Inequivalent Hadamard matrices from near normal sequences

Ilias S. Kotsireas
Department of Phys. and Comp. Sci.
Wilfrid Laurier University
Waterloo ON, N2L 3C5, Canada

Christos Koukouvinos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece

Dimitris E. Simos
Department of Mathematics
National Technical University of Athens
Zografou 15773, Athens, Greece

Abstract

In this paper, we construct inequivalent Hadamard matrices based on Yang multiplication methods for base sequences which are obtained from near normal sequences. This has been achieved by employing various Unix tools and sophisticated techniques, such as metaprogramming. In addition, we present a classification for near normal sequences of length $4n+1$, for $n \leq 11$ and some of these for $n = 12, 13, 14$ and 15, taking into account previously known results. Finally, we improve several constructive lower bounds for inequivalent Hadamard matrices of large orders.

Keywords: Autocorrelation function, classification, Base sequences, Near normal sequences, Yang multiplication methods, Hadamard matrices, T-sequences, T-matrices.

MSC classification: Primary 05B20, Secondary 68R05, 68W30.

JCMCC **75** (2010), pp. 105-115

1 Introduction

Let x_1, ..., x_t be commuting indeterminates. An orthogonal design X of order n and type $(s_1, \ldots, s_t)$ denoted OD$(n; s_1, \ldots, s_t)$, where s_1, ..., s_t are positive integers, is a matrix of order n with entries from $\{0, \pm x_1, \ldots, \pm x_t\}$, such that

$$XX^t = \left(\sum_{i=1}^{t} s_i x_i^2 \right) I_n,$$

where X^t denotes the transpose of X and I_n denotes the identity matrix of order n. Orthogonal designs are used in Combinatorics, Statistics, Coding Theory, Telecommunications and other areas. For more details on orthogonal designs see [5, 16] and on Hadamard matrices see [3, 17].

Given the sequence $A = (a_1, \ldots, a_n)$ of length n the *non-periodic autocorrelation function* $N_A(s)$ (abbreviated as NPAF), is defined as

$$N_A(s) = \sum_{i=1}^{n-s} a_i a_{i+s} \ , \qquad s = 0, 1, \ldots, n-1. \tag{1}$$

Given A as above of length n, the *periodic autocorrelation function* $P_A(s)$ (abbreviated as PAF) is defined, reducing $i + s$ modulo n, as

$$P_A(s) = \sum_{i=1}^{n} a_i a_{i+s} \ , \qquad s = 0, 1, \ldots, n-1. \tag{2}$$

The concepts of the periodic (PAF) and non-periodic (NPAF) autocorrelation functions are thoroughly described in [8]. The reversed sequence A^* of A is defined as $(a_n, \ldots, a_1)$. For given sequences $A = (a_1, a_2, \ldots, a_{m+1})$ and $C = (c_1, c_2, \ldots, c_m)$, the interleaved sequence A/C of A and C is defined as $A/C = (a_1, c_1, a_2, c_2, \ldots, a_m, c_m, a_{m+1})$.

2 Classification of near normal sequences

Definition 1 *A quadruple $(E, F; G, H)$ of $(0, \pm 1)$ sequences is a set of near normal sequences for length $n = 4m + 1$ (abbreviated as $NNS(n)$) if the following conditions are satisfied.*

1. *$E = (1, X/O_{m-1})$, $F = (Y/O_{m-1})$ where X and Y are $(1, -1)$ sequences of length m and O_{m-1} is the sequence of zeros of length $m-1$, i.e., E and F are respectively of lengths $2m$ and $2m-1$; G and H are $(0, \pm 1)$ sequences of length $2m$, such that $G + H$ is a $(1, -1)$ sequence of length $2m$.*

2. *$N_E(s) + N_F(s) + N_G(s) + N_H(s) = 0$, $s = 1, \ldots, 2m - 1$.*

Remark 1 The sequences G and H of this definition are quasi-symmetric, i.e., if $g_k = 0$, then $g_{2m+1-k} = 0$ and also if $h_k = 0$, then $h_{2m+1-k} = 0$.

