AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **73(1)** (2019), Pages 207–219

New infinite families of Williamson Hadamard matrices

Santiago Barrera Acevedo Heiko Dietrich

Monash University
School of Mathematical Sciences
Clayton, VIC 3800
Australia
santiago.barrera.acevedo@monash.edu heiko.dietrich@monash.edu

Abstract

Due to the Hadamard Conjecture, Williamson matrices (WM) and Williamson type matrices (WTM) of order $4n$ have been primarily investigated for odd n. Several constructions for this case have been introduced, leading to finite and infinite families of WMs and WTMs. The aim of this paper is to present new families of WMs and WTMs with blocks of even order. Let q and r be prime powers congruent to 1 modulo 4. There are WMs of order $4a(q+1)$ for every $a \in \{1, 11, 17, 23, 29, 33, 39, 43\}$. If $\gcd(q+1, r+1) = 2$, then there is a WM of order $2(q+1)(r+1)$. There are WMs of order $2^b(q+1)$ and WTMs with circulant blocks of order $2^c(q+1)$ for every $b \in \{2, \ldots, 7\}$ and $c \in \{5, 6\}$. We prove these results and more by exploiting a recently established correspondence between perfect quaternionic sequences and relative difference sets.

1 Introduction

A Hadamard matrix (HM) of order n is an $n \times n$ matrix H with entries in $\{-1, 1\}$ such that $HH^\intercal = nI_n$ where I_n is the $n \times n$ identity matrix. HMs have found numerous applications in areas such as cryptography, coding theory, and signal theory; we refer to the books of Horadam [13] and Seberry [29] for details and references. Mathematically, the driving force behind HMs is the famous Hadamard Conjecture, which claims that there exist HMs of order $4n$ for every n.

A **Williamson type (Hadamard) matrix** (WTM) is a Hadamard matrix of the form

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

ISSN: 2202-3518

where the blocks A, B, C, D are $n \times n$ matrices such that

$$AA^\intercal + BB^\intercal + CC^\intercal + DD^\intercal = 4nI_n \tag{2}$$

and

$$XY^\intercal = YX^\intercal \text{ for all } X, Y \in \{A, B, C, D\}. \tag{3}$$

Note that $\{A, B, C, D\}$, with properties (2) and (3), is a *short amicable set*, as considered in [11]. Moreover, if the blocks are symmetric circulant, then H is a **Williamson (Hadamard) matrix** (WM), see the construction in [40, (8)]. Recall that an $n \times n$ matrix $M = (m_{r,c})$ is circulant if $m_{r,c} = m_{0,(c-r) \bmod n}$ for all $r, c = 0, \ldots, n-1$. As a special class of HMs, WMs and WTMs have applications in various areas, such as wireless communication (code division multiple access, see [31]) and coding theory (Hadamard full propelinear codes, see [23]). Because of the Hadamard Conjecture, WTMs have been primarily investigated for odd n: Given a WM or WTM of order $4n$ with n odd, one can use a tensor product construction [13, Lemma 2.1] or a recursive construction presented by Spence [34] to produce HMs of order $2^t n$ for all $t > 2$. However, the tensor construction does not yield WTMs, and the recursive construction produces WTMs with non-circulant blocks. In fact, Horadam asks in [13, Research Problem 2]: What proportion of (orders of) WTMs are WMs? Seberry [26] was one of the first who studied WTMs of order $8n$; these matrices are of particular interest when no WTM of order $4n$ is known.

Schmidt [24] introduced WMs with group-invariant blocks, and presented a correspondence between such WMs and relative difference sets in certain non-abelian groups, including quaternion groups. In [4] we have established a correspondence between certain quaternionic perfect sequences and certain relative difference sets. Together, this yields a correspondence between certain quaternionic perfect sequences and certain WMs and WTMs; we make this correspondence explicit in Section 2. We subsequently apply it to produce new families of WMs and WTMs; our results are reported in Section 3.

1.1 Notation

Let $\mathbb{R}$ be the real numbers and let $\mathbb{H}$ be the real quaternions with $\mathbb{R}$-basis $\{1, \mathtt{i}, \mathtt{j}, \mathtt{k}\}$ satisfying $\mathtt{i}^2 = \mathtt{j}^2 = \mathtt{k}^2 = \mathtt{ijk} = -1$. We consider the multiplicative groups $Q_8 = \{\pm 1, \pm\mathtt{i}, \pm\mathtt{j}, \pm\mathtt{k}\}$ and $Q_{24} = Q_8 \cup qQ_8 \cup q^2Q_8$, where $\mathtt{q} = (1 + \mathtt{i} + \mathtt{j} + \mathtt{k})/2$, and write $h \mapsto h^*$ for the $\mathbb{R}$-linear complex conjugation on $\mathbb{H}$; note that $q^*Q_8 = q^2Q_8$. For a positive integer n, the cyclic group of order n is denoted by C_n. We now recall some crucial definitions.

An (m, n, k, λ)-**relative difference set** (RDS) in a group G of order mn, relative to a normal subgroup N of order n, is a k-subset $R \subseteq G$ with the property that the list of elements ab^{-1} with distinct $a, b \in R$ contains each element of $G \setminus N$ exactly λ times and does not contain any element of N. It is common to identify $R \subseteq G$ with an element $R = \sum_{r \in R} r$ in the group ring $\mathbb{R}[G]$; writing $R^{(-1)} = \sum_{r \in R} r^{-1}$, it follows that $R \subseteq G$ is an (m, n, k, λ)-RDS if and only if $RR^{(-1)} = k + \lambda(G - N)$ in $\mathbb{R}[G]$.

