UCLV
Universidad Central
"Marta Abreu" de Las Villas

MFC
Facultad de Matemática
Física y Computación

Departamento de
Matemática

TRABAJO DE DIPLOMA

Título del trabajo: "Equivalencia geométrica de la conjetura de Hadamard"

Autores del trabajo: Carlos M. Bosch Machado

Tutores del trabajo: Dr.C Eberto Morgado.

Santa Clara, junio, 2018

Agradecimientos

A mi tutor, Dr. C. Eberto Morgado por todo su apoyo, dedicación y motivación que hicieron posible realizar este trabajo.

A mis compañeros y amistades, que me ayudaron mucho, que me apoyaron a lo largo del trayecto.

A mis profesores, que me enseñaron todo lo que me permitió llevar a cabo este trabajo.

A mis padres y a Ana Beatriz por su ejemplo cotidiano y empuje constante. A toda mi familia por las fuerzas y los ánimos dados.

A Aisseli, por todo su amor y apoyo incondicional.

RESUMEN

Desde 1893 el matemático francés Jacques S. Hadamard comenzó su estudio sobre las matrices que hoy llevan su nombre, surgió la llamada conjetura de Hadamard, el cual sigue siendo un problema de interés tanto teórico como práctico. En el presente trabajo se hará una reseña sobre los principales resultados conocidos sobre las matrices de Hadamard, así como un resultado propio basado en cierta equivalencia geométrica de la conjetura.

Palabras claves:
Matrices, Hadamard, Grupos, Boole

Contenido

Introducción

El interés por las matrices de Hadamard (aunque fueron consideradas por primera vez en 1867 en un problema de teselaciones), surge a finales del siglo XIX cuando Hadamard demuestra que este tipo de matrices facilitan soluciones para el problema de hallar la matriz cuadrada de orden n con entradas reales $|a_{ij}| < k$ para cierto $k > 0$, de determinante máximo. En verdad, para una matriz A de este tipo, se tiene que $|A| \leq k^n n^{\frac{n}{2}}$, cota que se alcanza para una matriz $k * H$ siendo H una matriz de Hadamard de orden n, Además Hadamard demostró que este tipo de matrices son las únicas que alcanzan dicha cota.[1]

En la actualidad son muchas las aplicaciones de las matrices de Hadamard, ejemplo en la criptografía, para la estimación de caracteres binarios que se alteran (cambian su valor) al recibir un mensaje, o en el uso de la transformada de Walsh-Hadamard, un algoritmo rápido para computar algunas secuencias con buenas propiedades criptográficas o para el procesamiento de imágenes, tanto para compresión con pérdida de pixeles como para algoritmos de inteligencia artificial en la rama de computación afectiva. Más recientemente han venido surgiendo aplicaciones en la computación cuántica que requiere el uso de matrices de Hadamard.[2]

Preguntas científicas:

1. ¿Existen matrices de Hadamard para cualquier orden múltiplo de 4?
2. ¿Cómo construir una matriz de Hadamard de un orden específico?

La primera pregunta veremos que coincide con la conjetura de Hadamard, la cual sigue siendo un problema abierto, de la segunda pregunta se verán algunas construcciones conocidas y se propondrá una construcción la cual no es computacionalmente superior a las conocidas, pero con la capacidad de probar la existencia de una gran cantidad de valores para los cuales existe matriz de Hadamard. Dicho esto, podemos plantear el objetivo general de la tesis.

Objetivo:

- Lograr un avance teórico con respecto a la conjetura de Hadamard, mediante el uso de un enfoque novedoso.

De acuerdo al objetivo señalado se puede establecer que el objeto de investigación es la conjetura de Hadamard y el campo de acción de dicha investigación se va a centrar en las matrices de Hadamard y en cómo construirlas.

Para cumplir con el objetivo planteado se traza un plan de trabajo el cual será:

1. Conocer y profundizar en los principales resultados conocidos sobre matrices de Hadamard y sobre la famosa conjetura.
2. Plantear los fundamentos teóricos que sean necesarios para llevar a cabo el objetivo general
3. Proponer un algoritmo matemático que genere matrices de Hadamard de algunos ordenes, desarrollar ejemplos de dicho algoritmo para observar sus resultados en casos pequeños y manejables por una persona.
4. Demostrar que dicho algoritmo es capaz de generar matrices de Hadamard de orden múltiplo de 8.

Se puede ver reflejado en los puntos 3 y 4 a tratar que hay novedad científica, más adelante veremos algunas cotas asintóticas para la existencia de matrices de Hadamard, las cuales están actualizadas y el resultado final del trabajo presente es cualitativamente superior a las encontradas en bibliografías consultadas.

Capítulo 1: Introducción a las matrices de Hadamard y fundamentos teóricos.

En el presente capítulo se tratarán la mayoría de los resultados conocidos sobre matrices de Hadamard, así como la teoría necesaria para llegar a resultados que permitirán lograr un avance cualitativo en la conjetura de Hadamard. Se comenzará por aclarar las definiciones lingüísticas y el significado matemático de axiomas, teoremas y conjeturas, luego se desarrollarán todos los fundamentos teóricos que serán necesarios para culminar el trabajo. Por último, se verá la definición de matriz de Hadamard y sus construcciones más frecuentes para algunos tamaños.

1.1 Axiomas, Teoremas y Conjeturas.

Axioma:

Un axioma es una proposición asumida dentro de un cuerpo teórico sobre la cual descansan otros razonamientos y proposiciones deducidas de esas premisas.

Introducido originalmente por los matemáticos griegos del período helenístico, el axioma se consideraba como una proposición “evidente” y que se aceptaba sin requerir demostración previa. La palabra *axioma* proviene del sustantivo griego ἀξίωμα, que significa “lo que parece justo” o, que se le considera evidente, sin necesidad de demostración. El término viene del verbo griego ἀξιόειν (axioein), que significa “valorar”, que a su vez procede de ἄξιος (axios): “valioso” o “digno”. Entre los filósofos griegos antiguos, un axioma era lo que parecía verdadero sin necesidad de prueba alguna.

