Perfect Sequences over the Quaternions and Relative Difference Sets

Santiago Barrera-Acevedo

June 9, 2017
Definitions

Autocorrelation of a sequence

An ordered $n$-tuple $S = (s_0, \ldots, s_{n-1})$ of elements from a set $\mathcal{A} \subset \mathbb{C}$ is called a finite sequence. The set $\mathcal{A}$ is called an alphabet and the number $n$ is called the length of the sequence.

We define, for all $t \in \{0, \ldots, n - 1\}$, the $t$-autocorrelation value of $S$ as

$$AC_S(t) = \sum_{l=0}^{n-1} s_l s_{l+t}^*$$

where $s_{l+t}^*$ is the complex conjugation of $s_{l+t}$, and the indices $l$ and $l + t$ are taken modulo $n$. 

Santiago Barrera-Acevedo

Perfect Sequences over Quaternions and RDS
Perfect sequences

The autocorrelation sequence of $S$ is defined as $AC_S = (AC_S(0), \ldots, AC_S(n - 1))$, with $AC_S(0)$ being the peak-value and all other values being off-peak values.

The sequence $S$ has constant off-peak autocorrelation if all its off-peak autocorrelation values are equal. In particular, $S$ is perfect if all its off-peak autocorrelation values are zero.

The sequences $S_1 = (1, 1, 1, -1)$ and $S_2 = (1, 1, i, 1, 1, -1, i, -1)$ over the binary and quaternary alphabet, respectively, are perfect since we have $AC_{S_1} = (4, 0, 0, 0)$ and $AC_{S_2} = (8, 0, 0, 0, 0, 0, 0, 0)$. 
Applications

Sequences with “good” autocorrelation properties, such as being perfect, have important applications in information technology, for example, in digital watermarking, frequency hopping patterns for radar or sonar communications and signal correlation (synchronisation of signals).

In this work we focus exclusively on the mathematical aspects of sequences with good autocorrelation.
It is very difficult to construct perfect sequences over 2nd-, 4th-, and in general over $n$-th roots of unity.\textsuperscript{†}

It is conjectured that perfect sequences over $n$-th roots of unity do not exist for lengths greater that $n^2$, Ma and Ng [7].

Due to the importance of perfect sequences and the difficulty to construct them over $n$-th roots of unity, there has been some focus on other classes of sequences with good autocorrelation.

One of these classes has been introduced by Kuznetsov [5], who defined perfect sequences over the quaternion algebra.

\textsuperscript{†}This problem is related to the construction of (generalised) circulant Hadamard matrices over $n$-th roots of unity.
**Definitions**

**Quaternions** \( \mathbb{H} \)

The quaternion algebra \( \mathbb{H} \) is a 4-dimensional real vector space with \( \mathbb{R} \)-basis \( \{1, i, j, k\} \) and non-commutative multiplication defined by

\[
i^2 = j^2 = k^2 = -1 \quad \text{and} \quad ij = k.
\]

It follows from these relations that

\[
jk = i, ki = j, ji = -k, kj = -i, \quad \text{and} \quad ik = -j.
\]

The \( \mathbb{R} \)-linear complex conjugation on \( \mathbb{H} \) is denoted \( h \mapsto h^* \), and uniquely defined by

\[
1^* = 1, i^* = -i, j^* = -j, \quad \text{and} \quad k^* = -k.
\]

The norm of a quaternion \( q \), denoted by \( ||q|| \), is defined by

\[
||q|| = qq^*.
\]
Definitions

Note that the basic quaternions $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ form a group under multiplication, the **quaternion group** of order 8.

The multiplicative group consisting of all elements

$$\{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$$

(where signs may be taken in any combination) is the so-called binary tetrahedral group and has size 24. By abuse of notation we call it the **quaternion group** $Q_{24}$.

In the following, we often decompose $Q_{24}$ into the cosets

$$Q_{24} = Q_8 \cup qQ_8 \cup q^*Q_8$$

where $q = \frac{1+i+j+k}{2}$. 


