Revista de Matemática: Teoría y Aplicaciones 2011 **18**(2) : 193–214
cimpa – ucr issn: 1409-2433

BÚSQUEDA DE MATRICES DE HADAMARD A TRAVÉS DE SECUENCIAS DE TURYN

SEARCH OF HADAMARD MATRICES BY TURYN SEQUENCES*

Eduardo Piza†

Received: 26 Aug 2010; Revised: 9 May 2011;
Accepted: 10 May 2011

Resumen

En este artículo estudiamos las matrices de Hadamard y algunos algoritmos para generarlas. Revisamos varios aspectos teóricos en torno a la conjetura de Hadamard, que afirma que todo entero positivo múltiplo de 4 es un número de Hadamard. Posteriormente se describen los métodos de Kronecker, Sylvester, Paley, Williamson, Goethals-Seidel, Cooper-Wallis, Baumert-Hall, Ehlich y conjuntos diferencia suplementarios. Se establece la *criba de Hadamard*: 668 es el menor orden para el cual se desconoce si existe una matriz de Hadamard. Finalmente proponemos algoritmos de recocido simulado para hallar matrices de Hadamard a partir de secuencias Turyn. Hallamos excelentes soluciones con este método de búsqueda.

---

*Investigación realizada con el apoyo económico del Deutscher Akademischer Austausch Dienst (DAAD) y la Universidad de Costa Rica.

†Centro de Investigación en Matemática Pura y Aplicada (CIMPA), Universidad de Costa Rica. San José, Costa Rica. E-Mail: eduardojpiza@hotmail.com.

Palabras clave: matrices de Hadamard, recocido simulado, optimización combinatoria.

Abstract

In this paper we study the Hadamard matrices and some algorithms to generate them. We review some theoretical aspects about Hadamard's conjecture, which asserts that every positive integer multiple of 4 is a Hadamard number. Then we describe the methods of Kronecker, Sylvester, Paley, Williamson, Goethals-Seidel, Cooper-Wallis, Baumert-Hall, Ehlich and supplementary difference sets. Subsequently we settle the *Hadamard sieve*: 668 is lowest order for which is unknown if there exist an Hadamard matrix. Finally we propose a simulated annealing algorithms as alternative to find Hadamard matrices from Turyn sequences. We found excellent solutions with this search method.

Keywords: Hadamard matrices, simulated annealing, combinatorial optimization.

Mathematics Subject Classification: 15B34, 05B20, 90C27.

1 Introducción

Una *matriz de Hadamard* de orden n es una matriz H de tamaño $n \times n$ con entradas $+1$ y -1, tal que

$$HH^t = nI. \tag{1}$$

De la definición está claro que cualesquiera dos columnas (o filas) de H son ortogonales. Evidentemente esta propiedad no cambia si permutamos las filas o columnas o si multiplicamos alguna fila o columna por -1: estas matrices son llamadas *equivalentes*. Dada una matriz de Hadamard, podemos encontrar otra equivalente en la cual la primera fila y la primera columna consistan enteramente de $+1$'s. Tal matriz de Hadamard se denomina *normalizada*. Claramente las filas restantes (si las hubiese) deben tener tantos $+1$ como -1. Por consiguiente, si $n \neq 1$ entonces n debe ser par. Algunos ejemplos de matrices de Hadamard de órdenes pequeños ($n = 1$, $n = 2$ y $n = 4$) son

$$(1), \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad \begin{pmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & - & - & + \end{pmatrix}, \tag{2}$$

donde para abreviar en el último ejemplo solamente se indicaron los signos de las entradas.

Hadamard (ver [10]) consideró el siguiente problema. Sea $A = (a_{ij})$ una matriz $n \times n$ con entradas reales, tales que $|a_{ij}| \leq 1$. ¿Qué tal grande puede ser el determinante de A (en valor absoluto)? Esto es, se trata de resolver el problema de optimización

$$\begin{array}{l} \text{Maximizar} \\ \text{sujeto a } |a_{ij}| \leq 1 \end{array} |\det A|. \tag{3}$$

Como cada fila de A es un vector con longitud euclídea $\leq \sqrt{n}$, entonces el determinante no puede ser mayor que $n^{n/2}$, pues el valor absoluto del determinante de una matriz A es el volumen n-dimensional del paralelepípedo engendrado por los vectores fila de A en el espacio n-dimensional $\mathbb{R}^n$. Esto es, se satisface la desigualdad

$$|\det(A)| \leq n^{n/2}. \tag{4}$$

En el caso de matrices A con entradas complejas, la desigualdad (4) se alcanza con la matriz de Vandermonde de las raíces de la unidad, como fue demostrado por Faddeev and Sominskii (ver [8]) en 1965. Originalmente Hadamard demostró (ver [10]) que en el caso de matrices con entradas reales, la desigualdad (4) se alcanza en la solución óptima del problema (3) *con una igualdad* solamente para $n = 1$, $n = 2$ o para ciertos múltiplos de 4. Además demostró que las matrices reales que resuelven el problema (3) y que también satisfacen la desigualdad (4) *con igualdad* son precisamente las ahora llamadas matrices de Hadamard H de orden n, cuyas entradas consisten de ± 1 y sus filas (también sus columnas) son ortogonales: $HH^t = nI_n$.

El anterior problema es conocido en la literatura como el *problema del determinante maximal* y ha sido profusamente investigado durante más de 100 años, aunque todavía no se conoce la solución en el caso general. Por ejemplo, aún se desconoce la solución para $n = 19$: tan solo se dispone de burdas aproximaciones. La desigualdad de Hadamard (4) juega un papel importante en el desarrollo de la teoría de ecuaciones integrales lineales creada por Fredholm en 1900 y particularmente por esta razón han sido establecidas muchas demostraciones y generalizaciones. Modernamente se han encontrado conecciones entre las matrices de Hadamard y otros campos de las matemáticas tales como la teoría de números, la combinatoria y la teoría de grupos. Las matrices de Hadamard además han sido utilizadas para mejorar la precisión de los espectrómetros, para realizar diseños experimentales en estadística aplicados a la agricultura y para diseñar códigos auto-correctores de errores en mensajes e imágenes trasmitidas desde el espacio.

2 Algunos resultados teóricos

Un resultado teórico muy sencillo es el siguiente. Contrasta con su recíproco, el cual es un importante problema abierto en matemática.

Teorema 1 ***(Hadamard)*** *Si H es una matriz de Hadamard de orden n, entonces $n = 1$, o $n = 2$ o n es múltiplo de 4.*

DEMOSTRACIÓN: Sea $n > 2$. Normalizamos H, obteniendo una matriz de Hadamard $\widehat{H}$ equivalente. En $\widehat{H}$ permutamos las columnas de tal forma que las primeras tres filas de la matriz resultante sean

$$\begin{array}{cccc} ++\cdots++ & ++\cdots++ & ++\cdots++ & ++\cdots++ \\ ++\cdots++ & ++\cdots++ & --\cdots-- & --\cdots-- \\ \underbrace{++\cdots++}_{a \text{ columnas}} & \underbrace{--\cdots--}_{b \text{ columnas}} & \underbrace{++\cdots++}_{c \text{ columnas}} & \underbrace{--\cdots--}_{d \text{ columnas}} \end{array}$$

Tenemos entonces $a+b+c+d = n$ y los tres productos internos entre estas tres primeras filas arrojan las ecuaciones $a+b-c-d = 0$, $a-b+c-d = 0$, $a-b-c+d = 0$. Sumando estas cuatro ecuaciones, obtenemos $n = 4a$, demostrando el teorema (en forma similar se demuestra también que $4b = 4c = 4d = n$). ■

Una de las más famosas conjeturas en el área de los diseños combinatorios establece que para cada orden n múltiplo de 4 existe una matriz de Hadamard de orden n. Ésta es conocida como la *conjetura de Hadamard*, aunque en realidad es atribuida a Paley en 1933. Es aún un problema abierto en matemáticas que se encuentra lejos de ser demostrado o refutado. Los menores órdenes n múltiplos de 4 para los cuales aún no se conoce una matriz de Hadamard asociada son 668, 716, 876 y 892. Hasta hace poco el menor orden era 428, pero en 2005 Khagharani y Tayfeh-Rezaie hallaron una matriz de Hadamard de orden 428 utilizando algoritmos de Goethals-Seidel (ver [12]). Existen varios algoritmos para generar matrices de Hadamard de muy diversos órdenes. En la próxima sección estudiaremos los más importantes. Sin embargo, no todos los órdenes (múltiplos de 4) sucumben ante los algoritmos conocidos.