Let G be a group of size n. An $n \times n$ matrix A is **G-invariant** (or G-developed) if the rows and columns of $A = (a_{g,h})$ can be indexed with elements $g, h \in G$ such that $a_{gk,hk} = a_{g,h}$ for all $g, h, k \in G$. Note that A is circulant if and only if A is C_n-invariant. Here we denote a WM and WTM with G-invariant blocks by ***G*-WM** and ***G*-WTM**, respectively. A **quaternion type HM** is a HM of the form (1) whose blocks satisfy (2) and $WX^\intercal - XW^\intercal + YZ^\intercal - ZY^\intercal = 0$ for all $\{W, X, Y, Z\} = \{A, B, C, D\}$. In the following we say that a WTM is circulant or symmetric if this property holds for its blocks.

2 From perfect quaternionic sequences to Williamson type matrices

Let $S = (s_0, \ldots, s_{n-1})$ be a (periodic) sequence over a quaternion alphabet $\mathcal{A} \subseteq \mathbb{H}$, that is, we use the convention that $s_z = s_{z \bmod n}$ for all $z \in \mathbb{Z}$. For $t \in \mathbb{Z}$, the right periodic t-autocorrelation value of S is

$$\mathrm{AC}_S^{\mathrm{R}}(t) = \sum_{r=0}^{n-1} s_r s_{r+t}^*,$$

and S is **perfect** if $\mathrm{AC}^{\mathrm{R}}(S) = (\mathrm{AC}_S^{\mathrm{R}}(0), \ldots, \mathrm{AC}_S^{\mathrm{R}}(n-1)) = (*, 0, \ldots, 0)$. The non-commutativity of $\mathbb{H}$ also admits the concept of left periodic autocorrelations, however, perfection does not depend on this choice, see [18, Lemma 1]. We refer to [4, 6, 18, 19] for more details on perfect quaternionic sequences. Note that finite (multiplicative) subgroups of $\mathbb{H}$ are classified (see [35]), and there are only few types of such subgroups; this is the reason why one often restricts alphabets to Q_8, $Q_8 \cup \mathtt{q}Q_8$, or $Q_{24} = Q_8 \cup \mathtt{q}Q_8 \cup \mathtt{q}^2 Q_8$; recall that Q_8 and Q_{24} are multiplicative groups and $\mathtt{q} = (1 + \mathtt{i} + \mathtt{j} + \mathtt{k})/2$.

Our computational investigation of perfect quaternionic sequences has exhibited three types of symmetries. We say a sequence $S = (s_0, \ldots, s_{n-1})$ has **symmetry I** if $s_r = s_{n-r}$ for all $r = 1, \ldots, n-1$; a sequence with this symmetry is also known as palindromic [19, Example 2]. The sequence S has **symmetry II** if n is even and $s_{r+\frac{n}{2}} = (-1)^r s_r$ for all $r = 0, \ldots, n/2 - 1$. Lastly, S has **symmetry III** if n is divisible by 4 and $s_{2r+e+\frac{n}{2}} = (-1)^r s_{2r+e}$ for all $r = 0, \ldots, n/4 - 1$ and $e = 0, 1$. Examples of sequences with symmetry I, II, and III are S_1, S_2, S_3, respectively, in Table 2.

In the next section we construct infinite families of WMs based on perfect sequences with these symmetries. There we use the composition of sequences $S = (s_0, \ldots, s_{l-1})$ and $U = (u_0, \ldots, u_{m-1})$, defined as $S \times U = (s_0 u_0, \ldots, s_{lm-1} u_{lm-1})$. If l and m are co-prime and S and U are perfect, then $S \times U$ is perfect as well, see [19]. Moreover, certain symmetries are preserved under composition.

Lemma 2.1 *Let S and U be sequences of co-prime lengths l and m, respectively, with odd l. If U has symmetry $\sigma \in \{\mathrm{II}, \mathrm{III}\}$, then so has $S \times U$. If S and U both have symmetry* I*, then so has $S \times U$.*

Proof: Write $S = (s_0, \ldots, s_{l-1})$ and $U = (u_0, \ldots, u_{m-1})$. First suppose $\sigma = \mathrm{II}$; the case $\sigma = \mathrm{III}$ is analogous. Note that m is even, and since $lm/2 \equiv 0 \bmod l$ and $(l-1)m/2 \equiv 0 \bmod m$, it follows from

$$s_{r+lm/2}u_{r+lm/2} = s_r u_{r+(l-1)m/2+m/2} = s_r u_{r+m/2} = s_r(-1)^r u_r = (-1)^r s_r u_r$$

that $S \times U$ has symmetry σ. If both S and U have symmetry I, then $s_{lm-r}u_{lm-r} = s_{l-r}u_{m-r} = s_r u_r$ shows that $S \times U$ has symmetry I. □

We proved the following result in [4].

Theorem 2.2 ([4]) *There is a one to one correspondence between perfect sequences of length n over $Q_8 \cup \mathtt{q}Q_8$ and $(4n, 2, 4n, 2n)$-RDS in $C_n \times Q_8$ relative to $Z(Q_8)$.*

Schmidt [24, Theorem 2.1] established the following correspondence.

Theorem 2.3 ([24]) *Let G be an abelian group of order n. A G-WM of order $4n$ exists if and only if there is a $(4n, 2, 4n, 2n)$-RDS in $G \times Q_8$ relative to $Z(Q_8)$.*

Theorems 2.2 and 2.3 provide a correspondence between C_n-WMs of order $4n$ and perfect sequences of length n over $Q_8 \cup \mathtt{q}Q_8$. We now make this correspondence explicit; it follows from a straightforward, but tedious analysis of the proofs of these theorems that our construction below is correct.

