nuevos resultados y cada resultado tiene su respectiva demostración.

8. Se trabajo con la transformada discreta de Fourier de valores vectoriales (VV DFT) definida por J. J. Benedetto y J. J. Donatelli [16], y se desarrolla una modificación, utilizando un nuevo concepto propuesto en este trabajo, denominado vectores complejos armónicos. Además se obtienen nuevos resultados para la VV DFT, con sus respectivas demostraciones.
9. Se trabajó con 4 definiciones, equivalentes en norma $p$, de la función discreta de ambigüedad de valores vectoriales (VV DAF), para $p \in \mathbb{Z}^+$ y $p = \infty$. Se obtienen nuevos resultados para la VV DFT, con sus respectivas demostraciones.
10. Se utilizó el concepto de matrices de arreglos para trabajar una representación matricial de la VV DFT y VV DAF. Se obtuvieron nuevos resultados, con sus respectivas demostraciones.
11. Para la VV DAF, se extiendió el trabajo de L. Auslander y R. Tolimieri [46**?** ]:
    - Utilizando la VV DAF T-0, VV DAF T-1 y VV DAF T-3, se relacionó cada VV DAF con el grupo de Heisenberg.
    - Se desarrolló un proceso de decimación para VV DAF T-3, sobre el conjunto $\mathbb{Z}_{N^2} \times \mathbb{Z}_{N^2}$, para $N$ primo.
12. Se desarrolló un nuevo método criptográfico utilizando la DAF T-0, DAF T-1 y DAF T-3.
13. Se extendió el trabajo de P. J. Davies [30], para el caso de matrices de arreglos circulantes.

Durante el desarrollo de este trabajo, se ha identificado varios tópicos que se presentan como posibles trabajos a desarrollar en el futuro. Como primer tópico se considera la generalización del concepto de matrices de arreglos donde una entrada arbitraria de esa matriz se pueda definir como un tensor generalizado de datos. En ese caso se necesita demostrar que el conjunto de matrices de arreglos mantiene la estructura de un álgebra asociativa. Como segundo tópico se desea incursionar en el estudio del espacio de caracteres y su interacción con funciones bidimensionales para

soluciones criptográficas. Como tercer tópico de investigación futura se desea extender la lista de funciones multidimensionales que admiten una representación discreta. Como cuarto tópico se desea estudiar la relación entre la función de ambigüedad de valores vectoriales y representaciones armónicas multidimensionales, en particular la transformada fraccional de Fourier y la transformada chirp-Fourier. Como quinto y último tópico de trabajo futuro, se desea abordar el estudio de matrices de arreglos sobre grupos finitos.

REFERENCIAS BIBLIOGRÁFICAS


[1] H.-I. Choi and W.J. Williams. Improved time-frequency representation of multicomponent signals using exponential kernels. *Acoustics, Speech and Signal Processing, IEEE Transactions on*, 37(6):862 –871, June 1989.

[2] F. Hlawatsch and G.F. Boudreaux-Bartels. Linear and quadratic time-frequency signal representations. *Signal Processing Magazine, IEEE*, 9(2):21 –67, April 1992.

[3] Dongsheng Wu and J.M. Morris. Discrete cohen's class of distributions. In *Time-Frequency and Time-Scale Analysis, 1994., Proceedings of the IEEE-SP International Symposium on*, pages 532 –535, oct 1994.

[4] J.R. O'Hair and B.W. Suter. The zak transform and decimated time-frequency distributions. *Signal Processing, IEEE Transactions on*, 44(5):1099 –1110, May 1996.

[5] Leon Cohen. Generalized Phase-Space Distribution Functions. *Journal of Mathematical Physics*, 7(5):781–786, 1966.

[6] P.J. Loughlin and K.L. Davidson. Modified cohen-lee time-frequency distributions and instantaneous bandwidth of multicomponent signals. *Signal Processing, IEEE Transactions on*, 49(6):1153 –1165, jun 2001.

[7] James W. Cooley and John W. Tukey. An Algorithm for the Machine Calculation of Complex Fourier Series. *Mathematics of Computation*, 19(90):297–301, 1965.

[8] E. Wigner. On the Quantum Correction For Thermodynamic Equilibrium. *Physical Review Online Archive (Prola)*, 40(5):749–759, June 1932.