Por otra parte, el número de matrices de Hadamard no-equivalentes entre sí de orden n solamente se conoce para $n \leq 28$: para los órdenes 1, 2, 4, 8, 12, 16, 20, 24 y 28 hay únicamente 1, 1, 1, 1, 1, 5, 3, 60 y 487 matrices de Hadamard no-equivalentes. Esta aparente explosión combinatoria sugiere fuertemente la validez de la conjetura de Hadamard.

Cercanamente relacionadas con las matrices de Hadamard están las denominadas matrices de conferencia. Una *matriz de conferencia* C de

orden n es una matriz $n \times n$ con 0's en la diagonal, $+1$ o -1 en las otras posiciones y con la propiedad

$$CC^t = (n-1)I. \tag{5}$$

El nombre (matriz de conferencia) proviene de una aplicación de estas matrices a los circuitos telefónicos ideada por V. Belevitch (1950) (ver [4]), quien estudió las llamadas redes ideales no-disipativas, consistentes en transformaciones usadas para establecer conexiones de redes de conferencias telefónicas.

Se demuestra fácilmente que si C una matriz de conferencia de orden $n \neq 1$, entonces n es par. Además, a partir de una matriz de conferencia C de orden n, permutando filas y columnas y luego multiplicando algunas filas y columnas por -1, se pueden hallar una matrices de conferencia equivalentes a la original pero con la característica que son simétricas cuando $n \equiv 2 \pmod 4$ y antisimétricas cuando $n \equiv 0 \pmod 4$ (ver [13]).

Teorema 2 *Si C es una matriz de conferencia antisimétrica, entonces $I + C$ es una matriz de Hadamard.*

DEMOSTRACIÓN: $(I+C)(I+C)^t = I+C+C^t+CC^t = I+(n-1)I = nI$. ■

Teorema 3 *Si C es una matriz de conferencia simétrica de orden n, entonces*

$$H = \begin{pmatrix} I+C & -I+C \\ -I+C & -I-C \end{pmatrix} \tag{6}$$

es una matriz de Hadamard de orden $2n$.

DEMOSTRACIÓN: Basta calcular HH^t y se obtiene el resultado. ■

Sea A una matriz de tamaño $m \times n$ con entradas a_{ij} y sea B otra matriz cualquiera. La matriz

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}, \tag{7}$$

consistente en mn bloques con el tamaño de B, se llama producto de Kronecker de las matrices A y B y se denota $A \otimes B$.

Teorema 4 *Si H_m y H_n son matrices de Hadamard de órdenes m y n respectivamente, entonces $H_m \otimes H_n$ es una matriz de Hadamard de orden mn.*

DEMOSTRACIÓN: Realizando cálculos directos podemos previamente demostrar las siguientes dos propiedades:

$$\begin{aligned}(A \otimes B)(C \otimes D) &= (AC) \otimes (BD)\\ (A \otimes B)^t &= A^t \otimes B^t.\end{aligned}$$

Tomemos $A = C = H_m$ y $B = D = H_n$. El resultado se obtiene de la definición de matriz de Hadamard y del hecho que $I_m \otimes I_n = I_{mn}$. ■

3 Método de Sylvester

La aplicación iterada del teorema precedente, empezando con la matriz de Hadamard de orden 2

$$H_2 = \begin{pmatrix} + & + \\ + & - \end{pmatrix}, \tag{8}$$

nos lleva a las *matrices de Sylvester* $S(k)$ de orden 2^k, que son productos iterados de Kronecker de k copias de la matriz de Hadamard H_2. Por ejemplo,

$$S(2) := \left(\begin{array}{cc|cc} + & + & + & + \\ + & - & + & - \\ \hline + & + & - & - \\ + & - & - & + \end{array}\right) \tag{9}$$

Formalmente, $S(1) := H_2$ y $S(k+1) := H_2 \otimes S(k)$, para $k \in \mathbb{N}^*$. Las matrices de Sylvester fueron descubiertas en 1887 por J. J. Sylvester y tienen algunas propiedades especiales: son normalizadas, simétricas, tienen traza nula y sus elementos en las restantes filas y columnas distintas a la primera tienen la misma cantidad de 1's que -1's. Las matrices de Sylvester guardan estrecha relación con las funciones de Walsh.

4 Método de Paley

Vamos a utilizar una construcción directa de algunas matrices de conferencia para órdenes específicos, que junto con los teoremas 2 y 3 nos proporcionarán matrices de Hadamard para ciertos órdenes distintos a 2^k. En el resto de la presente sección q denotará una potencia positiva de un primo impar. En el campo $\mathbb{F}_q$ definimos la función χ (llamada *símbolo de Legendre*) mediante

$$\chi(x) = \begin{cases} 0, & \text{si } x = 0,\\ 1, & \text{si } x \text{ es un cuadrado no nulo},\\ -1, & \text{si } x \text{ no es un cuadrado.}\end{cases}$$

Claramente χ es una función multiplicativa: para cada $x, y \in \mathbb{F}_q$ tendremos $\chi(x)\chi(y) = \chi(xy)$. Debido a que en $\mathbb{F}_q$ hay tantos cuadrados no nulos como no-cuadrados, entonces

$$\sum_{x \in \mathbb{F}_q} \chi(x) = 0. \tag{10}$$

Ahora, sea $c \in \mathbb{F}_q$, con $c \neq 0$. La ecuación (10) implica que

$$\sum_{b \in \mathbb{F}_q} \chi(b)\chi(b+c) = -1. \tag{11}$$

En efecto, si en (11) ignoramos el término de índice $b = 0$ (que es 0) y luego escribimos $\chi(b+c) = \chi(b)\chi(1+cb^{-1})$, notamos que cuando b recorre todos los elementos no-nulos del campo entonces $1+cb^{-1}$ recorre cada valor excepto 1. A continuación numeramos los elementos de $\mathbb{F}_q$: $0 = a_0$, a_1, $\ldots$, a_{q-1}. Definimos la matriz $Q = (q_{ij})$ de tamaño $q \times q$ (llamada *matriz de Jacobsthal*) mediante

$$q_{ij} := \chi(a_i - a_j), \quad 0 \leq i, j < q. \tag{12}$$

Nótese que Q es simétrica si $q \equiv 1 \pmod 4$ y antisimétrica si $q \equiv 3 \pmod 4$. Como una consecuencia directa de las propiedades de χ y de la fórmula (11) encontramos que $QQ^t = qI - J$ y $QJ = JQ = O$ (aquí J es la matriz de 1's). Se define la matriz C de tamaño $q+1 \times q+1$ mediante

$$C := \begin{pmatrix} 0 & 1 & 1 & \ldots & 1 \\ \pm 1 & & & & \\ \vdots & & & Q & \\ \pm 1 & & & & \end{pmatrix}, \tag{13}$$

donde los signos de los términos ± 1 son seleccionados de tal manera que C sea simétrica o antisimétrica. De las propiedades de Q se deduce que C es una matriz de conferencia de orden $q+1$. Esta construcción es debida a Paley (1933) (ver [15]) y las matrices de conferencia de este tipo son usualmente llamadas *matrices de Paley*. En el caso especial en que q es un número primo, la matriz Q es llamada *circulante*. Resumimos la construcción anterior en el siguiente teorema, consecuencia de la discusión anterior y de los teoremas 2 y 3.