First, consider a perfect sequence $S = (s_0, \ldots, s_{n-1})$ over $Q_8 \cup \mathtt{q}Q_8$. Using Table 1, the entries of S define the entries of the matrix

$$\mathrm{R}(S) = \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ b_0 & b_1 & \ldots & b_{n-1} \\ c_0 & c_1 & \ldots & c_{n-1} \\ d_0 & d_1 & \ldots & d_{n-1} \end{pmatrix}.$$

For example, if $s_r = \mathtt{i}$, then $(a_r, b_r, c_r, d_r) = (1, -1, -1, 1)$. The matrix $\mathrm{WM}(S)$ corresponding to S has circulant blocks whose first rows are the rows a, b, c, d of $\mathrm{R}(S)$; by construction, $\mathrm{WM}(S)$ is a C_n-WM of order $4n$. Conversely, for a C_n-WM M of order $4n$ let $\mathrm{R}(M)$ be the $4 \times n$ matrix consisting of the first rows of the circulant blocks of M. Via Table 1, the r-th column of $\mathrm{R}(M)$ determines a symbol s_r, and this yields a perfect sequence $\mathrm{PS}(M) = (s_0, \ldots, s_{n-1})$ over $Q_8 \cup \mathtt{q}Q_8$.

We give an example. Starting with the perfect sequence $S = (1, \mathtt{i}, -1, \mathtt{i})$, we obtain a matrix $\mathrm{R}(S)$ with rows $a = (-1, 1, 1, 1)$, $b = (-1, -1, 1, -1)$, $c = (-1, -1, 1, -1)$, and $d = (-1, 1, 1, 1)$, and eventually a $\mathrm{WM}(S)$ of order 16. Conversely, if $a = d = (-1, 1)$ and $b = c = (-1, -1)$ are the first rows of the circulant blocks of a WM M of order 8, then we obtain $\mathrm{PS}(M) = (1, \mathtt{i})$.

In conclusion, we present the following correspondence.

Theorem 2.4 *Let S be a perfect sequence of length n over $Q_8 \cup \mathtt{q}Q_8$ and let M be a C_n-WM of order $4n$. Then $\mathrm{WM}(S)$ is a C_n-WM of order $4n$ and $\mathrm{PS}(M)$ is a perfect sequence of length n over $Q_8 \cup \mathtt{q}Q_8$; in particular, $\mathrm{WM}(\mathrm{PS}(M)) = M$ and $\mathrm{PS}(\mathrm{WM}(S)) = S$.*

s_r	1	−1	i	−i	j	−j	k	−k	q	−q	qi	−qi	qj	−qj	qk	−qk
a_r	−1	1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
b_r	−1	1	−1	1	1	−1	−1	1	−1	1	1	−1	1	−1	−1	1
c_r	−1	1	−1	1	−1	1	1	−1	−1	1	−1	1	1	−1	1	−1
d_r	−1	1	1	−1	−1	1	−1	1	−1	1	1	−1	−1	1	1	−1

Table 1: The correspondence between circulant Williamson matrices and perfect sequences

3 New orders of Williamson type matrices

As motivated in the previous sections, it is of interest to investigate the possible orders of (circulant and symmetric) WTMs. The aim of this section is to provide new examples of such WMs and WTMs; our first proposition describes a new infinite family of WMs.

Proposition 3.1 *For every prime power $q \equiv 1 \bmod 4$ there exists a WM of order $4(q+1)$.*

Proof: It is shown in [6, Theorem 6] that there exists a perfect sequence (of symmetry type I) of length $q+1$ over Q_8; now Theorem 2.4 implies the claim. □

Conversely, we can also use Theorem 2.4 to construct a new infinite family of perfect sequences. Turyn [36] showed that for every prime power $q \equiv 1 \bmod 4$ there is a WM of order $2(q+1)$. The blocks A, B, C, D of such a **Turyn type WM** are circulant, symmetric, A and B differ only on the main diagonal, and $C = D$. If (a_r), (b_r), (c_r), (d_r) are the first rows of A, B, C, D, respectively, then these conditions force that exactly three of a_0, b_0, c_0, d_0 are equal and, if $r \neq 0$, then exactly two or all of a_r, b_r, c_r, d_r are equal. Moreover, the symmetry of the blocks shows that $a_r = a_{n-r}$, $b_r = b_{n-r}$, $c_r = c_{n-r}$, and $d_r = d_{n-r}$ for all $r = 0, \ldots, (n-1)/2$, where $n = (q+1)/2$. Now Theorem 2.4 yields:

Proposition 3.2 *For every prime power $q \equiv 1 \bmod 4$ there exists a perfect sequence $(s_0, \ldots, s_{(q+1)/2})$ over $Q_8 \cup \mathtt{q}Q_8$ with symmetry* I*, such that $s_0 \in \mathtt{q}Q_8$ and $s_r \in Q_8$ for $r \neq 0$.*

For example, abbreviating ± 1 as $\pm$, the first rows of the blocks of a Turyn type WM M of order $4 \cdot 31$ are

$$\begin{aligned} a, b &= (\pm - - - + + + - + - + + + + - + + - + + + + - + - + + + - - -) \\ c = d &= (+ - + + - - - - - + - + + - - + + - - + + - + - - - - - - + + -). \end{aligned}$$

Via Table 1, this yields the perfect sequence $\mathrm{PS}(M) = S_4$ in Table 2.

