New infinite families of skew-Hadamard matrices

Jennifer Seberry and Ken Finlayson
School of IT and Computer Science
University of Wollongong
NSW 2522
Australia

Abstract

We give a new construction for skew-Hadamard matrices. This gives new infinite families of skew-Hadamard matrices including 43 new skew-Hadamard matrices of order $4q < 4000$.

Key words and phrases: Williamson matrices, sequences, autocorrelation, negacyclic, Goethals-Seidel
AMS Subject Classification: Primary 05B20, Secondary 62K05, 62K10

1 Introduction

An *Hadamard matrix* H of order n is a square $(1, -1)$ matrix having inner product of distinct rows zero. Hence $HH^T = nI_n$. We note that $n = 1, 2$ or $n \equiv 0 \pmod 4$.

A matrix $A+I$ is *skew-type* if A has zero diagonal and $A^T = -A$. A skew-type Hadamard matrix is said to be *skew-Hadamard.*

Circulant matrices of order n are polynomials in the shift matrix

$$S = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & & 1 \\ 1 & 0 & 0 & & 0 \end{pmatrix}.$$

Negacyclic matrices of order n are polynomials in the nega-shift matrix

$$NS = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & & 1 \\ -1 & 0 & 0 & & 0 \end{pmatrix}.$$

The *back-diagonal matrix* R of order n is the matrix whose elements r_{ij} are given by

$$r_{ij} = \begin{cases} 1 & \text{if } i+j = n+1, \\ 0 & \text{otherwise} \end{cases}$$

where $i, j = 1, \ldots, n$. We note that if A, B are polynomial in S or NS then $A(BR)^T = (BR)A^T$.

Lemma 1 *If A is a circulant matrix of odd order, then XAX, where $X = diag(1, -1, 1, -1, \ldots, 1)$, is a negacyclic matrix.*

Lemma 2 *If A is a symmetric circulant matrix of odd order, then XAX is a skew-type negacyclic matrix.*

2 Williamson Matrices

Williamson's famous theorem is:

Theorem 1 (Williamson [?]) *Suppose there exist four symmetric circulant $(1, -1)$ matrices A, B, C, D of order n. Further, suppose*

$$A^2 + B^2 + C^2 + D^2 = 4nI_n$$

(we call such matrices Williamson matrices*). Then*

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix} \tag{1}$$

is an Hadamard matrix of order $4n$ of Williamson type *or* quaternion type.

In order to construct skew-Hadamard matrices, Goethals and Seidel relaxed the symmetric property in their theorem.

Theorem 2 (Goethals-Seidel [?]) *Suppose there exist four circulant $(1, -1)$ matrices A, B, C, D of order n. Further, suppose*

$$AA^T + BB^T + CC^T + DD^T = 4nI_n.$$

Then

$$GS = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & D^TR & -C^TR \\ -CR & -D^TR & A & B^TR \\ -DR & C^TR & -B^TR & A \end{bmatrix} \tag{2}$$

is an Hadamard matrix of order $4n$ of Goethal-Seidel type. *(Here R is the back diagonal matrix.) If A is skew-type, then GS is skew-Hadamard.*

Theorem 3 (Xia-Liu) *There exist four Williamson matrices of order q^2 for all $q \equiv 1 \pmod 4$ a prime power. The negation of each matrix has row sum q.*

One of us (Seberry) has a list on the computer of odd integers $q < 40,000$ for which Williamson matrices exist (see Seberry and Yamada [?]). The following list gives sources for the matrices used in this paper.

The matrices listed as w1 and w2 are most certainly circulant.

Key	Method	Explanation
w1	$\{1, ..., 33, 37, 39, 41, 43\}$	[?, ?, ?]
w2	$\frac{p+1}{2}$	$p \equiv 1 \pmod 4$ a prime power, [?, ?, ?]
wx	q^2	$q \equiv 1 \pmod 4$ a prime power, [?]

3 Results

We now consider the case where the circulant matrices in Theorem 2 are replaced by negacyclic matrices and obtain the following:

Theorem 4 *If there exist negacyclic matrices A, B, C, D of odd order n with the property*

$$AA^T + BB^T + CC^T + DD^T = 4nI_n$$

then

$$SF = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & D^TR & -C^TR \\ -CR & -D^TR & A & B^TR \\ -DR & C^TR & -B^TR & A \end{bmatrix} \quad (3)$$

gives an Hadamard matrix of order $4n$. If A is skew-type then SF is skew-Hadamard.

Theorem 5 *If there exist four Williamson matrices of odd order n then there exists a skew-Hadamard matrix of order $4n$.*

Proof. Using Lemma 1 we can construct four negacyclic matrices of order n from the four Williamson matrices. It follows from Theorem 4 that a Hadamard matrix of order $4n$ exists.

By Lemma 2 we know that the four constructed negacyclic matrices will be skew-type. And since matrix (3) is also skew-type, it follows that the resulting Hadamard matrix is skew-Hadamard. □

Theorem 6 *If $p \equiv 1 \pmod 4$ is prime then there exists a skew-Hadamard matrix of order $2(p+1)$.*

Proof. If $p \equiv 1 \pmod 4$ then there exist two circulant symmetric $(0, 1, -1)$ matrices P, Q of size $\frac{p+1}{2}$ where P has zero diagonal and the matrices have the property

$$PP^T + QQ^T = pI_{\frac{p+1}{2}}.$$

So $A = P + I, B = P - I, C = D = Q$ are four Williamson matrices of order $\frac{p+1}{2}$. Thus, by Theorem 5, there exists a skew-Hadamard matrix of order $2(p+1)$. □

Theorem 7 *There exist skew-Hadamard matrices of order $4q^2$ when $q \equiv 1 \pmod 4$ is a prime power.*

Proof. By Theorem 3, we know that there exist four Williamson matrices of order q^2 when $q \equiv 1 \pmod 4$ is a prime power. Hence by Theorem 5 there is a skew-Hadamard matrix of order $4q^2$. □

These results lead to 43 new skew-Hadamard matrices of order $4q < 4000$ for $q \in$ {69, 97, 145, 169, 177, 225, 229, 261, 265, 289, 301, 309, 385, 429, 441, 465, 481, 489, 505, 517, 549, 565, 577, 549, 565, 577, 597, 601, 609, 625, 649, 661, 681, 717, 745, 777, 805, 829, 841, 849, 861, 889, 901, 925, 937, 957, 997}. For six of these cases, $q \in \{177, 505, 577, 661, 829, 997\}$, no skew-Hadamard matrix of order $2^t q$ was known for any t.