© Revista de Matemática: Teoría y Aplicaciones 2019 **26**(2) : 253–279
cimpa – ucr issn: 1409-2433 (Print), 2215-3373 (Online)
doi: https://doi.org/10.15517/rmta.v26i2.38317

SECUENCIAS TIPO TURYN

TURYN TYPE SEQUENCES

Esteban Segura Ugalde* Eduardo Piza Volio†

Received: 19/Nov/2018; Revised: 27/May/2019;
Accepted: 28/May/2019

*Universidad de Costa Rica, Escuela de Matemática y Centro de Investigación en Matemática Pura y Aplicada CIMPA, San José, Costa Rica. E-Mail: esteban.seguraugalde@ucr.ac.cr
†Misma dirección que/Same address as: E. Segura. E-Mail: eduardo.piza@ucr.ac.cr

Resumen

En este artículo estudiamos fundamentalmente las denominadas *secuencias tipo Turyn* y algunos algoritmos heurísticos para generarlas. La importancia de estas secuencias estriba, al menos, en el hecho de que pueden ser empleadas en la construcción de algunas matrices de Hadamard de órdenes $4(3m-1)$, donde m es el largo de la *secuencia tipo Turyn* a través del uso del teorema de Goethals-Seidal. Simplificamos la demostración del teorema de Turyn (ver Teorema 3). Además, hallamos algunos resultados teóricos interesantes (ver Teorema 5). Finalmente, desarrollamos varios algoritmos heurísticos eficientes, comparables a los algoritmos ya conocidos, que generan secuencias tipo Turyn de tamaños menores o iguales a 40.

Palabras clave: secuencias tipo Turyn; teorema de Goethals-Seidal; matrices de Hadamard; recocido simulado; optimización combinatoria.

Abstract

In this paper we study the so called *Turyn type sequences* and some heuristics algorithms to generate them. The importance of these sequences lies, at least, in the fact that they can be used to construct some Hadamard matrices of order $4(3m-1)$, where m is the length of the *Turyn type sequence* through the theorem of Goethals-Seidal. We simplify the proof of Turyn's theorem (see Theorem 3). In addition, we find some interesting theoretical results (see Theorem 5). Finally, we develop several efficient heuristic algorithms, comparable to the algorithms already known, that generate Turyn type sequences of sizes less than or equal to 40.

Keywords: Turyn type sequences; Goethals-Seidel theorem; Hadamard matrices; simulated annealing; combinatorial optimization.

Mathematics Subject Classification: 05B20, 05B30, 15B34, 90C27.

1 Introducción

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

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

De la definición anterior, está claro que cualesquiera dos columnas (o filas) de H son ortogonales. Evidentemente, esta propiedad de ortogonalidad no cambia si permutamos las filas o las columnas, o si multiplicamos alguna fila o columna por -1; las matrices resultantes 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 en el último ejemplo, para abreviar, solamente se indicaron los signos de las entradas.

Hadamard [14] consideró el siguiente problema: Sea $A = (a_{ij})$ una matriz $n \times n$ con entradas reales, tales que $|a_{ij}| \leq 1$. ¿Qué tan grande puede llegar a ser el determinante de A (en valor absoluto)? Es decir, se trata de resolver el problema de optimización

$$\underset{\text{sujeto a } |a_{ij}| \leq 1}{\text{Maximizar}} \; |\det(A)|. \tag{3}$$

Debido a la restricción $|a_{ij}| \leq 1$, entonces cada fila de A es un vector con longitud euclídea menor o igual a $\sqrt{n}$, de donde 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, siempre se satisface la desigualdad

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

En el caso de matrices A con entradas complejas, *la igualdad* en (4) se alcanza con la matriz de Vandermonde de las raíces n-ésimas de la unidad, como fue demostrado por Faddeev and Sominskii [12].

Originalmente Hadamard demostró [14] que en el caso de matrices con entradas reales, *la igualdad* en (4) se alcanza en la solución óptima del problema (3) 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 están en $\{-1, 1\}$ y sus filas (también sus columnas) son ortogonales: $HH^t = nI_n$.

El problema anterior es conocido en la literatura como el *problema del determinante maximal* y ha sido profundamente 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 $n = 22$; tan solo se dispone de burdas aproximaciones [4]. 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 se han realizado muchas investigaciones y generalizaciones [5].

Modernamente se han encontrado algunas conexiones entre las matrices de Hadamard y otros campos de las matemáticas, tales como la teoría de números [8], la combinatoria, los espacios de Banach [19] y la teoría de grupos [16]. Las matrices de Hadamard además han sido utilizadas para mejorar la precisión de los espectrómetros [28], para realizar diseños experimentales en estadística aplicados a la agricultura [7], para el diseño de claves criptográficas y para el diseño de códigos auto-correctores de errores en mensajes e imágenes trasmitidas desde el espacio lejano, entre otros diversos problemas aplicados [21, 2, 6].

2 Conjetura de Hadamard

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

Teorema 1 [14] *Si H es una matriz de Hadamard de orden n, entonces $n = 1$, o $n = 2$ o n es múltiplo de 4.*

Demostración. La demostración es sencilla y puede consultarse en [24]. ■

El recíproco de este teorema es la famosa *conjetura de Hadamard*, la cual afirma que para cada orden positivo n múltiplo de 4 existe una matriz de Hadamard de orden n. En realidad, esta conjetura es atribuida a Paley desde 1933. Se trata de un problema abierto en matemáticas que se encuentra muy lejos de ser demostrado o refutado.

Existen gran cantidad de métodos y algoritmos para generar matrices de Hadamard de muy diversos órdenes [24], entre los cuales mencionamos algunos; construcciones de Paley (I y II), construcciones de Kronecker, construcciones de Sylvester, el método de Williamson, el método de Goethals-Seidel, el método de Baumer-Hall, el método de Cooper-Wallis, el método de Ehlich, el método de Miyamoto, el método de Scarpis y el método de las construcciones de conjuntos diferencia suplementarios. Algunos de estos métodos construyen matrices de Hadamard de infinidad de órdenes, aunque ni siquiera todos los métodos conocidos juntos consiguen generar algunas matrices de Hadamard de órdenes muy particulares.

Por ejemplo, las construcciones de Paley [25] encuentran matrices de Hadamard de órdenes $q+1$, cuando $q \equiv 3(mod\,4)$, y órdenes $2(q+1)$, cuando $q \equiv 1(mod\,4)$, donde q es cualquier potencia positiva de un primo impar. Sin embargo, estas construcciones de Paley dejan por fuera gran cantidad de múltiplos de 4, entre ellos 40, 56, 64, 92, 96, 100, 104, 112, 116, 120, 136, 144, 156, 160, 172, 176, 184 y 188, para citar órdenes por debajo de 200.

Por otra parte, la construcción de Sylvester funciona solamente para los órdenes que sean potencias de 2 y se trata de un caso particular de la construcción de Kronecker [24]. Esta última establece que si H_n y H_m son matrices de Hadamard de órdenes n y m respectivamente, entonces $H_n \otimes H_m$ (el producto de Kronecker) es una matriz de Hadamard de orden nm.

Y está el poderoso método de Miyamoto [23], que requiere de una larga y compleja búsqueda computacional de ciertas matrices preliminares. Miyamoto obtuvo éxito con su método hallando matrices de Hadamard para los siguientes órdenes: 292, 332, 356, 404, 412, 436, 452, 508, 596, 604, 692, 772, 788, 876, 932, 964, 996, y algunos otros órdenes por encima de 1000.

En la Figura 1 se presenta la *criba de Hadamard*, una representación gráfica de los primeros múltiplos de 4, entre 4 y 1000, indicándose cuál de los métodos anteriormente mencionados es efectivo para la construcción de una matriz de Hadamard. En la figura, se anota el método más fácil empleado en la generación, Sylvester (órdenes 4, 8, 16, etc.), Paley (órdenes 12, 20, 28, etc.), Kronecker (órdenes 24, 40, 48, etc.), Williamson (órdenes 92, 100, 116, etc.), Goethals-Seidel (órdenes 188, 236, 260, etc.), Baumert-Hall (órdenes 372, 612), Enlich (orden 324), Miyamoto (órdenes 436, 452, 692), Scarpis (orden 756), Wallis (órdenes 836, 996), Conjuntos Diferencia Suplementarios (órdenes 412, 604, 508, etc.), Cooper-Wallis (órdenes 476, 552). 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, 892, 1004, 1132, 1244, 1388, 1436, 1676, 1772, 1852, 1912, 1916, 1948 y 1964.