[9] G. San Antonio, D.R. Fuhrmann, and F.C. Robey. Mimo radar ambiguity functions. *Selected Topics in Signal Processing, IEEE Journal of*, 1(1):167 – 177, june 2007.

[10] A. Kebo, I. Konstantinidis, J.J. Benedetto, M.R. Dellomo, and J.M. Sieracki. Ambiguity and sidelobe behavior of cazac coded waveforms. In *Radar Conference, 2007 IEEE*, pages 99 –103, april 2007.

[11] L. Auslander and R. Tolimieri. Computing decimated finite cross-ambiguity functions. *Acoustics, Speech and Signal Processing, IEEE Transactions on*, 36(3):359 –364, mar 1988.

[12] M.S. Richman, T.W. Parks, and R.G. Shenoy. Discrete-time, discrete-frequency, time-frequency analysis. *Signal Processing, IEEE Transactions on*, 46(6):1517 –1527, June 1998.

[13] R. Tolimieri and S. Winograd. Computing the ambiguity surface. *Acoustics, Speech and Signal Processing, IEEE Transactions on*, 33(5):1239 – 1245, oct 1985.

[14] Richard Tolimieri, Myoung An, and Chao Lu. *Algorithms for Discrete Fourier Transform and Convolution (Signal Processing and Digital Filtering)*. Springer, oct 1997.

[15] J.J. Benedetto and J.J. Donatelli. Ambiguity function and frame-theoretic properties of periodic zero-autocorrelation waveforms. *Selected Topics in Signal Processing, IEEE Journal of*, 1(1):6 –20, june 2007.

[16] J.J. Benedetto and J.J. Donatelli. Frames and a vector-valued ambiguity function. In *Signals, Systems and Computers, 2008 42nd Asilomar Conference on*, pages 8 –12, oct. 2008.

[17] D. Rodriguez, J. Seguel, and E. Cruz. Algebraic methods for the analysis and design of time-frequency signal processing algorithms. In *Circuits and Systems, 1993., ISCAS '93, 1993 IEEE International Symposium on*, pages 196 –199

vol.1, may 1993.

[18] A. Graham. *Kronecker products and matrix calculus: with applications*. Ellis Horwood series in mathematics and its applications. Horwood, 1981.

[19] Charles F. van Loan. The ubiquitous kronecker product. *J. Comput. Appl. Math.*, 123:85–100, November 2000.

[20] J. R. Johnson, R. W. Johnson, D. Rodriguez, and R. Tolimieri. A methodology for designing, modifying, and implementing fourier transform algorithms on various architectures. *Circuits, Systems, and Signal Processing*, 9:449–500, 1990.

[21] Alan J. Laub. *Matrix Analysis For Scientists And Engineers*. Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2004.

[22] P. A. Regalia and S. K. Mitra. Kronecker products, unitary matrices, and signal processing applications. *SIAM Rev.*, 31:586–613, December 1989.

[23] Carla D. Moravitz Martin and Charles F. Van Loan. A jacobi-type method for computing orthogonal tensor decompositions. *SIAM J. Matrix Anal. Appl.*, 30:1219–1232, September 2008.

[24] M. An, A.K. Brodzik, and R. Tolimieri. *Ideal sequence design in time-frequency space: applications to radar, sonar, and communication systems*. Applied and numerical harmonic analysis. Birkhäuser, 2008.

[25] F. Franchetti, M. Puschel, Y. Voronenko, S. Chellappa, and J.M.F. Moura. Discrete fourier transform on multicore. *Signal Processing Magazine, IEEE*, 26(6):90 –102, november 2009.

[26] R. Tolimieri, M. An, C. L

"u, and C.S. Burrus. *Mathematics of multidimensional Fourier transform algorithms*. Signal processing and digital filtering. Springer, 1997.

[27] P. Kumhom, J.R. Johnson, and P. Nagvajara. Design, optimization, and implementation of a universal fft processor. In *ASIC/SOC Conference, 2000.*

*Proceedings. 13th Annual IEEE International*, pages 182 –186, 2000.

[28] G.H. Golub and C.F.V. Loan. *Matrix computations*. Johns Hopkins studies in the mathematical sciences. Johns Hopkins University Press, 1996.

