CIMAT

Centro de Investigación en Matématicas CIMAT Monterrey
Maestría en Cómputo Estadístico

Construcción de matrices ortogonales y cuasiortogonales de gran tamaño

Sebastian Ramírez Jiménez

Proyecto de investigación final de Álgebra Matricial

Dr. Ángel David Reyes Figueroa

Monterrey, Nuevo León
6 de diciembre de 2022

Construcción de matrices ortogonales y cuasiortogonales de gran tamaño

Sebastian Ramírez Jiménez

Resumen

En esta investigación se estudian los conceptos esenciales para comprender con claridad el concepto de matrices ortogonales, por lo que puede considerarse como una introducción accesible a la teoría de matrices ortogonales y cuasi ortogonales. Se revisan diversos tipos de matrices ortogonales y cuasi-ortogonales y otras matrices con la propiedad que su inversa se pueda calcular con muy poco trabajo computacional, como las matrices Hadamard. Se estudian las propiedades algebraicas y geométricas más importantes que nos permitan obtener estas matrices mediante métodos de construcción clásicos, y mediante *construcción por bloques.* Finalmente, se enlistan de manera breve algunas potenciales aplicaciones de las matrices cuasi ortogonales. Todas las propiedades preeliminares se han estudiado para llegar facilmente al concepto de las matrices ortogonales y cuasi ortogonales, así como para comprender una caracterización de los grupos ortogonales y otra de las matrices cuasi ortognales. Estas propiedades se estudian en el espacio $\mathbb{K}^n$, con particular interés cuando $\mathbb{K} = \mathbb{R}, \mathbb{C}$ o $\mathbb{H}$. Se revisan los siguientes temas.

1. Producto interno estándar y norma estándar en $\mathbb{K}^n$

2. Ortogonalidad y ortonormalidad de vectores.

3. Matrices ortogonales y unitarias; propiedades algebraicas. Caracterizaciones de los grupos ortogonales, utilizando las propiedades que permiten preservar la norma y de producto interno de vectores. Grupos de matrices ortogonales especiales.

4. Matrices ortogonales e isometrías. Propiedades algebraicas y geométricas.

5. Matrices cuasi-ortogonales, matrices de Hadamard y sus construcciones clásicas.

6. Construcción de matrices cuasi ortogonales por bloques.

7. Potenciales aplicaciones en comunicación inalámbrica, codificación de información y procesamiento de imágenes.

Contenido

Capítulo 1

Preeliminares

A continuación se revisan algunos conceptos fundamentales sobre las matrices ortogonales, ortonormalidad; una caracterización útil de los grupos ortogonales y algunas descripciones de estos grupos para dimensiones pequeñas.

1.1. El producto interno estándar

Para comprender el estudio del producto interno en $\mathbb{K}^n$, se requiere recordar qué es la norma y el conjugado del elemento $k \in \mathbb{K}$. Se denotan como $|k|$ a su norma y como $\overline{k}$ a su conjugado. Por ejemplo, si $k \in \mathbb{R}$, entonces decimos que su norma $|k|$ es el valor absoluto y su conjugado es él mismo. Si $k = a + b\mathbf{i} \in \mathbb{C}$, su norma se define como $|k| := \sqrt{a^2 + b^2}$ y su conjugado, como $\overline{k} := a - b\mathbf{i}$. Un ejemplo más, si $k = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$, su norma es $|k| := \sqrt{a^2 + b^2 + c^2 + d^2}$ y su conjugado es $\overline{k} := a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$.

En todos estos casos se verifica que para si $k, k_1, k_2 \in \mathbb{K}$, entonces,

$$\overline{k_1 \cdot k_2} = \overline{k_1} \cdot \overline{k_2}, \tag{1.1}$$

$$k \cdot \overline{k} = \overline{k} \cdot k = |k|^2. \tag{1.2}$$

Además, las propiedades (1) y (2) implican que

$$|k_1 \cdot k_2| = |k_1| \cdot |k_2|. \tag{1.3}$$

Con estos conceptos y propiedades ya podemos definir un producto entre elementos k de $\mathbb{K}^n$, a los que llamaremos vectores. Se define el *producto interno estándar en* $\mathbb{K}^n$ (también llamado producto vectorial) como la función $\langle\ ,\ \rangle : \mathbb{K}^n \times \mathbb{K}^n \longrightarrow \mathbb{K}^n$, que está dada como sigue

$$\langle X, Y\rangle = \langle (x_1, x_2, ..., x_n), (y_1, y_2, ..., y_n)\rangle_{\mathbb{K}} := x_1 \cdot \overline{y_1} + x_2 \cdot \overline{y_2} + \cdots + x_n \cdot \overline{y_n}.$$

Observe que de (2), para todo $X \in \mathbb{K}^n$, su producto interno con sí mismo $\langle X, X\rangle_{\mathbb{K}}$ es un número real mayor o igual que 0 e igual a cero solo cuando $X = (0, 0, ..., 0)$. Esta observación permite definir la *norma estándar en* $\mathbb{K}^n$, que es una función de $\mathbb{K}^n$ en los reales no-negativos, dada por

$$|X|_{\mathbb{K}} := \sqrt{\langle X, X\rangle_{\mathbb{K}}}.$$

El producto interno tiene una importante cantidad de propiedades, la siguiente proposición condensa algunas que resultan útiles (Tapp, 2005). .

Proposición 1.

Para cualesquiera $X, Y, Z \in \mathbb{K}^n$ y $\lambda \in \mathbb{K}$, se cumple lo que sigue

(i) $\langle X, Y + Z\rangle = \langle X, Y\rangle + \langle X, Z\rangle$,

(ii) $\langle X + Y, Z\rangle = \langle X, Z\rangle + \langle Y, Z\rangle$,

(iii) $\langle \lambda X, Y\rangle = \lambda\langle X, Y\rangle$ y $\langle X, \lambda Y\rangle = \langle X, Y\rangle\overline{\lambda}$,

(iv) $\overline{\langle X, Y\rangle} = \langle Y, X\rangle$.

Nota: Observe que se pueden omitir los subíndices de $\mathbb{K}$ siempre que no exista la posibilidad de confusiones.

Capítulo 2

Ortogonalidad y ortonormalidad de vectores

2.1. El concepto de ortogonalidad

Para estudiar al grupo de matrices ortogonales es preciso comprender el concepto de ortogonalidad. Decimos que dos vectores no nulos $X, Y \in \mathbb{K}^n$ son *ortogonales* si su producto interno estándar es cero, es decir, si $\langle X, Y\rangle = 0$. Al generalizar este concepto a un conjunto de vectores, se piensa en si será fácil determinar una base cuyos elementos sean ortogonales entre sí. Una *base* $\{X_1, X_2, \ldots, X_n\}$ de $\mathbb{K}^n$ se dice que es *ortonormal* si $\langle (X_i, Y_j)\rangle$ es igual a 1 si $i = j$ y es igual a cero si $i \neq j$. Esto es, los vectores tienen norma igual a 1 y son mutuamente ortogonales. En general se puede definir una base estándar para el espacio $\mathbb{K}^n$, *la base estándar ortonormal del espacio* $\mathbb{K}^n$ se describe por el conjunto

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

Con lo anterior se puede comprender la noción de ortonormalidad de vectores, por ejemplo, en $\mathbb{R}^n$ y $\mathbb{C}^n$. En $\mathbb{R}^n$ el producto interno estándar es el familiar *producto punto*, descrito geométricamente en términos del ángulo θ entre los vectores $X, Y \in \mathbb{R}^n$ como sigue

$$\langle (X, Y)\rangle_{\mathbb{R}} \ = \ |X|_{\mathbb{R}} \cdot |Y|_{\mathbb{R}} \cos\theta. \tag{2.1}$$

Para el caso complejo sucede que el producto interno de dos vectores, también llamado *hermitiano*, es también un número complejo y el significado geométrico de cada una de sus partes, la real y la imaginaria, se debe interpretar de manera independiente. Una de las maneras más claras de hacerlo es en términos de la siguiente *identificación.*

$$\begin{aligned} &f := f_n : \mathbb{C}^n \longrightarrow \mathbb{R}^{2n}, \text{ dada por} \\ &f_n(a_1 + b_1\mathbf{i}, a_2 + b_2\mathbf{i}, \ldots, a_n + b_n\mathbf{i}) = (a_1, b_1, a_2, b_2, \ldots, a_n, b_n). \end{aligned} \tag{2.2}$$

De esta es fácil comprobar que para cualesquiera $X, Y \in \mathbb{C}^n$,

$$\langle X, Y\rangle_{\mathbb{C}} = \langle f(X), f(Y)\rangle_{\mathbb{R}} + \mathbf{i}\langle f(X), f(\mathbf{i}Y)\rangle_{\mathbb{R}},$$

y que

$$|X|_{\mathbb{C}} = |f(X)|_{\mathbb{R}}.$$

Además si $X, Y \in \mathbb{C}^n$ son ortogonales, como consecuencia del producto punto de $\mathbb{R}^n$, se tiene que

$$\langle f(X), f(Y)\rangle_{\mathbb{R}} \;=\; 0 \quad \text{y} \quad \langle f(X), f(\mathbf{i}Y)\rangle_{\mathbb{R}} \;=\; 0.$$

Por tanto, el estudio de la ortogonalidad en $\mathbb{C}^n$ se puede simplificar a un estudio con vectores reales de tamaño $2n$. Estas observaciones nos permiten construir la siguiente proposición.

Proposición 2.

Sea $\beta := \{X_1, X_2, \ldots, X_n\}$ una base de $\mathbb{C}^n$, β es una base ortonormal si y solo si $\{f(X_1), f(\mathbf{i}X_1), f(X_2), f(\mathbf{i}X_2), \ldots, f(X_n), f(\mathbf{i}X_n)\}$ es una base ortonormal en $\mathbb{R}^{2n}$.