$4 = 2^2$	$204 = 2(101+1)$	$404 =$ Goe-Sei	$604 =$ Supl.Di.Sets	$804 = 2(401+1)$
$8 = 2^3$	$208 = 4 \otimes 52$	$408 = 2 \otimes 204$	$608 = 8 \otimes 76$	$808 = 2 \otimes 404$
$12 = 11+1$	$212 = 211+1$	$412 =$ Supl.Di.Sets	$612 =$ Baumert-Hall	$812 = 811+1$
$16 = 2^4$	$216 = 2 \otimes 108$	$416 = 8 \otimes 52$	$616 = 2 \otimes 308$	$816 = 4 \otimes 204$
$20 = 19+1$	$220 = 2(109+1)$	$420 = 419+1$	$620 = 619+1$	$820 = 2(409+1)$
$24 = 2 \otimes 12$	$224 = 8 \otimes 28$	$424 = 2 \otimes 212$	$624 = 4 \otimes 156$	$824 = 2 \otimes 412$
$28 = 3^3+1$	$228 = 227+1$	$428 =$ Goe-Sei	$628 =$ Williamson	$828 = 827+1$
$32 = 2^5$	$232 = 2 \otimes 116$	$432 = 4 \otimes 108$	$632 = 2 \otimes 316$	$832 = 8 \otimes 104$
$36 = 2(17+1)$	$236 =$ Goe-Sei	$436 =$ Miyamoto	$636 =$ Williamson	$836 =$ Wallis
$40 = 2 \otimes 20$	$240 = 4 \otimes 60$	$440 = 2 \otimes 220$	$640 = 20 \otimes 32$	$840 = 2 \otimes 420$
$44 = 43+1$	$244 = 3^5+1$	$444 = 443+1$	$644 = 643+1$	$844 = 2(421+1)$
$48 = 4 \otimes 12$	$248 = 2 \otimes 124$	$448 = 16 \otimes 28$	$648 = 2 \otimes 324$	$848 = 4 \otimes 212$
$52 = 2(5^2+1)$	$252 = 251+1$	$452 =$ Miyamoto	$652 =$ Supl.Di.Sets	$852 =$ Supl.Di.Sets
$56 = 2 \otimes 28$	$256 = 2^8$	$456 = 2 \otimes 228$	$656 = 4 \otimes 164$	$856 = 2 \otimes 428$
$60 = 59+1$	$260 =$ Goe-Sei	$460 =$ Williamson	$660 = 659+1$	$860 = 859+1$
$64 = 2^6$	$264 = 2 \otimes 132$	$464 = 4 \otimes 116$	$664 = 2 \otimes 332$	$864 = 8 \otimes 108$
$68 = 67+1$	$268 =$ Williamson	$468 = 467+1$	**668** $=$ desconocido	$868 =$ Supl.Di.Sets
$72 = 2 \otimes 36$	$272 = 4 \otimes 68$	$472 = 2 \otimes 236$	$672 = 8 \otimes 84$	$872 = 2 \otimes 436$
$76 = 2(37+1)$	$276 = 2(137+1)$	$476 =$ Cooper-Wallis	$676 = 2(337+1)$	$876 =$ Supl.Di.Sets
$80 = 4 \otimes 20$	$280 = 2 \otimes 140$	$480 = 8 \otimes 60$	$680 = 2 \otimes 340$	$880 = 4 \otimes 220$
$84 = 83+1$	$284 = 283+1$	$484 =$ Williamson	$684 = 683+1$	$884 = 883+1$
$88 = 2 \otimes 44$	$288 = 8 \otimes 36$	$488 = 2 \otimes 244$	$688 = 4 \otimes 172$	$888 = 2 \otimes 444$
$92 =$ Williamson	$292 =$ Williamson	$492 = 491+1$	$692 =$ Miyamoto	**892** $=$ desconocido
$96 = 8 \otimes 12$	$296 = 2 \otimes 148$	$496 = 4 \otimes 124$	$696 = 2 \otimes 348$	$896 = 28 \otimes 32$
$100 =$ Williamson	$300 = 2(149+1)$	$500 = 499+1$	$700 = 2(349+1)$	$900 = 2(449+1)$
$104 = 2 \otimes 52$	$304 = 4 \otimes 76$	$504 = 2 \otimes 252$	$704 = 16 \otimes 44$	$904 = 2 \otimes 452$
$108 = 107+1$	$308 = 307+1$	$508 =$ Supl.Di.Sets	$708 = 2(353+1)$	$908 = 907+1$
$112 = 4 \otimes 28$	$312 = 2 \otimes 156$	$512 = 2^9$	$712 = 2 \otimes 356$	$912 = 4 \otimes 228$
$116 =$ Williamson	$316 = 2(157+1)$	$516 =$ Williamson	**716** $=$ desconocido	$916 = 2(457+1)$
$120 = 2 \otimes 60$	$320 = 16 \otimes 20$	$520 = 2 \otimes 260$	$720 = 4 \otimes 180$	$920 = 2 \otimes 460$
$124 = 2(61+1)$	$324 =$ Enlich	$524 = 523+1$	$724 =$ Supl.Di.Sets	$924 = 2(461+1)$
$128 = 2^7$	$328 = 2 \otimes 164$	$528 = 4 \otimes 132$	$728 = 2 \otimes 364$	$928 = 8 \otimes 116$
$132 = 131+1$	$332 = 331+1$	$532 =$ Cooper-Wallis	$732 =$ Williamson	$932 =$ Miyamoto
$136 = 2 \otimes 68$	$336 = 4 \otimes 84$	$536 = 2 \otimes 268$	$736 = 8 \otimes 92$	$936 = 2 \otimes 468$
$140 = 139+1$	$340 = 2(13^2+1)$	$540 =$ Williamson	$740 = 739+1$	$940 =$ Supl.Di.Sets
$144 = 4 \otimes 36$	$344 = 2 \otimes 172$	$544 = 8 \otimes 68$	$744 = 2 \otimes 186$	$944 = 4 \otimes 236$
$148 = 2(73+1)$	$348 = 347+1$	$548 = 547+1$	$748 = 2(373+1)$	$948 = 947+1$
$152 = 2 \otimes 76$	$352 = 8 \otimes 44$	$552 = 2 \otimes 276$	$752 = 4 \otimes 188$	$952 = 2 \otimes 476$
$156 =$ Williamson	$356 =$ Goe-Sei	$556 =$ Williamson	$756 =$ Scarpis	$956 =$ Goe-Sei
$160 = 8 \otimes 20$	$360 = 2 \otimes 180$	$560 = 4 \otimes 140$	$760 = 2 \otimes 380$	$960 = 16 \otimes 60$
$164 = 163+1$	$364 = 2(181+1)$	$564 = 563+1$	$764 =$ Goe-Sei	$964 =$ Miyamoto
$168 = 2 \otimes 84$	$368 = 4 \otimes 92$	$568 = 2 \otimes 284$	$768 = 24 \otimes 32$	$968 = 2 \otimes 484$
$172 =$ Williamson	$372 =$ Baumert-Hall	$572 = 571+1$	$772 =$ Miyamoto	$972 = 971+1$
$176 = 4 \otimes 44$	$376 = 2 \otimes 188$	$576 = 16 \otimes 36$	$776 = 2 \otimes 388$	$976 = 4 \otimes 244$
$180 = 179+1$	$380 = 379+1$	$580 = 2(17^2+1)$	$780 = 2(389+1)$	$980 =$ Goe-Sei
$184 = 2 \otimes 92$	$384 = 12 \otimes 32$	$584 = 2 \otimes 292$	$784 = 4 \otimes 196$	$984 = 2 \otimes 492$
$188 =$ Goe-Sei	$388 = 2(193+1)$	$588 = 587+1$	$788 =$ Miyamoto	$988 =$ Supl.Di.Sets
$192 = 191+1$	$392 = 2 \otimes 196$	$592 = 4 \otimes 148$	$792 = 2 \otimes 396$	$992 = 8 \otimes 124$
$196 = 2(97+1)$	$396 = 2(197+1)$	$596 =$ Miyamoto	$796 = 2(397+1)$	$996 =$ Wallis
$200 = 199+1$	$400 = 4 \otimes 100$	$600 = 2 \otimes 300$	$800 = 8 \otimes 100$	$1000 = 2 \otimes 500$

Figura 1: Criba de Hadamard: primeros múltiplos de 4 hasta 1000 y un método empleado para hallar una matriz de Hadamard del orden correspondiente.

Los menores órdenes n positivos y múltiplos de 4 para los cuales, hasta hace poco, aún no se conocía una matriz de Hadamard asociada eran 428, 668, 716, 764, 892 y algunos otros mayores que 1000. Sin embargo, en el año 2005 Khagharani y Tayfeh-Rezaie [17] hallaron una matriz de Hadamard de orden 428 utilizando el teorema de Goethals-Seidel y *secuencias tipo Turyn*. Y en el año 2008 Đoković [10] redujo aún más la lista, pues halló una matriz de Hadamard de orden 764 utilizando también el teorema de Goethals-Seidel, pero esta vez utilizando el método de *conjuntos diferencia suplementarios*. Entonces, la lista de los múltiplos de 4 menores que 1000 para los cuales aún no se conoce una matriz de Hadamard del orden correspondiente es 668, 716 y 892.