Definition 2 *Two sets of near normal sequences $NNS(n)$, $(E, F; G, H)$ and $(E', F'; G', H')$, are said to be equivalent if one can be obtained from the other through the following isomorphic transformations:*

(i) $E' = E$ or $-E$, $S' = S, S^*$ or $-S$ for $S = F, G$ and H;

(ii) $S' = S$ for $S = E$ and F, $G' = G_s + H_k$ and $H' = H_s + G_k$, where G_s, H_s and G_k, H_k are the symmetric and skew parts of G, H respectively;

(iii) $S' = S^e$ or S^0 for $S = E, F, G$ and H, where S^e and S^0 indicate that S^e and S^0, are obtained from S by changing the signs of even and odd subscripts, respectively;

(iv) $S' = S$ for $S = E$ and F, $G' = H$ and $H' = G$;

(v) E', F', G' and H' are obtainable by any number of combinations of (i), (ii), (iii) and (iv).

Some sets of near normal sequences are given in [10] and [21]. We now present a complete classification of near normal sequences $NNS(n)$, $n = 4m+1$. Table 1, lists $I(n)$ number of inequivalent $NNS(n)$ for $1 \le m \le 11$, i.e. $5 \le n \le 45$.

m	1	2	3	4	5	6	7	8	9	10	11
n	5	9	13	17	21	25	29	33	37	41	45
$I(n)$	1	2	2	3	8	14	11	24	20	18	32

Table 1: List of inequivalent $NNS(n)$ for $5 \le n \le 45$.

Sets of near normal sequences $NNS(n)$, $n = 4m + 1$ are also found for $m = 12, 13, 14$ and 15, i.e. $n = 49, 53, 57$ and 61.

m	12	13	14	15
n	49	53	57	61
$S(n)$	12	2	3	4

Table 2: Sets of $NNS(n)$ for $49 \le n \le 61$.

All inequivalent $NNS(n)$ for $5 \le n \le 45$ are accessible online off the web page of C. Koukouvinos, `http://www.math.ntua.gr/~ckoukouv/nnseq.htm`.

3 Metaprogramming for near normal sequences

A prolific method for constructing orthogonal designs and Hadamard matrices uses T-matrices or T-sequences. This method rely on Base sequences and Yang numbers as its main characteristics. Yang's multiplications Theorems on T-sequences use suitable sequences, which are derived from Base sequences of small length, to produce T-sequences of larger length. The aforementioned Base sequences can be produced, among other methods, from near normal sequences. Thus, we are able to construct T-matrices of large orders and with the aid of the Goethals-Seidel array, which is an orthogonal design of special interest, we generate Hadamard matrices in various orders. The structure and the number of steps encountered for an interpretation of these methods in terms of a computer implementation, shows that it is an ideal case for metaprogramming.

3.1 Yang multiplication methods

We give the necessary definitions needed for establishing the theoretical background of Yang's multiplications Theorems on T-sequences. For further details on sequences with zero autocorrelation and multiplication methods for T-sequences we refer the interest reader to [6, 8] and [9, 10, 18, 19, 20].

Definition 3 *Four $(-1,1)$ sequences A, B, C, D of lengths $n+p, n+p, n, n$ are Base sequences, (abbreviated as $BS(n+p,n)$) if:*

1. $N_A(s)+N_B(s)+N_C(s)+N_D(s)=\begin{cases} 0, & s=1,\ldots,n-1 \\ 4n+2p, & s=0 \end{cases}$

2. $N_A(s)+N_B(s)=0, s=n,\ldots,n+p-1$

whereas with N_X we denote the non-periodic autocorrelation function of a sequence X.

We give now a reformulation of a well-known result ([10, 21]), which exhibits the relation of Base sequences to near normal sequences and is crucial to our implementation.