name	length	symm.	sequence
S_1	18	I	$(\mathbf{1}, \mathtt{k}, -1, -\mathtt{i}, -1, \mathtt{j}, 1, -\mathtt{i}, 1, \mathbf{i}, 1, -\mathtt{i}, 1, \mathtt{j}, -1, -\mathtt{i}, -1, \mathtt{k})$
S_2	16	II	$(\mathbf{1}, \mathtt{i}, \mathtt{j}, -\mathtt{k}, 1, -\mathtt{k}, -\mathtt{j}, \mathtt{i}, \mathbf{1}, -\mathtt{i}, \mathtt{j}, \mathtt{k}, 1, \mathtt{k}, -\mathtt{j}, -\mathtt{i})$
S_3	16	III	$(\mathbf{i}, \mathbf{-j}, 1, 1, \mathtt{i}, \mathtt{j}, \mathtt{k}, -\mathtt{k}, \mathbf{i}, \mathbf{-j}, -1, -1, \mathtt{i}, \mathtt{j}, -\mathtt{k}, \mathtt{k})$
S_4	31	I	$(\mathtt{qk}, 1, -\mathtt{j}, -\mathtt{j}, \mathtt{j}, \mathtt{j}, \mathtt{j}, 1, \mathtt{j}, -\mathtt{j}, \mathtt{j}, -1, -1, \mathtt{j}, 1, -1, -1, 1, \mathtt{j}, -1, -1, \mathtt{j}, -\mathtt{j}, \mathtt{j}, 1, \mathtt{j}, \mathtt{j}, \mathtt{j}, -\mathtt{j}, -\mathtt{j}, 1)$
S_5	2	I	$(1, \mathtt{i})$
S_6	4	I	$(1, \mathtt{i}, -1, \mathtt{i})$
S_7	8	I	$(1, 1, \mathtt{i}, -1, 1, -1, \mathtt{i}, 1)$
S_8	16	I	$(1, -1, 1, -\mathtt{i}, -1, \mathtt{i}, 1, 1, 1, 1, 1, \mathtt{i}, -1, -\mathtt{i}, 1, -1)$
S_9	32	I	$(1, \mathtt{i}, -1, -\mathtt{j}, -\mathtt{j}, -1, 1, \mathtt{k}, 1, -\mathtt{k}, 1, 1, -\mathtt{j}, \mathtt{j}, -1, -\mathtt{i}, 1, -\mathtt{i}, -1, \mathtt{j}, -\mathtt{j}, 1, 1, -\mathtt{k}, 1, \mathtt{k}, 1, -1, -\mathtt{j}, -\mathtt{j}, -1, \mathtt{i})$
S_{10}	64	I	$(1, 1, -\mathtt{j}, -\mathtt{i}, 1, \mathtt{j}, -1, -\mathtt{k}, -1, -\mathtt{i}, 1, -1, 1, \mathtt{k}, \mathtt{j}, \mathtt{j}, 1, -\mathtt{j}, \mathtt{j}, -\mathtt{k}, 1, 1, 1, \mathtt{i}, -1, \mathtt{k}, -1, -\mathtt{j}, 1, \mathtt{i}, -\mathtt{j}, -1,$ $1, -1, -\mathtt{j}, i, 1, -\mathtt{j}, -1, \mathtt{k}, -1, \mathtt{i}, 1, 1, 1, -\mathtt{k}, \mathtt{j}, -\mathtt{j}, 1, \mathtt{j}, \mathtt{j}, \mathtt{k}, 1, -1, 1, -\mathtt{i}, -1, -\mathtt{k}, -1, \mathtt{j}, 1, -\mathtt{i}, -\mathtt{j}, 1)$
S_{11}	32	II	$(1, \mathtt{i}, \mathtt{i}, \mathtt{j}, 1, \mathtt{k}, 1, -\mathtt{k}, -1, -\mathtt{j}, \mathtt{i}, -\mathtt{i}, -1, -1, 1, -1, 1, -\mathtt{i}, \mathtt{i}, -\mathtt{j}, 1, -\mathtt{k}, 1, \mathtt{k}, -1, \mathtt{j}, \mathtt{i}, \mathtt{i}, -1, 1, 1, 1)$
S_{12}	16	III	$(1, -\mathtt{k}, \mathtt{j}, -\mathtt{j}, 1, \mathtt{k}, \mathtt{i}, \mathtt{i}, 1, -\mathtt{k}, -\mathtt{j}, \mathtt{j}, 1, \mathtt{k}, -\mathtt{i}, -\mathtt{i})$
S_{13}	11	I	$(\mathtt{qi}, 1, \mathtt{j}, -\mathtt{i}, -\mathtt{j}, -\mathtt{k}, -\mathtt{k}, -\mathtt{j}, -\mathtt{i}, \mathtt{j}, 1)$
S_{14}	17	I	$(\mathtt{q}, 1, \mathtt{j}, -\mathtt{i}, \mathtt{j}, -\mathtt{k}, -\mathtt{j}, -1, 1, 1, -1, -\mathtt{j}, -\mathtt{k}, \mathtt{j}, -\mathtt{i}, \mathtt{j}, 1)$
S_{15}	23	I	$(\mathtt{qk}, 1, -\mathtt{j}, \mathtt{i}, \mathtt{i}, -\mathtt{i}, \mathtt{k}, -\mathtt{j}, -1, -\mathtt{i}, -\mathtt{k}, 1, 1, -\mathtt{k}, -\mathtt{i}, -1, -\mathtt{j}, \mathtt{k}, -\mathtt{i}, \mathtt{i}, \mathtt{i}, -\mathtt{j}, 1)$
S_{16}	29	I	$(\mathtt{q}, \mathtt{j}, \mathtt{k}, -1, -\mathtt{k}, -1, \mathtt{k}, 1, -1, -\mathtt{k}, 1, -\mathtt{k}, \mathtt{k}, \mathtt{i}, \mathtt{i}, \mathtt{i}, \mathtt{k}, -\mathtt{k}, 1, -\mathtt{k}, -1, 1, \mathtt{k}, -1, -\mathtt{k}, -1, \mathtt{k}, \mathtt{j})$
S_{17}	33	I	$(\mathtt{qk}, -\mathtt{j}, -\mathtt{k}, \mathtt{k}, -1, \mathtt{j}, -\mathtt{i}, 1, -\mathtt{i}, -1, -\mathtt{k}, \mathtt{i}, \mathtt{j}, -1, \mathtt{k}, \mathtt{j}, \mathtt{i}, \mathtt{i}, \mathtt{j}, \mathtt{k}, -1, \mathtt{j}, \mathtt{i}, -\mathtt{k}, -1, -\mathtt{i}, 1,$ $-\mathtt{i}, \mathtt{j}, -1, \mathtt{k}, -\mathtt{k}, -\mathtt{j})$
S_{18}	39	I	$(\mathtt{q}, \mathtt{j}, \mathtt{j}, -\mathtt{i}, -\mathtt{j}, \mathtt{i}, -\mathtt{k}, \mathtt{k}, -\mathtt{k}, -\mathtt{j}, -\mathtt{i}, -\mathtt{i}, -\mathtt{k}, -1, -\mathtt{k}, -\mathtt{j}, \mathtt{k}, \mathtt{i}, -\mathtt{i}, -\mathtt{j}, -\mathtt{j}, -\mathtt{i}, \mathtt{i}, \mathtt{k}, -\mathtt{j},$ $-\mathtt{k}, -1, -\mathtt{k}, -\mathtt{i}, -\mathtt{i}, -\mathtt{j}, -\mathtt{k}, \mathtt{k}, -\mathtt{k}, \mathtt{i}, -\mathtt{j}, -\mathtt{i}, \mathtt{j}, \mathtt{j})$
S_{19}	43	I	$(\mathtt{qi}, \mathtt{i}, 1, -\mathtt{j}, -\mathtt{k}, -1, \mathtt{i}, \mathtt{i}, -1, -\mathtt{i}, \mathtt{j}, -\mathtt{i}, 1, -1, 1, -\mathtt{k}, \mathtt{j}, \mathtt{j}, -\mathtt{j}, -\mathtt{k}, -\mathtt{i}, -\mathtt{j}, -\mathtt{j}, -\mathtt{i}, -\mathtt{k},$ $-\mathtt{j}, \mathtt{j}, \mathtt{j}, -\mathtt{k}, 1, -1, 1, -\mathtt{i}, \mathtt{j}, -\mathtt{i}, -1, \mathtt{i}, \mathtt{i}, -1, -\mathtt{k}, -\mathtt{j}, 1, \mathtt{i})$

