A Hadamard matrix of order 428[*]

H. Kharaghani[a,b,†] B. Tayfeh-Rezaie[a]

[a]*Institute for studies in theoretical Physics and Mathematics (IPM)*
P.O.Box 19395-5746*, Tehran, Iran*
[b]*Department of Mathematics and Computer Science*
University of Lethbridge
Lethbridge, Alberta, Canada

Dedicated to Professor Stratis Kounias on the occasion of his retirement

Abstract

Four Turyn type sequences of lengths $36, 36, 36, 35$ are found by a computer search. These sequences give new base sequences of lengths $71, 71, 36, 36$ and are used to generate a number of new T-sequences. The first order of many new Hadamard matrices constructible using these new T-sequences is 428.

Keywords: Hadamard matrices, Turyn type sequences, base sequences, T-sequences, Yang numbers
MR Subject Classification: 05B20, 05B05

1 Introduction

For a given sequence $A = (a_0, a_1, \ldots, a_{n-1})$ of length n, the *nonperiodic autocorrelation function* N_A is defined as

$$N_A(s) = \sum_{i=0}^{n-1-s} a_i a_{i+s} \quad \text{for} \quad s = 0, 1, \ldots, n-1, \quad \text{and} \quad N_A(s) = 0 \quad \text{for} \quad s \geq n.$$

For the sequence A, the associated *Hall polynomial* h_A is defined by

$$h_A(t) = \sum_{i=0}^{n-1} a_i t^i.$$

[*] Supported partially by a grant from IPM.
[†] Supported by an NSERC grant. Corresponding author, email: kharaghani@uleth.ca.

We further associate the real function f_A defined by $f_A(\theta) = |h_A(e^{i\theta})|^2$. Note that f_A is a nonnegative periodic function with a period 2π. Furthermore, it is easy to see that

$$f_A(\theta) = N_A(0) + 2\sum_{j=1}^{n-1} N_A(j)\cos j\theta, \tag{1}$$

(and thus $f_A(2\pi - \theta) = f_A(\theta)$).

Four $(-1, 1)$ sequences A, B, C, D of lengths $n + p$, $n + p$, n, n are called *base sequences* if

$$(N_A + N_B + N_C + N_D)(s) = 0, \quad \text{for} \quad s \geq 1.$$

Four $(0, \pm 1)$ sequences A, B, C, D of length n are called T-*sequences* if

$$(N_A + N_B + N_C + N_D)(s) = 0, \quad \text{for} \quad s \geq 1,$$

and in each position exactly one of the entries of A, B, C, D is nonzero.

If A, B, C, D are base sequences of lengths $n+p$, $n+p$, n, n, then the sequences $\big(\frac{1}{2}(A + B), 0_n\big)$, $\big(\frac{1}{2}(A - B), 0_n\big)$, $\big(0_{n+p}, \frac{1}{2}(C + D)\big)$, $\big(0_{n+p}, \frac{1}{2}(C - D)\big)$, where 0_m denotes a sequence of zero entries of length m, form T-sequences of length $2n + p$. T-sequences of length n can be used to construct Hadamard matrices of order $4n$. The standard procedure is to start with T-sequences T_1, T_2, T_3, T_4 of length n. To each sequence T_i, there corresponds a circulant matrix with the entries of T_i as its first row, denoted by the same notation T_i. Let

$$\begin{aligned}
A_1 &= T_1 + T_2 + T_3 + T_4,\\
A_2 &= -T_1 + T_2 + T_3 - T_4,\\
A_3 &= -T_1 - T_2 + T_3 + T_4,\\
A_4 &= -T_1 + T_2 - T_3 + T_4.
\end{aligned}$$

Then the matrix

$$H = \begin{pmatrix} A_1 & A_2R & A_3R & A_4R \\ -A_2R & A_1 & A_4^tR & -A_3^tR \\ -A_3R & -A_4^tR & A_1 & A_2^tR \\ -A_4R & A_3^tR & -A_2^tR & A_1 \end{pmatrix},$$

where R is the back diagonal identity matrix of order n, is a Hadamard matrix of order $4n$. For more information on sequences, we refer the reader to [2, 7].