Limitaciones de los sistemas axiomáticos:

A mediados del siglo XX, Kurt Gödel demostró sus famosos teoremas de incompletitud. Estos teoremas mostraban que, aunque un sistema de axiomas recursivos estuviera bien definido y fuera consistente, los sistemas axiomáticos con esos sistemas de axiomas sufren de limitaciones graves. Es importante notar aquí la restricción de que el sistema de axiomas sea recursivamente enumerable,

es decir, que el conjunto de axiomas forme un conjunto recursivamente enumerable dada una codificación o gödelización de los mismos. Esa condición técnica se requiere ya que si el conjunto de axiomas no es recursivo entonces la teoría ni siquiera será decidible.

Con esa restricción Gödel demostró, que si la teoría admite un modelo de cierta complejidad siempre hay una proposición *P* verdadera pero no demostrable. Gödel prueba que en cualquier sistema formal que incluya aritmética puede generarse una proposición *P* mediante la cual se afirme que *este enunciado no es demostrable*.

Teorema:

Un teorema es una proposición que afirma una verdad demostrable. En matemáticas, es toda proposición que partiendo de un supuesto (hipótesis), afirma una racionabilidad (tesis) no evidente por sí misma.

También puede decirse que un teorema es una fórmula bien formada que puede ser demostrada dentro de un sistema formal, partiendo de axiomas u otros teoremas. Demostrar teoremas es un asunto central en la lógica matemática. Los teoremas también pueden ser expresados en lenguaje natural formalizado.

Los teoremas generalmente poseen un número de premisas que deben ser enumeradas o aclaradas de antemano. La conclusión del teorema es una afirmación lógica o matemática que es verdadera bajo las condiciones dadas. El contenido informativo del teorema es la relación que existe entre las hipótesis y la tesis o conclusión.

Un teorema requiere de un marco lógico; este marco consistirá en un conjunto de axiomas (sistema axiomático) y un proceso de inferencia, el cual permite derivar teoremas a partir de los axiomas y teoremas que han sido derivados, pero no son axiomas.

En lógica proposicional y de primer orden, cualquier afirmación demostrada se denomina teorema. Más concretamente en lógica se llama demostración a una secuencia finita de fórmulas bien formadas (fórmulas lógicas bien formadas) F_1, ..., F_n, tales que cada F_i es o bien un axioma o bien un teorema que se sigue de dos fórmulas anteriores F_j y F_k (tales que $j<i$ y $k<i$) mediante una regla de deducción. Dada una demostración como la anterior si el elemento final F_n no es

un axioma entonces es un teorema. Resumiendo lo anterior puede decirse formalmente, un teorema es una fórmula bien formada, que no es un axioma, y que puede ser el elemento final de alguna demostración, es decir, un teorema es una fórmula bien formada para la cual existe una demostración.

Conjetura:

Por conjetura se entiende el juicio que se forma (moral, ético o matemático) de las cosas o sucesos por indicios y observaciones. En matemáticas, el concepto de conjetura se refiere a una afirmación que se supone cierta, pero que no ha sido probada ni refutada hasta la fecha. Una vez que se demuestra la veracidad de una conjetura, esta pasa a ser considerada un teorema de pleno derecho y puede utilizarse como tal para construir otras demostraciones formales.

1.2 Teoría Previa.

1.2.1- Espacios afines y conjunto de puntos afínmente independientes.

Se dice que un punto P es combinación lineal afín de los n puntos $P_1, P_2, \dots P_n$ si se tiene que existen escalares a_i tales que $P = a_1 * P_1 + a_2 * P_2 + \cdots + a_n * P_n$, siendo $a_1 + a_2 + \cdots + a_n = 1$. Por ejemplo, una recta es el conjunto de los puntos que son combinaciones lineales afines de dos cualesquiera de sus puntos. Un sistema de n puntos $P_1, P_2, \dots, P_n$ es afínmente independiente si ninguno de ellos es combinación lineal afín de los demás. Por ejemplo, un conjunto de tres puntos no colineales, o de cuatro puntos no coplanares, es un conjunto afínmente independiente.

En un espacio de dimensión n se pueden tener sistemas de puntos afínmente independientes de hasta $n + 1$ vectores del espacio.

1.2.2- Producto Kronecker de matrices.

Si $A = (a_{ij})$ es una matriz $m \times m$ y $B_1, B_2, \ldots, B_m$ son matrices $n \times n$, el producto de Kronecker $A \otimes (B_1, B_2, \ldots, B_m)$ es la matriz cuadrada de orden $mn \times mn$ siguiente:

$$\begin{pmatrix} a_{11}B_1 & \cdots & a_{1m}B_m \\ \vdots & \ddots & \vdots \\ a_{m1}B_1 & \cdots & a_{mm}B_m \end{pmatrix}$$

Que es la matriz resultante de multiplicar cada fila de A por el sistema de matrices B_i y escribirlo como matriz en bloque.

En el caso que $B_1 = B_2 = \cdots = B_m = B$ se denota como $A \otimes B$ al producto Kronecker de dos matrices A y B.[3]

1.2.3- Operaciones en $\mathbb{Z}_2$-espacios.

Sea $\mathbb{Z}_2^n$ un espacio vectorial sobre el campo $\mathbb{Z}_2$ sus operaciones son:

El producto por un escalar como producto componente a componente, o sea:

$$\alpha x = (\alpha \odot x_1, \alpha \odot x_2, \ldots, \alpha \odot x_n)$$

Donde $\alpha \odot x_i = \alpha * x_i \, mod\,(2)$.

La suma de vectores, extendida como suma por componentes:

$$x + y = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$$

Donde $x_i \oplus y_i = x_i + y_i \, mod(2)$.