Table 2: Certain quaternionic perfect sequences used in some proofs

Motivated by finding perfect sequences of large lengths over Q_{24}, Kuznetsov [19, Example 2] performed a computational search on palindromic perfect sequences of the form

$$(1, \mathtt{j}, x_0, x_1, \ldots, x_t, x_t, \ldots, x_1, x_0, \mathtt{j}, 1, \mathtt{q})$$

with $x_0, \ldots, x_t \in Q_8$; he found such sequences for lengths $5, 7, 9, 11, 13, 17, 19, 23$. Proposition 3.2 shows that there exists an infinite family of perfect sequences over $Q_8 \cup \mathtt{q}Q_8$ of the form proposed by Kuznetsov; we call these **quaternionic Turyn sequences**: they have odd length, symmetry I, and exactly one entry from $\mathtt{q}Q_8 \subseteq Q_{24}$.

Proposition 3.3 *Let $q \equiv 1 \bmod 4$ be a prime power, $a \in \{1, \ldots, 6\}$, and $b \in \{4, 5\}$.*

a) *There are perfect sequences over $Q_8 \cup \mathtt{q}Q_8$ with symmetry* I *and length $2^a(q+1)/2$, symmetry* II *and length $2^b(q+1)/2$, and symmetry* III *and length $16(q+1)/2$, respectively.*

b) *There are WMs of order* $2^{a+1}(q+1)$*, and WTMs of order* $2^{b+1}(q+1)$ *and* $32(q+1)$ *with circulant blocks having first rows with symmetry* II *and* III*, respectively.*

Proof: In Table 2, perfect sequences of lengths $2, 4, 8, 16, 32, 64$ with symmetry I are $S_5, \ldots, S_{10}$, perfect sequences of lengths 16 and 32 with symmetry II are S_2 and S_{11}, and S_{12} is a perfect sequence of length 16 with symmetry III. Using composition of sequences of co-prime lengths, see [19], we can combine quaternionic Turyn sequences and $S_2, S_5, \ldots, S_{12}$ to perfect sequences of even length with the desired symmetries, see Lemma 2.1. This proves a); part b) follows with Theorem 2.4. □

In the following, we consider the parameter set

$$T = \{(q+1)/2 \mid q \equiv 1 \bmod 4 \text{ prime power}\}$$

of Turyn type WMs (see [36]); recall that each such WM has order $4n$ with $n \in T$.

Lemma 3.4 *For every* $r > 1$ *there are infinitely many* $a_1, \ldots, a_r \in T$ *which are pairwise co-prime.*

Proof: Let $q \equiv 1 \bmod 4$ be a prime power and define $a_i = (q^{(2^i)}+1)/2$ for $i = 1, \ldots, r$; note that each $a_i \in T$. We claim that $\gcd(a_i, a_j) = 1$ for each $1 \le i < j \le r$. To this end, observe that $q^{(2^i)} = 2a_i - 1$ and $q^{(2^j)} = (2a_i - 1)^{2^{j-i}} = 2a_i u + 1$ for some integer u. Now $a_j = (2a_i u + 2)/2 = a_i u + 1$, hence $\gcd(a_i, a_j) = 1$, which proves the claim. □

This observation shows that we have the following infinite series of WMs, WTMs, and perfect sequences.

Proposition 3.5 *For* $m \ge 1$ *let* $u_1, \ldots, u_m \in T$ *be pairwise co-prime; let* $s, r \ge 0$ *with* $s + r \ge 1$*.*

a) *There is a perfect sequence of length* $2u_1u_2$ *over* $Q_8 \cup \mathsf{q}Q_8$ *and a WM of order* $8u_1u_2$*.*

b) *There is a perfect sequence over* Q_{24} *of length* $2^t u_1 \ldots u_m$ *for each* $t \in \{0, \ldots, 6\}$*.*

c) *If* $q_1, \ldots, q_{r+s}$ *are prime powers, each congruent to* 1 *modulo* 4*, then there exists a WTM of order* $4 \cdot 2^s q_1 \ldots q_r (q_1 + 1) \ldots (q_r + 1)(q_{r+1} + 1) \ldots (q_{r+s} + 1)$*.*