Otro problema distinto es hallar el número de matrices de Hadamard no-equivalentes entre sí, de orden n. Hasta la fecha solamente se conoce la solución para $n \leq 32$ [18], para los órdenes 1, 2, 4, 8, 12, 16, 20, 24, 28 y 32 hay únicamente 1, 1, 1, 1, 1, 5, 3, 60, 487 y 13 710 027 matrices de Hadamard no-equivalentes, respectivamente. Esta aparente explosión combinatoria sugiere fuertemente la validez de la conjetura de Hadamard.

3 Teorema de Goethals-Seidel

A continuación se estudia el método de Goethals-Seidel [13] para encontrar matrices de Hadamard, que ha sido efectivo en muchos casos donde fallan todos los demás métodos.

Teorema 2 [13] *Sean A, B, C y D matrices circulantes de orden n con entradas en $\{-1,1\}$ 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*

$$H = \begin{pmatrix} A & BR & CR & DR \\ -BR & A & D^tR & -C^tR \\ -CR & -D^tR & A & B^tR \\ -DR & C^tR & -B^tR & A \end{pmatrix}, \tag{5}$$

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

Demostración. Puede consultarse en [13]. ■

Si bien el teorema anterior tiene una demostración elemental y es una poderosa herramienta para hallar matrices de Hadamard de órdenes obtusos, la cosa no es tan sencilla como parece, pues el teorema requiere hallar las 4 matrices circulantes A, B, C, D, que cumplan $AA^t + BB^t + CC^t + DD^t = 4nI_n$. Básicamente, hay dos caminos principales para intentar construir estas matrices circulantes A, B, C, D:

i) Utilizar el método de los *conjuntos diferencia suplementarios* [11, 26, 27], que es el camino adoptado por varios investigadores, entre ellos Seberry y Đoković (este último halló en 2008 la matriz de Hadamard de orden 764 con ese método).

ii) Construir una *secuencia tipo Turyn* de algún orden apropiado [17, 24], con la cual la construcción de las matrices circulantes A, B, C, D, queda automáticamente garantizada, como veremos más adelante. Este es el enfoque que siguieron Kharaghani y Tayfeh-Rezaie para hallar en 2005 la matriz de Hadamard de orden 428. Es también el enfoque que nosotros seguimos en nuestra actual investigación.

Ambos caminos requieren en su momento crítico de la utilización intensiva de cálculos con una computadora, para hallar ciertas configuraciones muy específicas.

Un comentario adicional debe hacerse: el método de Goethals-Seidel no ofrece solución para cada entero positivo n (si así fuese, sería una demostración formal de la conjetura de Hadamard). En efecto, en 1999 se demostró [9, 15] por enumeración exhaustiva de posibilidades (fuerza bruta) que para $n = 35$ no existen matrices circulantes A, B, C, D, con valores en $\{-1, 1\}$ tales que $AA^t + BB^t + CC^t + DD^t = 140I_{35}$, de donde el método de Goethals-Seidal es del todo inaplicable para hallar una matriz de Hadamard de orden $140 = 4 \cdot 35$. Sin embargo, con el simple método de Paley se encuentra una matriz de Hadamard de orden 140, ya que $140 = 139 + 1$, y 139 es un número primo tal que $139 \equiv 3 \pmod 4$.

4 Secuencias tipo Turyn

Las funciones de autorrelación no-periódicas, así como los conceptos de *secuencias base* y *secuencias tipo Turyn* se definen a continuación. La principal referencia de estas definiciones puede consultarse en [29].

Definición 1 *Para una secuencia finita* $A = (a_1, a_2, \ldots, a_m)$ *de largo* m*, la* función de autocorrelación no-periódica*,* N_A*, se define mediante*

$$N_A(s) = \begin{cases} \sum_{i=1}^{m-s} a_i a_{i+s}, & \text{si } s = 0, 1, \ldots, m-1 \\ 0, & \text{si } s \geq m. \end{cases} \tag{6}$$

Definición 2 *Un conjunto de cuatro secuencias finitas* X*,* Y*,* Z*,* W*, de números en* $\{-1, +1\}$ *de largos* m*,* m*,* m *y* $m-1$ *se denomina* tipo Turyn *si*

$$(N_X + N_Y + 2N_Z + 2N_W)(s) = 0, \quad \text{para } s \geq 1. \tag{7}$$

Definición 3 *Un conjunto de cuatro secuencias finitas* α*,* β*,* γ*,* δ*, de números en* $\{-1, +1\}$ *de largos* $m+p$*,* $m+p$*,* m*,* m *se denominan* secuencias base *si*

$$(N_\alpha + N_\beta + N_\gamma + N_\delta)(s) = 0, \quad \text{para } s \geq 1. \tag{8}$$

El resultado siguiente nos permite utilizar un conjunto de *secuencias tipo Turyn* para construir un conjunto de *secuencias base*, de una manera muy específica. Tómese nota que la secuencia (A, B) no es otra cosa que los términos de A seguidos por los términos de B.

Teorema 3 [29] *Si* X*,* Y*,* Z*,* W*, son* secuencias tipo Turyn *de largos* m*,* m*,* m*,* $m-1$*, entonces las secuencias* $\alpha = (Z, W)$*,* $\beta = (Z, -W)$*,* $\gamma = X$*, y* $\delta = Y$*, forman un conjunto de* secuencias base *de largos* $2m-1$*,* $2m-1$*,* m*,* m *respectivamente.*

Demostración. A continuación presentamos una prueba directa e independiente de la de Turyn [29]: que las secuencias α, β, γ y δ tienen los largos $2m-1$, $2m-1$, m, m es obvio. Probemos que α, β, γ y δ forman un conjunto de *secuencias base*, esto es, que $(N_\alpha + N_\beta + N_\gamma + N_\delta)(s) = 0$, para todo $s \geq 1$.

Ahora, debido a que $\gamma = X$ y $\delta = Y$, tendremos que $N_\gamma = N_X$ y $N_\delta = N_Y$. Entonces, es suficiente demostrar que para cada $s \geq 1$ se cumple la identidad $(2N_Z + 2N_W)(s) = (N_\alpha + N_\beta)(s)$.

Primeramente, obsérvese que cuando $s \geq 2m-1$ todas las auto-correlaciones no periódicas son nulas, por definición: $N_Z(s) = N_W(s) = N_\alpha(s) = N_\beta(s) = 0$.

En el caso en que $1 \leq s < 2m-1$ tendremos:

$$\begin{aligned}
(N_\alpha + N_\beta)(s) &= \sum_{i=1}^{2m-1-s} (\alpha_i\alpha_{i+s} + \beta_i\beta_{i+s}) \\
&= \sum_{i=1}^{m-s} (\alpha_i\alpha_{i+s} + \beta_i\beta_{i+s}) + \sum_{i=m-s+1}^{m} (\alpha_i\alpha_{i+s} + \beta_i\beta_{i+s}) \\
&\quad + \sum_{i=m+1}^{2m-1-s} (\alpha_i\alpha_{i+s} + \beta_i\beta_{i+s}) \\
&= \sum_{i=1}^{m-s} (z_i z_{i+s} + z_i z_{i+s}) + \sum_{i=m-s+1}^{m} (z_i w_{i+s} + z_i(-w_{i+s})) \\
&\quad + \sum_{i=m+1}^{2m-1-s} (w_i w_{i+s} + (w_i w_{i+s})) \\
&= 2N_Z(s) + 0 + 2N_W(s).
\end{aligned}$$

■

Definición 4 *Un conjunto de cuatro secuencias Q, T, U, V, de números en $\{-1,0,1\}$ todas de largo m se llama un conjunto de* T-secuencias *si*

$$(N_Q + N_T + N_U + N_V)(s) = 0, \tag{9}$$

para cada $s \geq 1$ y además, en cada posición, exactamente una de las entradas de Q, T, U, V, es no-nula.

Si tenemos un conjunto de *secuencias base*, el siguiente resultado nos permite construir un conjunto de *T-secuencias* muy específico.

Teorema 4 [29] *Si α, β, γ, δ, es un conjunto de* secuencias base *de largos $m+p$, $m+p$, m, m, entonces las secuencias definidas por $Q = \left(\frac{1}{2}(\alpha+\beta), \boldsymbol{0}_m\right)$, $T = \left(\frac{1}{2}(\alpha-\beta), \boldsymbol{0}_m\right)$, $U = \left(\boldsymbol{0}_{m+p}, \frac{1}{2}(\gamma+\delta)\right)$, $V = \left(\boldsymbol{0}_{m+p}, \frac{1}{2}(\gamma-\delta)\right)$, donde $\boldsymbol{0}_r$ denota la secuencia de largo r de entradas nulas, forman un conjunto de* T-secuencias *de largo $2m+p$.*

Demostración. Simplificamos la primera parte de la prueba aportada por Turyn. Que cada una las secuencias formadas tiene largo $2m+p$ es obvio, de la construcción.