Si además consideramos el producto de vectores como el producto por componentes:

$$x * y = (x_1 \odot y_1, x_2 \odot y_2, \ldots, x_n \odot y_n)$$

El espacio presenta estructura de k-álgebra. Además tiene característica 2 o sea $x + x = 0 \; \forall x \in \mathbb{Z}_2^n$

Esta estructura se puede dotar también de una métrica conocida como distancia de Hamming:

$$d(x,y) = cntB(x+y)$$

Donde $cntB(x) = cantidad\ de\ componentes\ iguales\ a\ 1\ de\ x$.

1.2.4- Matrices de Conferencia.

Un grupo de matrices comunes asociadas a las matrices de Hadamard son las llamadas matrices de conferencia (nombradas así por su aplicación en los circuitos telefónicos).

Una matriz es de conferencia si tiene 0 en su diagonal principal y ± 1 en las demás posiciones y cumple que:

$$C_n C_n^t = (n-1) I_n$$

Se tiene que si C_n es una matriz de conferencia de orden $n > 1$, entonces n es múltiplo de 2.

Además se tienen los resultados que, si C_n es una matriz de conferencia simétrica entonces $H_{2*n} = \begin{pmatrix} I_n + C_n & -I_n + C_n \\ -I_n + C_n & -I_n - C_n \end{pmatrix}$ es una matriz de Hadamard y si C_n es una matriz de conferencia antisimétrica entonces $I_n + C_n$ es una matriz de Hadamard.[4]

1.2.5 – Simplex en un espacio n-dimensional

Concepto de conjunto convexo: Un subconjunto A del espacio $\mathbb{R}^n$ se llama convexo, si para cualesquiera dos puntos P, Q el segmento que los une está contenido en A. La envoltura convexa de un conjunto A es el menor conjunto convexo que contiene a A, esto es equivalente a la intersección de todos los conjuntos convexos que contienen a A.

Concepto de simplex: Un simplex, en el espacio euclidiano $\mathbb{R}^n$, es definido como la envoltura convexa de un conjunto de m puntos, m≤n+1, que sean afínmente independientes.

Simplex Regular: Un simplex se llama regular si la distancia entre dos cualesquiera de sus puntos es la misma. Por ejemplo, son simplexes regulares un triángulo equilátero y un tetraedro regular. Este último es una figura de cuatro vértices y cuatro caras, siendo éstas triángulos equiláteros.

1.3 Matrices de Hadamard.

Fueron inventadas por Sylvester en 1867, aunque en 1893 fueron consideradas por Hadamard y es a él a quien deben su nombre. Una matriz de Hadamard es una matriz cuadrada $n \times n$, de componentes enteros, iguales a -1 o a 1, tal que sus vectores filas son ortogonales(para el producto escalar usual en $\mathbb{R}^n$) dos a dos. Esto significa que el producto escalar de dos cualesquiera de sus filas es igual a cero.[5]

1.3.1- Propiedades.

Hadamard demostró que para una tal matriz el número n es necesariamente igual a 2 o es un múltiplo de 4, esto es, de la forma $n = 4k$, siendo k un número natural. Comparando dos de las filas resulta que la mitad de los componentes adyacentes son del mismo signo mientras que la otra mitad son de signo contrario. Esto implica que n es necesariamente un número par. Una matriz de Hadamard continúa siéndolo si se multiplica por -1 cualquiera de sus filas o de sus columnas. Lo mismo ocurre si se permutan sus filas o sus columnas. Dos matrices de Hadamard se consideran equivalentes si una se obtiene de la otra por permutación de filas o columnas, o cambio de signo de algunas de sus filas o columnas. En cada clase de equivalencia podemos elegir una matriz cuya primera fila está formada solo por unos.

Si H_n es una matriz de Hadamard de $n \times n$, donde la primera fila está formada sólo por unos, entonces $\frac{n(n-1)}{2}$ es el número de entradas iguales a -1 mientras que $\frac{n(n+1)}{2}$ es el número de entradas iguales a 1.

Una matriz de Hadamard de tamaño n es solución del llamado problema del determinante máximo. Es decir, tiene el determinante máximo posible, en valor absoluto, para cualquier matriz compleja con componentes a_{ij} tales que $|a_{ij}| \leq 1$ (Brenner y Cummings 1972). Este máximo valor es $n^{\frac{n}{2}}$. Una definición equivalente de matriz de Hadamard viene dada por la igualdad $H_n H_n^t = nI_n$ donde I_n denota a la matriz identidad y H_n^t es la matriz transpuesta de H_n.

1.3.2 - Métodos de construcción de matrices de Hadamard.

En el presente epígrafe se presentarán algunas de las construcciones más conocidas y a su vez las más simples de matrices de Hadamard, existen muchas más, las cuales se basan en otro tipo de ideas.

Construcción de Sylvester:

Teorema: El producto Kronecker de matrices de Hadamard es una matriz de Hadamard

Luego sea $H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ una matriz de Hadamard de orden 2 pues $H_2 H_2^t = 2I_2$ entonces se puede definir de manera recursiva $H_{2^k} = H_2 \otimes H_{2^{k-1}}$ son matrices de Hadamard de orden potencia de 2. Esta construcción es la más conocida, tiene sus aplicaciones en transformadas discretas donde se utilizan algoritmos basados en la construcción de Sylvester para reducir el tamaño de una imagen con la menor perdida de información posible, también en la criptografía para el cálculo del error aproximado de la cantidad de información que se pierde con respecto al mensaje original.[6]

Construcción de Payley:

Vamos a utilizar una construcción directa de algunas matrices de conferencia para ordenes específicos. En el resto de la presente sección q denotará una potencia positiva de un primo impar. En el campo $\mathbb{GF}_q$ se define la función $\mathcal{X}$ llamada símbolo de Legendre mediante:

$$\mathcal{X}(x) = \begin{cases} 0, & si\ x = 0 \\ 1, si\ \exists\ a \mid a^2 \equiv x \\ -1, si \nexists\ a \mid a^2 \equiv x \end{cases}$$

Enumerando los elementos de $\mathbb{GF}(q)$ como $0 = a_0, a_1, , \dots, a_{q-1}$ defínanse la matriz $Q = (q_{ij})$ de tamaño qxq (llamada matriz de Jacobsthal) mediante:

$$q_{ij} = \mathcal{X}(a_i - a_j), 0 \leq i, j < q$$

Nótese que Q es simétrica si $q \equiv 1\ (mod\ 4)$ y antisimétrica si $q \equiv 3$

$(mod\ 4)$.