Proof:

a) The infinite family of Turyn type WMs provides a perfect sequence of length u_1 over $Q \cup \mathsf{q}Q_8$. The infinite family of perfect sequences over Q_8 reported in [6] provides a sequence of length $2u_2$, cf. Proposition 3.1. By assumption, $1 = \gcd(u_1, u_2) = \gcd(u_1, 2u_2)$; note that each element of T is odd. The composition of series of co-prime lengths (see the discussion around Lemma 2.1) yields a perfect symmetry type I sequences of length $2u_1u_2$ over $Q_8 \cup \mathsf{q}Q_8$; Theorem 2.4 produces a WM of order $8u_1u_2$.

b) For each r, there is a Turyn type WM of order $4u_r$, and hence a perfect sequence over $Q_8 \cup \mathfrak{q}Q_8$ of length u_r. We now use composition of sequences of co-prime lengths to get a perfect sequence of length $u_1 \dots u_m$ over $Q_8 \cup \mathfrak{q}Q_8 \cup \mathfrak{q}^*Q_8 \subseteq Q_{24}$. Composing this sequence with the perfect sequences of lengths $2, 4, 8, 16, 32, 64$ listed above proves the claim.

c) Proposition 3.1 yields WMs of order $4(q_{r+1}+1), \dots, 4(q_{r+s}+1)$, respectively. It is shown in [25] (see also [29, Corollary 4.12]) that there exist WTMs of order $2q_1(q_1+1), \dots, 2q_r(q_r+1)$, respectively. It is shown in [32, Corollary 25] that WMs and WTMs of order $4u$ and $4v$ can be used to construct a WTM of order $8uv$; applying this construction to our WTMs and the WTMs from [25] proves the claim. □

Proposition 3.6 *Let $s \in \{1, 11, 17, 23, 29, 33, 39, 43\}$. For each integer $m \geq 1$, there exist infinitely many pairwise co-prime $u_1, \dots, u_m \in T$ such that the following holds.*

a) *There is a perfect sequence of length $2su_1$ over $Q_8 \cup \mathfrak{q}Q_8$ with symmetry* I*, and a WM of order $8su_1$.*

b) *For each $v \in \{0, 1\}$ there is a perfect sequence of length $2^v su_1 \dots u_m$ over Q_{24} with symmetry* I.

Proof: Lemma 3.4 shows that for every $m \geq 1$ there are infinitely many $u_1, \dots, u_m \in T$ which are pairwise co-prime; by the same argument we can also assume that each $\gcd(u_i, s) = 1$. The infinite family of perfect sequences over Q_8 reported in [6] (cf. Proposition 3.1) provides a sequence of length $2u_1$. The sequences $S_{13}, \dots, S_{19}$ in Table 2 have length $11, 17, 23, 29, 33, 39, 43$, respectively. Now Lemma 2.1 and Theorem 2.4 yield a perfect sequence of length $2su_1$ over $Q_8 \cup qQ_8$ with symmetry I and a WM of order $8su_1$. Proposition 3.5b) yields a perfect sequence of length $u_1 \dots u_m$ over Q_{24}; it has symmetry I, see Lemma 2.1 and the the proof of Proposition 3.1. We can also get a sequence of length $2u_1 \dots u_m$ by composing the above sequence of length $2u_1$ with a sequence of length $u_2 \dots u_m$ obtained from Proposition 3.5. Another composition with $S_{13}, \dots, S_{19}$ yields a sequence of length $2^v su_1 \dots u_m$ over Q_{24} with symmetry I. □

The results of this section produce several infinite sets of orders for WMs and WTMs. Most of these orders are of the form $4n$ where n is divisible by some power of 2, whereas focus in the literature has mainly been on odd n, see the brief overview in Appendix 3. (A notable exception is Seberry's work, e.g. [26], where she considered WTMs of order $8n$.) As the list in Appendix A shows, results on new orders of WTMs are scattered throughout the literature, and complete classifications only exist for orders less than 100. It is therefore difficult to identify which are the unknown orders of WMs and WTMs. However, since we focus on even n, most of the orders we provide are new and lead to new WTMs. We note that our results are not capable of showing that there exist WMs of order $8n$ with $n \in \{35, 47, 53, 59\}$; these odd n are of interest since it is known that there exist no WMs of order $4n$.

Appendix A

We summarise some results on WMs and WTMs, focusing on work that introduced new orders of WTMs. Unless specified otherwise, these matrices have order $4n$ where the parameter n is given below. For further reading on WMs and WTMs we refer to [13, 29].

1944: Williamson [40] introduced WMs and constructed examples for all $n \leqslant 21$ and $n = 25, 37, 43$.

1965: Baumert et al. [3] found a WM for $n = 23$.

1965: Baumert and Hall [2] performed an exhaustive search for WMs with odd $n \in \{3, \ldots, 23\}$; they introduced quaternion type HMs and described a construction that generates, from a single WM, infinitely many quaternion type HMs with symmetric but non-circulant blocks.

1972: Turyn [36] showed that for every prime power $q \equiv 1 \bmod 4$ there is a WM with $n = (q+1)/2$; this infinite family is known as Turyn type WMs.

1973: Whiteman [38] provided an alternative construction for Turyn type WMs.

1973: Seberry [25] proved that for every prime power $q \equiv 1 \bmod 4$ there is a WTM with $n = q(q+1)/2$ and non-circulant and non-symmetric blocks.

1974: Seberry [26] described two constructions for WMs with even order blocks; she found new WMs for $n = 2m$ with $m \in \{39, 203, 303, 333, 689, 915, 1603\}$. She also described constructions for WTMs with $n = 2m$ where $4m$ is the order of a WTM, $n = 2s(4s+1)$ where $4s+1$ is a prime power and $s \in \{1, 3, 5, \ldots, 25\}$, and $n = (q+1)(q+2)$ where $q \equiv 1 \bmod 4$ is a prime power such that $4(q+1)$ the order of a symmetric HM.