Primeramente vamos a probar que en cada posición, exactamente una de las entradas es no-nula. En las primeras $m+p$ posiciones, las entradas en U y V son claramente nulas. Más aún, si una entrada en Q es nula, entonces la correspondiente entrada a en α debe ser la negación de la correspondiente entrada b en β, y por consiguiente tendremos que $\frac{1}{2}(a-b)=\pm 1$, que coincide con la entrada en T. En forma análoga, si la entrada en T es nula, entonces las entradas correspondientes a y b en α y β deben ser iguales, de manera que $\frac{1}{2}(a+b)=\pm 1$, coincidiendo con la entrada en Q. Por consiguiente, exactamente una de estas entradas es no-nula. Reemplazando Q por U, T por V, α por γ y β por δ, el argumento anterior garantiza el resultado para las últimas m posiciones.

Finalmente, considere $(N_Q+N_T+N_U+N_V)(s)$. Claramente, cuando $s \geq 2m+p$, esta cantidad es nula, de la definición de N. Ahora, cuando $1 \leq s < 2m+p$, tendremos lo siguiente:

$$\begin{aligned}
(N_Q+N_T+N_U+N_V)(s) &= \sum_{i=1}^{2m+p-s} (q_i q_{i+s} + t_i t_{i+s} + u_i u_{i+s} + v_i v_{i+s}) \\
&= \sum_{i=1}^{m+p-s} (q_i q_{i+s} + t_i t_{i+s} + u_i u_{i+s} + v_i v_{i+s}) \\
&\quad + \sum_{i=m+p-s+1}^{m+p} (q_i q_{i+s} + t_i t_{i+s} + u_i u_{i+s} + v_i v_{i+s}) \\
&\quad + \sum_{i=m+p+1}^{2m+p-s} (q_i q_{i+s} + t_i t_{i+s} + u_i u_{i+s} + v_i v_{i+s}).
\end{aligned}$$

Observe que en la última expresión, cada $q_{i+s}=t_{i+s}=0$, cuando $i \geq m+p$, mientras que cada $u_i=v_i=0$, cuando $i \leq m+p$. Entonces, sustituyendo los valores de las *secuencias base* originales, la última expresión simplifica a:

$$\begin{aligned}
\cdots &= \sum_{i=1}^{m+p-s} \tfrac{1}{2}(\alpha_i+\beta_i)\tfrac{1}{2}(\alpha_{i+s}+\beta_{i+s}) + \tfrac{1}{2}(\alpha_i-\beta_i)\tfrac{1}{2}(\alpha_{i+s}-\beta_{i+s}) \\
&\quad + \sum_{i=1}^{m-s} \tfrac{1}{2}(\gamma_i+\delta_i)\tfrac{1}{2}(\gamma_{i+s}+\delta_{i+s}) + \tfrac{1}{2}(\gamma_i-\delta_i)\tfrac{1}{2}(\gamma_{i+s}-\delta_{i+s}) \\
&= \sum_{i=1}^{m+p-s} \left(\tfrac{1}{2}\alpha_i\alpha_{i+s} + \tfrac{1}{2}\beta_i\beta_{i+s}\right) + \sum_{i=1}^{m-s} \left(\tfrac{1}{2}\gamma_i\gamma_{i+s} + \tfrac{1}{2}\delta_i\delta_{i+s}\right) \\
&= \frac{1}{2}\left(N_\alpha + N_\beta + N_\gamma + N_\delta\right)(s) = 0.
\end{aligned}$$

■

Tomemos ahora $p = m - 1$ y consideremos cualquier conjunto de *T-secuencias* Q, T, U, V, de largo $2m + p = 3m - 1$. Procedemos a definir las matrices circulantes con los mismos nombres, Q, T, U, V, de órdenes $3m - 1$, cuyas primeras filas son las correspondientes secuencias. Más aún, construimos las siguientes cuatro matrices, de órdenes $3m - 1$:

$$\begin{aligned} A &= Q + T + U + V, \\ B &= -Q + T + U - V, \\ C &= -Q - T + U + V, \\ D &= -Q + T - U + V. \end{aligned}$$

Luego, de la definición de conjunto de *T-secuencias*, cada entrada de las matrices anteriores esta en $\{-1, 1\}$, pues solo una de las posiciones de Q, T, U, V, es no-nula. Además, Turyn demostró [29] que cada matriz A, B, C, D, es circulante y $AA^t + BB^t + CC^t + DD^t = 4(3m-1)I_{3m-1}$[1]. Por consiguiente, aplicando el teorema de Goethal-Seidel, se deduce la existencia de una matriz de Hadamard H de orden $4(3m - 1)$. Resumiendo,

Corolario 1 *Sean X, Y, Z, W,* secuencias tipo Turyn *de largos m, m, m, $m-1$ respectivamente. Entonces, existe una matriz de Hadamard de orden $4(3m-1)$, construida a partir de X, Y, Z, W.*

Esto es lo que hicieron Kharaghani y Tayfeh-Razaie, [17] para construir una matriz de Hadamard de orden $428 = 4(3m - 1)$, donde $m = 36$, a partir de las siguientes *secuencias tipo Turyn* X, Y, Z, W, 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, empleando un algoritmo de fuerza bruta:

---

[1] En el caso que nos ocupa, las cuatro secuencias Q, T, U, V, son precisamente, por definición, $Q = (Z, \mathbf{0}_{2m-1})$, $T = (\mathbf{0}_m, W, \mathbf{0}_m)$, $U = \big(\mathbf{0}_{2m-1}, \frac{1}{2}(X+Y)\big)$, $V = \big(\mathbf{0}_{2m-1}, \frac{1}{2}(X-Y)\big)$. Además, al calcular directamente $AA^t = (Q+T+U+V)\left(Q^t+T^t+U^t+V^t\right)$ queda un producto de 16 términos, que simplifica como $AA^t = 4QQ^t$. Análogamente se calculan directamente los productos BB^t, CC^t, DD^t, obteniéndose la simplificación

$$AA^t + BB^t + CC^t + DD^t = 4(QQ^t + TT^t + UU^t + VV^t).$$

Es un tanto más difícil el cálculo que sigue para demostrar que la anterior cantidad es $4(3m-1)I_{3m-1}$ [29].

```
X = + + + − − − − + + − + − + − − − − − + + + + − + + − + + + +
    − − − − + −
Y = + − + + + + + − − + − + − − + − − + + − − + + + + − + + + +
    − − − + + −
Z = + − + + + + + − + − − + + + + − + + + − + + − − + + + − + −
    − + − − − +
W = + + + − + − − − − − + + − − + − + + + − − + − + − + + + − +
    + + + − +
```

Para hallar una matriz de Hadamard de orden $668 = 4(3m-1)$, donde $m = 56$ (el menor orden sobre el cual aún no se conoce matriz de Hadamard), bastaría entonces con hallar *secuencias tipo Turyn* X, Y, Z, W, de largos 56, 56, 56, 55, asunto que está siendo estudiado profusamente a través de todo tipo de métodos heurísticos, dado que para ese tamaño 56 se considera que el método de la fuerza bruta es absolutamente impracticable para hallar *secuencias tipo Turyn* [22], por el crecimiento exponencial del tiempo de cálculo requerido.

5 El álgebra de las secuencias tipo Turyn

5.1 Propiedades adicionales de las secuencias tipo Turyn

Las principales propiedades de las secuencias tipo Turyn son resumidas en el siguiente teorema. Las partes (b) y (d) del teorema son resultados novedosos de los autores. La parte (d) estaba mal enunciada y mal demostrada en las referencias y ningún autor posterior lo había notado. En las otras partes del teorema se brinda una demostración alternativa más simple.

Teorema 5 *Sea X, Y, Z, W, un conjunto de secuencias tipo Turyn de largo m. Sean x, y, z, w, las sumas de las entradas de X, Y, Z, W, respectivamente. Entonces:*

(a) [29] *m es par, o $m = 1$.*

(b) (Piza, Segura) *Cuando $m > 1$ entonces x, y, z son pares y w es impar.*

(c) [20] $x^2 + y^2 + 2z^2 + 2w^2 = 6m - 2$.

(d) (Piza, Segura) *Cuando $m > 1$ tendremos $x + y + m \equiv 2(mod\, 4)$*[2].

(e) [29] *Cuando $m > 1$, entonces $x_i\, x_{m-i+1} + y_i\, y_{m-i+1} = 0$, para $i \in \{2, 3, \ldots, m/2\}$.*

[2]Este resultado está mal enunciado y demostrado en [20], en el cual enuncian $x + y \equiv 2(mod\, 4)$, lo cual es incorrecto para $m = 2, 6, 10, 14, \ldots$

Demostración.