Lo cual nos permite formar la matriz $C_{q+1} = \begin{pmatrix} 0 & 1 & \dots & 1 \\ \pm 1 & \dots & \dots & \dots \\ \vdots & \dots & & Q \\ \pm 1 & \dots & & \end{pmatrix}$ donde el signo de la primera columna se escoge de forma tal que la matriz de conferencia sea simétrica o antisimétrica luego se puede asegurar gracias a esto que:

Para todo $q = p^k$ existe una matriz de Hadamard de orden $q + 1$ si $q \equiv 3\ (mod 4)$ y de orden $2(q + 1)$ si $q \equiv 1(mod 4)$.

Ejemplo para $p = 7$:

$$Q = \begin{pmatrix} 0 & 1 & 1 & -1 & 1 & -1 & -1 \\ -1 & 0 & 1 & 1 & -1 & 1 & -1 \\ -1 & -1 & 0 & 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 0 & 1 & 1 & -1 \\ -1 & 1 & -1 & -1 & 0 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 0 \end{pmatrix}$$

Como $7 \equiv 3(mod4)$ entonces $C_8 = \begin{pmatrix} 0 & 1 \\ -1 & Q \end{pmatrix}$ es una matriz de conferencia antisimétrica y $C_8 + I_8$ es una matriz de Hadamard de tamaño 8.[7]

Matrices cocíclica:

Sea $(G,\odot)$ un grupo de $4t$ elementos , $G = \{g_1 = 1, g_2, \dots, g_{4t}\}$. Se define como matriz cocíclica sobre G a la matriz:

$$M_f = \begin{pmatrix} f(g_1,g_1) & f(g_1,g_2) & \cdots & f(g_1,g_{4t}) \\ f(g_2,g_1) & f(g_2,g_2) & \cdots & f(g_2,g_{4t}) \\ \vdots & \vdots & \ddots & \vdots \\ f(g_{4t},g_1) & f(g_{4t},g_1) & \cdots & f(g_{4t},g_{4t}) \end{pmatrix}$$

Cuya entrada (i,j) viene dada por la función $f(g_i,g_j)$, donde f es un 2-ciclo sobre $(G,\odot)$, es decir, una función $f: GxG \to \{1,-1\}$ que cumple:

$$f(g_i,g_j) * f(g_i g_j, g_k) = f(g_j,g_k) * f(g_i, g_j g_k) \qquad \forall 1 \le i,j \le 4t$$

Proposición: Una matriz cocíclica es de Hadamard si y solo si la suma de los elementos de cualquier fila, salvo la primera, es nula, o sea si $\sum_{j=1}^{4t} f(g_i,g_j) = 0$, con $2 \le i \le 4t$.[8]

Es de destacar las ventajas de trabajar con matrices cocíclicas de Hadamard:

1. El test cocíclico, para comprobar que una matriz cociclica es de Hadamard, actúa en $O(t^2)$, mejor que el algoritmo usual para las matrices de Hadamard, no necesariamente cociclicas, que tiene complejidad $O(t^3)$
2. El espacio de búsqueda se reduce de $\binom{4t}{2t}_{4t-1}$ que es el de todas las matrices binarias con la primera fila en 1s y las demás con la mitad de sus componentes 1 y las otras -1 , a 2^s , suponiendo que G tiene una base para 2-cocíclos de tamaño s.[9]

Capítulo 2: Conjetura de Hadamard.

En el presente capítulo se presenta la conjetura de Hadamard con los principales avances que se conocen sobre la misma. Se propone un método de construcción de matrices de Hadamard basado en la inmersión de un 3-simplex en el espacio $\mathbb{Z}_2^n$, luego se tratan varios ejemplos particulares del método y se trata de buscar una regularidad a la hora de generalizar el algoritmo a seguir. Finalmente se formalizan las ideas seguidas durante el proceso de construcción.

2.1 Presentación de la Conjetura y su equivalencia geométrica.

Hadamard demostró que para una tal matriz el número n es necesariamente igual a 1, 2 o es un múltiplo de 4, esto es, de la forma $n = 4k$, siendo k un número natural. Esta demostración se basa en el hecho de que si una matriz H_n es de Hadamard entonces: negar una de sus filas o columnas resulta en una matriz de Hadamard, además permutar filas o columnas resulta también en una matriz de Hadamard. Con esto se puede escribir cualquier matriz de Hadamard de forma que sus tres primeras filas sean:

$$\begin{pmatrix} 1 & 1 & 1 & & 1 & 1 & 1 & & 1 & 1 & 1 & & 1 & 1 & 1 \\ -1 & -1 & -1 & \dots & -1 & -1 & -1 & \dots & 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & 1 & 1 & & -1 & -1 & -1 & & 1 & 1 & 1 & & -1 & -1 & -1 \end{pmatrix}$$

Denominando a los 4 bloques como i, j, k, l se tiene el sistema dado por la ortogonalidad de las filas:

$$\begin{cases} i + j - k - l = 0 \\ i - j + k - l = 0 \\ i - j - k + l = 0 \end{cases}$$

De donde se puede obtener que $i = j = k = l$ luego $n = 4i$ para algún $i \in \mathbb{N}$.[10]

2.1.1- Conjetura de Hadamard:

La conjetura de Hadamard, atribuida a Payley surge a partir de la pregunta de si el reciproco de la demostración de Hadamard de que si existe una matriz de Hadamard de orden mayor que 2 entonces dicha matriz es de orden múltiplo de 4.

Conjetura de Hadamard: Para todo n múltiplo de 4, es decir $n = 4k$, para algún k natural, existe alguna matriz de Hadamard de tamaño n.