1975: Seberry [27] constructed a list of WTMs for $n = 93$, and $n = s(4s-1)$ and $n = s(4s+3)$ with $s \in \{1, 3, 5, \ldots, 25\}$.

1967: Whiteman [39] presented a construction for WTMs of same order as Seberry's infinite family [25].

1977: Spence [34] used a recursive construction to show that for each prime power $q \equiv 1 \bmod 4$ and each $r \geqslant 0$ there is a WTM with $n = 2q^r(q+1)$ with symmetric but non-circulant blocks.

1979: Yamada [43] introduced Williamson type j matrices and reported their existence for $n = 29, 37, 41$; they investigated Turyn type matrices of type j in their 1982 paper [44].

1981: Agayan and Sarukhanyan [1] described recursive formulas for the construction of WTMs; they reported WTMs for $n = 2m$ for certain m in the range $35, \ldots, 3913$.

1984: Turyn [37] showed the existence of WTMs with $n = 9^m$ and $m \in \mathbb{N}$.

1985: Yamamoto and Yamada [22] introduced circulant quaternion Hadamard matrices leading to WMs via Gauss sums.

1986: Seberry [28] reported WTMs with $n = 363, 1183, 1805, 2601, 3174, 5103$.

1988: Koukouvinos and Kounias [16] found four non-equivalent classes of WMs for $n = 33$.

1990: Seberry and Yamada [32] described a product construction for HMs using so-called M-structures: WTMs of order $4u$ and $4v$ yield a WTM for $n = 2uv$. Let $q \equiv 1 \bmod 4$ be a prime power. If $(q+1)/2$ is a prime power or $(q+3)/2$ is the order of a symmetric conference matrix (see [7]), then there is a symmetric WTM with $n = (q+2)$; if there is a WTM with $n = (q-1)$ or a HM of order $(q-1)/2$, then there is a WTM for $n = q$. If there exist symmetric conference matrices of order $(q-1)/2$ or a symmetric HM of order $(q-1)/2$, then there is a symmetric WTM with $n = q$. They also proved that under certain assumptions WTMs with $n \in \{q, q+2, 2q+1\}$ exist.

1990: Koukouvinos and Kounias [17] proved that there are no WMs for $n = 39$.

1991: Xia [41] proved the existence of WMs with $n = tq^2$ for $q \equiv 1 \bmod 4$ a prime power and t an integer in $\{2k+1 \mid 0 \leqslant k \leqslant 16\} \cup \{37, 59, 61, 67\} \cup \{2^i \cdot 10^j \cdot 26^k + 1 \mid i, j, k \geqslant 0\}$.

1992: Doković [8] showed that there is one equivalence class of WMs for $n = 29, 31$, respectively.

1992: Seberry and Yamada [33] discussed a construction for WTMs with symmetric blocks based on Miyamoto's work [21].

1993: Doković [9] determined, up to equivalence, all WMs with $n = 33, 35, 39$; he showed that there is no WM for $n = 35$.

1995: Doković [10] determined, up to equivalence, all WMs with $n = 25, 37$.

1999: Schmidt [24] introduced WMs with group-invariant blocks and established a correspondence to certain relative difference sets in non-abelian groups. He also reported an infinite family of relative difference sets in certain dicyclic groups, supporting Ito's Conjecture on Hadamard groups [15].

2002: Horton et al. [14] constructed WMs with $n = 41, 43, 45$.

2003: Seberry et al. [31] constructed several WMs for certain odd parameters $n \leqslant 63$.

2005: Xia et al. [42] constructed WTMs with $n = q^2$ for $q \equiv 1 \bmod 4$ a prime power.

2008: Holzmann et al. [12] determined, up to equivalence, all WMs with $n = 35, 47, 53, 59$; they proved there are no WMs for $n = 47, 53, 59$.

2012: Lang and Schneider [20] determined the equivalence classes of Turyn type WMs up to $n = 99$.

2017: Seberry and Balonin [30] constructed two infinite families of HMs related to WTMs (variation of signs in (1), called *propus array*).

2018: Barrera Acevedo and Dietrich [5] reported new families of WMs and Ito matrices whose blocks are developed over abelian groups.

Acknowledgements

The authors thank both referees for their suggestions to improve the paper.

References

[1] S. S. Agayan and A. G. Sarukhanyan, Recurrence formulas for the construction of Williamson type matrices, *Mathematical notes of the Academy of Sciences of the USSR* 30, (1981), 796–804.

[2] L. D. Baumert and M. Hall, Hadamard matrices of Williamson Type, *Math. Comp.* 19 (1965), 442–447.

[3] L. D. Baumert, S. W. Golomb and M. Hall, Discovery of an Hadamard matrix of order 92, *Bull. Amer. Math. Soc.* 68 (1962), 237–238.

[4] S. Barrera Acevedo and H. Dietrich, Perfect Sequences over the Quaternions and $(4n, 2, 4n, 2n)$-Relative Difference Sets in $C_n \times Q_8$, *Cryptogr. Commun.* 10 (2017), 357–368.

[5] S. Barrera Acevedo and H. Dietrich, Relative difference sets and Hadamard matrices from perfect quaternionic arrays, *Math. Comput. Sci.* 12 (2018), 397–406.

[6] S. Barrera Acevedo and T. E. Hall, Perfect Sequences of Unbounded Lengths over the Basic Quaternions, In: *Sequences and Their Applications—SETA2012* (Eds. T. Helleseth and J. Jedwab), Lec. Notes. Comp. Sci. 7280 (2012), 159–167.

[7] V. Belevitch, Theory of $2n$-terminal networks with application to conference telephony, *Elect. Commun.* 27 (1950), 231–244.

[8] D. Ž. Doković, Williamson Matrices of Orders $4 \cdot 29$ and $4 \cdot 31$, *J. Combin. Theory (Ser. A)* 59 (1992), 309–311.