Theorem 1 *Let $n = 4m+1$. Then $(E, F; G, H)$ with $E = (1, X/O_{m-1})$ and $F = (Y/O_{m-1})$, are near normal sequences, if and only if the $(1,-1)$ sequences $A = (1, X/Y)$, $B = (1, X/-Y)$, $C = G+H$, $D = G-H$ of lengths $2m+1$, $2m+1$, $2m$, $2m$, respectively, are Base sequences.*

Definition 4 *If A, B, C, D are Base sequences of lengths $n+1, n+1, n, n$ then the sequences $(\frac{1}{2}(A+B))$, $(\frac{1}{2}(A-B))$, $(\frac{1}{2}(C+D))$, $(\frac{1}{2}(C-D))$ are called suitable or Yang sequences.*

Definition 5 *Four sequences X, Y, Z, W of length n with entries $(-1, 0, 1)$ are called T-sequences, (abbreviated as $TS(n)$) if:*

1. $|x_i| + |y_i| + |z_i| + |w_i| = 1$, $i = 1, \ldots, n$.

2. $N_X(s) + N_Y(s) + N_Z(s) + N_W(s) = \begin{cases} 0, & s = 1, \ldots, n-1 \\ n, & s = 0 \end{cases}$

Definition 6 *Four circulant matrices T_1, T_2, T_3, T_4 of order t with entries $(-1, 0, 1)$ are called T-matrices if:*

1. $T_i * T_j = 0, i \neq j$ *($*$ denotes the Hadamard product)*

2. $T_1T_1^T + T_2T_2^T + T_3T_3^T + T_4T_4^T = tI_t$.

We recall that T-sequences always yield T-matrices, since a T-sequence of length n can be used as the first row of a circulant matrix which results in a T-matrix of order n, but not conversely.

In a series of papers in 1982 and 1983, Yang [18, 19, 20] found that Base sequences can be multiplied by $3, 7, 13$ and $2g + 1$, where g is a Golay number: $g = 2^a 10^b 26^c$, $a, b, c \geq 0$. These are instances of what are termed Yang numbers. The results of these papers on multiplication methods can be restated as follows; If there is a multiplication method which uses suitable sequences of lengths $n + p, n + p, n, n$ to produce T-sequences of length $y(2n + p)$, then y is called a Yang number. The existence of Yang numbers is given in the following proposition [8], see also [9, 17, 21].

Proposition 1 *Yang numbers are known for $y \epsilon \{3, 5, 7, \ldots, 33, 37, 39, 41, 45, 49, 51, 53, 57, 59, 61, 65, 81\}$ and all $y = 2g + 1 > 81$, when g is a Golay number.*

It is well known that if there exists T-sequences of length t and Williamson matrices of order w then there exists a Hadamard matrix of order $4tw$.

Let B_i, $i = 1, 2, 3, 4$ be circulant matrices of order n with entries in $\{0, \pm x_1, \pm x_2, \ldots, \pm x_k\}$ satisfying

$$\sum_{i=1}^{4} B_i B_i^T = \sum_{i=1}^{k} (s_i x_i^2) I_n.$$

Then, the Goethals-Seidel array

$$G = \begin{pmatrix} B_1 & B_2R & B_3R & B_4R \\ -B_2R & B_1 & B_4^TR & -B_3^TR \\ -B_3R & -B_4^TR & B_1 & B_2^TR \\ -B_4R & B_3^TR & -B_2^TR & B_1 \end{pmatrix},$$

where R is the back-diagonal identity matrix, is an $OD(4n; s_1, s_2, \ldots, s_k)$ (see [5, page 107]).

If there are four sequences A_1, A_2, A_3, A_4 of length n with entries from $\{0, \pm x_1, \pm x_2, \pm x_3, \pm x_4\}$ with zero periodic or non-periodic autocorrelation function, then these sequences can be used as the first rows of circulant matrices $B_i = circ(A_i)$, $i = 1, 2, 3, 4$, which can be used in the Goethals-Seidel array to form an $OD(4n; s_1, s_2, s_3, s_4)$.

The following theorem given in [2], deals with the case of trivial Williamson matrices and was taken into account in our Maple implementation.

Theorem 2 *Suppose there exist circulant T-matrices (or equivalent T-sequences) T_i, $i = 1, \ldots, 4$ of order n. Let a, b, c, d be commuting variables. Then the matrices,*

$$\begin{aligned} A &= aT_1 + bT_2 + cT_3 + dT_4 \\ B &= -bT_1 + aT_2 + dT_3 - cT_4 \\ C &= -cT_1 - dT_2 + aT_3 + bT_4 \\ D &= -dT_1 + cT_2 - bT_3 + aT_4 \end{aligned}$$

can be used in the Goethals-Seidel array to obtain an $OD(4n; n, n, n, n)$ and an Hadamard matrix of order $4n$.