(a) Realizamos una prueba alternativa y simplificada a la utilizada por Turyn. Utilizaremos el hecho que si $a, b \in \{-1, 1\}$, entonces se cumple $a+b \equiv ab + 1(mod\, 4)$. Sea N una abreviatura de $(N_X + N_Y + 2N_Z + 2N_W)$. Ahora, $N(m-1) = x_1x_m + y_1y_m + 2z_1z_m = 0$. Por consiguiente, $x_1 + y_1 + x_m + y_m - 2 + 2z_1z_m \equiv 0(mod\, 4)$, de donde

$$x_1 + y_1 + x_m + y_m \equiv 0\ (mod\, 4). \tag{10}$$

Por otra parte, $N(m-2) = x_1x_{m-1} + x_2x_m + y_1y_{m-1} + y_2y_m + 2z_2z_{m-1} + 2z_2z_m + 2w_1w_{m-1} = 0$. Luego, $x_1 + y_1 + x_2 + y_2 + x_{m-1} + y_{m-1} + x_m + y_m \equiv 2(mod\, 4)$. Utilizando (10) tendremos:

$$x_2 + y_2 + x_{m-1} + y_{m-1} \equiv 2\ (mod\, 4). \tag{11}$$

Continuando de esta manera, se demuestra inductivamente que, para $1 < s \leq \lceil \frac{m}{2} \rceil$, al simplificar $N(s) = 0$ se obtiene

$$x_s + y_s + x_{m-s+1} + y_{m-s+1} \equiv 2\ (mod\, 4). \tag{12}$$

Ahora supongamos que $m > 1$ fuese un número impar, digamos $m = 2k + 1$. Luego, $\lceil \frac{m}{2} \rceil = k + 1$, de donde simplificando $N(k+1) = 0$ y aplicando (12) obtenemos

$$x_{k+1} + y_{k+1} + x_{k+1} + y_{k+1} \equiv 2\ (mod\, 4), \tag{13}$$

esto es, $2(x_{k+1} + y_{k+1}) \equiv 2(mod\ 4)$, lo cual es imposible, pues la suma $x_{k+1} + y_{k+1} \in \{-2, 0, 2\}$. Por consiguiente, m es un número par.

(b) Claramente x, y, z son la suma de una cantidad *par* de 1's o -1's, de donde son todos pares, mientras que w es la suma de una cantidad *impar* de 1's o -1's, de donde w es impar.

(c) Simplificación de la prueba de [20]: Calculamos directamente las cantidades x^2, y^2, $2z^2$ y $2w^2$ y luego sumamos:

$$\begin{aligned}
x^2 &= \left(\sum_{i=1}^{m} x_i\right)^2 = \sum_{i=1}^{m} x_i^2 + 2\sum_{s=1}^{m-1}\sum_{i=1}^{m-s} x_i x_{i+s} = m + 2\sum_{s=1}^{m-1} N_X(s),\\
y^2 &= \left(\sum_{i=1}^{m} y_i\right)^2 = \sum_{i=1}^{m} y_i^2 + 2\sum_{s=1}^{m-1}\sum_{i=1}^{m-s} y_i y_{i+s} = m + 2\sum_{s=1}^{m-1} N_Y(s),\\
2z^2 &= 2\left(\sum_{i=1}^{m} z_i\right)^2 = 2\sum_{i=1}^{m} z_i^2 + 4\sum_{s=1}^{m-1}\sum_{i=1}^{m-s} z_i z_{i+s} = 2m + 4\sum_{s=1}^{m-1} N_Z(s),\\
2w^2 &= 2\left(\sum_{i=1}^{m-1} w_i\right)^2 = 2\sum_{i=1}^{m-1} w_i^2 + 4\sum_{s=1}^{m-1}\sum_{i=1}^{m-s} w_i w_{i+s} = 2(m-1) + 4\sum_{s=1}^{m-1} N_W(s).
\end{aligned}$$

Luego, sumando obtenemos:

$$x^2+y^2+2z^2+2w^2=6m-2+2\sum_{s=1}^{m-1}(N_X+N_Y+2N_Z+2N_W)(s)=6m-2.$$

(d) Las ecuaciones (10-12) establecen:

$$\begin{aligned}
x_1+y_1+x_m+y_m &\equiv 0\ (mod\,4),\\
x_2+y_2+x_{m-1}+y_{m-1} &\equiv 2\ (mod\,4),\\
x_3+y_3+x_{m-2}+y_{m-2} &\equiv 2\ (mod\,4),\\
&\ \vdots\\
x_{\frac{m}{2}}+y_{\frac{m}{2}}+x_{\frac{m}{2}+1}+y_{\frac{m}{2}+1} &\equiv 2\ (mod\,4).
\end{aligned}$$

Al sumar ambos extremos, obtenemos $x+y\equiv 2\left(\frac{m}{2}-1\right)=m-2\ (mod\,4)$, de donde $x+y+m\equiv 2m-2\equiv -2\equiv 2\ (mod\,4)$.

(e) Simplificación de la prueba de [20]: De la fórmula (12) se deduce que exactamente tres de los términos x_s, y_s, x_{m-s+1}, y_{m-s+1} son iguales a 1 y el otro término es igual a -1, o bien exactamente tres de los términos son iguales a -1 y el otro término es igual a 1. En cualquiera de las posibilidades tendremos,

$$x_s x_{m-s+1}+y_s y_{m-s+1}=0,\quad s=2,\ldots,m/2.$$

■

5.2 Forma canónica de las secuencias tipo Turyn

Considere una secuencia numérica cualquiera $A=\{a_1,\ldots,a_m\}$. Definimos las siguientes tres operaciones elementales sobre A:

- Al *negar* la secuencia A obtenemos $-A=\{-a_1,\ldots,-a_m\}$.
- Al *invertir* la secuencia A obtenemos $A'=\{a_m,a_{m-1},\ldots,a_1\}$.
- Al *alternar* la secuencia A obtenemos $A^*=\{a_1,\ -a_2,\ a_3,\ -a_4,\ldots,\ (-1)^{m-1}a_m\}$.

Es fácil demostrar que dada una *secuencia tipo Turyn* X,Y,Z,W, de largo m, con $m>1$, entonces cualquiera de las siguientes cuatro transformaciones elementales aplicadas sobre X, Y, Z, W, producen también *secuencias tipo Turyn*:

1. Negar cualquiera de X, Y, Z, W.
2. Invertir cualquiera de X, Y, Z, W.
3. Alternar todas las cuatro secuencias X, Y, Z, W.
4. Intercambiar X y Y.

Definición 5 *Denotemos por $TT(m)$ el conjunto de las* secuencias tipo Turyn *de largo m. Decimos que dos* secuencias tipo Turyn *$S_1 = (X_1; Y_1; W_1; Z_1) \in TT(m)$ y $S_2 = (X_2; Y_2; W_2; Z_2) \in TT(m)$ son equivalentes, si S_1 puede transformarse en S_2 por la aplicación de un número finito de las anteriores transformaciones elementales.*

Esta noción claramente establece una relación de equivalencia en $TT(m)$. Al conjunto de clases de equivalencia lo denotamos por $\{TT(m)\}$. Para encontrar representantes exclusivos de las clases de equivalencia $E \in \{TT(m)\}$, introducimos el concepto de forma canónica de una *secuencia tipo Turyn*.

Definición 6 ***(Forma canónica)*** *Decimos que una* secuencia tipo Turyn *X, Y, Z, W, se encuentra en la forma canónica si se cumplen las siguientes seis condiciones:*

(i) $x_1 = x_m = y_1 = y_m = z_1 = w_1 = 1$.

(ii) Si i es el índice mínimo tal que $x_i \neq x_{m+1-i}$, entonces $x_i = 1$.

(iii) Si i es el índice mínimo tal que $y_i \neq y_{m+1-i}$, entonces $y_i = 1$.

(iv) Si i es el índice mínimo tal que $z_i = z_{m+1-i}$ entonces $z_i = 1$.

(v) Si i es el índice mínimo tal que $w_i\, w_{m-i} \neq w_{m-1}$ entonces $w_i = 1$.

(vi) Suponga que $m > 2$. Si $x_2 \neq y_2$, entonces $x_2 = 1$. Si $x_2 = y_2$, entonces $x_{m-1} = 1$, $y_{m-1} = -1$.

Obsérvese que si $m > 1$, entonces la condición (i) y la ecuación (7) implican que $z_m = -1$.

Teorema 6 [3] *Cada clase de equivalencia $E \subseteq \{TT(m)\}$, tiene al menos un miembro que se encuentra en la forma canónica.*

Demostración. La prueba es sencilla y se reproduce de [3] con el propósito de justificar posteriormente la ecuación (14). Sea $S = (X; Y; Z; W) \in E$ una *secuencia tipo Turyn* arbitraria. Al aplicarle los primeros tres tipos de transformaciones elementales, vemos que es posible obtener una nueva *secuencia tipo Turyn* equivalente a S que satisfaga la condición (i). Una sola transformación elemental de cada tipo (o ninguna) es suficiente.

Para satisfacer la condición (ii), simplemente reemplazamos la secuencia X por su negación $-X$ si fuese necesario: obtenemos de esa forma una nueva *secuencia tipo Turyn* equivalente a S. Similarmente, intercambiamos Y por $-Y$ si fuera necesario, con el fin de obtener una *secuencia tipo Turyn* equivalente a S que satisfaga la condición (iii).

Para satisfacer la condición (iv) reemplazamos (si fuera necesario) Z por $-Z'$. Para satisfacer la condición (v) buscamos si en W existe el índice i tal que $w_i w_{m-i} \neq w_{m-1}$. En caso afirmativo, tendremos que $1 < i \leq m/2$. Entonces, si $w_{m-1} = 1$ bastaría con reemplazar W por W', mientras que si $w_{m-1} = -1$ bastaría con reemplazar W por $-W'$. En ambos casos obtenemos una *secuencia tipo Turyn* equivalente a S que satisface la condición (v).