Por último, para el caso $\mathbb{K} = \mathbb{H}$ el producto interno es también llamado *s*impléctico. Análogamente que en el caso de $\mathbb{C}^n$, la mejor forma de interpretar $\mathbf{i}$, $\mathbf{j}$ y $\mathbf{k}$ de manera geométrica es con una aplicación.

$$h := f_{2n} \circ g_n : \mathbb{H}^n \longrightarrow \mathbb{R}^{4n}. \tag{2.3}$$

En la cual $g_n : \mathbb{H}^n \longrightarrow \mathbb{C}^{2n}$ es la función dada por

$$g_n(z_1 + w_1\mathbf{j}, z_2 + w_2\mathbf{j}, \ldots, z_n + w_n\mathbf{j}) = (z_1, w_1, z_2, w_2, \ldots, z_n, w_n).$$

Se puede verificar, análogamente, que

$$\begin{aligned}\langle X, Y\rangle_{\mathbb{H}} \;=\; & \langle h(X), h(Y)\rangle_{\mathbb{R}} \;+\; \mathbf{i}\langle h(X), h(\mathbf{i}Y)\rangle_{\mathbb{R}} \\ & +\; \mathbf{j}\langle h(X), h(\mathbf{j}Y)\rangle_{\mathbb{R}} \;+\; \mathbf{k}\langle h(X), h(\mathbf{k}Y)\rangle_{\mathbb{R}},\end{aligned}$$

y también que

$$|X|_{\mathbb{H}} = |h(X)|_{\mathbb{R}}.$$

Por lo tanto, para estudiar la ortogonalidad de cuaterniones basta estudiar vectores complejos de tamaño $2n$ y por la Proposición 2 entonces es suficiente el estudio de la ortogonalidad de los vectores reales, en este caso de tamaño $4n$. Con lo anterior podemos establecer la siguiente proposición.

Proposición 3.

Diremos que $\{X_1, X_2, \ldots, X_n\}$ es una base ortonormal de $\mathbb{H}^n$ si y solo si

$$\{h(X_1), h(\mathbf{i}X_1), h(\mathbf{j}X_1), h(\mathbf{k}X_1), \ldots, h(X_n), h(\mathbf{i}X_n), h(\mathbf{j}X_n), h(\mathbf{k}X_n)\}$$

es una base ortonormal en $\mathbb{R}^{4n}$.

De las dos proposiciones anteriores obtenemos una importante herramienta para manejar vectores ortonormales en $\mathbb{C}^n$ y $\mathbb{H}^n$ en términos de vectores reales del tamaño respectivo (Shafarevich and Remizov, 2009). La siguiente proposición es importante para completar el estudio sobre ortogonalidad pues relaciona el producto escalar y la norma de dos vectores distintos. Las siguientes desigualdades usadas en la proposición se siguen de la ecuación (4) cuando $\mathbb{K} = \mathbb{R}$.

Proposición 4. (Desigualdad de Schwarz).

Para cualesquiera $X, Y, \in \mathbb{K}^n$,

$$|\langle X, Y\rangle| \leq |X| \cdot |Y|.$$

Demostración. (Tapp [1]). Sean $X, Y \in \mathbb{K}^n$. Sea $\alpha := \langle X, Y\rangle$. Suponemos que $X \neq 0$ (de lo contrario la prueba es trivial). Para toda $\lambda \in \mathbb{K}^n$, se cumple que

$$\begin{aligned} 0 \leq \ | \lambda X + Y| \ &= \ \langle \lambda X + Y, \ \lambda X + Y\rangle \\ &= \lambda\langle X, X\rangle\overline{\lambda} + \lambda\langle X, Y\rangle + \overline{\lambda}\langle Y, X\rangle + \langle Y, Y\rangle \\ &= |\lambda|^2|X|^2 + \lambda\langle X, Y\rangle + \overline{\lambda\langle X, Y\rangle} + |Y|^2 \\ &= |\lambda|^2|X|^2 + 2Re(\lambda\alpha) + |Y|^2 \end{aligned}$$

Eligiendo $\lambda = -\overline{\alpha}/|X|^2$ nos da

$$0 \leq |\alpha|^2/|X|^2 - 2|\alpha|^2/|X|^2 + |Y|^2,$$

lo cual prueba que $|\alpha| \leq |X| \cdot |Y|$ como se deseaba. □

Con la proposición anterior se completan las propiedades relevantes sobre la base ortonormal estándar de un espacio vectorial, estas permiten determinar varias caracterizaciones de los grupos de matrices ortogonales (Geramita and Seberry, 1979).

Capítulo 3

Grupos ortogonales de matrices

3.1. Caracterización de los grupos ortogonales

Si A es una matriz $n \times n$ con entradas en $\mathbb{K}$, definimos la transformación lineal $R_A : \mathbb{K}^n \to \mathbb{K}^n$ por $R_A(X) = XA$, para $X \in \mathbb{K}^n$. Notemos que la multiplicación por A es por la derecha, porque X es un vector fila.

Para cada $n \geq 1$ definimos al conjunto

$$\mathcal{O}_n(\mathbb{K}) := \{A \in GL_n(\mathbb{K}) |\ \langle XA, YA\rangle = \langle X, Y\rangle \text{ para todo } X, Y \in \mathbb{K}^n\}$$

como el *grupo ortogonal sobre el espacio* $\mathbb{K}$ de orden n. Esto es el conjunto de todas las matrices invertibles $n \times n$ con entradas en $\mathbb{K}$ tales que $\langle XA, YA\rangle = \langle X, Y\rangle$ para todo $X, Y \in \mathbb{K}^n$, es decir, que preservan el producto vectorial de cualquier par de vectores en $\mathbb{K}^n$ al multiplicar por la derecha. Este grupo se denota por $\mathcal{O}_n(\mathbb{K})$ para cualquier espacio $\mathbb{K}^n$, sin embargo para espacios de dimensión pequeña se tiene su propia notación.

Para $\mathbb{K} = \mathbb{R}$ se denota como $O(n)$ y se le llama *grupo ortogonal*. Para el caso $\mathbb{K} = \mathbb{C}$, al grupo ortogonal se le denota como $U(n)$ y se le llama *grupo unitario*; y para $\mathbb{K} = \mathbb{H}$ se denota como $Sp(n)$ y se llama *grupo simpléctico* (Geramita and Seberry, 1979).

Es sencillo ver que $\mathcal{O}_n(\mathbb{K})$ es un subgrupo de $GL_n(\mathbb{K})$ con la multiplicación usual de matrices. Sus elementos se llaman matrices ortogonales, unitarias o simplécticas para el espacio vectorial respectivo. Para describir su forma, es útil denotar al *conjugado transpuesto* de $A \in M_n(\mathbb{K})$ como $A^* := \overline{A}^T$, donde $\overline{A}$ es la matriz que se obtiene al conjugar todas las entradas de A. Esta descripción se hace en la siguiente proposición.

Proposición 5.

Para toda $A \in GL_n(\mathbb{K})$ las siguientes afirmaciones son equivalentes.

(i) $A \in \mathcal{O}_n(\mathbb{K})$.

(ii) R_A preserva bases ortonormales, es decir, si $\{X_1, X_2, \ldots, X_n\}$ es una base ortonormal de $\mathbb{K}^n$, entonces $\{R_A(X_1), R_A(X_2), \ldots, R_A(X_n)\}$ también es una base ortonormal.

(iii) Las filas de A forman una base ortonormal de $\mathbb{K}^n$.

(iv) $A \cdot A^* = I$, donde I denota la matriz identidad correspondiente.

Demostración. (i) $\Rightarrow$ (ii) resulta obvia por la definición de R_A. (ii) $\Rightarrow$ (iii) porque las filas de A son iguales a $\{R_A(e_1), R_A(e_2), \ldots, R_A(e_n)\}$. Para ver que (iii) $\Leftrightarrow$ (iv) note que para cada entrada en el producto dado

$$\begin{aligned}(A \cdot A^*)_{ij} &= (\text{fila } i \text{ de } A) \cdot (\text{columna } j \text{ de } A^*) \\ &= (\text{fila } i \text{ de } A) \cdot (\text{fila } j \text{ de } \overline{A})^T \\ &= \langle (\text{fila } i \text{ de } A) \cdot (\text{fila } j \text{ de } A) \rangle.\end{aligned}$$

y como las filas de A forman una base ortonormal, esta entrada es igual a 1 si $i = j$ e igual a cero si $i \neq j$, es decir $A \cdot A^* = I$, y recíprocamente. Finalmente, probaremos que (iii) $\Rightarrow$ (i). Si las filas de A son ortonormales, entonces para cualesquiera $X = (x_1, x_2, \ldots, x_n)$, $Y = (y_1, y_2, \ldots, y_n) \in \mathbb{K}^n$

$$\begin{aligned}\langle R_A(X), R_A(Y)\rangle &= \left\langle \sum_{l=1}^{n} x_l(\text{fila } l \text{ de} A), \sum_{s=1}^{n} y_s(\text{fila } s \text{ de} A) \right\rangle \\ &= \sum_{l,s=1}^{n} x_l \langle (\text{fila } l \text{ de} A), (\text{fila } s \text{ de} A)\rangle \overline{y_s} \\ &= x_1\overline{y_1} + \cdots + x_n\overline{y_n} \\ &= \langle X, Y\rangle.\end{aligned}$$

Esto es A, es una matriz ortogonal. □

Geométricamente, el grupo ortogonal $O(n)$ es el grupo de matrices A para las cuales la transformación lineal $R_A : \mathbb{R}^n \to \mathbb{R}^n$ preserva el producto interno estándar de vectores y por tanto también preserva la norma de vectores. De la ecuación (4) sobre la relación geométrica entre el ángulo entre vectores y el producto interno es claro que también se preserva tal ángulo. Entonces tales trasformaciones podrían visualizarse como "movimientos rígidos" en $\mathbb{R}^n$, es decir, aquellas que conservan distancias y ángulos entre vectores, éstas son las rotaciones, traslaciones y reflexiones. Los significados geométricos de $U(n)$ y $Sp(n)$ se describen claramente en términos del grupo ortogonal $O(n)$ considerando ciertos homomorfismos. Sean ρ_n y Ψ_n los siguientes homomorfismos inyectivos.

$$\rho_n : GL_n(\mathbb{C}) \to GL_{2n}(\mathbb{R}) \quad \text{y} \quad \Psi_n : GL_n(\mathbb{H}) \to GL_{2n}(\mathbb{C}).$$

Estos homomorfismos de grupos nos ayudan a demostrar que todo grupo de matrices es en sí un grupo de matrices reales. Es decir, bastaría estudiar el grupo ortogonal de matrices reales, para comprender el grupo ortogonal $\mathcal{O}_n(\mathbb{K})$, tal como se revisó en la sección anterior para las bases ortonormales. Asimismo nos ayudan a comprender la descripción geométrica del grupo unitario de matrices $U(n)$ y del grupo simpléctico de matrices $Sp(n)$. Esto se consigue con la siguiente proposición.