Teorema 5 *Si q es la potencia de un primo impar, entonces existe una matriz de Hadamard de orden $q+1$ si $q \equiv 3 \pmod 4$, mientras que existe una matriz de Hadamard de orden $2(q+1)$ si $q \equiv 1 \pmod 4$.*

+	+	+	+	+	+	+	+	+	+	+	+
−	+	+	−	+	+	+	−	−	−	+	−
−	−	+	+	−	+	+	+	−	−	−	+
−	+	−	+	+	−	+	+	+	−	−	−
−	−	+	−	+	+	−	+	+	+	−	−
−	−	−	+	−	+	+	−	+	+	+	−
−	+	−	−	+	−	+	+	−	+	+	+
−	+	+	−	−	+	−	+	+	−	+	+
−	+	+	+	−	−	+	−	+	+	−	+
−	−	+	+	+	−	−	+	−	+	+	+
−	+	−	+	+	+	−	−	+	−	+	+

+	+	+	+	+	+	−	+	+	+	+	+
+	+	+	−	−	+	+	−	+	−	−	+
+	+	+	+	−	−	+	+	−	+	−	−
+	−	+	+	+	−	+	−	+	−	+	−
+	−	−	+	+	+	+	−	−	+	−	+
+	+	−	−	+	+	+	+	−	−	+	−
−	+	+	+	+	+	−	−	−	−	−	−
+	−	+	−	−	+	−	−	−	+	+	−
+	+	−	+	−	−	−	−	−	−	+	+
+	−	+	−	+	−	−	+	−	−	−	+
+	−	−	+	−	+	−	+	+	−	−	−
+	+	−	−	+	−	−	−	+	+	−	−

Figura 1: *Matrices de Hadamard de orden 12 construidas con el método de Paley de órdenes* $12 = 11 + 1$ *(q=11) y* $12 = 2(5 + 1)$ *(q=5), respectivamente.*

5 Método de Williamson

Con el algoritmo de Paley se pueden hallar matrices de Hadamard de la mayoría de los órdenes n, con $n \equiv 0 \pmod 4$, $n \leq 100$, excepto para $n = 92$. Debieron transcurrir unos 30 años entre el resultado de Paley y el descubrimiento de una matriz de Hadamard de orden 92, hecho por Baumert, Golomb y Hall en 1962 (ver [2], [11]). El método que ellos emplearon ya había sido desarrollado por Williamson en 1944 (ver [20]), pero sin embargo depende de una búsqueda computacional para hallar unas matrices específicas y en 1944 no existían las computadoras de hoy día. El método de Williamson se basa en el siguiente resultado.

Teorema 6 *Considere 4 matrices* simétricas A_i, $1 \leq i \leq 4$, *de orden* n, *con* n *impar y entradas* ± 1. *Suponga que estas matrices* conmutan entre sí *y satisfacen la relación*

$$A_1^2 + A_2^2 + A_3^2 + A_4^2 = 4nI_n. \tag{14}$$

Entonces, la matriz H *definida por bloques mediante*

$$H = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ -A_2 & A_1 & -A_4 & A_3 \\ -A_3 & A_4 & A_1 & -A_2 \\ -A_4 & -A_3 & A_2 & A_1 \end{pmatrix} \tag{15}$$

es una matriz de Hadamard de orden $4n$.

Demostración: Un cálculo directo demuestra que

$$HH^t = I_4 \otimes (A_1^2 + A_2^2 + A_3^2 + A_4^2) = 4nI_{4n}, \quad \blacksquare \tag{16}$$

Williamson consideró (ver [20]) el caso particular en el cual A_1, A_2, A_3 y A_4 son matrices *circulantes simétricas* $\mathrm{Circ}\,(c_0, c_1, \ldots, c_k, c_k, \ldots, c_1)$ de entradas ± 1. Las matrices circulantes conmutan entre sí, de manera que solamente falta elegir las matrices A_i apropiadas de forma tal que cumplan la relación (14).

Por construcción, cada una de las filas en estas matrices A_i suman lo mismo: $c_0 + 2(c_1 + \cdots + c_k)$, número que es impar. Denotando a este número por a_i, para $i = 1, 2, 3, 4$, obtenemos entonces de la condición (14) y del hecho que las matrices A_i son circulantes simétricas, la relación

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = 4n. \tag{17}$$

Lo anterior reduce el espacio de búsqueda computacional: primeramente deben hallarse las soluciones *impares* a la ecuación $a_1^2+a_2^2+a_3^2+a_4^2 = 4n$ y después se buscan las matrices A_i en (15) circulantes y simétricas de orden n, con entradas ± 1 y cuyas filas sumen a_i. El método no ofrece garantía absoluta de éxito.

+ + +	− + +	− + +	− + +
+ + +	+ − +	+ − +	+ − +
+ + +	+ + −	+ + −	+ + −
+ − −	+ + +	+ − −	− + +
− + −	+ + +	− + −	+ − +
− − +	+ + +	− − +	+ + −
+ − −	− + +	+ + +	+ − −
− + −	+ − +	+ + +	− + −
− − +	+ + −	+ + +	− − +
+ − −	+ − −	− + +	+ + +
− + −	− + −	+ − +	+ + +
− − +	− − +	+ + −	+ + +

Figura 2: *Matriz de Hadamard de orden 12 hallada con el método de Williamson.*

Por ejemplo, para hallar una matriz de Hadamard de orden 12 con el método de Williamson, tendremos $n = 3$. Fácilmente encontramos las siguientes cuatro matrices que cumplen la relación $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 12$, donde $(a_1, a_2, a_3, a_4) = (9, 1, 1, 1)$: $A_1 = \mathrm{Circ}\,(+, +, +)$, $A_2 = A_3 = A_4 = \mathrm{Circ}\,(-, +, +)$. La matriz de Hadamard de orden 12 correspondiente es mostrada en la Figura 2.

Este fue el método empleado por Baumert, Golomb y Hall (ver [2], [11]) para hallar por vez primera la matriz de Hadamard de orden $92 = 4 \cdot 23$,

mediante las matrices

$$\begin{aligned}
A_1 &= \text{Circ}\,(+\,+\,-\,-\,-\,+\,-\,-\,-\,+\,-\,+\,+\,-\,+\,-\,-\,-\,+\,-\,-\,-\,+),\\
A_2 &= \text{Circ}\,(+\,-\,+\,+\,-\,+\,+\,-\,-\,+\,+\,+\,+\,+\,+\,-\,-\,+\,+\,-\,+\,+\,-),\\
A_3 &= \text{Circ}\,(+\,+\,+\,-\,-\,-\,+\,+\,-\,+\,-\,+\,+\,-\,+\,-\,+\,+\,-\,-\,-\,+\,+),\\
A_4 &= \text{Circ}\,(+\,+\,+\,-\,+\,+\,+\,-\,+\,-\,-\,-\,-\,-\,-\,+\,-\,+\,+\,+\,-\,+\,+),
\end{aligned}$$

en las cuales se se verifica que $a_1 = -5$, $a_2 = 7$, $a_3 = 3$, $a_4 = 3$, con $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 92$.