Remark 2 It is obvious that a Hadamard matrix of order $4n$ is obtained if we set $a = b = c = d = 1$ in the previous theorem.

3.2 Implementation

Metaprogramming is not a new concept, and has been successfully employed before in sequences with zero non-periodic autocorrelation function [7]. Before continuing we will list some uses of metaprogramming:

- Generation - metacode that generates code
- Transformation - metacode that modifies code (similar to generation)
- Translation - transformation into another language
- Analysis - metacode that analyzes code

We wrote a metaprogram that satisfies the previous principles and accepts as input an html file with near normal sequences and produces the individual near normal sequences files that produce a Maple file which is executed and generate the corresponding Hadamard matrices for specific Yang numbers. The metaprogram is using bash shell as its metalanguage whilst the object-language that each program is manipulated is the Computer Algebra System, Maple. We expanded the `YangMultiplications`

Maple package, first given in [7], for the purposes of our metaprogram. In addition, a sed/awk script is used to transform each Hadamard matrix in a format suitable for inclusion in the Magma Hadamard matrices database. Some of the principal difficulties in the design of this program lie in the dynamic production of the values of the variables that capture the characteristics of the near normal sequences in the input file, i.e. the length of each $NNS(n)$, the number of sets of $NNS(n)$ for a specific n and the list of different variables.
The file that contains the sets of $NNS(n)$ can be found in C. Koukouvinos web page at `http://www.math.ntua.gr/~ckoukouv/nnseq.htm`. The Computer Algebra System, Maple provides an excellent way for performing symbolic and numerical computations, especially when we have to interpret methods that are based on combinatorial mathematics.

We implemented the Yang multiplication methods for Base sequences in Maple, in order to achieve the best possible flexibility in terms of portability with other Computational Algebra Systems, such as Magma. We wrote a Maple package, that contains the necessary routines for the generation of Hadamard matrices from near normal sequences. An overview of the main routines is given below.

The Maple procedures

NearNormalSeqs2BaseSeqs This routine accepts as input near normal sequences of length $2n+1$ and gives output Base sequences of lengths $n+1, n+1, n, n$. It exhibits the relation of near normal sequences to Base sequences and is an interpretation of Theorem 1.

BaseSeqs2YangSeqs This routine accepts as input Base sequences of lengths $n+1, n+1, n, n$ and gives output suitable (Yang) sequences of lengths $n+1, n+1, n, n$. This is an auxiliary routine and is used as an intermediate step to transform the Base sequences to Yang sequences.

YangSeqs2TSeqs This routine accepts as input suitable (Yang) sequences of lengths $n+1, n+1, n, n$ and the Yang number y and gives output T-sequences of length $y(2n+1)$. Current implementation includes the multiplication methods for $y = 3, 5, 7, 9, 11$. This routine is used to produce T-sequences of larger length derived from Yang sequences.

TSeqs2Hadamard This routine accepts as input T-sequences of length n and gives as output a Hadamard matrix of order $4n$. T-sequences of length n are used to form T-matrices of order n, which are then plugged-in the Goethals-Seidel array to produce an $OD(4n; n, n, n, n)$ and subsequently using Remark 2, we construct a Hadamard matrix of order $4n$.

Furthermore, we give the Maple source code of the routine which is called in the bash script and it is responsible for the generation of Hadamard matrices from near normal sequences.

```
YangMultiplications[YangMultiplication2HM] := proc(nn1,nn2,nn3,nn4,y)

local HM, b1, b2, b3, b4, bsy1, bsy2, bsy3, bsy4, X1, Y1, Z1, W1, ot;

b1, b2, b3, b4 := NearNormalSeqs2BaseSeqs(nn1,nn2,nn3,nn4);
bsy1, bsy2, bsy3, bsy4 := BaseSeqs2YangSeqs(b1,b2,b3,b4);
X1, Y1, Z1, W1 := YangSeqs2TSeqs(bsy1,bsy2,bsy3,bsy4,y);
ot := nops(X1);
HM := Matrix(TSeqs2Hadamard(X1,Y1,Z1,W1,ot));

RETURN(HM);

end proc;
```

4 Results

We executed the metaprogram for all available near normal sequences, $NNS(n)$ given in section 2., and generated the corresponding Hadamard matrices of order $4yn$, for each $y = 3, 5, 7, 9, 11$ whereas y is a Yang number. The smallest Hadamard matrix constructed is of order 60, while the largest Hadamard matrix constructed is of order 2684. The whole database of the generated Hadamard matrices in Magma format is available on request.