Proposición 6.

(i) $\rho_n(U(n)) = O(2n) \cap \rho_n(GL_n(\mathbb{C}))$.

(ii) $\Psi_n(Sp(n)) = U(2n) \cap \Psi_n(GL_n(\mathbb{H}))$.

(iii) $(\rho_{2n} \circ \Psi_n)(Sp(n)) = O(4n) \cap (\rho_{2n} \circ \Psi_n)(GL_n(\mathbb{H}))$.

Como $U(n)$ es isomorfo a su imagen, $\rho_n(U(n))$, la parte (i) nos dice que $U(n)$ es isomorfo al grupo de matrices ortogonales reales $2n \times 2n$ que corresponden a una matriz compleja $n \times n$ bajo el homomorfismo ρ_n. En otras palabras, $U(n)$ es isomorfo al grupo de movimientos rígidos de $\mathbb{R}^{2n}$ que preservan la estructura compleja estándar. Similarmente, la parte (iii) dice que $Sp(n)$ es isomorfo al grupo de matrices ortogonales reales $4n \times 4n$ que provienen de una matriz $n \times n$ con entradas en $\mathbb{H}$ bajo el homomorfismo $\rho_{2n} \circ \Psi_n$.

Demostración. Presentamos solo la demostración de (i), puesto que (ii) es similar y (iii) se sigue de (i) y (ii). La idea más sencilla es usar la igualdad de (5). Notemos primeramente que para toda $A \in M_n(\mathbb{C})$ se cumple

$$\rho_n(A^*) = \rho_n(A)^*.$$

Ahora si $A \in GL_n(\mathbb{C})$, entonces $\rho_n(A) \cdot \rho_n(A)^* = \rho_n(A) \cdot \rho_n(A^*) = \rho_n(A \cdot A^*)$, lo cual muestra que $A \in U(n)$ si y solo si $\rho_n(A) \in O(2n)$. □

Ya comentamos que $\mathcal{O}(n)$ es el grupo de matrices A, para las cuales R_A preserva el producto interno de vectores y por tanto también las normas de vectores, el siguiente resultado dice que si R_A preserva la norma, entonces automáticamente preserva el producto interno.

Proposición 7. (Caracterización de grupos ortogonales).

$$\mathcal{O}_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) : \quad |R_A(X)| = |X| \text{ para todo } X \in \mathbb{K}^n\}.$$

Demostración. Para probar el caso $\mathbb{K} = \mathbb{R}$ mostraremos que el producto interno está totalmente determinado por la norma. Resolviendo la ecuación

$$|X+Y|^2_{\mathbb{R}} = \langle X+Y, X+Y\rangle_{\mathbb{R}} = \langle X, X\rangle_{\mathbb{R}} + \langle Y, Y\rangle_{\mathbb{R}} + 2\langle X, Y\rangle_{\mathbb{R}}$$

para $\langle X, Y\rangle_{\mathbb{R}}$ obtenemos que

$$\langle X, Y\rangle_{\mathbb{R}} = \frac{1}{2}(|X+Y|^2_{\mathbb{R}} - |X|^2_{\mathbb{R}} - |Y|^2_{\mathbb{R}}).$$

Así que si R_A preserva la norma, entonces también preserva los productos internos en $\mathbb{R}$, puesto que este último se describe en términos de las normas, según la última igualdad. □

Desafortunadamente, el argumento anterior no funciona para $\mathbb{K} = \mathbb{C}$ o $\mathbb{H}$, puesto que es difícil despejar el producto interno que nos interesa de una fórmula similar a la que inicia la demostración. Sin embargo, es posible demostrar estos casos a partir del caso real con ayuda de las funciones definidas para la Proposición 6. Supongamos que $A \in GL_n(\mathbb{C})$, es tal que $R_A : \mathbb{C}^n \to \mathbb{C}^n$ preserva la norma. Entonces $R_{\rho_n(A)} : \mathbb{R}^{2n} \to \mathbb{R}^{2n}$, también preserva la norma, por lo que para cualquiera $X \in \mathbb{C}^n$ se tiene que,

$$|R_{\rho_n(A)}(f_n(X))|_{\mathbb{R}} = |f_n(R_A(X))|_{\mathbb{R}} = |R_A(X)|_{\mathbb{C}} = |X|_{\mathbb{C}} = |f_n(X)|_{\mathbb{R}}$$

Por lo tanto $\rho_n(A) \in O(n)$, lo cual implica que $A \in U(n)$, por la Proposición 6. Similarmente se puede demostrar que si $A \in GL_n(\mathbb{H})$ y preserva la norma entonces $A \in Sp(n)$.

Con lo anterior, se concluye que el estudio del grupo ortogonal $O(n)$ es indispensable para poder entender y comprender al grupo $\mathcal{O}(n)$, al menos en los casos revisados. También obtuvimos una caracterización importante de los grupos ortogonales la cual permite estudiarlo como un grupo de matrices las cuales preservan la norma de vectores. Esto es

$$\begin{aligned}\mathcal{O}_n(\mathbb{K}) &= \{A \in GL_n(\mathbb{K}) : \ \langle XA, YA\rangle \ = \ \langle X, Y\rangle \text{ para todo } X, Y \in \mathbb{K}^n\} \\ &= \{A \in GL_n(\mathbb{K}) : \ |R_A(X)| = |X| \text{ para todo } X \in \mathbb{K}^n\}.\end{aligned}$$

3.2. Grupos de matrices ortogonales especiales

Dentro de los grupos ortogonales que se han revisado existen algunos de especial importancia e interés. En esta sección se definen algunos de los subgrupos de matrices ortogonales que resultan importantes. Iniciamos con una observación importante.

Proposición 8.

Si $A \in \mathcal{O}_n(\mathbb{K}),$ entonces $|\det(A)| = 1.$

Demostración. Como $A \cdot A^* = I$, donde I denota la matriz identidad correspondiente, entonces

$$1 = \det(A \cdot A^*) = \det(A) \cdot \det(A^*) = \det(A) \cdot \overline{\det(A)} = |\det(A)|^2.$$

Lo que quedaría por mostrar de manera detallada es que efectivamente $\det(A^*) = \overline{\det(A)}$. Usemos el hecho que $\det(A) = \det(A^*)$, inicialmente se puede verificar para $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$. El caso en los cuaterniones se sigue del caso complejo, pues para una matriz con entradas de cuaterniones, $\det(A)$ es $\det(\psi_n(A))$, y $\det(\psi_n(A^*)) = \det(\psi_n(A))^*$. □

La interpretación de esta proposición depende del campo $\mathbb{K}$ en cuestión. Si $A \in O(n)$, entonces $\det(A) = \pm 1$. Si $A \in U(n)$, entonces $\det(A) = \exp^{i\theta}$, para algún $\theta \in [0, 2\pi)$. Y si $A \in Sp(n)$, entonces $\det(A) = 1$.

De esto, el subgrupo de matrices

$$SO(n) := \{A \in O(n) : \ \det(A) = 1\}$$

se llama el *grupo especial ortogonal*, mientras que el subgrupo de matrices

$$SU(n) := \{A \in U(n) : \ \det(A) = 1\}$$

es llamado el *grupo especial unitario*. Ambos son subgrupos del grupo lineal general. Hay que notar que $SO(n)$ comprende las matrices cuyos determinantes solo

toman un valor de dos valores posibles, mientras que $SU(n)$ comprende las matrices unitarias cuyos determinantes toman un valor de una infinidad de valores posibles en el círculo unitario.

3.3. Grupos de dimensión pequeña

A continuación se describen casos concretos relevantes de estos subgrupos ortogonales considerando valores de n pequeños. En primer lugar, el grupo ortogonal $O(1) = \{1, -1\}$ y el grupo especial ortogonal $SO(1) = \{(1)\}$ son isomorfos a los únicos grupos con 2 y un elemento, respectivamente.

Ahora, si $A \in O(2)$, entonces sus dos filas forman una base ortonormal de $\mathbb{R}^2$, por lo que su primer fila es un vector unitario arbitrario de $\mathbb{R}^2$, el cual puede ser escrito como $(\cos\theta, \sin\theta)$ para algún $\theta \in [0, 2\pi]$. La segunda fila es unitaria y ortogonal a la primera, la cual deja dos elecciones: $(-\sin\theta, \cos\theta)$ o $(\sin\theta, -\cos\theta)$. Para la primera elección el determinante es $\det(A) = 1$ y para la segunda elección, $\det(A) = -1$. Así se tiene lo siguiente:

$$SO(2) = \left\{ \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} : \ \theta \in [0, 2\pi) \right\},$$

$$O(2) = SO(2) \cup \left\{ \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} : \ \theta \in [0, 2\pi) \right\}.$$

El subgrupo especial ortogonal $SO(2)$ es identificado con el conjunto de puntos en un círculo, cuya operación de grupo es la adición de ángulos. Y el grupo ortogonal $O(2)$ es la unión disjunta de dos círculos. Es interesante que esta unión disjunta de círculos tenga una operación de grupos.