Respecto a la conjetura se han logrado varias aproximaciones, algunas formas de construirlas como las vistas en el capítulo 1, otras de carácter asintótico, como, por ejemplo:

Seberry demostró que dado un número impar $m > 3$, existe una matriz de Hadamard de orden $2^t m \; \forall t \geq 2\log_2(m-3) + 1$. [11, 12]

Craigen demostró que para todo número positivo impar m existe una matriz de Hadamard de orden $2^{2b}m$ siendo b el número de dígitos no nulos de la representación binaria de m. [13]

Recientemente ha sido demostrado que $\forall \epsilon > 0$ el conjunto de números impares k para los cuales hay una matriz de Hadamard de orden $k2^{2+\epsilon+\log_2 k}$ tiene densidad positiva en el conjunto de los números naturales. De igual modo se ha demostrado que hay una matriz cociclica de Hadamard de orden $2^{10+t}q$ para $t \geq 8[\frac{\log_2(q-1)}{10}]$ siendo q un número impar.[14, 15]

2.1.2 Equivalencia de la conjetura.

Definición: Sea B_n una matriz booleana de orden n se llama asociada a una matriz de Hadamard si cumple que existe una matriz de Hadamard H_n tal que $B_n = \frac{H_n + E_n}{2}$ donde E_n denota a la matriz tautológica(igual a 1 en todas sus posiciones).

Proposición 1:

Si B_n es una matriz booleana asociada a una matriz de Hadamard entonces las filas de B_n definen un simplex regular en $\mathbb{Z}_2^n$ con lados de longitud $\frac{n}{2}$ para la distancia Hamming y $\sqrt{\frac{n}{2}}$ para la distancia euclidiana.

Demostración:

Si B_n asociada a una matriz de Hadamard H_n entonces sea H_i la i-ésima fila de la matriz, entonces $\sum_{k=1}^{n} h_{ik}h_{jk} = < H_i, H_j >= 0 \; \forall i \neq j$ implica que la cantidad de posiciones en que coinciden H_i y H_j es igual a la cantidad de posiciones distintas, luego la cantidad de posiciones en la cual difieren es $\frac{n}{2}$ que es la distancia Hamming para las filas de la matriz booleana asociada. Luego como de distancia Hamming a distancia euclidiana el $\mathbb{Z}_2^n$ se puede pasar hallando la raíz cuadrada de la distancia Hamming entonces se cumple la proposición.

Proposición 2:

Si se tiene un simplex de n vértices en $\mathbb{Z}_2^n$ de lados $\frac{n}{2}$ para n múltiplo de 4 entonces existe una matriz de Hadamard de orden n.

Demostración:

Sea el simplex $V = \{P_1, P_2, \dots, P_n\}$ se cumple que $< P_i, P_j >= 0 \; \forall \; i \neq j$ por lo cual se puede construir una matriz booleana B_n tal que $H_n = 2B_n - E_n$, es una matriz de Hadamard, pues el producto de sus filas distintas es cero y el producto de cada fila consigo misma es igual a 1.

Juntando las proposiciones 1 y 2 se tiene la conjetura equivalente a la de Hadamard.

Conjetura 1: Para todo espacio $\mathbb{Z}_2^{4k}$ existe un simplex de $4k$ vértices y con sus lados de longitud $2k$.

Proposición 3:

Si existe un simplex como en la conjetura 1, entonces existe uno tal que tiene un vértice en el origen.

Demostración:

Partiendo del hecho que las distancias son invariantes a traslaciones y que una traslación en $\mathbb{Z}_2^{4k}$ es la suma definida en dicho espacio, entonces si trasladamos $V = \{P_1, P_2, \dots, P_n\}$, sumándole por ejemplo P_1 se tiene que $V' = \{0, P_2 \oplus P_1, \dots, P_{4k} \oplus P_1\}$ es también un simplex como el enunciado en la conjetura pero además uno de sus vértices se encuentra en el origen, lo que también implica que los demás tienen tantos 1s como 0s en sus coordenadas.

2.2 Método de construcción propuesto y casos particulares.

Consideremos ahora la siguiente matriz de Hadamard:

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 \end{pmatrix}$$

Si vemos su matriz booleana asociada es $B_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ se puede notar que las filas de la misma presentan una estructura equivalente a la de grupo isomorfo a un grupo 4 de Klein, donde la característica del grupo es 2. O sea que la suma de dos elementos no nulos distintos es igual al tercero y que cualquier otra suma es igual a cero, y la equivalencia viene dada por la operación unaria negación, o sea que resultado valido para la primera fila igual a n 1s es también valido para primera fila con n 0s.

Supongamos que queremos una matriz de Hadamard de tamaño $n = 4k$, considérese el siguiente método:

1. Tomemos el grupo de Klein y extendámoslo a $\mathbb{Z}_2^{4k}$ cambiando cada 1 por k 1s, y cada 0 por k 0s.Luego de esto se tiene una matriz de $4 \times n$ que cumple con los criterios dados para el simplex(o sea 4 puntos del simplex si es que existe).

2. Tomemos un vector de traslación que forme un ángulo de 60 grados con los del simplex (suponiendo que halla alguno) y hallar el coseto correspondiente al grupo de Klein, añadirlo al simplex.

Asumiendo que el proceso se puede reiterar $k-1$ veces sin alterar la propiedad de simplex se tendría una matriz asociada de Hadamard de orden n.

Primeramente, preguntémonos si esta construcción es válida para cualquier tamaño:

Al menos en cada espacio existen 2^{n-2} cosetos a seleccionar, y de ellos $\frac{\binom{4k}{2k}}{4}$ cumplen además que su vector de traslación está a distancia $2k$ del origen. Lo cual nos indica que la construcción es posible para cualquier tamaño, pero esto en general no es cierto.

Por ejemplo sea el 3-simplex $B_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$, para extenderlo debemos hallar un vector de norma 2 y ángulo de 60 grados con respecto a los ya existentes en el grupo.