[29] I.S. Gradshteyn, I.M. Ryzhik, and A. Jeffrey. *Table of integrals, series, and products*. Academic Press, 2000.

[30] P.J. Davis. *Circulant matrices*. Chelsea Publishing Series. Chelsea, 1994.

[31] P. M. Woodward. *Probability and Information Theory, with Applications to Radar*. McGraw-Hill, New York, 1953.

[32] J.J. Benedetto, I. Konstantinidis, and M. Rangaswamy. Phase-coded waveforms and their design. *Signal Processing Magazine, IEEE*, 26(1):22 –31, jan. 2009.

[33] Leon Cohen. *Time-frequency analysis: theory and applications*. Prentice-Hall, Inc., Upper Saddle River, NJ, USA, 1995.

[34] R. Tolimieri. Radar ambiguity functions and group theory. *SIAM J. Math. Anal.*, 16:577–601, 1985.

[35] R. Isermann. *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer, 2006.

[36] J. Zak. Finite translations in solid-state physics. *Phys. Rev. Lett.*, 19:1385–1387, Dec 1967.

[37] Christopher Heil. A Discrete Zak Transform. Technical Report MTR-89W00128, The MITRE Corporation, McLean, Virginia, 1989.

[38] A.J.E.M. Janssen. The Zak Transform: a signal transform, and coherent states. *Philips J. Res*, 43:23–69, 1988.

[39] R. Tolimieri and M. An. *Time-frequency representations*. Applied and numerical harmonic analysis. Birkhäuser Boston, 1998.

[40] M. An, A. Brodzik, I. Gertner, and R. Tolimieri. Weyl-heisenberg systems and the finite zak transform. In Yehoshua Zeevi and Ronald Coifman, editors, *Signal and Image Representation in Combined Spaces*, volume 7 of *Wavelet Analysis*

*and Its Applications*, pages 3 – 21. Academic Press, 1998.

[41] N. Polyak and W.A. Pearlman. Filters and filter banks for periodic signals, the zak transform, and fast wavelet decomposition. *Signal Processing, IEEE Transactions on*, 46(4):857 –873, apr 1998.

[42] Helmut Bölcskei and Franz Hlawatsch. Discrete Zak Transforms, Polyphase Transforms, and Applications. *IEEE Trans. Signal Processing*, 45:851–866, 1997.

[43] L. Auslander and R. Tolimier. *On finite Gabor expansion of signals*, pages 13–23. Springer-Verlag, London, UK, 1990.

[44] Andrzej K. Brodzik. Characterization of zak space support of a discrete chirp. *IEEE Transactions on Information Theory*, 53(6):2190–2203, 2007.

[45] A.K. Brodzik. Signal extrapolation in the real zak space. *Signal Processing, IEEE Transactions on*, 50(8):1957 –1964, aug 2002.

[46] L. Auslander and R. Tolimieri. Radar ambiguity functions and group theory. *j-SIAM-J-MATH-ANA*, 16(3):577–601, May 1985.

[47] N. Bourbaki. *Elements of Mathematics: Algebra 1.* Springer, 1998.

[48] D.G. Antzoulatos and A.A. Sawchuk. Hypermatrix algebra: Theory. *CVGIP: Image Understanding*, 57(1):24 – 41, 1993.

[49] L. Auslander and R. Tolimieri. Is computing with the fast fourier transform pure or applied mathematics. *Bull. Amer. Math. Soc.*, 1:847–897, Nov 1979.

# MARCO COMPUTACIONAL PARA EL TRATAMIENTO ARMÓNICO DE REPRESENTACIONES BIDIMENSIONALES

Juan Pablo Soto Quirós
juan.soto8@upr.edu
Departamento de Matemáticas
Consejero: Domingo Rodríguez
Grado: Ph.D
Fecha de Graduación: Noviembre 2011

En este trabajo se desarrollará un marco computacional de las representaciones en tiempo y frecuencias desarrolladas a partir la función discreta de ambigüedad. El arquetipo computacional se basará en estructuras matriciales, que se elaboraran a partir de las representaciones algebraicas de las funciones bidimensionales. Además, se desarrolla el concepto de un espacio de matrices de arreglos, para el estudio de la transformada discreta de Fourier de valores vectoriales y la función de ambigüedad de valores vectoriales, con el fin de desarrollar un marco computacional para estos dos conceptos.