Definitions

Let $S = (s_0, \ldots, s_{n-1})$ be a sequence of length $n$ over an arbitrary quaternion alphabet. We define, for all $t \in \{0, \ldots, n-1\}$, the left and right $t$-autocorrelation values of $S$ as

$$AC^L_S(t) = \sum_{l=0}^{n-1} s_i^* s_{l+t} \quad \text{and} \quad AC^R_S(t) = \sum_{l=0}^{n-1} s_{l} s_{l+t}^*$$

| $t$ | $AC^L_S$ | $||AC^L_S||$ | $AC^R_S$ | $||AC^R_S||$
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>6</td>
<td>36</td>
<td>6</td>
<td>36</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2$j + 2k$</td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>$-1 + 3i - j - k$</td>
<td>12</td>
<td>$-1 + i + j - k$</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>$-1 - 3i + j + k$</td>
<td>12</td>
<td>$-1 - i - j + k$</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>$-2j - 2k$</td>
<td>8</td>
</tr>
</tbody>
</table>
Perfect Sequences over Quaternions

A sequence $S = (s_0, \ldots, s_{n-1})$ of length $n$ over an arbitrary quaternion alphabet is called left (right) perfect when all left (right) off-peak $t$-autocorrelation values are equal to zero, for $t \in \{1, \ldots, n - 1\}$.

$$S = (i, j, -k, j, i, 1, k, -1, k, 1)$$

$$\text{AC}_S^L = (10, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

$$\text{AC}_S^R = (10, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

Theorem (Kuznetsov [5])

Let $S$ be a sequence over an arbitrary quaternion alphabet. Then the sequence $S$ is right perfect if and only if it is left perfect.
Motivation

Kuznetsov and Hall [6] showed a construction of a perfect sequence of length 5, 354, 228, 880 over $\mathbb{Q}_{24}$.

At this point two main questions were stated: Are there perfect sequences of unbounded lengths over $\mathbb{Q}_{24}$? If so, is it possible to restrict the alphabet size to a small one, say the basic quaternions $\mathbb{Q}_8 = \{1, -1, i, -i, j, -j, k, -k\}$?

**Theorem (Barrera Acevedo and Hall [4])**

There exists a family of perfect sequences over $\mathbb{Q}_8$ of length $n = p^a + 1 \equiv 2 \mod 4$, where $p$ is prime and $a \in \mathbb{N}$. 
Symmetry type 1

A sequence $S = (s_0, \ldots, s_{n-1})$ has symmetry type 1 if $s_r = s_{n-r}$ for $r = 1, \ldots, n - 1$.

Length 8: $(1, 1, i, -1, 1, -1, i, 1)$

Length 10: $(1, i, -1, -i, j, -i, -1, i)$

Length 11: $(1, k, -j, -i, -1, q, -1, -i, -j, k, 1)$

Length 16: $(1, i, -1, i, j, k, -j, -i, -j, k, j, i, -1, i)$
Symmetry of perfect sequences over the quaternions

Symmetry type 2

A sequence $S = (s_0, \ldots, s_{n-1})$ has symmetry type $2^\dagger$ if $n$ is even and $s_{r+n/2} = (-1)^r s_r$ for all $r = 0, \ldots, \frac{n}{2} - 1$.

Length 8: $(1, 1, i, -1, 1, -1, i, 1)$

Length 16: $(1, -1, 1, -i, -1, i, 1, 1, 1, 1, 1, i, -1, -i, 1, -1)$

Length 32: $(1, -1, 1, -i, i, -j, 1, -k, 1, k, -j, -i, 1, 1, 1, 1, i, i, j, 1, k, 1, -k, -1, -j, i, -i, -1, -1)$

\[\dagger\text{A sequence can have symmetry type 1 and 2.}\]
Symmetry type 3

A sequence \( S = (s_0, \ldots, s_{n-1}) \) has symmetry type 3 if \( n \) is divisible by 4 and \( s_{2r+e+\frac{n}{2}} = (-1)^r s_{2r+e} \) for \( r = 0, \ldots, \frac{n}{2} - 1 \) and \( e = 0, 1 \).