Luego, considere al grupo especial unitario de dimensión 1, $SU(1) = \{(1)\}$ y el grupo unitario de la misma dimensión: $U(1) = \{(\exp^{i\theta}) : \theta \in [0, 2\pi)\}$, el cual es

isomorfo al grupo cíclico $SO(2)$, o considere al grupo simpléctico $Sp(1) = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : \ a^2 + b^2 + c^2 + d^2 = 1\}$ que es el grupo de cuaterniones unitarios, el cual es identificado naturalmente con la esfera tridimensional $S^3 \subset \mathbb{R}^4 \cong \mathbb{H}$. De hecho, el producto de dos cuaterniones unitarios es un cuaternión, así que debemos mencionar que la multiplicación de cuaterniones proporciona una operación de grupo en la esfera de 3 dimensiones. Por tanto, sucede que S^1, S^2 y S^3 son la únicas esferas que también son grupos. Una relación importante entre estos subgrupos es que el grupo especial ortogonal para $n = 2$ es isomorfo al grupo simpléctico $Sp(1)$. Es decir, $SU(2) \cong Sp(1)$. Esto se prueba en la siguiente proposición.

Proposición 9.

$SU(2)$ es isomorfo a $Sp(1)$.

Demostración. Usando el homomorfismo $\Psi_1 : GL_1(\mathbb{H}) \to GL_2(\mathbb{C})$ se puede notar que

$$\Psi_1(Sp(1)) = \left\{ \begin{bmatrix} z & w \\ -\overline{w} & \overline{z} \end{bmatrix} : \ z, w \in \mathbb{C} \text{ tales que } |z|^2 + |w|^2 = 1 \right\}$$

es un subgrupo del grupo unitario $U(2)$, a saber, las matrices unitarias 2 x 2 (cuaterniónico-lineales). Calculando los determinantes de tales matrices se muestra que $\Psi_1(Sp(1)) \subset SU(2)$, que de hecho forman un subgrupo del grupo especial ortogonal $SU(2)$. Se desea probar la igualdad, así que Ψ_1 determina un isomorfismo entre $Sp(1)$ y $SU(2)$. Sea $A = \begin{bmatrix} z_1 & w_1 \\ w_2 & z_2 \end{bmatrix} \in SU(2)$. Es fácil determinar que $A^{-1} = \dfrac{1}{\det(A)} \begin{bmatrix} z_2 & -w_1 \\ -w_2 & z_1 \end{bmatrix}$. En nuestro caso, $\det(A) = 1$ y $\begin{bmatrix} z_2 & -w_1 \\ -w_2 & z_1 \end{bmatrix} = A^{-1} = A^* = \begin{bmatrix} \overline{z_1} & \overline{w_2} \\ \overline{w_1} & \overline{z_2} \end{bmatrix}$, lo cual dice que $z_2 = \overline{z_1}$ y que $w_2 = -\overline{w_1}$. Por lo tanto, se sigue que $\Psi_1(Sp(1)) = SU(2)$, como se quería. □

Capítulo 4

Matrices ortogonales e isometrías

4.1. Matrices ortogonales

Continuando con la descripción de los grupos ortogonales, se describe al grupo ortogonal $O(n)$ geométricamente como el grupo de isometrías de $\mathbb{R}^n$. Para entender el concepto de isometría recordemos que la distancia entre puntos $X = (x_1, \ldots, x_n)$ y $Y = (y_1, \ldots, y_n)$ en $\mathbb{R}^n$ está dada por

$$dist(X, Y) := |X - Y| = \sqrt{((x_1 - y_1)^2 + \ldots + (x_n - y_n)^2)}.$$

Así una función $f : \mathbb{R}^n \to \mathbb{R}^n$ es llamada una *isometría* si para todos $X, Y \in \mathbb{R}^n$, $dist(f(X), f(Y)) = dist(X, Y)$. La descripción geométrica se expone en la siguinete proposición.

Proposición 10.

(i) Si $A \in O(n)$ entonces $R_A : \mathbb{R}^n \to \mathbb{R}^n$ es una isometría.

(ii) Si $f : \mathbb{R}^n \to \mathbb{R}^n$ es una isometría con $f(0) = 0$, entonces $f = R_A$ para alguna $A \in O(n)$. En particular, f es lineal.

Demostración. Para cualquier matriz $A \in O(n)$ y para cualesquiera vectores

$X, Y \in \mathbb{R}^n$,

$$dist(R_A(X), R_A(Y)) = |R_A(X) - R_A(Y)| = |R_A(X - Y)|$$
$$= |X - Y| = dist(X, Y),$$

ya que R_A preserva la norma usual de $\mathbb{R}^n$, como se revisó anteriormente. Esto prueba que R_A es una isometría. Recíprocamente, suponga que f es una isometría para la cual $f(0) = 0$, entonces para cualquier $X \in \mathbb{R}^n$,

$$|f(x)| = dist(f(X), 0) = dist(f(X), f(0)) = dist(X, 0) = |X|,$$

lo cual muestra que f preserva normas. Ya mostramos (en la Proposición 7) que el producto interno está determinado por la norma, así que f también preserva el producto interno, es decir, para cualesquiera $X, Y \in \mathbb{R}^n$,

$$\langle f(X), f(Y)\rangle = \langle X, Y\rangle.$$

Ahora, sea A una matriz cuya i-ésima fila es $f(e_1)$, así que $f(e_i) = R_A(e_i)$ para cualquier $i = 1, \ldots, n.$. De este modo, $A \in O(n)$, pues sus filas son ortonormales. Probaremos que $f = R_A$, mostrando que $g = (R_a)^{-1} \circ f$ es la función identidad. Observe que g es isometría con $g(0) = 0$, así que preserva la norma y el producto interno como antes, y $g(e_i) = e_i$ para cualquier $i = 1, \ldots, n$. Sea $X \in \mathbb{R}^n$, si escribimos $X = \sum a_i e_i$ y $g(X) = \sum b_i e_i$. Entonces,

$$b_i = \langle g(X), e_i\rangle = \langle g(X), g(e_i)\rangle = \langle X, e_i\rangle = a_i,$$

lo cual prueba que $g(X) = X$, así que g es la función identidad. □

Por tanto, el grupo ortogonal $O(n)$ es el grupo de isometrías de $\mathbb{R}^n$ que fijan el origen y que, por tanto, mapean la esfera $S^{n-1} \subset \mathbb{R}^n$ en sí misma (Gorbachev et al., 2018). Por ejemplo, los elementos de $O(3)$ representan funciones del "globo" $S^2 \subset \mathbb{R}^3$ en sí mismo. Veremos a continuación que los elementos de $SO(3)$ representan movimientos físicos reales del globo.

Para entender la diferencia entre el grupo ortogonal $O(3)$ y el grupo especial ortogonal $SO(3)$, debemos discutir la orientación de $\mathbb{R}^3$. Una base ortonormal ordenada

de $\mathbb{R}^3$, como $\{X_1, X_2, X_3\}$, se llama *base diestra* si $X_1 \times X_2 = X_3$, donde $\times$ denota el producto cruz vectorial en $\mathbb{R}^3$. Visualmente, esto significa que si los dedos de su mano derecha están curvados de X_1 hacia X_2, luego tu pulgar apuntará en la dirección de X_3.

Proposición 11.

Sea $A \in O(3)$. Entonces $A \in SO(3)$ si y solo si las filas de A,

$$R_A(e_1), R_A(e_2), R_A(e_3),$$

forman una base ortonormal diestra.

Demostración. Sea $R_A(e_1) = (a, b, c)$ y $R_A(e_2) = (d, e, f)$ las dos primeras filas de A. La tercera fila es de longitud unitaria y ortogonal a ambas, lo que deja dos opciones:

$$R_A(e_3) = \pm(R_A(e_1) \times R_A(e_2)) = \pm(bf - ce, cd - af, ae - bd).$$

Un cálculo rápido muestra que la opción "+" da $\det(A) > 0$, mientras que la opción "−" da $\det(A) < 0$. □

Los elementos de $SO(3)$ corresponden a "movimientos físicamente realizables" de un globo. Esta afirmación es imprecisa, pero se puede mostrar que cada elemento de $SO(3)$ es una rotación a través de algún ángulo alrededor de un eje único. Un elemento de $O(3)$ con determinante negativo da vuelta al globo terráqueo. Por ejemplo, $R_{diag}(-1, -1, -1)$ asigna cada punto del globo a su antípoda (su negativo). Este no es un movimiento físicamente ejecutable.

4.2. El grupo de isometrías del espacio euclidiano

Como hemos visto, se puede estudiar al grupo ortogonal sobre el espacio $\mathbb{R}$ mediante las isometrías del espacio euclidiano. Este conjunto de isometrías se denota como

$$\text{Isom}(\mathbb{R}^n) := \{f : \mathbb{R}^n \to \mathbb{R}^n : \quad f \text{ es una isometría}\}.$$

y resulta que es un grupo bajo la composición de funciones, es más, el subgrupo de isometrías que fijan el origen es isomorfo a $O(n)$. Una isometría f que no fija al origen no es lineal, por lo que no puede ser igual a R_A para ninguna matriz A. En este caso, sea $V = f(0)$, entonces la función $X \to f(X) - V$ es una isometría que fija al origen y por lo tanto es igual a R_A para alguna $A \in 0(n)$. Por lo tanto, una isometría arbitraria de $\mathbb{R}^n$ tiene la forma

$$f(X) = R_A(X) + V$$

para alguna $A \in O(n)$ y $V \in \mathbb{R}^n$. Este es un truco inteligente para representar cualquier isometría de $\mathbb{R}^n$ como una matriz, incluso las que no fijan el origen. Los programadores de gráficos utilizan este truco para rotar y trasladar objetos en la pantalla de la computadora a través de matrices. A continuación se describe el caso n = 3.