Existen familias infinitas de matrices de Hadamard generadas con el método de Williamson. En efecto, Turyn demostró (ver [17]) que si q es una potencia positiva de un primo impar que satisface $q \equiv 1 \pmod 4$, entonces existe una matriz de Hadamard H de orden $2(q+1)$ generada con el método de Williamson para $n = (q+1)/2$. Además, en su demostración se observa que las matrices A_1 y A_2 difieren solo en la diagonal principal y $A_3 = A_4$.

El método de Williamson no siempre produce resultados positivos. En efecto, se sabe (ver [6]) que del todo no existen matrices de Williamson para el orden $4n = 140$, luego de completarse una búsqueda computacional exhaustiva. Para formarse una idea del enorme tamaño de la búsqueda computacional que debe realizar el método de Williamson, se menciona que el tamaño del espacio de búsqueda para $4n = 148$ es de 32 387 862 644 280 configuraciones por analizar, correspondientes a las 5 soluciones positivas e impares de la ecuación $a_1^2 + a_2^2 + a_3^2 + a_4^2 = 148$: $(1, 1, 5, 11)$, $(1, 7, 7, 7)$, $(3, 3, 3, 11)$, $(3, 3, 7, 9)$, $(5, 5, 7, 7)$.

6 Método de Goethals-Seidel

La estructura del método de Williamson permite algunas generalizaciones importantes. En primer lugar, el lector puede comprobar fácilmente que en realidad las matrices simétricas de Williamson A_1, A_2, A_3, A_4 no necesitan conmutar entre sí, sino tal solo ser dos a dos "amigables" (decimos que dos matrices A y B son *amigables* si satisfacen la relación $AB^t = BA^t$). En efecto, con esta propiedad más general se sigue cumpliendo la identidad $HH^t = 4nI_{4n}$. Desde luego las matrices circulantes son un caso particular de las matrices amigables. Esto entonces da origen a una extensión del método de Williamson, llevando a soluciones más generales con matrices amigables A_1, A_2, A_3, A_4, denominadas también matrices de Williamson de tipo II.

Otra generalización a la estructura de Williamson la constituye el método de Goethals-Seidel desarrollado en 1967 (ver [9]), el cual se basa en el siguiente resultado.

Teorema 7 *Sean A, B, C y D matrices circulantes de orden n tales que $AA^t + BB^t + CC^t + DD^t = 4nI_n$ y sea R la matriz identidad "diagonal hacia atrás" de orden n, esto es, $R = (r_{ij})$, con $r_{ij} = 1$ si $i + j = n + 1$, y $r_{ij} = 0$ en otro caso. Entonces la matriz H definida por bloques mediante*

$$H = \begin{pmatrix} A & BR & CR & DR \\ -BR & A & D^tR & -C^tR \\ -CR & -D^tR & A & B^tR \\ -DR & C^tR & -B^tR & A \end{pmatrix} \tag{18}$$

es una matriz de Hadamard de orden $4n$.

DEMOSTRACIÓN: Un cálculo directo demuestra que $HH^t = I_4 \otimes (AA^t + BB^t + CC^t + DD^t) = 4nI_{4n}$. ■

Puede observarse que en el caso que A, B, C y D sean simétricas, nos encontramos frente al método de Williamson. Por otra parte, la búsqueda de las filas iniciales de A, B, C y D está relacionada con las denominadas "secuencias de autocorrelaciones nulas", noción que pasamos a precisar.

Para una secuencia finita $\alpha = (a_0, a_1, \ldots, a_{m-1})$ de largo m, la *función de autocorrelación no-periódica*, N_α, se define mediante

$$N_\alpha(s) = \begin{cases} \sum_{i=0}^{m-1-s} a_i a_{i+s}, & \text{si } s = 0, 1, \ldots, m-1 \\ 0, & \text{si } s \geq m. \end{cases} \tag{19}$$

Cuatro secuencias finitas α, β, γ, δ de números en $\{-1, +1\}$ de largos $2m-1$, $2m-1$, m, m respectivamente se denominan *secuencias base* si

$$(N_\alpha + N_\beta + N_\gamma + N_\delta)(s) = 0, \quad \text{para } s \geq 1. \tag{20}$$

Cuatro secuencias finitas α, β, γ, δ de números en $\{-1, 0, +1\}$ de largo m se denominan *T-secuencias* si

$$(N_\alpha + N_\beta + N_\gamma + N_\delta)(s) = 0, \quad \text{para } s \geq 1. \tag{21}$$

Cuatro secuencias finitas X, Y, Z, W de números en $\{-1, +1\}$ de largos m, m, m y $m-1$ respectivamente se denominan *secuencias tipo Turyn* si

$$(N_X + N_Y + 2N_Z + 2N_W)(s) = 0, \quad \text{para } s \geq 1. \tag{22}$$

Es posible construir secuencias base a partir de secuencias tipo Turyn y T-secuencias a partir de secuencias base. A continuación se explica como realizar tales construcciones (ver [18]):

(b) Si X, Y, Z, W son secuencias de Turyn de largos m, m, m, $m-1$ respectivamente, entonces las secuencias $\alpha = (Z, W)$, $\beta = (Z, -W)$, $\gamma = X$, $\delta = Y$ son secuencias base de largos $2m-1$, $2m-1$, m, m respectivamente.

(a) Si α, β, γ, δ son secuencias base de largos $2m-1$, $2m-1$, m, m respectivamente, entonces las secuencias $(\frac{1}{2}(\alpha+\beta), 0_m)$, $(\frac{1}{2}(\alpha-\beta), 0_m)$, $(0_{2m-1}, \frac{1}{2}(\gamma+\delta))$, $(0_{2m-1}, \frac{1}{2}(\gamma-\delta))$ forman cuatro T-secuencias de largo $3m-1$. Aquí 0_m y 0_{2m-1} denotan la secuencias de ceros de largos m y $2m-1$ respectivamente.

Finalmente, las T-secuencias de largo $3m-1$ se utilizan para construir matrices de Hadamard de orden $4(3m-1)$. El procedimiento consiste (ver [16]) en hallar una T-secuencia T_1, T_2, T_3, T_4 de largo $3m-1$ y asociar a cada secuencia T_i la matriz circulante cuya primera fila es precisamente la secuencia T_i. Estas matrices circulantes las denotamos con la mismas letras T_1, T_2, T_3, T_4 y definimos

$$\begin{aligned} A &= T_1 + T_2 + T_3 + T_4, \\ B &= -T_1 + T_2 + T_3 - T_4, \\ C &= -T_1 - T_2 + T_3 + T_4, \\ D &= -T_1 + T_2 - T_3 + T_4. \end{aligned}$$

Entonces las matrices A, B, C, D satisfacen el teorema 7. Por consiguiente, basta con encontrar secuencias de Turyn de largos m, m, m, $m-1$. Esto es lo que hicieron Kharaghani y Tayfeh-Razaie (ver [12]) para construir una matriz de Hadamard de orden $428 = 4(3m-1)$, donde $m = 36$, a partir de las siguientes secuencias de Turyn de largos 36, 36, 36, 35, las cuales fueron encontradas con ayuda de un "cluster" de 16 PCs de 2.6 GHz, después de 12 horas de cálculo:
$X = (+++---++-+-+-----++++-++-++++----+-)$,
$Y = (+-++++++--+-+--+--++-+-++++-++++---++-)$,
$Z = (+-++++++-+--++++-+++-++--+++-+--+---+)$,
$W = (+++-+-----++--+-+++--+-+-+++-++++-+)$.