Four $(-1, 1)$ sequences X, Y, Z, W of lengths n, n, n, $n - 1$ are said to be of *Turyn type* if

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

Turyn in his 1974 monumental paper [8] proved the following result.

Theorem 1 [8] *If X, Y, Z, W are Turyn type sequences of lengths n, n, n, $n-1$, then the sequences $A = (Z, W)$, $B = (Z, -W)$, $C = X$, $D = Y$ are base sequences of lengths $2n-1$, $2n-1$, n, n.*

This theorem shows that Turyn type sequences of lengths n, n, n, $n-1$ can be used to find T-sequences of length $3n-1$ and thus Hadamard matrices of order $4(3n-1)$. Turyn [8] found these sequences for $n = 4, 6, 8$. By a computer search Turyn type sequences for $n = 10, 12, \ldots, 24$ were constructed in [4]. Kounias and Sotirakoglou complemented the result of [4] and found Turyn type sequences for $n = 26, 28, 30, 32, 34$ in [5]. In this paper, we construct Turyn type sequences for $n = 36$. This results in a number of new T-sequences. As a consequence we have a large number of new Hadamard matrices with the first one being of order 428. This is the smallest order for which the Hadamard determinant conjecture was not known to be true. Historically, the previously unknown case was order 268 which was constructed by Sawade in [6] by a computer search some twenty years ago.

2 Facts on Turyn type sequences

In this section we mention all those properties that we use to speed up our search for Turyn type sequences. In what follows $X = (x_0, \ldots, x_{35})$, $Y = (y_0, \ldots, y_{35})$, $Z = (z_0, \ldots, z_{35})$, $W = (w_0, \ldots, w_{34})$ are Turyn type sequences of lengths n, n, n, $n-1$. One of the most important properties of these sequences is stated in the following theorem.

Theorem 2 [3, 4] *n is even and for $i = 1, 2, \ldots, n-2$, we have*

$$x_i x_{n-1-i} + y_i y_{n-1-i} = 0.$$

If x, y, z, w are the sums of the entries of X, Y, Z, W, respectively, then we have

$$x^2 + y^2 + 2z^2 + 2w^2 = 214.$$

The assumption

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

and (1) leads to the very useful identity

$$(f_X + f_Y + 2f_Z + 2f_W)(\theta) = 6n - 2, \quad \text{for all} \quad \theta.$$

This identity restricts the values attained by each of $f_X(\theta)$, $f_Y(\theta)$, $2f_Z(\theta)$, $2f_W(\theta)$, and their partial sums. It is a standard technique to use this identity to eliminate improper sequences and it has been used extensively in the search for Williamson and similar orthogonal matrices.

The following presetting of some entries is possible. We may assume that the first entry in each of the sequences is 1 by multiplying any sequence by a minus, if necessary. We may also take the last entry of Z to be 1. This follows from the fact that if the odd indexed entries of all sequences are negated simultaneously, then the new sequences remain Turyn type. This and (2) applied at $s = n-1$ show that $x_{n-1} = y_{n-1} = -1$. Let i be the least number such that $x_i = x_{n-1-i}$. Then we may let $x_i = x_{n-1-i} = 1$ by reversing and then multiplying X by -1, if necessary. The same argument applies to Y. In fact, by applying Theorem 2, we can assume that $x_1 = x_{n-2} = 1$. Now let i be the least number such that $z_i \neq z_{n-1-i}$. Then we can take $z_i = -z_{n-1-i} = 1$ by reversing Z, if necessary. Finally, let $i < \frac{n}{2} - 1$ be the least number such that $w_i = -w_{n-2}w_{n-2-i}$. Then we may take $w_i = -w_{n-2}w_{n-2-i} = 1$ by reversing W, if necessary, and then multiplying it by -1, if necessary.