Sea $A \in O(3)$ y $V = (v_1, v_2, v_3) \in \mathbb{R}^n$. Representaremos la isometría $f(X) = R_A(X) + V$ mediante la matriz:

$$F := \begin{bmatrix} A & 0 \\ V & 1 \end{bmatrix} := \begin{bmatrix} A_{11} & A_{12} & A_{13} & 0 \\ A_{21} & A_{22} & A_{23} & 0 \\ A_{31} & A_{32} & A_{33} & 0 \\ v_1 & v_2 & v_3 & 1 \end{bmatrix} \in GL_4(\mathbb{R})$$

Sea $X = (x_1, x_2, x_3) \in \mathbb{R}^3$. Denote $(X, 1) = ((x_1, x_2, x_3, 1) \in \mathbb{R}^4$. Observe que

$$(X, 1) \cdot F = (R_A(X) + V, 1) \in \mathbb{R}^4.$$

De esta forma, F representa a f. La composición de dos isometrías, como las representadas por $F_1 = \begin{bmatrix} A_1 & 0 \\ V_1 & 1 \end{bmatrix}$ y $F_2 = \begin{bmatrix} A_2 & 0 \\ V_2 & 1 \end{bmatrix}$, es la isometría representada por el producto:

$$\begin{bmatrix} A_1 & 0 \\ V_1 & 1 \end{bmatrix} \cdot \begin{bmatrix} A_2 & 0 \\ V_2 & 1 \end{bmatrix} = \begin{bmatrix} a_1 \cdot A_2 & 0 \\ R_{A_2}(V_1) + V_2 & 1 \end{bmatrix}.$$

La multiplicación de matrices es bastante útil aquí. Nos permitió ver de inmediato que la isometría $X \to R_{A_1}(X) + V_1$ seguida de la isometría $X \to R_{A_2}(X) + V_2$ es la isometría $X \to R_{A_1 \cdot A_2}(X) + R_{A_2}(V_1) + V_2$.

Las ideas anteriores también funcionan para valores de n distintos de 3. Concluimos que $\mathrm{Isom}(\mathbb{R}^n)$ es isomorfo al siguiente subgrupo de $GL_{n+1}(\mathbb{R})$:

$$\mathrm{Isom}(\mathbb{R}^n) \cong \left\{ \begin{bmatrix} A & 0 \\ V & 1 \end{bmatrix} : \ A \in O(n) \text{ y } V \in \mathbb{R}^n \right\}.$$

Observe que el siguiente subgrupo de $\mathrm{Isom}(\mathbb{R}^n)$ es isomorfo a $((\mathbb{R}^n), +)$, que denota $\mathbb{R}^n$ bajo la operación de grupo de la adición de vectores:

$$\mathrm{Trans}(\mathbb{R}^n) = \left\{ \begin{bmatrix} I & 0 \\ V & 1 \end{bmatrix} : \quad V \in \mathbb{R}^n \right\}.$$

Este es el grupo de isometrías de $\mathbb{R}^n$ que solo trasladan y no rotan. Es interesante que $((\mathbb{R}^n), +)$ sea isomorfo a un grupo de matrices.

Capítulo 5

Matrices cuasi ortogonales y construcciones clásicas

5.1. Definición de las matrices cuasi ortogonales

Hasta el momento se han revisado características importantes del grupo ortogonal de matrices. Ahora es preciso definir a las matrices de este grupo, pues de hecho al grupo ortogonal se le llama así por las propiedades de estas matrices relacionadas con la ortogonalidad de vectores. Con el concepto de ortogonalidad de vectores se pueden definir este tipo de matrices. Decimos que una matriz $A \in GL_n(\mathbb{K})$ es *ortogonal* si sus filas forman una base ortonormal del espacio $\mathbb{K}^n$, es decir, si son vectores con norma igual a 1 y son mutuamente ortogonales. Esto es, para $i \neq j$, se cumple que $\langle(\text{fila } i \text{ de } A) \cdot (\text{fila } j \text{ de } A)\rangle = 0$, y para $i = j$ se tiene que $\langle(\text{fila } i \text{ de } A) \cdot (\text{fila } i \text{ de } A)\rangle = \mid \text{fila } i \text{ de } A \mid^2 = 1$. O equivalentemente, decimos que A es una matriz ortogonal si $A \cdot A^* = I$, donde I denota la matriz identidad correspondiente, por el inciso (iv) de la proposición 5.

De esta observación es sencillo concluir que la inversa de la matriz A coincide con su matriz conjugada transpuesta A^*. Y para el caso $\mathbb{K} = \mathbb{R}$, la inversa de A coincide con su transpuesta. Así que la obtención de la inversa de esta matriz se puede

calcular rápidamente. En general, esta propiedad es de constante interés dentro del estudio del Álgebra Lineal y sus aplicaciones. Como ya revisamos, las matrices ortogonales poseen ciertas propiedades algebraicas y geométricas destacadas y útiles, sin embargo existen varias generalizaciones de las matrices ortogonales que aparecen de manera frecuente en algunas áreas de aplicación. Por ejemplo, sea $A \in GL_n(\mathbb{K})$ tal que

$$A \cdot A^T = A^T \cdot A = \lambda I_n, \tag{5.1}$$

para algún $\lambda \in \mathbb{K}$, y que este escalar λ esté relacionado con los valores de la misma matriz A o con su tamaño. A este grupo de matrices las denominaremos *matrices cuasi ortogonales*. También existen otros tipos de generalizaciones que para algunos autores resultan iguales o les llaman igual, éstas son la matrices ortogonales y rotaciones generalizadas. En lo sucesivo trataremos con matrices cuasi ortogonales pues es claro que si $\lambda = 1$ entonces se tendrían en particular a las matrices ortogonales, por lo que las matrices cuasi ortogonales resultan una generalización sencilla de estas últimas. Una clase importante de matrices cuasi ortogonales es el conjunto de matrices Hadamard.

5.2. Matrices Hadamard

Una *matriz de Hadamard* H de orden n es una matriz cuadrada con entradas ± 1 tales que

$$HH^T = nI_n, \tag{5.2}$$

donde H^T es la matriz traspuesta de H, y I_n es la matriz identidad de orden n. En particular, las matrices de Hadamard son un tipo de matrices cuasi ortogonales, más aún, por la definición anterior las filas de H son mutuamente ortogonales. Los

ejemplos para los órdenes más pequeños $n = 1, 2$ y 4 son

$$(1), \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}.$$

El estudio inicial de las matrices Hadamard se remonta a más de 150 años, cuando Sylvester publicó algunos primeros ejemplos (1867) de orden 2^t (Horadam, 2011). Entre sus estudios se destaca la propiedad de que si H es una matriz Hadamard, entonces

$$\begin{bmatrix} H & H \\ H & -H \end{bmatrix} \tag{5.3}$$

también lo es. En los ejemplos de arriba se utilizó esta *construcción*. Hacia 1893, el matemático Hadamard publicó ejemplos para los órdenes 12 y 20, con lo que mostró que estas matrices, que llevan su nombre, podrían existir en otros órdenes distintos a potencias de 2. También trabajó buscando el máximo determinante de matrices cuadradas cuyas entradas toman un valor de una infinidad de valores posibles en el disco unitario, y finalmente mostró que este determinante máximo $n^{n/2}$ se alcanza por matrices con entradas de $\{\pm 1\}$ si y solamente si esta matriz es Hadamard. Su aporte más significativo fue demostrar que estas matrices existen sólo si $n = 1, 2$ o es múltiplo de 4. Esto abrió un gran campo de investigación y uno de los problemas más antiguos sin resolver: dada $n = 1, 2$ o que sea múltiplo de 4, ¿existe una matriz Hadamard de este orden? Esto se conoce como la Conjetura de Hadamard y es uno de los problemas abiertos más antiguos de las matemáticas.

Otro de los problemas a resolver que ha provocado una intensa investigación al respecto es cómo construir matrices de gran tamaño que preserven la propiedad dada por la ecuación (5.1) (Horadam, 2011). Existe una gran cantidad de técnicas de construcción de matrices Hadamard, pero hasta ahora, no se conoce ninguna secuencia aritmética infinita cuyos términos sean órdenes de la matrices Hadamard. Sin embargo, si es posible clasificar estas técnicas en tres gandes clases:

1. Métodos usando teoremas de recursión o multiplicación,

2. Métodos *plug-in*,

3. Métodos directos.

Para los dos primeros, el fundamento principal es *el producto tensorial*, también llamado producto directo o producto de Kronecker. Sean $A = [a_{ij}]$ una matriz de orden m y $B_1, B_2, \cdots, B_m$ matrices de orden n. Su producto tensorial es la matriz cuadrada de orden mn, definida por

$$A \otimes [B_1, B_2, \cdots, B_m] = \begin{bmatrix} a_{11}B_1 & a_{12}B_1 & \cdots & a_{1m}B_1 \\ a_{21}B_2 & a_{22}B_2 & \cdots & a_{2m}B_2 \\ \vdots & \vdots & \cdots & \vdots \\ a_{m1}B_m & a_{m2}B_m & \cdots & a_{mm}B_m \end{bmatrix}, \tag{5.4}$$

o $A \otimes B = [aijB]$, donde $B = B_1 = B_2 = \cdots = B_m$.

5.3. Construcciones clásicas de matrices Hadamard

Se denomina *construcción* al algoritmo, técnica o metodología empleada para conseguir una matriz Hadamard, que en general utiliza otras matrices con ciertas formas o propiedades adicionales y que genera toda una familia, finita o infinta, de matrices Hadamard. Existen cuatro familias importantes de matrices Hadamard, descubiertas y estudiadas ampliamente durante el siglo pasado. Estas familias son la base principal de la extensa variedad de construcciones. Es son las familias de Sylvester, de Paley, y de Williamson y los diseños Hadamard (Verde Star, 2019).

De la definición dada en 5.1 y de la propiedad 5.2, se obtienen algunas construcciones elementales:

Proposición 12.

Sea H una matriz Hadamard de orden n, como en 5.1, su inversa está dada por $H^{-1} = n^{-1}H^T$, entonces

(i) la *negación* $-H$ de H es una matriz Hadamard;

(ii) la traspuesta H^T de H es una matriz Hadamard;

(iii) si M es una matriz Hadamard de orden m, el producto tensorial $M \otimes H$ es una matriz Hadamard de orden mn;

(iv) y sea la matriz $\mathcal{S}_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, entonces, para $t \geq 1, (\otimes^t \mathcal{S}_1) \otimes H$ es una matriz Hadamard de orden $2^t n$.

Definimos como *matrices Sylvester-Hadamard* a las matrices en la familia dada en el inciso (iv) $\{\mathcal{S}_t = \otimes^t \mathcal{S}_1 : t \geq 1\}$. Estas matrices han llegado a tener tantas descripciones alternativas casi como sus aplicaciones, y fueron de las primeras en estudiarse, todas estas son de orden $2^t t$ para $t \geq 1$ y son simétricas.