7 Método de Baumert-Hall

El método de Baumer-Hall (ver [3]) se basa en la siguiente observación. Considérese una matriz de Hadamard de orden $4n$ obtenida por el método de Williamson a través de las matrices A_1, A_2, A_3 y A_4 de orden n, simétricas y que commutan entre si, como en el teorema 6. Entonces,

podemos construir una nueva matriz de Hadamard H del doble del tamaño de la anterior de la siguiente forma:

$$H = \begin{pmatrix} \alpha & \beta & \gamma & \delta \\ -\beta & \alpha & -\delta & \gamma \\ -\gamma & \delta & \alpha & -\beta \\ -\delta & -\gamma & \beta & \alpha \end{pmatrix}, \tag{23}$$

donde

$$\alpha = \begin{pmatrix} A_1 & A_2 \\ A_2 & A_1 \end{pmatrix}, \quad \beta = \begin{pmatrix} A_1 & -A_2 \\ -A_2 & A_1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} A_3 & A_4 \\ A_4 & A_3 \end{pmatrix}, \quad \delta = \begin{pmatrix} A_3 & -A_4 \\ -A_4 & A_3 \end{pmatrix}.$$

Más aún, las matrices α, β, γ y δ son también simétricas y conmutan entre sí, de manera que el método puede repetirse una y otra vez, poniendo en evidencia que existen matrices de Hadamard para cualquier orden del tipo $2^i 4n$, con $i \in \mathbb{N}$. Utilizando esta idea simple, Baumert y Hall construyeron por primera vez una matriz de Hadamard de orden 156 que no había sido posible construir con los otros métodos conocidos.

8 Método de Cooper-Wallis

Una interesante manera de combinar las matrices de Williamson con las T-secuencias del método de Goethals-Seider se describe a continuación. Sean A_1, A_2, A_3, A_4 matrices de Williamson de orden n y sean T_1, T_2, T_3, T_4 matrices circulantes de orden m obtenidas a partir de cuatro T-secuencias de orden m. Sean X, Y, Z y W las matrices definidas por

$$\begin{array}{rcccccccc} X & = & T_1 \otimes A_1 & + & T_2 \otimes A_2 & + & T_3 \otimes A_3 & + & T_4 \otimes A_4, \\ Y & = & T_1 \otimes -A_2 & + & T_2 \otimes A_1 & + & T_3 \otimes A_4 & + & T_4 \otimes -A_3, \\ Z & = & T_1 \otimes -A_3 & + & T_2 \otimes -A_4 & + & T_3 \otimes A_1 & + & T_4 \otimes A_2, \\ W & = & T_1 \otimes -A_4 & + & T_2 \otimes A_3 & + & T_3 \otimes -A_2 & + & T_4 \otimes A_1. \end{array} \tag{24}$$

Cooper y Wallis demostraron (ver [5]) que la siguiente es una matriz H de Hadamard de orden $4nm$:

$$H = \begin{pmatrix} X & YR & ZR & WR \\ -YR & X & -W^tR & Z^tR \\ -ZR & W^tR & X & -W^tR \\ -WR & -Z^tR & Y^tT & X \end{pmatrix}. \tag{25}$$

De esa forma hallaron una matriz de Hadamard de orden $532 = 4nm$, donde $n = 7$ y $m = 19$, a partir de una matriz de Williamson de orden $4n = 28$ y otra de Goethals-Seider de orden $4m = 76$.

9 Método de Ehlich

El método de Ehlich (1965) es completamente constructivo y sigue las ideas originales de Paley para obtener el siguiente resultado.

Teorema 8 *Sean n y $n-2$ ambos potencias de primos impares tal que $n \equiv 3 \pmod 4$. Entonces existe una matriz de Hadamard de orden $(n-1)^2$ dada por*

$$H = \begin{pmatrix} 1 & \mathbf{e}_{n(n-2)}^t \\ \mathbf{e}_{n(n-2)} & K \end{pmatrix}, \tag{26}$$

donde $K = Q \otimes G + I_{n-2} \otimes (J_n - I_n) + J_{n-2} \otimes I_n$, con Q y G las matrices de Jacobsthal de órdenes $n-2$ y n respectivamente, definidas en (12) y $\mathbf{e}_{n(n-2)}$ el vector columna de 1's de tamaño $n(n-2)$.

DEMOSTRACIÓN: Ver ([7]). ∎

Por ejemplo, $n = 19$ y $n-2 = 17$ son primos tales que $19 \equiv 3 \pmod 4$. Luego, existe una matriz de Hadamard de orden $324 = (n-1)^2$ definida de acuerdo a (26). No se conoce otro método para este orden específico.

10 Método de Miyamoto

Miyamoto encontró en 1991 el siguiente método constructivo.

Teorema 9 *Sea q la potencia de un primo tal que $q \equiv 1 \pmod 4$. Suponga que existe una matriz de Hadamard de orden $q-1$. Entonces, existe una matriz de Hadamard de orden $4q$.*

CONSTRUCCIÓN: los detalles de la demostración del resultado anterior pueden consultarse en [14]. La construcción es la siguiente. Sea $q+1 = 2m+2$. Considérese la matriz de conferencia C en (13) de orden $q+1$, en la cual permutamos filas y columnas para obtener la matriz

$$S = \begin{pmatrix} 0 & 1 & \mathbf{e}^t & \mathbf{e}^t \\ 1 & 0 & \mathbf{e}^t & -\mathbf{e}^t \\ \mathbf{e} & \mathbf{e} & -C_1 & C_2 \\ \mathbf{e} & -\mathbf{e} & C_2^t & C_4 \end{pmatrix}, \tag{27}$$

donde C_1 y C_4 son simétricas de orden m y $\mathbf{e}$ denota el vector de 1's de largo m. Sea K la matriz de Hadamard de orden $q-1$ de la hipótesis, particionada en bloques de tamaño m:

$$K = \begin{pmatrix} K_1 & K_2 \\ -K_3 & K_4 \end{pmatrix}. \tag{28}$$

Definimos las matrices $U = U_{ij}$, $V = V_{ij}$ por bloques, mediante

$$U = \begin{pmatrix} C_1 & C_2 & \mathbf{0} & \mathbf{0} \\ -C_2^t & C_4 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & C_1 & C_2 \\ \mathbf{e} & -\mathbf{e} & -C_2^t & C_4 \end{pmatrix}, \quad V = \begin{pmatrix} I & \mathbf{0} & K_1 & K_2 \\ \mathbf{0} & I & K_3 & -K_4 \\ -K_1^t & -K_3^t & I & \mathbf{0} \\ -K_2^t & K_4^t & \mathbf{0} & I \end{pmatrix}. \tag{29}$$

Sean $T_{ij} = U_{ij} \otimes \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right) + V_{ij} \otimes \left(\begin{smallmatrix} 1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$ y se definen los bloques de matrices X_{ij} mediante

$$X_{ij} = \begin{pmatrix} 1 & \mathbf{e}_{2m}^t \\ \mathbf{e}_{2m} & T_{ij} \end{pmatrix},\ i \neq j, \qquad X_{ii} = \begin{pmatrix} 1 & -\mathbf{e}_{2m}^t \\ -\mathbf{e}_{2m} & T_{ii} \end{pmatrix}\ i = j. \tag{30}$$

Entonces,

$$H = \begin{pmatrix} X_{11} & X_{12} & X_{13} & X_{14} \\ -X_{21} & X_{22} & X_{23} & X_{24} \\ -X_{31} & -X_{32} & X_{33} & X_{34} \\ -X_{41} & X_{42} & -X_{43} & X_{44} \end{pmatrix} \tag{31}$$

es la matriz de Hadamard de orden $4(2m+1) = 4q$ requerida.