3 The search

In this section we describe our search method to find Turyn type sequences $X = (x_0, \ldots, x_{35})$, $Y = (y_0, \ldots, y_{35})$, $Z = (z_0, \ldots, z_{35})$, $W = (w_0, \ldots, w_{34})$ of lengths 36, 36, 36, 35. For convenience, we append W with a zero to make it of length 36.

We first find and retain, by implementing the properties developed in the previous section, all partial sequences $X^* = (x_0, \ldots, x_5, *, *, \ldots, *, x_{30}, \ldots, x_{35})$, $Y^* = (y_0, \ldots, y_5, *, *, \ldots, *, y_{30}, \ldots, y_{35})$, $Z^* = (z_0, \ldots, z_5, *, *, \ldots, *, z_{30}, \ldots, z_{35})$, $W^* = (w_0, \ldots, w_5, *, *, \ldots, *, w_{30}, \ldots, w_{34}, 0)$ for which

$$(N_{X^*} + N_{Y^*} + 2N_{Z^*} + 2N_{W^*})(s) = 0, \quad \text{for} \quad s \geq 30.$$

For our purpose, the choice of 12 entries in each sequence is the best possible to maintain a feasible number of cases. There are $1,911,620$ solutions in total. The set $\mathcal{S}$ of all of these solutions will form an input data file for the algorithm. Now we describe the algorithm.

The Algorithm

1. We select x, y, z, w such that
$$x^2 + y^2 + 2z^2 + 2w^2 = 214.$$

2. We generate all sequences Z with the sum of entries equal to z and for which $f_Z(\theta) \leq 107$ for all $\theta \in \{\frac{j\pi}{100} \mid j = 1, 2, \ldots, 100\}$. We generate and save proper sequences according to their identical first and last six entries. We do the same for the sequences W with the sum w.

3. Choose a solution $\{X^*, Y^*, Z^*, W^*\}$ in $\mathcal{S}$. Let $\mathcal{Z}$ and $\mathcal{W}$ be those sequences Z and W found in Step 2 whose first and last six entries are identical to the first and last six entries of Z^* and W^*, respectively. For any $Z \in \mathcal{Z}$ and $W \in \mathcal{W}$ for which $f_Z(\theta) + f_W(\theta) \leq 107$ for all $\theta \in \{\frac{j\pi}{100} \mid j = 1, 2, \ldots, 100\}$, we proceed to fill in partial sequences X^* and Y^* step by step, using the crucial Theorem 2 and the identity (2), to find appropriate sequences X and Y: we already have the first and the last six entries of X and Y. So, we first find x_6, x_{29}, y_6, y_{29} by applying (2) at $s = 29$ and noting that $x_6 x_{29} + y_6 y_{29} = 0$ and continue by a backtracking procedure till the appropriate sequences X and Y are found. The implementation of the backtracking procedure involves an effective use of Theorem 2 and the requirement in Step 1 that the sums of entries of X and Y are $\pm x$ and $\pm y$, respectively, to truncate many branches in the backtracking trail. The procedure may terminate with no solution found. We repeat this step for every quadruple set of sequences in $\mathcal{S}$ till a solution is found. In case that there is no solution, the algorithm continues from Step 1.

We implemented the algorithm on a cluster of sixteen 2.6 GHz PCs with $x = 0$, $y = 6$, $z = 8$ and $w = 5$ and found the following solution after about 12 hours of computations.

$$\begin{aligned}
X &= (+ + + - - - - + + - + - + - - - - - + + + + - + + - + + + + - - - - + -),\\
Y &= (+ - + + + + + - - + - + - - + - - + + - - + + + + - + + + + - - - + + -),\\
Z &= (+ - + + + + + - + - - + + + + - + + + - + + - - + + + - + - - + - - - +),\\
W &= (+ + + - + - - - - - + + - - + - + + + - - + - + - + + + - + + + + - +).
\end{aligned}$$

The following result is now immediate from Theorem 1.