La siguiente clase de matrices Hadamard importante fue descubierta por Paley usando los residuos cuadráticos de cierto grupo finito $GF(q)$ de orden impar. Se define al *carácter cuadrático* χ de $g \in GF(q)$ como 1 si g es un residuo cuadrático en $GF(q)$, -1 si g es un residuo no cuadrático y 0 para $g_0 = 0$.

Proposición 13.

Para q una potencia de un número primo impar y $GF(q) = \{g_0 = 0, g_1, \ldots, g^{q-1}\}$, sea $Q = [\chi(g_i - g_j)]$ con $0 \leq i, j < q$, que en ocasiones se llama *matriz Jacobsthal*. Y sea

$$S = \begin{bmatrix} 0 & \mathbf{1} \\ \mathbf{1}^T & Q \end{bmatrix}$$

una matriz $(q+1) \times (q+1)$, donde $\mathbf{1}$ es un vector fila de unos. Entonces,

(i)(Matriz Paley-Hadamard tipo I). Si $q \equiv 3 \bmod 4$, entonces

$$P_q = \begin{bmatrix} \mathbf{1} & -\mathbf{1} \\ \mathbf{1}^T & Q + I_q \end{bmatrix},$$

es una matriz Hadamard de orden $q + 1$.

(ii)(Matriz Paley-Hadamard tipo II). Si $q \equiv 1 \bmod 4$, entonces

$$P'_q = \begin{bmatrix} S + I_{q+1} & S - I_{q+1} \\ S - I_{q+1} & -S - I_{q+1} \end{bmatrix},$$

es una matriz Hadamard de orden $2(q + 1)$.

Observe que la matriz Q es antisimétrica ($Q^T = -Q$) cuando $q \equiv 3 \bmod 4$ y simétrica cuando $q \equiv 1 \bmod 4$. Construyamos un ejemplo. Los residuos cuadráticos de $GF(7)$ son 1, 2 y 4 y la matriz Q es antisimétrica, entonces la matriz Paley-Hadamard Tipo 1 P_7 de orden 8 es

$$P_5 = \begin{bmatrix} 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \end{bmatrix},$$

Es posible extender esta familia de matrices. Consideremos los conjuntos $\{q_i, i \in I\}$ y $\{q'_i, j \in J\}$ de potencias primas congruentes a 3 mod 4 y 1 mod 4, respectivamente, entonces la matriz de la forma

$$(\otimes_{i \in I} P_{q_i}) \otimes (\otimes_{j \in J} P'_{q'_i}),$$

es una matriz Hadamard de orden $\prod_{i\in I}(q_i+1)\prod_{j\in J}2(q'_j+1)$. A toda esta famila de matrices las definimos como *matrices Paley-Hadamard*.

Otra construcción clásica corresponde a la construcción de la familia de matrices Williamson, esta es la más sencilla de los poderosos métodos llamados *plug-in* o de inserción para encontrar matrices Hadamard. Esta construcción maximiza el uso de tensores como generadores de matrices Hadamard, permitiendo remplazos de la matriz B_i dada en 5.3 por otras matrices que no sean matrices Hadamard necesariamente. A continuación se muestra la proposición que construye toda esta familia.

Proposición 14.

Si existen matrices cuyas entradas son $\{\pm 1\}$ A, B, C, D de orden w las cuales satisfacen

$$XY^T = YX^T \text{ para } X \neq Y \in \{A, B, C, D\},$$

y

$$AA^T + BB^T + CC^T + DD^T = 4wI_w,$$

entonces

$$\begin{bmatrix} A & B & C & D \\ B & -A & D & -C \\ C & -D & -A & B \\ D & C & -B & -A \end{bmatrix}$$

es una matriz Hadamard de orden $4w$.

A esta familia de matrices se llaman *matrices Williamson*. El principal medio por el cual se han encontrado matrices Williamson ha sido por las intensas investigaciones en algoritmos computacionales (Verde Star, 2019).

La última clase de matrices clásicas son los *diseños Hadamard*, las cuales son construidas directamente a partir de diseños de bloques cuadrados, basado en teoría de diseño combinatorio.

Capítulo 6

Construcción de matrices cuasi ortogonales por bloques

6.1. Construcción de matrices cuasi ortogonales por bloques

A continuación se presenta un tipo de construcción que utiliza matrices con entradas complejas a la que denominaremos simplemente como *construcción por bloques*. Esta construcción utiliza solamente transposiciones y cambios de signo de matrices en bloques. La caracterización de matrices cuasi ortogonales, las definiciones y proposiciones fueron tomadas del artículo de investigación (Verde Star, 2019), sobre construcciones de matrices cuasi ortogonales.

Se denota por $\mathcal{M}_n$ al conjunto de todas las matrices de tamaño n, para algún entero positivo n, con entradas complejas y se definen las funciones c y c^*:

$$c(A,B) = \begin{bmatrix} A & -B \\ B & A \end{bmatrix}, \quad c^*(A,B) = \begin{bmatrix} A & B \\ -B & A \end{bmatrix}, \tag{6.1}$$

donde las matrices A, B son matrices cuadradas del mismo tamaño. Las funciones

c y c^* van de $\mathcal{M}_n \times \mathcal{M}_n$ a $\mathcal{M}_n$, para un entero positivo n. Existe una relación entre ambas funciones: $c^*(A,B) = c(A,-B)$. Asímismo, observe que dadas otras dos matrices $C, D \in \mathcal{M}_n$ se cumple que

$$\begin{aligned} c(A,B)c(C,D) &= \begin{bmatrix} A & -B \\ B & A \end{bmatrix} \begin{bmatrix} C & -D \\ D & C \end{bmatrix} \\ &= \begin{bmatrix} AC - BD & -(AD + BD) \\ AD + BC & AC - BD \end{bmatrix} \\ &= c(AC - BD, AD + BC), \end{aligned} \tag{6.2}$$

y también,

$$\begin{aligned} c(A,B)c^*(A,B) &= \begin{bmatrix} A & -B \\ B & A \end{bmatrix} \\ &= \begin{bmatrix} A & -B \\ B & A \end{bmatrix} \begin{bmatrix} A & B \\ -B & A \end{bmatrix} \\ &= \begin{bmatrix} A^2 + B^2 & -(BA - AB) \\ BA - AB & A^2 + B^2 \end{bmatrix} \\ &= c(A^2 + B^2, BA - AB). \end{aligned} \tag{6.3}$$

Con ayuda de c y c^* es posible dar una definición para matrices cuasi ortogonales, a través de su construcción por bloques.

Sea $R \in \mathcal{M}_{2n}$ una matriz, diremos que R es una **matriz cuasi ortogonal** si y solamente si $R = c(A,B)$ para algunas matrices $A, B \in \mathcal{M}_n$ y se cumple que $c(A,B)c^*(A,B) = \lambda I_{2n}$ para algún $\lambda \in \mathbb{C}$, distinto a cero. Si para una matriz cuasi ortogonal se cumple que $\lambda = 1$ entonces la llamaremos **rotación generalizada**.

Esta definición de una matriz cuasi ortogonal se obtiene de última igualdad de la ecuación (12), para la que se cumple que

$$c(A,B)c^*(A,B) = c(A^2 + B^2, BA - AB) = \lambda I_{2n}. \tag{6.4}$$

Si por ejemplo,

$$A = B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

entonces,

$$\begin{aligned} c(A,B)c^*(A,B) &= c(A^2+B^2, BA-AB) \\ &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = 2I_4 \end{aligned}$$

Observe que en este ejemplo, las matrices A y B, conmutan entre sí. Ahora suponga que dadas las matrices $A, B, C, D \in \mathcal{M}_n$ son tales que $c(A,B)$ y $c(C,D)$ son matrices cuasi ortogonales y que las matrices A, B, C, D conmutan entre sí, entonces se tiene que

$$\begin{aligned} c(A,B)c(C,D) &= c(AC-BD, AD+BC) \\ &= c(CA-DB, CB+AD) \\ &= c(C,D)c(A,B). \end{aligned}$$

Es decir, las matrices $c(A,B)$ y $c(C,D)$ también conmutan entre sí. Por lo que $c(C,D)c(A,B) - c(A,B)c(C,D) = 0_n$, donde 0_n denota la matriz de tamaño n con entradas idénticamente iguales a cero. Si además se cumple que $A^2 + B^2 = \lambda_1 I_n$ y $C^2 + D^2 = \lambda_2 I_n$, para algunos λ_1, $\lambda_2 \in \mathbb{C}$, distintos de cero, entonces,

$$\begin{aligned} (AC-BD)^2 + (AD+BC)^2 &= A^2C^2 - 2ABCD \\ &\quad + B^2D^2 + A^2D^2 + 2ABCD + B^2C^2 \\ &= (A^2+B^2)(C^2+D^2) \\ &= (\lambda_1 I_n)(\lambda_2 I_n) \\ &= \lambda I_n, \quad \text{con } \lambda \in \mathbb{C}. \end{aligned}$$

De lo anterior, se tiene que

$$c(c(A,B)c(C,D))c^*(c(A,B)c(C,D)) = c(\lambda I_n, 0_n) = \lambda I_{2n},$$

donde I_{2n} denota la matriz identidad de tamaño $2n$. Por tanto, el producto $c(A,B)c(C,D)$ también es cuasi ortogonal. Esto se puede seguir de la definición de cuasi ortogonalidad, tomando en cuenta las propiedades de A, B, C, D. De la discución anterior, conseguimos una caracterización importante para las matrices cuasi ortogonales, que se resume en el siguiente lema.

Lema 15. Una matriz $R = c(A,B) \in \mathcal{M}_{2n}$ es cuasi ortogonal si y solamente si las matrices A y B conmutan y se cumple que $A^2 + B^2 = \lambda I_n$ para algún escalar $\lambda \in \mathbb{C}$ no cero.