11 Conjuntos diferencia suplementarios

El método de construcción de Goethals y Seidel (1967) fue generalizado a través de la teoría de grupos abelianos finitos arbitrarios por Wallis y Whiteman en 1972 (ver [19]). El método explota los conjuntos diferencia suplementarios que satisfacen ciertas condiciones y fue empleado por Djokovic (ver [6]) para construir matrices de Hadamard de órdenes $4n$, para $n = 37$, 39, 43, 65, 67, 81, 103, 113, 121, 127, 129, 133, 151, 157, 163, 169, 181, 217, 219, 241, 267 y 463.

Veamos la definición de conjuntos diferencia suplementarios. Sea G un grupo abeliano finito de orden n. Para un subconjunto $S \subseteq G$ y $a \in G$, sea $v(s, a)$ el número de pares ordenados $(x, y) \in S^2$ tales que $x - y = a$. Decimos que los subconjuntos $S_1, \ldots, S_k \subseteq G$ son conjuntos diferencia suplementarios con parámetros $(n; n_1, \ldots, n_k; \lambda)$ si $|S_i| = n_i$ y $\sum_{i=1}^{k} v(S_i, a) = \lambda$, para todo $a \in G - \{0\}$. Aquí $\lambda \in G$ es fijo.

Para construir matrices de Hadamard se necesita hallar 4 conjuntos diferencia suplementarios S_1, S_2, S_3, S_4 cuyos parámetros $(n; n_1, \ldots, n_4; \lambda)$ satisfagan la condición $n + \lambda = n_1 + n_2 + n_3 + n_4$. En efecto, el resultado de Wallis y Whiteman establece lo siguiente:

Teorema 10 *Para cada subconjunto S del grupo abeliano finito G, sea A_S la matriz de orden n cuyas filas y columnas están indexadas por los*

elementos de G y cuya entrada (x, y) es -1 si $y - x \in S$, mientras que el valor es $+1$ en otro caso. Sean A_1, A_2, A_3, A_4 las matrices obtenidas de esa manera a partir de 4 conjuntos diferencia suplementarios S_1, S_2, S_3, S_4 con parámetros $(n; n_1, n_2, n_3, n_4; \lambda)$. Obtenemos una matriz de Hadamard de orden $4n$ al reemplazar en el método de Goethals-Seidel las matrices A, B, C, D de la fórmula (18) por A_1, A_2, A_3, A_4 respectivamente.

DEMOSTRACIÓN: Ver ([19]). No vamos a comentar aquí la enorme dificultad algorítmica de encontrar tales conjuntos diferencia suplementarios. ■

12 Métodos de recocido simulado

Algunos de los algoritmos anteriormente descritos requieren en la fase final de una búsqueda computacional, la cual generalmente se hace en forma exhaustiva. El autor propone realizar búsquedas heurísticas basadas en algoritmos de recocido simulado (ver [1]).

Veamos un ejemplo. El método de Goethals-Seidel sirve para generar matrices de Hadamard de órdenes $4(3m-1)$, si podemos encontrar cuatro secuencias X, Y, Z, W de Turyn de números en $\{-1, 1\}$, de longitudes m, m, m, $m-1$ respectivamente (ver las ecuaciones (18), (19), (20), (21) y (22)). Vamos a explicar cómo hallar estas secuencias de Turyn para valores pequeños de m, usando un algoritmo de recocido simulado. Empezamos con cuatro secuencias de números en $\{-1, 1\}$ X, Y, Z, W de longitudes m, m, m y $m-1$ respectivamente, seleccionadas al azar. La idea es realizar sucesivamente modificaciones en tales secuencias hasta encontrar una secuencia Turyn. Para tal efecto, definimos la función objetivo $f(X, Y, Z, W)$, que debemos minimizar, de la siguiente forma:

$$\begin{aligned} f(X,Y,Z,W) &= \|N_X + N_Y + 2N_Z + 2N_W\|_1 \qquad (32)\\ &= \sum_{s=1}^{m-1} \left|N_X(s) + N_Y(s) + 2N_Z(s) + 2N_W(s)\right| \\ &= \sum_{s=1}^{m-1} |\theta(s)|, \end{aligned}$$

donde $\theta(s) = N_X(s) + N_Y(s) + 2N_Z(s) + 2N_W(s)$. Esto es, se trata de la norma en $\mathbb{R}^{m-1}$ de la suma de los valores absolutos.