Por último, para satisfacer la condición (vi) obsérvese que la ecuación (7), para $s = 2$, implica que exactamente una de las igualdades $x_2 = y_2$ y $x_{m-1} = y_{m-1}$ se cumple. Entonces, es suficiente con intercambiar X con Y (si fuese necesario). De esta forma, finalmente hemos construido una *secuencia tipo Turyn* que se encuentra en la forma canónica y que es equivalente a la original S. ■

Nótese que de todo lo anterior se deduce la ecuación

$$x_1\, x_m - y_1\, y_m = 0, \tag{14}$$

que contrasta con las ecuaciones del Teorema 5(e): $x_i\, x_{m-i+1} + y_i\, y_{m-i+1} = 0$, válidas para $i \in \{2, \ldots, m/2\}$.

Teorema 7 [3] *Para cada clase de equivalencia $E \in \{TT(m)\}$ existe una única* secuencia tipo Turyn $S = (X; Y; W; Z) \in E$ *que tiene la forma canónica.*

Demostración. Puede consultarse en [3]. ■

En la Figura 2 se presentan la cantidad de *secuencias tipo Turyn* de largo m no equivalentes entre sí. Estos cálculos fueron llevados a cabo a través de algoritmos de tipo enumerativo, que requieren gran cantidad de tiempo de CPU [3, 22].

m	2	4	6	8	10	12	14	16	18	20
Card($\{TT(m)\}$)	1	1	4	6	43	127	186	739	675	913
Horas CPU	<1	<1	<1	<1	<1	<1	<1	<1	<1	<1

m	22	24	26	28	30	32	34	36	38	40
Card($\{TT(m)\}$)	3105	3523	3753	4161	4500	6226	≈ 5056	≈ 3712	≥ 10	≥ 3
Horas CPU	<1	1	9	80	1100	8200	≈ 1900	≈ 12800	> 7600	> 36000

Figura 2: Número de *secuencias tipo Turyn* de largo m inequivalentes entre sí, de acuerdo a los estudios [3, 22].

5.3 Código hexadecimal de las secuencias tipo Turyn

Dada una *secuencia tipo Turyn* $S = (X; Y; Z; W)$ de largo m, es conveniente organizarla en el formato de 4 filas y asociar cada columna del arreglo resultante con un carácter hexadecimal. Esto se obtiene asociando la i-ésima columna de la secuencia S con

$$T_i = \begin{cases} 4(1-x_i) + 2(1-y_i) + (1-z_i) + \frac{1}{2}(1-w_i), & \text{si } i \in \{1, \dots, m-1\} \\ 2(1-x_m) + (1-y_m) + \frac{1}{2}(1-z_m), & \text{si } i = m. \end{cases}$$

El valor de cada T_i estará entonces en $\{0, 1, \dots, 15\}$, cuando $1 \leq i < m$, mientras que el valor de T_m estará en $\{0, 1, \dots, 7\}$. Escribimos $a = 10$, $b = 11$, $c = 12$, $d = 13$, $e = 14$, $f = 15$ y obtenemos que $T_1 T_2 \dots T_m$ es un número hexadecimal que representa a la secuencia S en forma compacta. Por ejemplo, la *secuencia tipo Turyn* de largo 16

```
X :  1  1 -1 -1 -1 -1  1  1  1 -1 -1 -1 -1 -1 -1  1
Y :  1 -1  1  1 -1  1 -1  1 -1 -1 -1  1 -1 -1 -1  1
Z :  1  1  1  1  1  1 -1  1  1 -1 -1 -1  1  1  1 -1
W :  1  1 -1 -1  1 -1 -1  1 -1 -1  1 -1  1 -1  1
```

tiene código hexadecimal 0499c9705febcdc1. De paso esta *secuencia tipo Turyn* se encuentra en la forma canónica.

6 Algoritmos para buscar secuencias tipo Turyn

Elegimos el largo m (par) de las *secuencias tipo Turyn* a buscar. Empezamos con las cuatro secuencias X, Y, Z, W, de entradas en $\{-1, 1\}$ generadas al azar, de largo m, m, m, $m-1$. Se procede a calcular las autocorrelaciones N_X, N_Y, N_Z, N_W y las sumas espectrales $\Theta(s) = N_X(s) + N_Y(s) + 2N_Z(s) + 2N_W(s)$ (ver la Figura 3). Calculamos también el valor de la función objetivo,

$$f(X, Y, Z, W) = \sum_{s=1}^{m-1} |\Theta(s)|. \tag{15}$$

Initial pseudo-Turyn type sequence, generated at random:

$s \longrightarrow$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
X :	1	1	−1	1	1	−1	1	1	1	1	1	1	−1	1	1	1	1	−1
Y :	1	1	−1	1	1	−1	1	1	1	1	−1	1	1	1	1	1	−1	−1
Z :	1	1	−1	−1	1	1	−1	1	−1	−1	1	−1	−1	−1	−1	1	1	1
W :	1	−1	−1	−1	−1	1	−1	−1	1	1	1	−1	−1	1	1	1	−1	
$N_X(s)$:	3	2	7	2	5	4	7	2	1	4	−1	2	1	0	3	0	−1	
$N_Y(s)$:	3	0	5	0	3	4	3	4	−1	−2	3	2	−1	2	1	−2	−1	
$N_Z(s)$:	1	−4	1	−4	1	2	−3	−4	−1	2	1	0	−3	−2	1	2	1	
$N_W(s)$:	2	−5	−4	1	8	−3	−6	−1	2	3	−4	−3	0	1	2	−1	0	
$\Theta(s)$:	12	−16	6	−4	26	6	−8	−4	2	12	−4	−2	−6	0	10	0	0	

Initial value of the objective function: $f(X, Y, W, Z) = 118$.

Figura 3: Ejemplo del proceso de búsqueda de una *secuencia tipo Turyn*, para $m = 18$. Algunas de las entradas de las secuencias son pre-fijadas de antemano, como por ejemplo $x_1 = y_1 = z_1 = w_1 = 1$, $x_m = y_m = -1$, $z_m = 1$.

Nuestro propósito es minimizar la función objetivo $f(X, Y, Z, W)$, para lo cual iremos variando las secuencias X, Y, Z, W. El mínimo global (si existiese[3]) se alcanzará cuando $f(X, Y, Z, W) = 0$, que corresponde precisamente a una *secuencia tipo Turyn* X, Y, W, Z.

6.1 Algoritmo $RS(m)$ sin restricciones

Este es un algoritmo del tipo *recocido simulado* $RS(m)$ [1] sin restricciones estructurales. Explicamos el método en forma suscinta: en cada etapa elegimos

[3]No hay garantía absoluta de la existencia de una *secuencia tipo Turyn* de cualquier largo m, si bien se han encontrado para todos los largos pares $m \leq 40$.

al azar un término de alguna de las secuencias X, Y, Z, W, y eventualmente al término elegido le cambiamos el signo.

El eventual cambio de signo (llamado "movimiento") es aceptado o rechazado de acuerdo a la regla de Metropolis, la cual consiste en aceptar el movimiento con probabilidad $\min\{1, e^{-\Delta f(X,Y,Z,W)/t}\}$, donde $t > 0$ es el parámetro de la temperatura del sistema, parámetro que, progresivamente, se va disminuyendo lentamente hacia 0, luego de mantenerlo sin cambio por un número fijo y largo de etapas (largo de las cadenas de Markov del algoritmo).

Con la regla de Metropolis se aceptan siempre aquellos movimientos que disminuyan o que al menos no aumenten el valor de la función objetivo, esto es, cuando $\Delta f(X,Y,Z,W) \leq 0$, mientras que aquellos movimientos que aumentan el valor de la función objetivo (esto es, cuando $\Delta f(X,Y,Z,W) > 0$) el cambio de signo se acepta con probabilidad $e^{-\Delta f(X,Y,Z,W)/t}$, probabilidad que cada vez es más pequeña, conforme el parámetro $t \downarrow 0$. Los detalles acerca de la temperatura inicial t_0, los diversos parámetros del algoritmo y el plan de enfriamiento del sistema se explican en el apéndice A. La teoría sobre los algoritmos de recocido simulado [1] garantiza la *convergencia asintótica* del método hacia un óptimo global de la función objetivo f en estudio, bajo condiciones de accesibilidad con probabilidad igualitaria de cada posible configuración del espacio de configuraciones, condiciones de reversibilidad y condiciones de enfriamiento adecuado del sistema. Todas estas condiciones se cumplen en nuestro algoritmo, de manera que, bien implementado, nuestro método eventualmente convergerá hacia un óptimo global, correspondiente a una secuencia Turyn (si esta existiese).