Definimos otro par más de funciones, s y s^*, como sigue. Si A y B son matrices cuadradas del mismo tamaño definimos

$$s(A,B) = \begin{bmatrix} A & B \\ B & A \end{bmatrix}, \qquad s^*(A,B) = \begin{bmatrix} A & -B \\ -B & A \end{bmatrix}. \tag{6.5}$$

Cada una de estas funciones manda un par de matrices cuadradas de $\mathcal{M}_n$ a una matriz en bloques simétrica en $\mathcal{M}_{2n}$, para cualquier entero positivo n. De s podemos definir las permutaciones por columnas y por renglones. Si multiplicamos la matriz $T \in \mathcal{M}_n$ por la matriz $s(0, I_n)$ del lado izquierdo entonces obtenemos una matriz en la que se han permutado las columnas de T. Si, por el contrario, multiplicamos la matriz T por $s(0, I_n)$, con esta última del lado derecho, entonces obtenemos una matriz en la que se han permutado los renglones la matriz T. Luego, tenemos que

$$s(0, I_n)c(A,B)s(0, I_n) = c(A,B) \quad A, B \in \mathcal{M}_n. \tag{6.6}$$

Por lo que las matrices $c(A,B)$ y $c^*(A,B)$ son similares, puesto que $(s(0,In))^2 = I_{2n}$. Como consecuencia las matrices $c(A,B)$ y $c^*(A,B)$ poseen el mismo determinante y el mismo polinomio característico. Por lo tanto, si $c(A,B)c^*(A,B) = \lambda I_{2n}$, entonces $\det(c(A,B))^2 = \lambda$.

Observe que si las matrices A y B conmutan entre sí, entonces $s(A,B)$ y $s^*(A,B)$ conmutan entre sí:

$$\begin{aligned} s(A,B)s^*(A,B) &= \begin{bmatrix} A & B \\ B & A \end{bmatrix} \begin{bmatrix} A & -B \\ -B & A \end{bmatrix} \\ &= \begin{bmatrix} A^2 - B^2 & -AB + BA \\ -AB + BA & A^2 - B^2 \end{bmatrix} \\ &= \begin{bmatrix} A^2 - B^2 & -BA + AB \\ -BA + AB & A^2 - B^2 \end{bmatrix} \\ &= \begin{bmatrix} A & -B \\ -B & A \end{bmatrix} \begin{bmatrix} A & B \\ B & A \end{bmatrix} \\ &= s^*(A,B)s(A,B). \end{aligned}$$

Ahora notemos que si A y B conmutan, entonces,

$$\begin{aligned} s(A,B)^2 &= \begin{bmatrix} A & B \\ B & A \end{bmatrix} \begin{bmatrix} A & B \\ B & A \end{bmatrix} \\ &= \begin{bmatrix} A^2 + B^2 & AB + BA \\ BD + AB & A^2 + B^2 \end{bmatrix} \\ &= \begin{bmatrix} A^2 + B^2 & 2AB \\ 2AB & A^2 + B^2 \end{bmatrix} \\ &= s(A^2 + B^2, 2AB). \end{aligned} \tag{6.7}$$

Y similarmente, $s^*(A,B)^2 = s(A^2+B^2, -2AB)$. Al sumar estos dos resultados obtenemos que

$$\begin{aligned} s(A,B)^2 + s^*(A,B)^2 &= \begin{bmatrix} A^2+B^2 & 2AB \\ 2AB & A^2+B^2 \end{bmatrix} + \begin{bmatrix} A^2+B^2 & -2AB \\ -2AB & A^2+B^2 \end{bmatrix} \\ &= 2\begin{bmatrix} A^2+B^2 & 0_n \\ 0_n & A^2+B^2 \end{bmatrix}. \end{aligned} \tag{6.8}$$

Observe que esta suma $s(A,B)^2 + s^*(A,B)^2$ es igual a $2\lambda I_{2n}$ si se cumple la misma hipótesis adicional de la caracterización de matrices cuasi ortogonales, dada en el Lema 15, esta es que $A^2+B^2 = \lambda I_n$. De esta observación, y lo dicho anteriormente, obtenemos el siguiente lema.

Lema 16. (Verde Star, 2019) Sean $A, B \in \mathcal{M}_n$ tales A y B conmutan y $A^2+B^2 = \lambda I_n$ para algún escalar $\lambda \in \mathbb{C}$ no cero. Entonces $s(A,B)$ y $s^*(A,B)$ conmutan y $s(A,B)^2 + s^*(A,B)^2 = 2\lambda I_{2n}$.

Si una matriz R es cuasi ortogonal como una construcción por bloques, como en el Lema 15, entonces existen matrices $A, B \in \mathcal{M}_n$ tales que $R = c(A,B)$, A y B conmutan y $A^2+B^2 = \lambda I_n$, para algún $\lambda \in \mathbb{C}$ no cero. Luego, por el Lema 16, se tiene que $s(A,B)$ y $s^*(A,B)$ también conmutan y $s(A,B) + s^*(A,B) = 2\lambda I_{2n}$, con la misma λ. De nueva cuenta por el Lema 15, se obtiene que $c(s(A,B), s^*(A,B))$ es una matriz cuasi ortogonal. Hemos obtenido el siguiente resultado.

Teorema 17. Sea $c(A,B) \in \mathcal{M}_{2n}$ una matriz cuasi ortogonal. Entonces, $c(s(A,B), s^*(A,B))$ es una matriz cuasi ortogonal en $\mathcal{M}_{4n}$, de tamaño $4n$ con entradas complejas.

Si repetimos este argumento y aplicamos los lemas 15 y 16 repetidamente, es posible construir matrices de tamaño 2^m para un entero positivo m. Extenda-

mos las propiedades de las funciones s y $s*$ considerando otra construcción por bloques $\sigma_m(A,B)$, como sigue. Sean $\sigma_0(A,B) = (A,B)$, para $A,B \in \mathcal{M}_n$, y $\sigma_1(A,B) = (s(A,B), s^*(A,B))$. Para $m \geq 1$ la definimos de manera recursiva como $\sigma_m(A,B) = (s(\sigma_{m-1}(A,B)), s^*(\sigma_{m-1}(A,B)))$. El tamaño de la matriz construida está indicado por m, pues $\sigma_m(A,B) \in \mathcal{M}_{n2^m}$. Escribiendo $\sigma_m(A,B)$ como $\sigma_m(A,B) = (\sigma_{m,1}(A,B), \sigma_{m,2}(A,B))$ esto permite observar que $\sigma_{m,1}(A,B)$ y $\sigma_{m,2}(A,B)$ son matrices que también son construidas por bloques y todos sus bloques están en $\{A,B,-A,-B\}$. Con esta notación podemos resumir lo anterior en el siguiente resultado.

Teorema 18. Sean A y B dos elementos de $\mathcal{M}_n$ tales que A y B conmutan y $A^2 + B^2 = \lambda I_n$, para algún λ distinto de cero. Entonces para cada entero no negativo m, las matrices $\sigma_{m,1}(A,B)$ y $\sigma_{m,2}(A,B)$ conmutan y satisfacen que

$$(\sigma_{m,1}(A,B))^2 + (\sigma_{m,2}(A,B))^2 = 2^m \lambda I_{n2^m}$$

y por lo tanto $c(\sigma_m(A,B))$ es una matriz cuasi ortogonal de $\mathcal{M}_{n2^{m+1}}$, de tamaño $n2^{m+1}$ con entradas complejas, construida con bloques de $\{A,B,-A,-B\}$.

Por ejemplo, si $A = B = [\sqrt{2}/2]$, se cumple que $A^2 + B^2 = 1$, y por lo tanto

$$c(\sigma_0(A,B)) = c(A,B) = \begin{bmatrix} A & -B \\ B & A \end{bmatrix} = \begin{bmatrix} \sqrt{2}/2 & -\sqrt{2}/2 \\ \sqrt{2}/2 & \sqrt{2}/2 \end{bmatrix}, \tag{6.9}$$

es una matriz cuasi ortogonal por el Lema 15. De hecho es ortogonal puesto que en este caso $\lambda = 1$, y también es del grupo ortogonal especial puesto que $\det A = 1$. Por el Lema 16, se sabe que $s(A,B)$ y $s^*(A,B)$ conmutan y además $s(A,B)^2 + s^*(A,B)^2 = 2I_2$. Aplicando el Teorema 17, la siguiente matriz es también cuasi

ortogonal en $\mathcal{M}_4$.

$$c(\sigma_1(A,B)) = c(s(A,B), s^*(A,B)) = \left[\begin{array}{cc|cc} A & B & -A & B \\ B & A & B & -A \\ -- & -- & -- & -- \\ A & -B & A & B \\ -B & A & B & A \end{array}\right]$$

$$= \left[\begin{array}{cc|cc} \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 \\ \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 \\ -- & -- & -- & -- \\ \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 \\ -\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 \end{array}\right], \tag{6.10}$$

Ahora, al aplicar los lemas 15 y 16 nuevamente, por el teorema 18, las matrices $\sigma_{2,1}(A,B)$ y $\sigma_{2,2}(A,B)$ conmutan y satisfacen que $(\sigma_{2,1}(A,B))^2 + (\sigma_{2,2}(A,B))^2 = 2^2\lambda I_{2^2} = 4\lambda I_4$. Y por tanto, la matriz $c(\sigma_2(A,B))$ es también una matriz cuasi ortogonal y se muestra a continuación. Como

$$s(\sigma_1(A,B)) = \left[\begin{array}{cc|cc} A & B & A & -B \\ B & A & -B & A \\ -- & -- & -- & -- \\ A & -B & A & B \\ -B & A & B & A \end{array}\right]$$

y

$$s^*(\sigma_1(A,B)) = \left[\begin{array}{cc|cc} A & B & -A & B \\ B & A & B & -A \\ -- & -- & -- & -- \\ -A & B & A & B \\ B & -A & B & A \end{array}\right],$$

entonces se tiene que

$$
\begin{aligned}
c(\sigma_2(A,B)) &= c(\sigma_{2,1}(A,B), \sigma_{2,2}(A,B)) \\
&= \left[\begin{array}{cc|cc|cc|cc}
A & B & A & -B & -A & -B & A & -B \\
B & A & -B & A & -B & -A & -B & A \\
-- & -- & -- & -- & -- & -- & -- & -- \\
A & -B & A & B & A & -B & -A & -B \\
-B & A & B & A & -B & A & -B & -A \\
-- & -- & -- & -- & -- & -- & -- & -- \\
A & B & -A & B & A & B & A & -B \\
B & A & B & -A & B & A & -B & A \\
-- & -- & -- & -- & -- & -- & -- & -- \\
-A & B & A & B & A & -B & A & B \\
B & -A & B & A & -B & A & B & A
\end{array}\right] \\
&= \left[\begin{array}{cc|cc|cc|cc}
\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & -\sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 \\
\sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & -\sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 \\
--- & --- & --- & --- & --- & --- & --- & --- \\
\sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & -\sqrt{2}/2 & -\sqrt{2}/2 \\
-\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & -\sqrt{2}/2 \\
--- & --- & --- & --- & --- & --- & --- & --- \\
\sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 \\
\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 \\
--- & --- & --- & --- & --- & --- & --- & --- \\
-\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 \\
\sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & -\sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2 & \sqrt{2}/2
\end{array}\right]
\end{aligned}
\tag{6.11}
$$