Furthermore, we conducted a search in our database for inequivalent Hadamard matrices for orders ranging from 60 to 1140, using the 4-profile criterion as implemented in Magma [1], to decide whether these Hadamard matrices are inequivalent. The results of this search are given in the following table; We denote with N_n the number of Hadamard matrices we constructed from near normal sequences, while with IN_n we denote the number of inequivalent Hadamard matrices found. We denote with n the order of the corresponding Hadamard matrices.

From the computational results presented in the previous table we conclude the following remark.

Remark 3 We note that all Hadamard matrices that are constructed using Yang multiplication methods on near normal sequences are inequivalent, since for each order we found that the corresponding 4-profiles are different.

In addition, one could check these Hadamard matrices for inequivalence, using the graph isomorphism criterion, which is more time consuming [1, 14].

n	N_n	IN_n	n	N_n	IN_n	n	N_n	IN_n	n	N_n	IN_n
60	1	1	100	1	1	108	2	2	140	1	1
156	2	2	180	3	3	204	3	3	220	1	1
252	10	10	260	2	2	300	14	14	324	2	2
340	3	3	348	11	11	364	2	2	396	26	26
420	8	8	444	20	20	468	2	2	476	3	3
492	18	18	500	14	14	540	32	32	572	2	2
580	11	11	588	20	20	612	3	3	636	2	2
660	23	23	684	3	3	700	14	14	732	4	4
740	20	20	748	3	3	756	8	8	812	11	11
820	18	18	900	45	45	924	31	31	980	12	12
1036	20	20	1044	11	11	1060	2	2	1100	14	14
1140	3	3									

Table 3: Inequivalent Hadamard matrices from near normal sequences.

4.1 New constructive lower bounds for inequivalent Hadamard matrices of large orders

We compared our results on inequivalent Hadamard matrices from near normal sequences given in the previous section with those given in [7], and concluded the following remark.

Remark 4 All Hadamard matrices constructed from near normal sequences are inequivalent with the Hadamard matrices constructed from base sequences for the following orders, $n = 108, 156, 180, 204, 220, 252, 260, 300, 324, 340, 348, 364, 396, 420, 444, 468, 476, 492, 500, 540, 572580, 588, 612, 636, 660, 684, 700, 732, 740, 748, 756, 812, 820, 900, 924, 980, 1036, 1044, 1060, 1100, 1140$, since for each order we found that the corresponding 4-profiles are different.

Thus, we establish new constructive lower bounds for inequivalent Hadamard matrices of large orders, by summing the numbers of inequivalent matrices given in previous section and those given in [7].

The complete classification for Hadamard matrices of order n is well known for $n \equiv 0 \pmod 4$, $n \leq 28$. For $n = 32, 36$ there are at least $3,578,006$ and $4,745,357$ inequivalent Hadamard matrices respectively, see [15]. There are also available other lower bounds on the number of inequivalent Hadamard matrices for various orders, see [4]. On the other hand, there are some theoretical results which provide huge lower bounds, see [11, 12, 13].

However, we believe that our constructive lower bounds on the number of inequivalent Hadamard matrices, which are presented in this section have value since these are coming from base and near normal sequences on Yang multiplication methods, one of the most powerful construction for Hadamard matrices. As already noted, this task has been accomplished by employing various Unix tools and sophisticated techniques, such as metaprogramming.

5 Acknowledgments

The research of the third author was financially supported by a scholarship awarded by the Secretariat of the Research Committee of National Technical University of Athens. All computations in Computer Algebra System, Maple have been performed remotely at the *Centre de calcul formel MEDICIS, École Polytechnique, Paris, France.* All computations in Computational Algebra System, Magma have been performed remotely at *SHARCnet* high performance computing clusters.