Theorem 3 *There are base sequences of lengths* 71, 71, 36, 36 *and therefore* T*-sequences of length* 107.

Corollary 1 *There is a Hadamard matrix of order* 428.

The matrix is available electronically at math.ipm.ac.ir/tayfeh-r/research.htm.

4 Some applications

In this section we combine some well known results with the base sequences found in the previous section to generate some new Hadamard matrices.

Theorem 4 [7] *If there are base sequences of lengths $n+p$, $n+p$, n, n and y is a Yang number, then there are T-sequences of length $y(2n+p)$.*

According to [7, page 482], Yang numbers are known for $y \in \{3, 5, \ldots, 33, 37, 39, 41, 45, 49, 51, 53, 57, 59, 61, 65, 81\}$ and all $y = 2g + 1 > 81$, where $g = 2^a 10^b 26^c$ (a, b, c nonnegative integers) is a Golay number. Using these results and the new base sequences obtained in the previous section, we get T-sequences of length $107y$, where y is a Yang number. Most of these T-sequences seem to be new.

It is well known that T-sequences of length n can be used to generate orthogonal designs $OD(4n; n, n, n, n)$, $OD(20n; 5n, 5n, 5n, 5n)$ and $OD(36n; 9n, 9n, 9n, 9n)$, see [7] for definitions and details. Therefore, there are $OD(428y; 107y, 107y, 107y, 107y)$, $OD(2140y; 535y, 535y, 535y, 535y)$ and $OD(3852y; 963y, 963y, 963y, 963y)$, where y is a Yang number. Finally, we deduce the existence of Hadamard matrices of orders $428yw$, $2140yw$ and $3852yw$, where y is a Yang number and w is the order of Williamson type matrices. Consequently, a large number of Hadamard matrices of new orders are obtained including those of orders $4n$ for $n \in \{107, 749, 1177, 2033, 2461, 3103, 3959, 4387, 4601, 5243, 5457, 5671, 6313, 6741, 6955, 7811, 9095, 9309, 9523, 9737, 9951\}$. We have used Craigen's tables of known Hadamard matrices and Williamson type matrices in [1] to compile our list. This leaves $4(167) = 668$ to be the smallest order of Hadamard matrices not known to exist.

Acknowledgement The work was completed while the first author was on sabbatical leave from the University of Lethbridge visiting IPM. He is thankful for their hospitality. The authors are greatly indebted to Professor Khosrovshahi for his encouragements, insights and thoughtfulness.

References

[1] R. Craigen, *Hadamard matrices and designs*, in CRC Handbook of Combinatorial Designs, C. J. Colbourn and J. H. Dinitz, eds., CRC Press, 1996, pp. 370–377.

[2] C. Koukouvinos, *Sequences with zero autocorrelation*, in CRC Handbook of Combinatorial Designs, C. J. Colbourn and J. H. Dinitz, eds., CRC Press, 1996, pp. 452–456.

[3] C. Koukouvinos, S. Kounias and K. Sotirakoglou, *On base and Turyn sequences*, Math. Comp. **55** (1990), no. 192, 825–837.

[4] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang and J. Yang, *On sequences with zero autocorrelation*, Des. Codes Cryptogr. **4** (1994), 327–340.

[5] S. Kounias and K. Sotirakoglou, *Construction of orthogonal sequences*, in Proceedings of the 14th Greek Statistical Conference, 2001, pp. 229–236, in Greek.

[6] K. Sawade, *A Hadamard matrix of order* 268, Graphs Combin. **1** (1985), no. 2, 185–187.

[7] J. Seberry and M. Yamada, *Hadamard matrices, sequences, and block designs*, in Contemporary Design Theory: A Collection of Surveys, J. H. Dinitz and D. R. Stinson, eds., John Wiley & Sons, Inc., 1992, pp. 431–560.

[8] R. J. Turyn, *Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings*, J. Combin. Theory Ser. A **16** (1974), 313–333.