Resumiendo el ejemplo, la matriz en (6.9) es una matriz cuasi ortogonal en $\mathcal{M}_2$, es decir de tamaño 2 y además es ortogonal especial, o del grupo especial ortogonal

$\mathcal{O}_2$, y es una matriz Toeplitz por la naturaleza del ejemplo. Las matrices en (6.10) son cuasi ortogonales en $\mathcal{M}_4$, y finalmente, las matrices en (6.11) son matrices cuasi ortogonales en $\mathcal{M}_8$. Debido a que en el ejemplo la $\lambda = 1$, todas las matrices anteriores son también matrices ortogonales. Siguiendo el Teorema 18, es posible obtener matrices cuasi ortogonales, y ortogonales de manera particular, en $\mathcal{M}_{n2^{m+1}}$.

Capítulo 7

Aplicaciones

Las matrices cuasi ortogonales son utilizadas ampliamente en la codificación de información, sobre todo en comunicación inalámbrica, procesamiento de imágenes y señales, o en áreas básicas de matemáticas como en Combinatoria. El tema no se limita al procesamiento de imágenes para métodos de compresión, ahora también tiene aplicaciones interdisciplinarias, como biomedicina, robótica, técnicas de marca de agua en esteganografía(Gorbachev et al., 2018). Estas son útiles para que las imágenes o incluso una señal similar a un ruido se almacenen en forma comprimida antes de ser transferidas a través de un enlace de comunicación o la línea inalámbrica, después se pueden editar mediante redimensionamiento o rotación. A continuación revisamos brevemente algunas aplicaciones de las matrices cuasi ortogonales y de las construcciones por bloques.

7.1. Procesamiento de imágenes

En procesamiento de imágenes en escala de grises es útil el uso de matrices ortogonales. Dada una trasformación ortogonal de una imagen digital esta puede representarse mediante un conjunto de imágenes para que sea una base ortonormal y puede ser procesada usando transformaciones ortogonales (Gorbachev et al., 2018). En distintos artículos de investigación se puede encontrar que esta representación permite trabajar con nuevas características con respecto a la dispersión

de datos. Para tal representación, se considera que la dispersión de datos digitales es importante en las aplicaciones, particularmente para las técnicas robustas de marca de agua. Se puede trabajar con una matriz de bloques, cuyos elementos son imágenes base. Esta matriz resulta útil para la representación de matrices multidimensionales, que pueden describir un conjunto de imágenes digitales.

Dada una cadena digital de datos estos se pueden transformar por la matrices cuasi ortogonales. Considerando la transformación ortogonal de los datos digitales, se pueden establecer dos propiedades sobre la distribución de datos. Se están dispersando y concentrando para ser útiles para los problemas de procesamiento de imágenes.

7.2. Comunicación Inalámbrica

La teoría de los diseños ortogonales se remonta a más de un siglo. Una de las primeras aplicaciones de los diseños ortogonales complejos fue para construir códigos de bloque de espacio-tiempo (STBC), que se utilizan para transmitir datos a través de canales inalámbricos de múltiples antenas de transmisión (Seberrya et al., 2005). Es posible dar una introducción a la codificación de bloques espacio-tiempo, y encontrar distintas técnicas de construcción para diseños ortogonales de procesamiento al complejo generalizado.

En algunos artículos realcionados con la comunicación inalámbrica es posible encontrar el uso de diseños ortogonales. Se define un *diseño ortogonal generalizado* de tipo $(s_1, s_2, \ldots, s_k)$ como una matriz A cuyas entradas están en el conjunto $X = \{0, \pm x_1, \pm x_2, \ldots, \pm x_k\}$ que satisfacen que

$$A^T A = \sum_{i=1}^{k} (s_i {x_i}^2) I_n.$$

En caso que X sea un conjunto de variables reales se dice que A es un *diseño ortogonal generalizado real*. En el caso complejo existen al menos dos de-

finiciones distintas dependiendo de cómo está definido el conjunto X. Si $X = \{0, \pm x_1, \pm x_2, \ldots, \pm x_k, \pm ix_1, \pm ix_2, \ldots, \pm ix_k\}$, entonces una matriz C que satisface que

$$C^H C = \sum_{i=1}^{k} (s_i {x_i}^2) I_n, \tag{7.1}$$

donde H denota el conjugado hermitiano, se dice un *diseño ortogonal complejo.*

El tipo $(s_1, s_2, \ldots, s_k)$ denota el número de repeticiones de cada valor del conjunto X en cada fila (y en cada columna), por lo que s_l son enteros. Así 7.1 puede reescribirse como sigue siguiendo cierta normalización:

$$C^H C = \sum_{i=1}^{k} {x_i}^2 I_n. \tag{7.2}$$

Asimismo, si $X = \{0, \pm z_1, \pm z_2, \ldots, \pm z_k, \pm {z_1}^*, \pm {z_2}^*, \ldots, \pm {z_k}^*\}$, donde z^* denota el conjugado complejo de z, entonces también es posible definir un *diseño ortogonal complejo* como sigue.

$$C^H C = \sum_{i=1}^{k} |z_i|^2 I_n. \tag{7.3}$$

Nótese que las últimas representaciones de los diseños ortogonales tienen la forma dada en 5.1 por lo que los diseños ortogonales son también matrices cuasi ortogonales, no necesariamente cuadradas. La aplicación de los diseños ortogonales en la comunicación inalalámbrica es básicamente para trasformar códigos de bloque de espacio-tiempo en matrices bloque iniciales muy parecidas a las revisadas en el capítulo anterior que al construirse sirven para trasmitir las comunicaciones inalámbricas de múltiples antenas. En (Spence, 1991) y (Seberrya et al., 2005) es posible encontrar mayor información al respecto y el uso un método muy similar de construcción de matrices cuasi ortogonales al que se utlizó con el Teorema 17. utilizando tipos con pocos o ningún ceros, y se discute la compensación entre tener pocos ceros y tasas altas, de sus propuestas de construcción.

Capítulo 8

Conclusiones

En la vida diaria el concepto de matrices es de gran relevancia, ya que las matrices se usan como contenedores para almacenar datos relacionados. Actualmente, las matrices son de mucha utilidad en problemas prácticos de la vida diaria. Sobre todo en aquellos que involucran Sistemas de Ecuaciones Lineales. En general, las matrices sirven para representar simples procesos de producción y flujos de producción. Para administración y finanzas es necesario si se conoce que para las ventas hay que llegar a un punto de equilibrio dado por la suma de utilidad - costos de producción, a groso modo. Como se revisó, en particular las matrices ortogonales y cuasiortogonales son de gran importancia para áreas como comunicación ináambrica o incluso procesamiento de imágenes.

El cálculo de matrices aleatorias de gran tamaño representa un gran costo computaciones, en particular estás matrices permiten transferencia de datos, por ejemplo. Sin embargo, es de particular intéres que las matrices presenten ciertas propiedades para que puedan manejarse de manera óptima. Las matrices ortogonales tienen propiedades básica pero podorosas para el cálculo de su inversa, como se revisó en los capítulos 2 y 3.

Posteriomente, se revisó algunas técnicas que permiten la construcción de estás matrices de forma recursiva y mantienen sus propiedades, en algunos algoritmos se puede lograr que la matriz se ortogonal o en todo caso cuasi-ortogonal.

Paralelo a la investigación se desarrolló un programa que pude consultarse en https://github.com/jbastianrj/computationalstatistics

Bibliografía

A. V. Geramita and J. Seberry. *Orthogonal designs, Lecture notes in pure and applied mathematics, Quadratic forms and Hadamard matrices. (Inglés) [Diseños ortogonales, apuntes de matemáticas puras y aplicadas, formas cuadráticas y matrices de Hadamard].* Marcel Dekker Inc., New York, USA, 1979.

V. Gorbachev, E. Kaynarova, A. Makarov, and E. Yakovleva. On block representations in Image Processing Problems. In *Recopilación la 23a Conferencia de la IEEE FRUCT ASSOCIATION*, pages 128–134, Rusia, 2018.

K. J. Horadam. *Hadamard Matrices and Their Applications. (Inglés) [Matrices Hadamard y sus aplicaciones].* Princeton University Press., USA, 2011.

J. Seberrya, S. A. Spenceb, and T. A. Wysockic. A construction technique for generalized complex orthogonal designs and applications to wireless communications. *Elsevier Inc.*, 405:163–176, 2005. doi: http://dx.doi.org/10.1016/j.laa.2005.03.008.

I. R. Shafarevich and A. O. Remizov. *Linejnaya algebra i geometriya. (Ruso) [Álgebra Linear y Geometría].* Fizmatlit, Moscow, 2009.

A. S. Spence. A journey of discovery: Orthogonal Matrices and Wireless Communications. *American Mathematical Society*, 479, 1991. doi: http://dx.doi.org/10.1090/conm/479.

K. Tapp. *Matrix groups for undergraduates. (Inglés) [Grupos de matriz para estudiantes universitarios.].* American Mathematical Society, Providence, RI, USA, 2005.

L. Verde Star. Construction of generalized rotations and quasi orthogonal matrices. *De Gruyter*, 7:107–113, 2019. doi: https://doi.org/110.1515/spma-2019-0010.