Cuando se emplean algoritmos de recocido simulado es de importancia contar con un método recursivo eficiente para calcular rápidamente $\Delta f(X,Y,Z,W)$, el cambio que produce en la función objetivo la posible aceptación de un movimiento, en este caso, de un cambio de signo en alguna de las entradas de las secuencias X, Y, Y o W.

Para ese fin, encontramos las fórmulas

$$\Delta(s) = \begin{cases} 2x_{i_0}(x_{i_0-s} + x_{i_0+s}), & \text{si } x_{i_0} \text{ fue seleccionado} \\ 2y_{i_0}(y_{i_0-s} + y_{i_0+s}), & \text{si } y_{i_0} \text{ fue seleccionado} \\ 4z_{i_0}(z_{i_0-s} + z_{i_0+s}), & \text{si } z_{i_0} \text{ fue seleccionado} \\ 4w_{i_0}(w_{i_0-s} + w_{i_0+s}), & \text{si } w_{i_0} \text{ fue seleccionado,} \end{cases} \tag{16}$$

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

$$\Delta f(X, Y, Z, W) = \sum_{s=1}^{M} |\theta(s)| - |\theta(s) - \Delta(s)|. \qquad (17)$$

En efecto, si por ejemplo en el curso del algoritmo x_{i_0} fue seleccionado, entonces, las únicas cantidades que cambian son las autocorrelaciones $N_X(s)$. Ahora bien, al cambiar x_{i_0} por $-x_{i_0}$, el nuevo valor de $N_X(s)$ es:

nuevo $N_X(s) = N_X(s) - 2x_{i_0}x_{i_0+s} - 2x_{i_0-s}x_{i_0} = N_X(s) - 2x_{i_0}(x_{i_0-s} + x_{i_0+s})$,

de donde $\Delta(s) = 2x_{i_0}(x_{i_0-s} + x_{i_0+s})$. Similares son los cálculos cuando son seleccionados y_{i_0}, z_{i_0}, o w_{i_0}.

Con este algoritmo hemos encontrado *secuencias tipo Turyn* de largos $m \leq 30$, hasta el momento. En la Sección 7 se muestran algunos de los resultados obtenidos, con los tiempos de cómputo para hallarlos.

6.2 Algoritmo recursivo ${}_pTT(n) \mid\mid RS(m-p-q) \mid\mid TT(n)_q$

Una variante interesante que también consideramos, es tratar de hallar *secuencias tipo Turyn* a través de algún tipo de recursión. Para ello modificamos el algoritmo anterior, con el fin de buscar la *secuencia tipo Turyn* $TT(m)$ mediante

$$TT(m) = {}_pTT(n) \mid\mid RS(m-p-q) \mid\mid TT(n)_q, \qquad (18)$$

donde ${}_pTT(n)$ se refiere a las *primeras* p columnas de una *secuencia tipo Turyn* $TT(n)$ más pequeña y ya precalculada, de largo n, mientras que $TT(n)_q$ se refiere a las *últimas* q columnas de $TT(n)$. Aquí, naturalmente, $n < m$, $0 \leq p$, $0 \leq q$ y $m-p-q > 1$. En las $m-p-q$ columnas centrales aplicamos el método de recocido simulado, $RS(m-p-q)$, descrito en la subsección anterior.

Desafortunadamente, luego de realizados gran cantidad de experimentos, no hemos encontrado ninguna recursión general que sirva para calcular $TT(m)$ basado en el cálculo previo de $TT(n)$, con $n < m$, excepto en algunos casos aislados y casuales, sin que estos sugieran un patrón general de recursión[4]. Sin embargo, el algoritmo recursivo es eficiente para hallar otras *secuencias tipo Turyn* de largo m a partir de algunas secuencias conocidas del mismo largo.

[4]Por ejemplo, para hallar $TT(18)$ sirve la recursión ${}_3TT(12) \mid\mid RS(12) \mid\mid TT(12)_3$ y para hallar $TT(20)$ sirve la recursión ${}_3TT(14) \mid\mid RS(14) \mid\mid TT(14)_3$, y para hallar $TT(22)$ sirve la recursión ${}_3TT(16) \mid\mid RS(16) \mid\mid TT(16)_3$, pero este patrón recursivo pareciera no funcionar con la búsqueda de $TT(24)$.

6.3 Algoritmo distribuido: $RS(m)$ con restricciones

También desarrollamos un algoritmo de recocido simulado $RS(m)$ en el cual las secuencias X, Y, Z y W siempre satisfagan las propiedades (b), (c) y (e) del Teorema 5.

Empezamos encontrando todas las soluciones enteras de la ecuación $x^2 + y^2 + 2z^2 + 2w^2 = 6m - 2$. Debido a la forma normal de una *secuencia tipo Turyn*, basta con considerar aquellas soluciones enteras donde x, y, z, w, sean no negativos, con x, y, z, pares, w impar y $x \leq y$. El algoritmo es entonces como sigue:

1. Seleccionamos alguna de las soluciones precalculadas de la ecuación $x^2 + y^2 + 2z^2 + 2w^2 = 6m - 2$ con las restricciones arriba señaladas y la prefijamos.

2. Seleccionamos al azar las secuencias iniciales X, Y, de largos x y y respectivamente, considerando previamente que $x_1 = y_1 = x_m = y_m = 1$.

3. Procedemos a realizar algunos cambios de los signos de las entradas de Y, de forma tal que se cumpla la propiedad $x_s x_{m+1-s} + y_s y_{m+1-s} = 0$, para $s = 2, \ldots, m/2$. En caso que esto no sea del todo posible, repetimos el paso 2.

4. Aplicamos, un algoritmo de recocido simulado para buscar las secuencias Z y W que completen una *secuencia tipo Turyn* (X, Y, Z, W), donde X y Y ya han sido establecidos en los pasos 2 y 3. En caso de fracaso, repetimos el algoritmo de recocido simulado un número prefijado de veces, luego de lo cual, si persistiese el fracaso, repetimos el algoritmo a partir del paso 2, en forma indefinida hasta obtener un eventual éxito.

Este es un algoritmo de tipo distribuido, en el sentido que permite distribuir el cálculo en varias computadoras, trabajando con las distintas soluciones precalculadas de la ecuación $x^2 + y^2 + 2z^2 + 2w^2 = 6m - 2$.

Hemos obtenido resultados muy similares con este algoritmo a los hallados con el primer algoritmo descrito en la subsección 6.1, aunque en tiempos mucho mayores. En la Figura 3 se muestra un ejemplo del proceso de búsqueda de una secuencia tipo Turyn para $m = 18$.

7 Soluciones encontradas y conclusiones

En la Figura 4, se presentan algunos de los mejores resultados obtenidos a través de los dos primeros algoritmos descritos. No se conocen aún *secuencias tipo Turyn* de largo mayor que 40. Es de observar que London [22] calculó una *secuencia tipo Turyn* de largo 40, utilizando un algoritmo de prueba y error, luego de aproximadamente 12.000 horas de CPU (algo más de 16 meses) usando cálculo distribuido en computadoras muy veloces. Los tiempos anteriormente requeridos para hallar *secuencias tipo Turyn* de largos 32, 34 y 36 eran de 8200 horas, 1900 horas y 12800 horas de CPU.

m	Código hexadecimal de la forma canónica	Tiempo	Método
2	01	$<$ 0.01 seg.	$RS(2)$
4	05e1	$<$ 0.01 seg.	$RS(4)$
6	0608d1	0.02 seg.	$RS(6)$
8	06e5c4d1	$<$ 0.01 seg.	$RS(8)$
10	052bb137c1	0.03 seg.	$RS(10)$
12	0683b9eeade1	1.16 seg.	$RS(12)$
14	0630219c8685d1	6.84 seg.	$RS(14)$
16	0499c9705febcdc1	15.66 seg.	$RS(16)$
18	00f7110507cb6a3561	180.27 seg.	$RR(16)$
20	064471d61096289cc3e1	61.27 seg.	${}_2TT(12)\|\|RS(16)\|\|TT(12)_2$
22	03e4f6e0461432b7d8eb71	4438.14 seg.	$RS(22)$
24	0c8c7d5dd3ef9487524fad41	22725.98 seg.	$RS(24)$
26	006ab07b11298e1a7ace93fe61	7283.19 seg.	$RS(26)$
28	07986035698a1527c1cfe5533331	92302.11 seg.	$RS(28)$
	Secuencias tipo Turyn halladas a partir de otras ya conocidas		
30	06b4b8bc718516ead522924d333331	711.70 seg.	${}_0TT(30)\|\|RS(18)\|\|TT(30)_{12}$
32	008d4c330f2d729c51bd474797518261	41.62 seg.	${}_0TT(32)\|\|RS(16)\|\|TT(32)_{16}$
34	00f50439112f66db41c9ef9699f7d5c561	40.72 seg.	${}_0TT(34)\|\|RS(18)\|\|TT(34)_{16}$
36	07f03896b7a66db3162bbf9331c0e0c5aad1	34.56 seg.	${}_0TT(36)\|\|RS(18)\|\|TT(36)_{18}$
38	00ff9d009077afe6fa383a34b1d3b24b92a551	45.09 seg.	${}_0TT(38)\|\|RS(18)\|\|TT(38)_{20}$
40	00648d1f010b4e82f58fb10b91b01a6b588ce361	31.17 seg.	${}_0TT(40)\|\|RS(18)\|\|TT(40)_{22}$

Figura 4: Lista de los mejores resultados (respecto al tiempo de cómputo) obtenidos de *secuencias tipo Turyn*, representadas en la forma canónica en el código hexadecimal. Para la últimas *secuencias tipo Turyn* de la lista anterior, se optimizaron los tiempos de cómputo utilizando el algoritmo recursivo $TT(m) = {}_pTT(n)||RS(m-p-q)||TT(n)_p$, partiendo de una *secuencia tipo Turyn* conocida, calculada en un tiempo mucho mayor.