References

[1] W. Bosma and J. Cannon, *Handbook of Magma Functions*, Version 2.9, Sydney, July, 2002.

[2] J. Cooper and J. S. Wallis, A Construction for Hadamard Arrays, *Bull. Austral. Math. Soc.*, 7, 1972, pp. 269-278.

[3] R. Craigen, Hadamard Matrices and Designs, in *The CRC Handbook of Combinatorial Designs*, (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, Fla., 1996, pp. 370-377.

[4] S. Georgiou, I. S. Kotsireas and C. Koukouvinos, Inequivalent Hadamard matrices of order $2n$ constructed from Hadamard matrices of order n, *J. Combin. Math. Combin. Comput.*, 63, 2007, pp. 65-79.

[5] A. V. Geramita and J. Seberry, *Orthogonal Designs. Quadratic Forms and Hadamard Matrices*, Lecture Notes in Pure and Applied Mathematics, 45. Marcel Dekker, Inc., New York, 1979.

[6] H. Kharaghani and C. Koukouvinos, Complementary, Base and Turyn Sequences, in *Handbook of Combinatorial Designs*, (eds. C.J. Colbourn and J.H. Dinitz), 2nd ed. Chapman and Hall/CRC Press, Boca Raton, Fla., 2006, pp. 317-321.

[7] I. S. Kotsireas, C. Koukouvinos and D. E. Simos, Inequivalent Hadamard matrices from base sequences, *Utilitas Math.*, to appear.

[8] C. Koukouvinos, Sequences with Zero Autocorrelation, in *The CRC Handbook of Combinatorial Designs*, C. J. Colbourn, J. H. Dinitz, Eds. CRC Press, 1996, Part IV, Chapter 42, 452-456.

[9] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang and J. Yang, On Sequences with zero Autocorrelation, *Des. Codes. Crypt.*, 4, 1994, pp. 327-340.

[10] C. Koukouvinos, S. Kounias, J. Seberry, C. H. Yang and J. Yang, Multiplication of Sequences with Zero Autocorrelation, *Australas. J. Combin.*, 10, 1994, pp. 5-15.

[11] C. Lam, S. Lam and V. D. Tonchev, Bounds on the number of affine, symmetric, and Hadamard designs and matrices, *J. Combin. Theory Ser. A*, 92, 2000, pp. 186-196.

[12] C. Lam, S. Lam and V. D. Tonchev, Bounds on the number of Hadamard designs of even order, *J. Combin. Designs*, 9, 2001, pp. 363-378.

[13] E. Merchant, Exponentially many Hadamard designs, *Des. Codes. Crypt.*, 38, 2006, pp. 297-308.

[14] B.D. McKay, Hadamard equivalence via graph isomorphism, *Discrete Math.*, 27, 1979, pp. 213-214.

[15] W.P. Orrick, Switching operations for Hadamard matrices, arXiv:math.CO/0507515, preprint.

[16] J. Seberry and R. Craigen, Orthogonal Designs, in *The CRC Handbook of Combinatorial Designs*, (eds. C.J. Colbourn and J.H. Dinitz), CRC Press, Boca Raton, Fla., 1996, pp. 400-406.

[17] J. Seberry and M. Yamada, Hadamard Matrices, Sequences and Block Designs, *in Contemporary Design Theory: A Collection of Surveys*, (eds. J.H. Dinitz and D.R. Stinson), John Wiley & Sons, New York, 1992, pp. 431-560.

[18] C. H. Yang, Hadamard Matrices and δ-Codes of Length 3n, *Proc. Amer. Math. Soc.*, 85, 1982, pp. 480-482.

[19] C. H. Yang, A Composition Theorem for δ-Codes, *Proc. Amer. Math. Soc.*, 89, 1983, pp. 375-378.

[20] C. H. Yang, Lagrange Identity for Polynomials and δ-Codes of Lengths $7t$ and $13t$, *Proc. Amer. Math. Soc.*, 88, 1983, pp. 746-750.

[21] C. H. Yang, On Composition of Four-Symbol δ-Codes and Hadamard Matrices, *Proc. Amer. Math. Soc.*, 107, 1989, pp. 763-776.