Ello da lugar al sistema de ecuaciones lineales siguiente:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0 \\ x_1 + x_2 &= 1 \\ x_1 + x_4 &= 1 \\ x_2 + x_3 &= 1 \end{aligned}$$

Cuya matriz ampliada del sistema es: $\begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ la cual al escalonarla se obtiene:

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

El cual es un sistema incompatible, o sea sin solución. De lo cual se puede concluir que existen valores para los cuales no se puede utilizar el método de construcción propuesto. Posteriormente estudiaremos cuales son estos valores.

Veamos un ejemplo en el cual se realiza la construcción de una matriz de Hadamard de forma satisfactoria con el método propuesto.

Extendiendo B_4 a una matriz de $4x8$ $\begin{pmatrix}1&1&1&1&1&1&1&1\\1&1&1&1&0&0&0&0\\1&1&0&0&0&0&1&1\\0&0&1&1&0&0&1&1\end{pmatrix}$ planteando el sistema ampliado $\begin{pmatrix}1&1&1&1&1&1&1&1&4\\1&1&1&1&0&0&0&0&2\\1&1&0&0&0&0&1&1&2\\0&0&1&1&0&0&1&1&2\end{pmatrix}$ la cual al escalonarla queda $\begin{pmatrix}1&1&1&1&1&1&1&1&4\\0&0&1&1&1&1&0&0&2\\0&0&0&0&1&1&1&1&2\\0&0&0&0&0&0&1&1&1\end{pmatrix}$ que es de rango 4 tanto la matriz como la ampliada del sistema lo cual implica que es compatible indeterminado, con 4 variables libres, que son $x_2, x_4, x_6\ y\ x_8$, por lo que existen $2^4 = 16$ soluciones del sistema entre los $\binom{8}{4} = 70$ vectores de norma 4 que hay en $\mathbb{Z}_2^8$. Tomando por ejemplo $x_2 = x_4 = x_6 = x_8 = 1$ obtenemos $v = (01010101)$ que es el vector de traslación, añadiendo este a los demás se obtiene la matriz.

$$B_8 = \begin{pmatrix}1&1&1&1&1&1&1&1\\1&1&1&1&0&0&0&0\\1&1&0&0&0&0&1&1\\0&0&1&1&0&0&1&1\\0&1&0&1&0&1&0&1\\1&0&1&0&0&1&0&1\\1&0&0&1&0&1&1&0\\0&1&1&0&0&1&1&0\end{pmatrix}$$

Que es una matriz booleana asociada a una matriz de Hadamard entonces sea $H_8 = 2B_8 - E_8$ es una matriz de Hadamard.

Formalicemos, para terminar, algunas ideas:

1. Al cambiar cada 1 por k 1s y cada 0 por k 0s lo que estamos haciendo es una aplicación inyectiva de $\mathbb{Z}_2^4 \to \mathbb{Z}_2^{4k}$ la cual convierte las distancias del primer espacio hacia el segundo multiplicándolas por k.
2. Al escalonar el sistema de ecuaciones lo hacemos inicialmente en $\mathbb{R}$, pero luego lo llevamos a $\mathbb{Z}_2$ en caso de existir soluciones en enteros, para ver si podemos obtener soluciones en el campo binario.

Capítulo 3: Generalización y demostración para matrices de Hadamard de tamaño 4k y 8k

En este capítulo se culmina la forma de generalizar el algoritmo propuesto en la tesis y se pasa a demostrar el resultado final del trabajo que es el caso $n = 8k$ lo cual compone el avance principal presentado en la tesis.

3.1 Generalización del método de construcción.

Supongamos ahora que quisiéramos construir una matriz de Hadamard de tamaño $n = 4k$, operando de la misma forma utilicemos el simplex $B_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ y sumergiendo el grupo de Klein en $\mathbb{Z}_2^{4k}$ se tiene de manera análoga que para que se pueda extender el grupo con uno de sus cosetos se debe cumplir que la distancia del vector de traslación a todos los del grupo debe ser k para que halla un ángulo de 60 grados entre todos los vectores del simplex.

Excepto por el primero que debe ser $2k$, con lo que queda el sistema ampliado $\begin{pmatrix} 1_k & 1_k & 1_k & 1_k & 2k \\ 0_k & 1_k & 1_k & 0_k & k \\ 0_k & 0_k & 1_k & 1_k & k \\ 0_k & 1_k & 0_k & 1_k & k \end{pmatrix}$, asumiendo que a_k representa a k repeticiones de a.

Llevada a la forma escalonada esta se convierte en:

$$\begin{pmatrix} 1_k & 1_k & 1_k & 1_k & 2k \\ 0_k & 1_k & 1_k & 0_k & k \\ 0_k & 0_k & 1_k & 1_k & k \\ 0_k & 0_k & 0_k & 2_k & k \end{pmatrix}$$

que es de rango 4, siendo también de rango 4 la matriz no ampliada del sistema de ecuaciones. Esto significa que el sistema es compatible, con $4k - 4 = 4(k - 1)$ variables libres. (Las variables no libres del sistema escalonado son $x_1, x_{k+1}, x_{2k+1}\ y\ x_{3k+1}$). Dándoles valores de ceros o unos a las variables libres se

obtendrían $2^{4(k-1)}$ diferentes soluciones. Pero estas soluciones serían en el campo de los números racionales. Se ve claramente que para k impar el sistema no tiene solución en enteros, luego, no la tiene con respecto al campo binario.

Veamos un ejemplo de la construcción para $n = 12$, y observemos que pasa.

Inserción del simplex $B_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$ en el hipercubo $\mathbb{Z}_2^{12}$. Reemplazando cada 0 por tres 0s y cada 1 por tres 1s, el conjunto de los cuatro vectores se convierte en:

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

el cual es también el conjunto de vértices de un simplex regular, pero ahora en el hipercubo $\mathbb{Z}_2^{12}$**.** En éste, los vectores no nulos son de norma 6 y sus distancias respectivas son también iguales a 6. (Nótese que en la inserción realizada las distancias se triplican).