Length 16: \((1, i, -j, j, 1, -i, -k, -k, 1, i, j, -j, 1, -i, k, k)\)
\(1, 1, -1, -1, 1, 1, -1, -1)\)

Length 48:
\((1, -qk, -j, j, -q, -i, -k, qj, 1, i, -qi, -j, 1, qk, k, k, -q, i, -j, -qi, 1, -i, qj, -k, 1, -qk, j, -j, -q, -i, k, -qj, 1, i, qi, j, 1, qk, -k, -k, -q, i, j, qi, 1, -i, -qj, k)\)
Relative difference sets

An \((m, n, l, \lambda)\)-relative difference set (RDS) \(R\) in a group \(G\) of order \(mn\), relative to a (forbidden) subgroup \(N\) of order \(n\), is a \(l\)-subset of \(G\) with the property that the list of quotients \(r_1 r_2^{-1}\) with distinct \(r_1, r_2 \in R\) contains each element in \(G \setminus N\) exactly \(\lambda\) times and does not contain the elements of \(N\).

We also call \(R\) an \((m, n, l, \lambda)\)-RDS or simply RDS.

For example \(R = \{1, i, j, k\}\) is a \((4, 2, 4, 2)\)-RDS in \(Q_8\) with forbidden subgroup \(N = \{1, -1\}\).

\[
\begin{array}{cccc}
1i^{-1} = -i & i1^{-1} = i & j1^{-1} = j & k1^{-1} = k \\
1j^{-1} = -j & ij^{-1} = -k & ji^{-1} = k & ki^{-1} = -j \\
1k^{-1} = -k & ik^{-1} = j & jk^{-1} = -i & kj^{-1} = i
\end{array}
\]
Group ring:

If $G$ is a multiplicatively written group and $K$ is a ring with 1, then the group ring

$$K[G] = \left\{ \sum_{g \in G} a_g g \mid a_g \in K \text{ and only finite } a_g \neq 0 \right\}$$

is the free $K$-module with basis $G$, equipped with the multiplication

$$\sum_{g \in G} a_g g \sum_{h \in G} b_h h = \sum_{g, h \in G} a_g b_h g h.$$

We identify the multiplicative identities $1_G$, $1_K$, and $1_{K[G]}$, and denote them all by 1.
Relative difference sets

Let $K[G]$ be a group ring, let $H \subseteq G$ be a subset, and $A \in K[G]$.

We identify $H$ with

$$H = \sum_{h \in H} h \in K[G].$$

In particular

$$G = \sum_{g \in G} g \in K[G].$$

If $A = \sum_{g \in G} a_g g$ then we define $A^{(-1)} = \sum_{g \in G} a_g g^{-1} \in K[G]$.

Proposition

$R \subseteq G$ is an $(m, n, l, \lambda)$-RDS if and only if in the group ring $\mathbb{Z}[G]

$$RR^{(-1)} = l + \lambda(G - N).$$
Theorem (Arasu, de Launey, and Ma [1, 2])

A perfect array of size $m \times n$ over 4th-roots of unity is equivalent to a $(2mn, 2, 2mn, mn)$-RDS in $\mathbb{Z}_m \times \mathbb{Z}_n \times \mathbb{Z}_4$ relative to $\mathbb{Z}_2$.

A perfect sequences of size $n$ over 4th-roots of unity is equivalent to a $(2n, 2, 2n, n)$-RDS in $\mathbb{Z}_n \times \mathbb{Z}_4$ relative to $\mathbb{Z}_2$.

