# A doubling construction for Williamson matrices

Curtis Bright
University of Waterloo

March 4, 2018

**Abstract**

A construction that generates Williamson matrices of order $2n$ from Williamson matrices of odd order $n$ is presented. The construction is completely constructive and only uses three simple sequence operations.

## 1 Introduction

Four square, symmetric, and circulant matrices of order $n$ with $\pm 1$ entries are known as *Williamson matrices* if they satisfy

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

where $I_n$ is the identity matrix of order $n$. Such matrices were first introduced by Williamson (1944), who proved that such matrices can be used to constuct a Hadamard matrix (a square matrix with $\pm 1$ entries whose rows are pairwise orthogonal) of order $4n$. Since Williamson matrices are circulant they are defined in terms of their first row and so it is convenient to instead think of Williamson matrices in terms of four sequences $(a_0, \dots, a_{n-1})$, $(b_0, \dots, b_{n-1})$, $(c_0, \dots, c_{n-1})$, $(d_0, \dots, d_{n-1})$. Since Williamson matrices are symmetric these sequences are also symmetric (i.e., $x_k = x_{n-k}$ for $k = 1, \dots, n-1$).

## 2 Preliminaries

A doubling construction for Hadamard matrices was originally given by Sylvester (1867) who showed that a Hadamard matrix of order $2n$ can be constructed from a Hadamard matrix of order $n$. Baumert and Hall (1965) provided a doubling construction for generalizations of Williamson matrices which are often referred to as *Williamson-type* matrices (Seberry and Yamada, 1992, Def. 3.3). Using complex Hadamard matrices, Turyn (1970) provided a construction which generates Williamson matrices of order $2^k n$ for $k = 1, 2, 3, 4$ from Williamson matrices of odd order $n$. In this paper we provide a simple doubling construction which works directly on the sequences which define Williamson matrices.

## 2.1 Correlation

Williamson matrices can also be defined in terms of a correlation function. The *periodic cross-correlation function* of two sequences $X = (x_0, \dots, x_{n-1})$ and $Y = (y_0, \dots, y_{n-1})$ is defined to be

$$\mathrm{PCF}_{X,Y}(s) := \sum_{k=0}^{n-1} x_k y_{k+s \bmod n}$$

and the *periodic autocorrelation function* of $X$ be a sequence is $\mathrm{PAF}_X(s) := \mathrm{PCF}_{X,X}(s)$. In (Bright, 2017, §3.1.1) it is shown that four symmetric sequences $A$, $B$, $C$, $D \in \{\pm 1\}^n$ form the initial rows of a set of Williamson matrices if and only if they satisfy

$$\mathrm{PAF}_A(s) + \mathrm{PAF}_B(s) + \mathrm{PAF}_C(s) + \mathrm{PAF}_D(s) = 0$$

for $s = 1, \dots, \lfloor n/2 \rfloor$. We refer to such sequences as *Williamson sequences*.

## 2.2 Sequence operations

Let $A = (a_0, \dots, a_{n-1})$ and $B = (b_0, \dots, b_{n-1})$ be sequences of order $n$. Our construction uses the following 3 types of operations.

1. Negation. Individually negate each entry of $A$, i.e., $-A := (-a_0, \dots, -a_{n-1})$.
2. Shift. Cyclically shift the entries of $A$ by an offset of $k$, i.e., $(a_k, a_{k+1}, \dots, a_{k-1})$ with indices taken modulo $n$.
3. Interleave. Interleave the entries of $A$ and $B$ in a perfect shuffle, i.e.,

$$A ⧢ B := (a_0, b_0, a_1, b_1, \dots, a_{n-1}, b_{n-1}).$$

If $n$ is odd we let $A'$ denote shifting $A$ by an offset of $(n-1)/2$, i.e.,

$$A' := (a_{(n-1)/2}, \dots, a_{n-1}, a_0, a_1, \dots, a_{(n-3)/2}).$$

Note that we have $\mathrm{PAF}_{-A}(s) = \mathrm{PAF}_A(s)$, $\mathrm{PAF}_{A'}(s) = \mathrm{PAF}_A(s)$, and

$$\mathrm{PAF}_{A ⧢ B}(s) = \begin{cases} \mathrm{PAF}_A(s/2) + \mathrm{PAF}_B(s/2) & \text{when } s \text{ is even,} \\ \mathrm{PCF}_{A,B}(\frac{s-1}{2}) + \mathrm{PCF}_{B,A}(\frac{s+1}{2}) & \text{when } s \text{ is odd.} \end{cases}$$

# 3 Doubling construction

Our doubling construction is captured by the following theorem.

**Theorem 1.** *Let $A$, $B$, $C$, $D$ be Williamson sequences of odd order $n$. Then*

$$A ⧢ B',\ (-A) ⧢ B',\ C ⧢ D',\ (-C) ⧢ D'$$

*are Williamson sequences of order* $2n$*.*

*Proof.* The fact that the constructed sequences have ±1 entries are of length $2n$ follows directly from the properties of the three types of operations used to generate them. The fact that they are symmetric follows from the fact that the sequences $X$ which appear to the left of ш satisfy $x_k = x_{n-k}$ for $k = 1, \dots, n-1$ and the sequences $Y$ which appear to the right of ш satisfy $y_k = y_{n-k-1}$ for $k = 0, \dots, n-1$ which are exactly the necessary properties for $X ш Y$ to be symmetric.

Let $L$ be the list containing the constructed sequences of order $2n$. To show these sequences are Williamson we need to show that

$$\sum_{X \in L} \mathrm{PAF}_X(s) = 0$$

for $s = 1, \dots, n$. When $s$ is even and in this range using the properties from Section 2.2 we obtain

$$\sum_{X \in L} \mathrm{PAF}_X(s) = 2 \sum_{X=A,B,C,D} \mathrm{PAF}_X(s/2) = 0$$

since $A$, $B$, $C$, $D$ are Williamson. When $s$ is odd we have that

$$\mathrm{PAF}_{(-X) ш Y}(s) = -\mathrm{PAF}_{X ш Y}(s)$$

and using this for $(X, Y) = (A, B')$ and $(C, D')$ derives the desired property. □

We remark that unlike the doubling constructions given by Sylvester and Baumert–Hall our doubling construction cannot be applied repeatedly because it only applies when $n$ is odd. When $n$ is even it is not possible to apply a shift to a symmetric sequence $Y$ of order $n$ to obtain a sequence $Y'$ which satisfies $y'_k = y'_{n-k-1}$ for $k = 0, \dots, n-1$ and this property is necessary to make the constructed sequences symmetric.

# References


LD Baumert and Marshall Hall. Hadamard matrices of the Williamson type. *Mathematics of Computation*, 19(91):442–447, 1965.

Curtis Bright. *Computational Methods for Combinatorial and Number Theoretic Problems*. PhD thesis, University of Waterloo, 2017.

Jennifer Seberry and Mieko Yamada. Hadamard matrices, sequences, and block designs. *Contemporary design theory: a collection of surveys*, pages 431–560, 1992.

James Joseph Sylvester. Thoughts on inverse orthogonal matrices, simultaneous sign-successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 34(232): 461–475, 1867.

Richard J. Turyn. Complex Hadamard matrices. In *Combinatorial structures and their applications*, pages 435–437. Gordon and Breach, 1970.

John Williamson. Hadamard's determinant theorem and the sum of four squares. *Duke Math. J*, 11(1):65–81, 1944.