Con nuestros algoritmos *recursivos*, podemos hallar *secuencias tipo Turyn* de largos 34, 36, 38, 40, diferentes de las ya conocidas, en menos de 1 minuto, utilizando computadoras de escritorio (procesadores Intel Core i7). Sin embargo, el fuerte crecimiento exponencial de este complejo problema limita el cálculo para órdenes superiores a 40, por lo que para intentar resolver este problema se podrían considerar dos opciones: el uso de computadoras más poderosas (con más memoria, más velocidad y trabajando en paralelo) o también considerar atacar el problema con una metodología distinta, que posiblemente dependerá de algún otro conocimiento teórico sobre las *secuencias tipo Turyn* que permita reducir drásticamente el tamaño del espacio de búsqueda.

En nuestro trabajo en marcha y a futuro, se estudiarán algoritmos heurísticos para la búsqueda de los llamados *conjuntos diferencia suplementarios* [11], que permitan la generación de matrices de Hadamard a través de los arreglos de Goethals-Seidel (ver Teorema 2).

Agradecimientos

Los autores desean agradecer a los colegas Adolfo Di Mare Hering y Mario Villalobos Arias, del Centro de Investigación en Matemática Pura y Aplicada CIMPA, quienes participaron parcialmente en la investigación actual y realizaron valiosos comentarios y revisiones del presente artículo.

Investigación patrocinada por la Universidad de Costa Rica, Proyecto N° 821-B6-276 del Centro de Investigación en Matemática Pura y Aplicada, CIMPA, de la Universidad de Costa Rica.

Los autores agradecen también el apoyo académico otorgado por el Deutsche Akademische Austauschdienst (DAAD).

Referencias

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

[2] S. Agaian, H. Sarukhanyan, K. Egiazarian, J. Astola, *Applications of Hadamard matrices in communication systems*, in: Hadamard Transforms, SPIE Press, Washington, 2001, pp. 419–448.

[3] D. Best, D.Z. Đoković, H. Kharaghani, H. Ramp, *Turyn type sequences: classification, enumeration and construction*, Journal of Combinatorial Designs **21** (2013), no. 1, 24–35.

[4] R. P. Brent, J. H. Osborn, *On minors of maximal determinant matrices*, Journal of Integer Sequences **16** (2013), article 13.4.2.

[5] W. A. Coppel, *Number Theory: An Introduction to Mathematics*, 2nd edition, Springer, Heidelberg, 2009.

[6] H. Evangelaras, C. Koukouvinos, J. Seberry, *Applications of Hadamard matrices*, Journal of Telecommunications and Information Technology (2003), no. 2, 3–10.

[7] H. Evangelaras, C. Koukouvinos, *On the use of Hadamard matrices in factorial designs*, Utilitas Mathematica **64** (2003).

[8] W. de Launey, *On the asymptotic existence of Hadamard matrices*, J. Combin. Theory Ser. A **116** (2009), no. 4, 1002–1008.

[9] D. Z. Đoković, *Williamson matrices of order* $4n$ *for* $n = 33, 35, 39$, Discrete Math. **115** (1993), no. 1-3, 267–271.

[10] D. Z. Đoković, *Hadamard matrices of order 764 exist*, Combinatorica **28** (2008), no. 4, 487–489.

[11] D. Z. Đoković, *Supplementary difference sets with symmetry for Hadamard matrices*, Operators and Matrices **3** (2009), no. 4, 557–569.

[12] D. K. Faddeev, I. S. Sominskii, *Problems in higher algebra*, W.H. Freeman, San Francisco, 1965, p. 331.

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

[14] J. Hadamard, *Résolution d'une question relative aux déterminants*, Bull. Sci. Math. **2** (1893), 240–246.

[15] J. Horton, C. Koukouvinos, J. Seberry, *A search for Hadamard matrices constructed from Williamson matrices*, Bulletin Institute of Combinatorics and its Applications **35** (2002), 75–88.

[16] W. M. Kantor, *Automorphism groups of Hadamard matrices*, Journal of Combinatorial Theory **6** (1969), no. 3, 279–281.

[17] H. Kharaghani, B. Tayfeh-Rezaie, *A Hadamard Matrix of Order 428*, Journal of Combinatorial Designs **13** (2005), no. 6, 435–440.

[18] H. Kharaghani, B. Tayfeh-Rezaie, *Hadamard matrices of order 32*, Journal of Combinatorial Designs **21** (2012), no. 5, 212-221.

[19] E. Kikianty, *Hermite-Hadamard inequality in the geometry of Banach spaces*, Ph.D. Thesis, University of Pretoria, 2010.

[20] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang, J. Yang, *On sequences with zero autocorrelation*, Designs, Codes and Criptography **4** (1994), no. 3, 327–340.

[21] C. Koukouvinos, D. E. Simos, *Encryption schemes based on Hadamard matrices with circulant cores*, Journal of Applied Mathematics & Bioinformatics **3** (2013), no. 1, 17–41.

[22] S. London, *Constructing new Turyn type sequences, T-sequences and Hadamard matrices*, Ph.D. Thesis, University of Illinois at Chicago, 2013.

[23] M. A. Miyamoto, *A construction of Hadamard matrices*, J. Combin. Theory Ser. A **57** (1991), no. 1, 86–108.

[24] E. Piza, *Búsqueda de matrices de Hadamard a través de secuencias de Turyn*, Revista de Matemática: Teoría y Aplicaciones **18** (2011), no. 2, 193–214.

[25] R. Paley, *On orthogonal matrices*, Journal Math. Phys. **12** (1933), no. 1-4, 311–320.

[26] J. Seberry, M. Yamada, *Hadamard matrices, sequences, and block designs*, Contemporary Design Theory: A Collection of Surveys, John Wiley & Sons Inc, New York, 1992, pp. 431–560.

[27] J. Wallis, *On supplementary difference sets*, Aequationes Mathematicae **8** (1972), no. 3, 242–257.

[28] N. J. Sloane, *Multiplexing methods in spectroscopy*, Mathematics Magazine **52** (1979), no. 2 ,71–80.

[29] R. J. Turyn, *Hadamard matrices, Baumert-Hall units, four-symbols sequences, pulse compression, and surface wave enconding*, J. Combin. Theory Ser. A **16** (1974), no. 3, 313–333.

Apéndice A: El plan de enfriamiento en RS

Los algoritmos de recocido simulado requieren del ajuste de algunos parámetros fundamentales, conocidos como el plan de enfriamiento del sistema. Los parámetros t_0, χ, λ, NLIMIT, NOVER, NCICLOS y NCAD deben ser variados con cierto grado de empirismo, para que se amolden al largo m de las *secuencias tipo Turyn* a calcular.

Temperatura inicial: t_0 es seleccionada de manera que la regla de Metropolis sea suficientemente tolerante al principio como para aceptar aproximadamente $\chi \times 100\%$ de "malos" movimientos (aquellos que aumentan el valor de la función objetivo), donde $\chi \in (0,1)$ es una constante preseleccionada (generalmente empleamos $\chi = 60\%$). Usualmente se preselecciona primero χ y se realiza una serie de corridas preliminares en falso, calculando el promedio de $\Delta f(X,Y,Z,W)$ para aquellos movimientos que aumenten la función objetivo, con el fin de estimar t_0 con este requisito. Esto se obtiene calculando $t_0{=}{-}\Delta f(X,Y,Z,W)_{\text{prom}}/\ln\chi$, pues de esa forma $e^{-\Delta f(X,Y,Z,W)/t_0}{\approx}\chi$.

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" movimientos con tal temperatura. Hemos experimentado con valores de NLIMIT $\in [10^5, 10^8]$ y NOVER $= \frac{1}{10}$ NLIMIT, dependiendo del tamaño m de las *secuencias tipo Turyn* buscadas.

Criterio de parada: un máximo de NCICLOS de temperatura son completados. Generalmente seleccionamos NCICLOS $= 400$, debido a que en la práctica la cantidad $t_{400} = t_0\lambda^{400}$ es una cantidad casi nula, independientemente del valor inicial t_0. Sin embargo, si en los últimos NCAD ciclos de temperatura no obtuviéramos ninguna mejora en la función objetivo, entonces el proceso es finalizado. Hemos utilizado experimentalmente valores de NCAD $= 3$ con resultados aceptables.