Planteando luego el sistema de ecuaciones lineales que resulta de buscar vectores de norma 6 que formen un ángulo de 60 grados con todos los del simplex B_4.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 6 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 3 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 3 \end{pmatrix}$$

La cual al escalonarla queda:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 6 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 3 \end{pmatrix}$$

Sistema que no tiene solución en enteros, Luego si tomamos el sistema con coeficientes en el campo binario se tiene:

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

Sistema que es incompatible, luego no hay soluciones, por tanto, el método es incapaz de producir una matriz de orden 12.

En general si $n = 4k$ y k es impar se puede generalizar el método de la siguiente forma:

El sistema dado sería: $\begin{pmatrix} 1_k & 1_k & 1_k & 1_k & 2k \\ 0_k & 1_k & 1_k & 0_k & k \\ 0_k & 0_k & 1_k & 1_k & k \\ 0_k & 1_k & 0_k & 1_k & k \end{pmatrix}$ el cual al escalonarlo queda:

$\begin{pmatrix} 1_k & 1_k & 1_k & 1_k & 2k \\ 0_k & 1_k & 1_k & 0_k & k \\ 0_k & 0_k & 1_k & 1_k & k \\ 0_k & 0_k & 0_k & 2_k & k \end{pmatrix}$ que no tiene soluciones en enteros, luego al llevarlo al campo binario resulta $\begin{pmatrix} 1_k & 1_k & 1_k & 1_k & 0 \\ 0_k & 1_k & 1_k & 0_k & 1 \\ 0_k & 0_k & 1_k & 1_k & 1 \\ 0_k & 0_k & 0_k & 0_k & 1 \end{pmatrix}$ un sistema que siempre es incompatible cuando k es impar. De donde se concluye que no existe solución para una matriz de Hadamard si $n = 4k$ con k impar.

Veamos qué pasa si k fuese par. Sea $k = 2k'$ trabajemos el sistema anterior en $\mathbb{Z}_2^{4k}$:

$\begin{pmatrix} 1_k & 1_k & 1_k & 1_k & 4k' \\ 0_k & 1_k & 1_k & 0_k & 2k' \\ 0_k & 0_k & 1_k & 1_k & 2k' \\ 0_k & 1_k & 0_k & 1_k & 2k' \end{pmatrix}$ el cual al escalonarlo resulta: $\begin{pmatrix} 1_k & 1_k & 1_k & 1_k & 4k' \\ 0_k & 1_k & 1_k & 0_k & 2k' \\ 0_k & 0_k & 1_k & 1_k & 2k' \\ 0_k & 0_k & 0_k & 2_k & 2k' \end{pmatrix}$

El cual, si tiene solución en los enteros, veamos qué ocurre si llevamos sus coeficientes al campo binario, luego de dividir la última fila entre 2:

$$\begin{pmatrix} 1_k & 1_k & 1_k & 1_k & 0 \\ 0_k & 1_k & 1_k & 0_k & 0 \\ 0_k & 0_k & 1_k & 1_k & 0 \\ 0_k & 0_k & 0_k & 1_k & k'(mod2) \end{pmatrix}$$

El cual tiene $2^{2(k-1)}$ soluciones binarias, las cuales forman vectores que se pueden seleccionar para formar un simplex de $4k$ vértices en $\mathbb{Z}_2^{4k}$. La cantidad de soluciones a escoger es suficiente como para plantear la conjetura de que para cualquier $k = 2k'$ esto es posible.

Conjetura 3.1: Para todo número entero no negativo t y para m impar existe una matriz de Hadamard de orden $2^{3+t}m$.

3.2 Demostración del caso $n = 8k$.

Se ha establecido que existen soluciones en el caso de $n = 8k$, llamemos a dichas soluciones como $t_i \; \forall \; i = 1,2,\dots,2^{2(k-1)}$veamos que al extender el simplex B_4 con cualquier t_i no se pierde la propiedad de que las distancias entre dos elementos del simplex es igual a $4k$.

Sean $b_i \; \forall \; i = 1,2,3,4$ los elementos del simplex B_4 sabemos que la cantidad de posiciones que son iguales a 1 en $b_i \oplus b_j$ es igual a $4k$, ahora como t_i está a distancia $4k$ de todos los vectores de B_4 y forma un ángulo de 60 grados con ellos tenemos que $t_i \oplus b_j$ cumple que tiene longitud $4k$. Sean $c_j \; \forall \; j = 1,2,3,4$ los vectores de la forma $c_j = t_i \oplus b_j$, ahora planteemos cual sería la longitud de cualquier arista, la cual no es más que la longitud de $c_j \oplus b_k = t_i \oplus b_j \oplus b_k = t_i \oplus b_i = c_i$, lo que implica que la suma de un elemento del coseto con un elemento del simplex cualquiera es un elemento del coseto, con lo que la longitud entre cualquier par de vectores es $4k$. Lo que significa que podemos poner cualquier t_i como vector de traslación para la matriz resultante.

Entonces se puede añadir $2k - 1$ cosetos a la solución, bueno excepto tal vez que los cosetos no se encuentren a distancia $4k$ entre ellos. Bastaría entonces para concluir la demostración probar que $t_i \oplus t_j = t_k$, o sea que el conjunto de soluciones del sistema de ecuaciones planteado sea cerrado bajo la suma en $\mathbb{Z}_2^{8k}$. Esto se debe a que si tomamos c_i como antes y d_j para otro coseto, entonces $c_i \oplus d_j = t_i \oplus b_k \oplus t_j \oplus b_l = t_i \oplus t_j \oplus b_m$ luego sería suficiente que el conjunto de soluciones del sistema que nos da el método planteado sea cerrado para la suma.