$4 = 2^2$	$172 =$ Williamson	$340 = 2(13^2 + 1)$	$508 =$ Supl.Di.Sets
$8 = 2^3$	$176 = 2 \otimes 2(43 + 1)$	$344 = 7^3 + 1$	$512 = 2^9$
$12 = 11 + 1$	$180 = 179 + 1$	$348 = 347 + 1$	$516 =$ Williamson
$16 = 2^4$	$184 = 2 \otimes 92$	$352 = 2^2 \otimes 2(43 + 1)$	$520 = 2 \otimes 260$
$20 = 19 + 1$	$188 =$ Goe-Sei	$356 =$ Goe-Sei	$524 = 523 + 1$
$24 = 23 + 1$	$192 = 191 + 1$	$360 = 359 + 1$	$528 = 2(263 + 1)$
$28 = 3^3 + 1$	$196 = 2(97 + 1)$	$364 = 2(181 + 1)$	$532 =$ Cooper-Wallis
$32 = 2^5$	$200 = 199 + 1$	$368 = 367 + 1$	$536 = 2 \otimes 268$
$36 = 2(17 + 1)$	$204 = 2(101 + 1)$	$372 =$ Baumert-Hall	$540 =$ Williamson
$40 = 2(19 + 1)$	$208 = 2(103 + 1)$	$376 = 2 \otimes 188$	$544 = 2(271 + 1)$
$44 = 43 + 1$	$212 = 211 + 1$	$380 = 379 + 1$	$548 = 547 + 1$
$48 = 47 + 1$	$216 = 2(107 + 1)$	$384 = 383 + 1$	$552 = 2 \otimes 2(137 + 1)$
$52 = 2(5^2 + 1)$	$220 = 2(109 + 1)$	$388 = 2(193 + 1)$	$556 =$ Williamson
$56 = 2(3^3 + 1)$	$224 = 223 + 1$	$392 = 2 \otimes 2(97 + 1)$	$560 = 2 \otimes 2(139 + 1)$
$60 = 59 + 1$	$228 = 227 + 1$	$396 = 2(197 + 1)$	$564 = 563 + 1$
$64 = 2^6$	$232 = 2 \otimes 116$	$400 = 2(199 + 1)$	$568 = 2(283 + 1)$
$68 = 67 + 1$	$236 =$ Goe-Sei	$404 =$ Goe-Sei	$572 = 571 + 1$
$72 = 71 + 1$	$240 = 239 + 1$	$408 = 2 \otimes 2(101 + 1)$	$576 = 2^2 \otimes 2(71 + 1)$
$76 = 2(37 + 1)$	$244 = 3^5 + 1$	$412 =$ Supl.Di.Sets	$580 = 2(17^2 + 1)$
$80 = 79 + 1$	$248 = 2 \otimes 2(61 + 1)$	$416 = 2 \otimes 2(103 + 1)$	$584 = 2 \otimes 292$
$84 = 83 + 1$	$252 = 251 + 1$	$420 = 419 + 1$	$588 = 587 + 1$
$88 = 2(43 + 1)$	$256 = 2^8$	$424 = 2(211 + 1)$	$592 = 2^2 \otimes 2(73 + 1)$
$92 =$ Williamson	$260 =$ Goe-Sei	$428 =$ Goe-Sei	$596 =$ Miyamoto
$96 = 2(47 + 1)$	$264 = 263 + 1$	$432 = 431 + 1$	$600 = 2 \otimes 2(149 + 1)$
$100 = 2(7^2 + 1)$	$268 =$ Williamson	$436 =$ Miyamoto	$604 =$ Supl.Di.Sets
$104 = 103 + 1$	$272 = 271 + 1$	$440 = 439 + 1$	$608 = 607 + 1$
$108 = 107 + 1$	$276 = 2(137 + 1)$	$444 = 443 + 1$	$612 =$ Baumert-Hall
$112 = 2 \otimes 2(3^3 + 1)$	$280 = 2(139 + 1)$	$448 = 2(223 + 1)$	$616 = 2(307 + 1)$
$116 =$ Williamson	$284 = 283 + 1$	$452 =$ Miyamoto	$620 = 619 + 1$
$120 = 2(59 + 1)$	$288 = 2 \otimes 2(71 + 1)$	$456 = 2(227 + 1)$	$624 = 2(311 + 1)$
$124 = 2(61 + 1)$	$292 =$ Williamson	$460 =$ Williamson	$628 =$ Williamson
$128 = 2^7$	$296 = 2 \otimes 2(73 + 1)$	$464 = 463 + 1$	$632 = 631 + 1$
$132 = 131 + 1$	$300 = 2(149 + 1)$	$468 = 467 + 1$	$636 =$ Williamson
$136 = 2(67 + 1)$	$304 = 2(151 + 1)$	$472 = 2 \otimes 236$	$640 = 2^2 \otimes 2(79 + 1)$
$140 = 139 + 1$	$308 = 307 + 1$	$476 =$ Cooper-Wallis	$644 = 643 + 1$
$144 = 2(71 + 1)$	$312 = 311 + 1$	$480 = 479 + 1$	$648 = 2 \otimes 324$
$148 = 2(73 + 1)$	$316 = 2(157 + 1)$	$484 =$ Williamson	$652 =$ Supl-DS
$152 = 151 + 1$	$320 = 2 \otimes 2(79 + 1)$	$488 = 487 + 1$	$656 = 2 \otimes 2(163 + 1)$
$156 =$ Williamson	$324 =$ Ehlich	$492 = 491 + 1$	$660 = 659 + 1$
$160 = 2(79 + 1)$	$328 = 2(163 + 1)$	$496 = 2^2 \otimes 2(61 + 1)$	$664 = 2(331 + 1)$
$164 = 163 + 1$	$332 = 331 + 1$	$500 = 499 + 1$	$668 =$??
$168 = 167 + 1$	$336 = 2(167 + 1)$	$504 = 503 + 1$	

Figura 3: **Criba de Hadamard:** *primeros múltiplos de 4 y alguna de sus matrices de Hadamard correspondientes. En la tabla se anota el método más fácil empleado en la generación: Sylvester, Paley, Kronecker, Williamson, Goethals-Seidel, Baumert-Hall, Enlich, Miyamoto, Conjuntos Diferencia Suplementarios. En algunos casos es posible aplicar varios de los métodos anteriores. El primer múltiplo de 4 para el cual no se conoce ninguna matriz de Hadamard es* 668. *Los otros órdenes aún por resolver y menores que 2000 son: 716, 764, 892, 956, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1852, 1912, 1916, 1948 y 1964.*

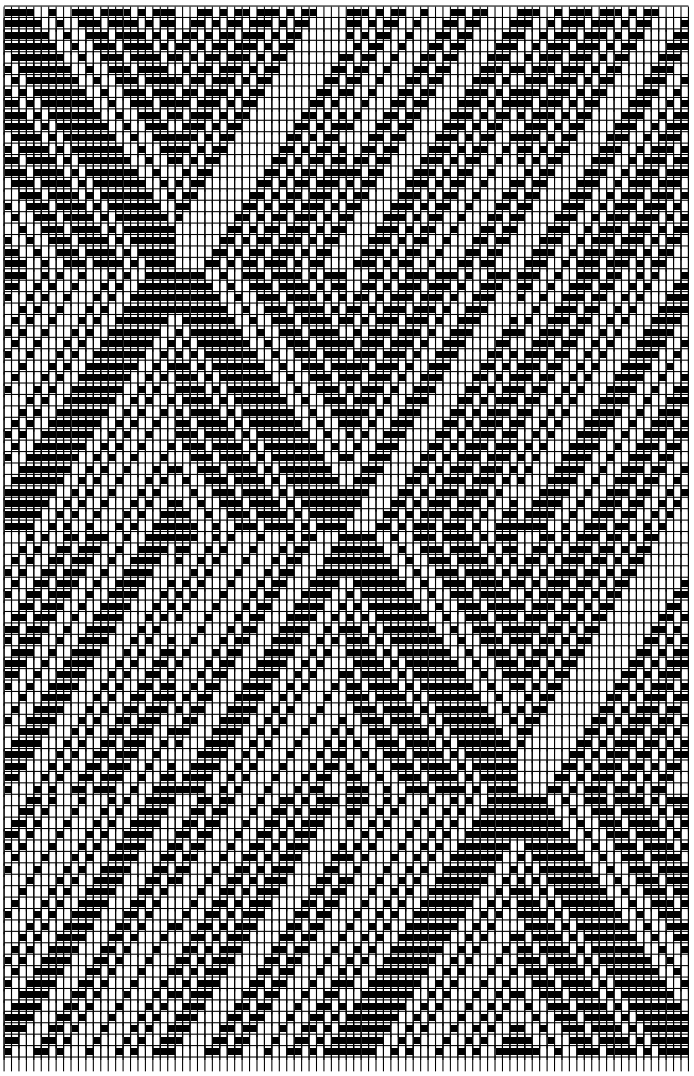

Figura 4: *Matriz de Hadamard de orden 92 a partir de una secuencia X, Y, Z, W de Turyn de longitud 8, construida con el algoritmo de recocido simulado en 0,61 segundos. Los cuadros negros representan a -1 y los blancos a 1, o viceversa.*

Para aplicar un algoritmo de recocido simulado, las perturbaciones en las entradas de las secuencias X, Y, Z, W consisten en lo siguiente. Se elige al azar una de las secuencias X, Y, Z, W, y se selecciona al azar una posición $i_0 \in \{1,\ldots,m\}$ (o bien $i_0 \in \{1,\ldots,m-1\}$, en el caso de la secuencia W). Entonces, la perturbación consiste en cambiar x_{i_0} (o bien y_{i_0}, o z_{i_0}, o w_{i_0}, según corresponda) por su negativo.