Theorem (Barrera Acevedo and Dietrich [3])

Let $q = (1 + i + j + k)/2$. There is a 1–1 correspondence between the perfect sequences of length $n$ over $Q_8 \cup qQ_8$ and the $(4n, 2, 4n, 2n)$-RDS in $\mathbb{Z}_n \times Q_8$ relative to $\mathbb{Z}_2$. 
For $n \in \mathbb{N} \setminus \{0\}$ let

$$C_n = \langle w \mid w^n = 1 \rangle \cong \mathbb{Z}_n,$$

$$G = \langle x, y \mid x^4 = y^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle \cong Q_8$$

and

$$G_n = C_n \times G \cong \mathbb{Z}_n \times Q_8.$$

Given a subset $R$ of $G_n$ we define the $(-1, 1)$-characteristic polynomial of $R$ as

$$T_R(w, x, y) = G_n - 2R,$$

where $G_n - 2R \in Z[G]$. 
From PS to RDS

Let $S$ be a perfect sequence of length $n$ over $Q_8 \cup qQ_8$.

1. Identify $S$ with the element $S(w) = \sum_{r=0}^{n-1} s_r w^r \in \mathbb{H}[\langle w \rangle]$.  
2. Define four polynomials $P_1(w), P_2(w), P_3(w)$ and $P_4(w)$ via 
   $$(1 + i + j + k)S(w) = P_1(w) + iP_2(w) + jP_3(w) + kP_4(w).$$
3. Consider the expression 
   $$T(w, x, y) = (1 - x^2)[P_1(w) + xP_2(w) + yP_3(w) + xyP_4(w)].$$
4. Solve for $R$ in the equation $T(w, x, y) = G_n - 2R$, so that $T(w, x, y) = T_R(w, x, y)$ becomes the $(-1, 1)$-characteristic polynomial of $R$.

Theorem 2 shows that $R$ is a $(4n, 2, 4n, 2n)$-RDS in $G_n$ relative to $\langle x^2 \rangle$.  

Santiago Barrera-Acevedo
Perfect Sequences over Quaternions and RDS
From RDS to PS

Let $R$ be a $(4n, 2, 4n, 2n)$-RDS in $G_n$ relative to $\langle x^2 \rangle$.

1. Let $T_R(w, x, y)$ be the $(-1, 1)$-characteristic polynomial of $R$. Define
   
   $$S(w) = \frac{1}{4} q^* T_R(w, i, j) \in \mathbb{H}[\langle w \rangle].$$

2. Identify the element $S(w) = \sum_{r=0}^{n-1} s_r w^r$ with the sequence $S = (s_0, \ldots, s_{n-1})$.

Theorem 2 shows that $S$ is a perfect sequence of length $n$ over $Q_8 \cup qQ_8$. 

Example

Given the perfect sequence $S = (i, j, -i, k, -i, j)$ we identify it with the element

$$S(w) = i + jw - iw^2 + kw^3 - iw^4 + jw^5 \in \mathbb{H}[\langle w \rangle].$$

We define the polynomials $P_1(w), P_2(w), P_3(w)$ and $P_4(w)$ via the expression

$$(1 + i + j + k)S(w) = P_1(w) + iP_2(w) + jP_3(w) + kP_4(w)$$

- $P_1(w) = -1 - w + w^2 - w^3 + w^4 - w^5$
- $P_2(w) = 1 - w - w^2 + w^3 - w^4 - w^5$
- $P_3(w) = 1 + w - w^2 - w^3 - w^4 + w^5$
- $P_4(w) = -1 + w + w^2 + w^3 + w^4 + w^5$
We consider

\[ T(w, x, y) = (1 - x^2)(P_1(w) + xP_2(w) + yP_3(w) + xyP_4(w)) \]
\[ = (1 - x^2)[(-1 - w + w^2 - w^3 + w^4 - w^5) + x(1 - w - w^2 + w^3 - w^4 - w^5) + y(1 + w - w^2 - w^3 - w^4 + w^5) + xy(-1 + w + w^2 + w^3 + w^4 + w^5)]. \]