Se puede apreciar la dificultad de demostrar que el conjunto solución del sistema sea cerrado para la suma, así que centrémonos en probar que existen suficientes vectores tal que su suma es una solución al sistema de ecuaciones. Para ello definamos la función $f: \mathbb{Z}_2^{4k-4} \rightarrow \mathbb{Z}_2^4$ tal que a un conjunto de variables libres le hace corresponder sus respectivas variables dependientes. Sea la relación inversa de f la misma tiene como imagen 16 conjuntos cada uno con 2^{4k-8} elementos, suficientes como para considerar solo el conjunto de soluciones que tiene por variables dependientes cuatro 0s. De estas se pueden tomar todas aquellas que compartan $\frac{k}{2}$ 1s y se diferencien en los otros $\frac{k}{2}$. Haciendo esto nos aseguramos que la suma de las soluciones tomadas posean $\frac{k}{2}$ 1s por lo que cumplen el criterio necesario para estar juntas en la solución. Luego solo queda ver cuántas de estas soluciones "buenas" hay. Si tomamos los $\frac{k}{2}$ en común de las $4k-4$ componentes que quedan, luego tenemos que escoger de las $4k-\frac{k}{2}-4$ componentes restantes hay que escoger $\frac{k}{2}$ para uno y $\frac{k}{2}$ para el otro. Fijando la parte en común se tienen en total $\binom{n-\frac{k}{2}-4}{\frac{k}{2}} * \binom{n-k-4}{\frac{k}{2}}$ formas de escoger las soluciones. Lo cual es mayor en casi todos los casos que $4k-4$ lo que nos asegura la existencia de al menos $k-1$ soluciones, suficiente para construir una matriz de Hadamard de orden $n=4k$ para k par.

Conclusiones Generales

En el presente trabajo se realizó un estudio sobre la conjetura de Hadamard, se vieron los principales resultados respecto tanto a construcciones de matrices de Hadamard como a los avances logrados el pos de demostrar la conjetura. A partir del análisis de la bibliografía y la investigación realizada se llegaron a las siguientes conclusiones:

- Se obtuvo una equivalencia a la conjetura de Hadamard a través de los espacios $\mathbb{Z}_2^{4k}$ que permitió proponer otra forma de construir matrices de Hadamard.
- Se propuso un algoritmo matemático para la construcción de matrices de Hadamard de los órdenes múltiplos de 8, pese a que no funciona para ningún múltiplo de 4 que no lo sea de 8.
- Se demostró que dicho algoritmo es capaz de generar una matriz de Hadamard para cualquier múltiplo de 8, con lo cual queda demostrado que existe dicha matriz de Hadamard en esos casos.

Se logró el objetivo principal encontrando una equivalencia geométrica que nos permitió llegar a un resultado superior a los alcanzados hasta ahora, que es la demostración de la conjetura que enuncia: para todo número entero no negativo t y para m impar existe una matriz de Hadamard de orden $2^{3+t}m$. Aunque no sea el fin de la historia de esta conjetura es al menos un paso importante.

Recomendación

1. Estudiar el caso general, tratando de lograr a partir de este resultado demostrar por completo la conjetura.

2. Buscar un método de construcción general para el caso de múltiplos de ocho que sea computacionalmente mejor que el orden exponencial que se plantea en el presente trabajo el cual pese a lograr una demostración de existencia, no posee utilidad práctica para valores mayores que 20.

Bibliografía.

1. Hadamard, J. *Resolution d'une question relative aux determinants.* Bull. des sciences math., 1893. **2**: p. 240-246.
2. Díaz-Caro, A. "Agregando medición al cálculo de van tonder." 2007. Master's thesis, Universidad Nacional de Rosario, Argentina.
3. Piza, E. *búsqueda de matrices de hadamard a través de secuencias de turyn.* Revista de Matemática: Teoría y Aplicaciones, 2011. **18**(2).
4. Belevitch, V. *Theorem of 2n-terminal networks with application to conference telephony.* Electr. Commun, 1950. **26**: p. 231-244.
5. Sylvester, J. J. *LX. Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers.* The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 1867. **34**(232): p. 461-475.
6. Armario, J. A. *On permanents of Sylvester Hadamard matrices.* arXiv preprint arXiv:1311.2427, 2013.
7. Paley, R. E. *On orthogonal matrices.* Studies in Applied Mathematics, 1933. **12**(1-4): p. 311-320.
8. Alzaga, B. G. "Matrices cocíclicas de hadamard sobre el grupo z_t x z_2^ 2. Descripción, clasificación y búsqueda." 2011. Universidad de Sevilla.
9. Álvarez, V., et al. *A genetic algorithm for cocyclic Hadamard matrices*. in *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*. 2006. Springer.
10. Horadam, K. J. *Hadamard matrices and their applications*. 2012: Princeton university press.
11. Seberry, J. *On the existence of Hadamard matrices.* 1976.
12. Seberry, J. and Yamada, M. *Hadamard matrices, sequences, and block designs.* Contemporary design theory: a collection of surveys, 1992: p. 431-560.
13. Craigen, R. and Kharaghani, H. *Hadamard matrices and Hadamard designs.* Handbook of Combinatorial Designs, 2007: p. 273-280.
14. de Launey, W. *On the asymptotic existence of Hadamard matrices.* Journal of Combinatorial Theory, Series A, 2009. **116**(4): p. 1002-1008.
15. de Launey, W. and Kharaghani, H. *On the asymptotic existence of cocyclic Hadamard matrices.* Journal of Combinatorial Theory, Series A, 2009. **116**(6): p. 1140-1153.
16. Álvarez, V., et al. *A system of equations for describing cocyclic Hadamard matrices.* Journal of Combinatorial Designs, 2008. **16**(4): p. 276-290.

17. Baliga, A. and Chua, J. *Self-dual codes using image restoration techniques*. in *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*. 2001. Springer.
18. Ito, N. *On Hadamard groups.* Journal of Algebra, 1994. **168**(3): p. 981-987.
19. Levenshtein, V. I. *Binary codes with correction for deletions and insertions of the symbol 1.* Problemy Peredachi Informatsii, 1965. **1**(1): p. 12-25.
20. Livinskyi, I. *Asymptotic existence of Hadamard matrices*. 2012: University of Manitoba (Canada).
21. Turyn, R. *Sequences with small correlation.* Error correcting codes, 1968: p. 195-228.
22. Williamson, J. *Hadamard's determinant theorem and the sum of four squares.* Duke Mathematical Journal, 1944. **11**(1): p. 65-81.