[9] D. Ž. Doković, Williamson Matrices of Orders $4n$ for $n = 33, 35, 39$, *Discrete Math.* 115 (1993), 267–271.

[10] D. Ž. Doković, Note on Williamson Matrices of Orders 25 and 37, *J. Combin. Math. Combin. Comput.* 18 (1995), 171–175.

[11] S. Georgiou, C. Koukouvinos and J. Seberry, Short amicable sets, *Int. J. Appl. Math.* 9 (2002), 161–187.

[12] W. H. Holzmann, H. Kharaghani and B. Tayfeh-Rezaie, Williamson Matrices up to Order 59, *Des. Codes Cryptogr.* 46 (2008), 343–352.

[13] K. J. Horadam, Hadamard Matrices and Their Applications, Princeton University Press 2007.

[14] J. Horton, C. Koukouvinos and J. Seberry, A Search for Hadamard Matrices constructed from Williamson Matrices, *Bull. Inst. Combin. Appl.* 35 (2002), 75–88.

[15] N. Ito, Note on Hadamard matrices of type Q, *Studia Sci. Math. Hungar.* 16 (1981), 389–393.

[16] C. Koukouvions and S. Kounias, Hadamard matrices of the Williamson Type of Order $4m$, $m = pq$ and Exhaustive Search for $m = 33$, *Discrete Math.* 68 (1988), 45–57.

[17] C. Koukouvions and S. Kounias, There are no circulant symmetric Williamson matrices of order 39, *J. Combin. Math. Combin. Comput.* 7 (1990), 161–169.

[18] O. Kuznetsov, Perfect sequences over the real quaternions, *Signal Des. Appl. Comm.* 2009. IWSDA'09. 4th Inter. Workshop 1 (2010), 8–11.

[19] O. Kuznetsov, Perfect Sequences over the Real Quaternions of Longer Length, *OJMS* 1 (2011), 17–20.

[20] W. Lang and E. Schneider, Turyn Type Williamson Matrices up to order 99, *Des. Codes Cryptogr.* 62 (2012), 79–84.

[21] M. Miyamoto, A construction for Hadamard matrices, *J. Combin. Theory (Ser. A)* 57 (1991), 86–108.

[22] K. Yamamoto and M. Yamada, Williamson Hadamard matrices and Gauss sums, *J. Math. Soc. Japan* 37 (1985), 703–717.

[23] J. Rifà and E. Suárez Canedo, Hadamard full propelinear code of type Q; rank and kernel, *Des. Codes Cryptogr.* (2017), doi.org/10.1007/s10623-017-0429-2.

[24] B. Schmidt, Williamson Matrices and a Conjecture of Ito's, *Des. Codes Cryptogr.* 17 (1999), 61–68.

[25] J. Seberry Wallis, Some Matrices of Williamson Type, *Utilitas Mathematica* 4 (1973), 147–154.

[26] J. Seberry Wallis, Williamson Matrices of Even Order, In: *Combinatorial Mathematics* (Ed. D. A. Holton), Lec.Notes in Math. 403 (1974), 132–142.

[27] J. Seberry Wallis, Construction of Williamson Type Matrices, *Lin. Multilin. Algebra* 3 (1975), 197–207.

[28] J. Seberry, A New Construction for Williamson-type Matrices, *Graphs Combin.* 2 (1986), 81–87.

[29] J. Seberry, *Orthogonal Designs. Hadamard Matrices, Quadratic Forms and Algebra*, Springer Intern. Pub. AG 2017.

[30] J. Seberry and N. A. Balonin, Two infinite families of symmetric Hadamard matrices, *Australas. J. Combin.* 69 (2017), 349–357.

[31] J. Seberry, B. J. Wysocki and T. A. Wysocki, Williamson-Hadamard spreading sequences for DS-CDMA applications, *J. Wireless Commun. Mobilie Comput.* 3 (2003), 597–607.

[32] J. Seberry and M. Yamada, On the Product of Hadamard Matrices, Williamson Matrices and other Orthogonal Matrices using M-Structures, *J. Combin. Math. Combin. Comput.* 7 (1990), 97–137.

[33] 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, New York (1992), 431–560.

[34] E. Spence, An infinite family of Williamson matrices, *J. Austral. Math. Soc. (Ser. A)* 24 (1977), 252–256.

[35] W. I. Stringham, Determination of the Finite Quaternion Groups, *Amer. J. Math.* 4 (1881), 345–357.

[36] R. Turyn, An Infinite Class of Williamson Matrices, *J. Combin. Theory (Ser. A)* 12 (1972), 319–321.

[37] R. Turyn, A special Class of Williamson Matrices and Difference sets, *J. Combin. Theory (Ser. A)* 36, (1984), 111-115.

[38] A. L. Whiteman, An Infinite Family of Hadamard Matrices of Williamson Type, *J. Combin. Theory (Ser. A)* 14 (1973), 334–340.

[39] A. L. Whiteman, Hadamard Matrices of Williamson Type, *J. Austral. Math. Soc.* 21 (1976), 481–486.

[40] J. Williamson, Hadamard's Determinant Theorem and the Sum of Four Squares, *Duke Math. J.* 11 (1944), 65–81.

[41] M.-Y. Xia, An Infinite Class of Supplementary Difference Sets and Williamson Matrices, *J. Combin. Theory (Ser. A)* 58 (1991), 310–317.

[42] M.-Y. Xia, T. Xia and J. Seberry, A New Method for Constructing Williamson Matrices, *Des. Codes Crypto.* 35 (2005), 191–209.

[43] M. Yamada, On the Williamson Type j Matrices of order $4 \cdot 29, 4 \cdot 41$ and $4 \cdot 37$, *J. Combin. Theory (Ser. A)* 27 (1979), 378–381.

[44] M. Yamada, On the Williamson Matrices of Turyn's Type and of Type j, *Commentarii Mathematici Universitatis Sancti Pauli* 31 (1982), 71–73.

(Received 7 May 2018; revised 7 Nov 2018)