We solve for \( R \) in the equation \( T(w, x, y) = G_6 - 2R \) so that \( T(w, x, y) = T_R(w, x, y) \) becomes the \((-1, 1)\)-characteristic polynomial of \( R \). This way we obtain a \((24, 2, 14, 12)\)-RDS in \( G_6 \) relative to \( \langle x^2 \rangle \)

\[ R = \{ 1, w, w^3, w^5, wx, w^2x, w^4x, w^5x, w^2x^2, w^4x^2, x^3, w^3x^3, w^2y, w^3y, w^4y, xy, x^2y, wx^2y, w^5x^2y, wxy^3, w^2xy^3, w^3xy^3, w^4xy^3, w^5xy^3 \}. \]
Given the \((12, 2, 12, 6)\)-RDS \(R = \{1, x^3, y^3, xy^3, w, wx, wy, wxy, w^2, w^2x, w^2y, w^2xy\}\) in \(G_3\) relative to \(\langle x^2 \rangle\), we find

\[
T_R(w, x, y) = G_3 - 2R = x^2 + x + y + xy + wx^2 + wx^3 + wy^3 + wxy^3 + w^2x^2 + w^2x^3 + w^2y^3 + w^2xy^3 - 1 - x^3 - y^3 - xy^3 - w - wx - wy - wxy - w^2 - w^2x - w^2y - w^2xy.
\]

We define

\[
S(w) = \frac{1}{4}q^*T_R(w, i, j) = \frac{1}{1+i+j+k} \left[ (-1 + i + j + k) + (-1 - i - j - k)w + (-1 - i - j - k)w^2 + (-1 + i + j + k) + (-1 - i - j - k)w + (-1 - i - j - k)w^2 \right] = \frac{1+i+j+k}{2} - w - w^2.
\]

We obtain the perfect sequence \(S = (q, -1, -1)\).
A **Hadamard matrix** of order $n$ is an $n \times n$ matrix $H$ with entries in $\{-1, 1\}$ such that

$$HH^\top = nI_n,$$

where $H^\top$ is the transpose of $H$ and $I_n$ is the identity matrix of order $n$.

**Applications**: Hadamard matrices have applications in different areas such as coding, cryptography and signal processing.

**Hadamard conjecture**: If $n$ is a multiple of 4 then a Hadamard matrix of order $n$ exists.†

**Families of Hadamard matrices**: Sylvester, Paley, Willamson (Turyn), Ito and Cocylic Hadamard matrices.

---

†Sylvester published in 1867 (exactly 150 years ago) the first examples of Hadamard matrices.
Williamson matrices

A square $n \times n$ matrix $H = (h_{r,c})$ with entries $h_{r,c}$ in row $r$ and column $c$ is **circulant** if $h_{r,c} = h_{0,c-r}$ for all $r, c = 0, \ldots, n - 1$, that is, the entries of $H$ are uniquely determined by its first row. A **Williamson (Hadamard) matrix** is a Hadamard matrix of order $4n$ of the form

$$
\begin{pmatrix}
A & B & C & D \\
-B & A & -D & C \\
-C & D & A & -B \\
-D & -C & B & A
\end{pmatrix}
$$

where the **components** $A, B, C$ and $D$ are $n \times n$ matrices such that

$$AA^\top + BB^\top + CC^\top + DD^\top = 4nI_n$$

and

$$XY^\top = YX^\top \text{ for all } X, Y \in \{A, B, C, D\}.$$
Perfect sequences and Williamson matrices

The components $A, B, C$ and $D$ that Williamson originally used were circulant and symmetric [10]. However, Seberry [8] showed that neither the circulant nor the symmetric properties are necessary conditions.

In this work we focus exclusively on circulant components.

**Theorem (Schmidt [9] Theorem 2.1)**

A Williamson matrix of order $4n$ with circulant components exists if and only if there is a $(4n, 2, 4n, 2n)$-relative difference set in $G_n \simeq Z_n \times Q_8$ relative to $\langle x^2 \rangle$.