Antes de realizar físicamente la perturbación en x_{i_0} (o bien y_{i_0}, o z_{i_0}, o w_{i_0}), se procede a calcular el cambio $\Delta(s)$ en la secuencia X mediante

$$\Delta(s) = \begin{cases} 2x_{i_0}(x_{i_0-s} + x_{i_0+s}), \text{ si } x_{i_0} \text{ fue seleccionado} \\ 2y_{i_0}(y_{i_0-s} + y_{i_0+s}), \text{ si } y_{i_0} \text{ fue seleccionado} \\ 4z_{i_0}(z_{i_0-s} + z_{i_0+s}), \text{ si } z_{i_0} \text{ fue seleccionado} \\ 4w_{i_0}(w_{i_0-s} + w_{i_0+s}), \text{ si } w_{i_0} \text{ fue seleccionado,} \end{cases} \tag{33}$$

para $s = 1,\ldots,M$, donde $M = \max\{m - i_0, i_0 - 1\}$. El cambio en la función objetivo si realizáramos la perturbación propuesta es entonces

$$\Delta f(X,Y,Z,W) = \sum_{s=1}^{M} |\theta(s)| - |\theta(s) - \Delta(s)|. \tag{34}$$

Si $\Delta f(X,Y,Z,W) \geq 0$, la perturbación produce una mejora al proceso y por consiguiente se acepta la perturbación incondicionalmente, actualizando:

$$\begin{aligned} x_{i_0} &\leftarrow -x_{i_0}, \text{ o bien } y_{i_0}, z_{i_0}, w_{i_0}, \\ N_X(s) &\leftarrow N_X(s) - \Delta(s), \text{ o bien } N_Y, N_Z, N_W, \\ \theta(s) &\leftarrow \theta(s) - \Delta(s) \\ f(X,Y,Z,W) &\leftarrow \sum_{s=1}^{M} |\theta(s)|. \end{aligned}$$

Si $\Delta f(X,Y,Z,W) < 0$, la perturbación produciría una peor configuración, la cual aún podría ser aceptada de acuerdo con la regla de Metropolis, cual es aceptar con probabilidad

$$e^{\Delta f(X,Y,Z,W)/\,t},$$

donde t es la temperatura del sistema. De esta manera, la probabilidad de aceptar una perturbación cualquiera (buena o mala) es igual a

$$\min\{1, e^{\Delta f(X,Y,Z,W)/\,t}\}, \tag{35}$$

que sigue la ley de Maxwell-Boltzmann. La implementación del algoritmo de recocido simulado utiliza el siguiente plan de enfriamiento:

Temperatura inicial: t_0 es seleccionada de manera que la regla de Metropolis sea suficientemente tolerante para aceptar al principio aproximadamente $\chi \times 100\%$ de "malas" configuraciones, donde $\chi \in (0,1)$ es una constante preseleccionada (generalmente empleamos $\chi = 60\%$). Se realiza una secuencia de corridas preliminares en falso con el fin de estimar t_0 con este requisito.

Enfriamiento: cada cierto número de etapas el sistema es enfriado lentamente, disminuyendo el valor de la temperatura t_k, utilizando un esquema geométrico: $t_{k+1} = \lambda \cdot t_k$, donde λ es una constante previamente seleccionada, empíricamente entre $[0.92, 0.98]$. Hemos obtenido buenos resultados con $\lambda = 0.97$ en nuestros experimentos.

Longitud de las cadenas de temperaturas: el parámetro de temperatura t_k es actualizado cada nLimit iteraciones, o bien cuando ya se han aceptado nOver "malas" configuraciones con tal temperatura. Hemos experimentado con valores de nLimit $\in [10^5, 10^7]$ y nOver $\in [10^4, 10^6]$, dependiendo del tamaño m de las secuencias Turyn buscadas.

Criterio de parada: un máximo de 150 ciclos de temperatura son completados, debido a que en la práctica la cantidad $t_{150} = t_0^{150}$ es casi nula, independientemente del valor inicial t_0. Sin embargo, si para los últimos nCad ciclos de temperatura no obtenemos ninguna mejora, entonces el proceso es finalizado. Hemos utilizado experimentalmente el parámetro nCad $= 3$ con resultados aceptables.

Hemos obtenido secuencias Turyn para todas las longitudes (pares) $m = 2k$, con $1 \leq k \leq 15$ en tiempos rápidos (inferiores a 1 hora) corriendo este algoritmo en una computadora de bolsillo (Aspire One). Aún no hemos encontrado soluciones para $m = 32$ en adelante. Nuestro objetivo es afinar el algoritmo seleccionando adecuadamente los parámetros χ, λ, nLimit, nOver, nCad, con el fin de buscar una posible solución para casos tales como $m = 56$, el cual corresponde precisamente a la búsqueda de la matriz de Hadamard de orden 668, el mínimo orden para el cual aún no se conoce la existencia de la misma.

Referencias

[1] Aarts, E.; Korst, J. (1990) *Simulated Annealing and Boltzmann Machines. A Stochastic Approach to Combinatorial Optimization and Neural Computing.* John Wiley & Sons, Chichester.

[2] Baumert, L.; Golomb, S.W.; Hall, M. (1962) "Discovery of a Hadamard matrix of order 92", *Bull. Amer. Math. Soc.* **68**(3): 237–238.

[3] Baumert, L.D.; Hall, M. (1965) "A new construction method for Hadamard matrices, *Bull. Amer. Math. Soc.* **71**: 169–170.

[4] Belevitch, V. (1950) "Theorem of $2n$-terminal networks with application to conference telephony", *Electr. Commun.* **26**: 231–244.

[5] Cooper, J.; Wallis, J.S. (1972) "A construction for Hadamard arrays", *Bull. Austral. Math. Soc.* **7**: 269–278.

[6] Djokovic, D.Z. (1993) "Williamson matrices of order $4n$ for $n = 33$, 35, 39", *Discrete Math.* **115**: 267–271.

[7] Ehlich, H. (1965) "Neue Hadamard-Matrizen", *Arch. Math.* **16**: 34–36.

[8] Faddeev, D.K.; Sominskii, I.S. (1965) *Higher Algebra Problems.* W.H. Freeman, San Francisco.

[9] Goethals, J.M.; Seidel, J.J. (1967) "Orthogonal matrices with zero diagonal", *Canadian Journal of Mathematics*, **19**: 1001–1010.

[10] Hadamard, J. (1893) "Résolution d'une question relative aux déterminants", *Bull. Sci. Math.* **17**: 240–246.

[11] Hall, M. (1992) *Combinatorial Theory*, second edition. Wiley Interscience, New York.

[12] Kharaghani, H.; Tayfeh-Rezaie, B. (2005) "A Hadamard matrix of order 428", *Journal of Combinatorial Designs* **13**: 435–440.

[13] van Lint, J.H.; Wilson, R.M. (2001) *A Course in Combinatorics*, second edition. Cambridge University Press, U.K.

[14] Miyamoto, M.A. (1991)" Construction of Hadamard matrices", *Journal of Combinatorial Theory, Series A*, **57**(1), 86–108.

[15] Paley, R. (1933) "On orthogonal matrices", *Journal Math. Phys.* **12**: 311–320.

[16] Seberry, J.; Yamada, M. (1992) "Hadamard matrices, sequences, and block designs", en: J.H. Dinitz & D.R. Stinson (Eds.) *Contemporary Design Theory: A Collection of Surveys*, Wiley, New York: 431–560.

[17] Turyn, R.J. (1972) "An infinite class of Williamson matrices", *Journal of Combinatorial Theory*, Series A, **12**: 319–321.

[18] Turyn, R.J. (1974) "Hadamard matrices, Baumert-Hall units, four-symbols sequences, pulse compression, and surface wave enconding", *Journal of Combinatorial Theory*, Series A, **16**: 313–333.

[19] Wallis, J.; Whiteman, A.L. (1972) "Some classes of Hadamard matrices with constant diagonal", *Bull. Austral. Math. Soc.* **7**: 233–249.

[20] Williamson, J. (1944) "Hadamard's determinant theorem and the sum of four squares", *Duke Mathematical Journal*, **11**: 65–81.