**Theorem**

A Williamson matrix of order $4n$ with circulant components is equivalent to a perfect sequence of length $n$ over $Q_8 \cup qQ_8$. 
Perfect sequences and Williamson matrices

<table>
<thead>
<tr>
<th>$s_r$</th>
<th>1</th>
<th>-1</th>
<th>i</th>
<th>-i</th>
<th>j</th>
<th>-j</th>
<th>k</th>
<th>-k</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_r$</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$b_r$</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$c_r$</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$d_r$</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>-1</td>
</tr>
</tbody>
</table>

Table 1: Correspondence between perfect sequences and circulant Williamson matrices

Consider a perfect sequence $S = (s_0, \ldots, s_{n-1})$ over $Q_8 \cup qQ_8$. From Table 1, the entries of $S$ define the entries of the matrix

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

**Theorem**

The Williamson matrix $W(S)$ corresponding to $S$ has circulant components whose first rows are the rows of $R(S)$. 

Santiago Barrera-Acevedo

Perfect Sequences over Quaternions and RDS
Conversely, if $W$ is a Williamson matrix of order $4n$ with circulant components, then define $R(M)$ as the $4 \times n$ matrix consisting of the first rows of the circulant components of $W$.

**Theorem**

*From Table 1, the $r$-th column of $R(M)$ uniquely determines a symbol $s_r$, and this defines the perfect sequence $PS(M) = (s_0, \ldots, s_{n-1})$ over $Q_8 \cup qQ_8$ corresponding to $W$.***

For example, the perfect sequence

$$S = (1, i, -1, -i, -1, j, -1, -i, -1, i)$$

yields a circulant Williamson matrix $WM(S)$ of order 40 with

$$R(S) = \begin{pmatrix}
-1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 \\
-1 & -1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \\
-1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 \\
-1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & 1
\end{pmatrix}$$
Perfect sequences and Williamson matrices

The circulant Williamson matrix with circulant components defined by

\[
R(M) = \begin{pmatrix}
-1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\
-1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\
-1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & 1 \\
-1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 \\
\end{pmatrix}
\]

yields the perfect sequence

\[
S = (1, k, -j, -i, j, i, 1, i, 1, i, j, -i, -j, k).
\]

Closer look to Williamson matrices

We consider the representation of the quaternions 1, i, j and k by 4 × 4 matrices over \( \mathbb{C} \), that is (abusing notation),

\[
1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -10 & 0 & 0 \\ \end{pmatrix}
\]
The original template considered by Williamson is the matrix

$$W = 1 \otimes A + i \otimes B + j \otimes C + k \otimes D,$$

where $M \otimes N$ denotes the Kronecker product of $M$ and $N$.

The condition $WW^T = 4nI_{4n}$ implies

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

and

$$XY^T + UV^T - YX^T - VU^T = 0,$$

for $X, Y, U, V \in \{A, B, C, D\}$. 
\( XY^T + UV^T - YX^T - VU^T = 0 \), for \( X, Y, U, V \in \{ A, B, C, D \} \)

1. When the components \( A, B, C \) and \( D \) are circulant and symmetric, their respective Williamson matrix induces a perfect sequence with symmetry type 1.

2. When the components \( A, B, C \) and \( D \) are circulant and the matrix \( XY^T \) is symmetric for every \( X, Y \in \{ A, B, C, D \} \), their respective Williamson matrix induces a perfect sequence with symmetry type 2 or 3.

3. Example of the general case (yet to be found).
WM of PS of length 50 and sym 1
WM of PS of length 48 and sym 2
WM of PS of length 48 and sym 3
WM of PS of length 110 and sym 1
WM of PS of length 112 and sym 2
WM of PS of length 112 and sym 3


S. Barrera Acevedo and H. Dietrich. Perfect Sequences over the Quaternions and \((4n, 2, 4n, 2n)\)-Relative Difference Sets in \(\mathbb{Z}_n \times \mathbb{Q}_8\). Cryptography and Communications, (2017).


