Perfect Sequences over the Quaternions and Relative Difference Sets

Santiago Barrera-Acevedo
Joint work with Heiko Dietrich

Monash University
Melbourne - Australia

July 2017

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

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

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

Perfect sequences

The **autocorrelation sequence** of S is defined as $\mathrm{AC}_S = (\mathrm{AC}_S(0), \ldots, \mathrm{AC}_S(n-1))$, with $\mathrm{AC}_S(0)$ 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 $\mathrm{AC}_{S_1} = (4, 0, 0, 0)$ and $\mathrm{AC}_{S_2} = (8, 0, 0, 0, 0, 0, 0, 0)$.

Definitions

It is very difficult to construct perfect sequences over 2nd-, 4th-, and in general over n-th roots of unity.

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.

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

$$i^2 = j^2 = k^2 = -1 \text{ and } ij = k.$$

It follows from these relations that

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

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

$$1^* = 1, i^* = -i, j^* = -j, \text{ and } k^* = -k.$$

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

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

$$\mathrm{AC}_S^L(t) = \sum_{l=0}^{n-1} s_l^* s_{l+t} \quad \text{and} \quad \mathrm{AC}_S^R(t) = \sum_{l=0}^{n-1} s_l s_{l+t}^*$$

Left and right AC values of $S = (j, j, -1, -k, i, -j)$				
t	AC_S^L	$\lvert\lvert\mathrm{AC}_S^L\rvert\rvert$	AC_S^R	$\lvert\lvert\mathrm{AC}_S^R\rvert\rvert$
0	6	36	6	36
1	0	0	$2j + 2k$	8
2	$-1 + 3i - j - k$	12	$-1 + i + j - k$	4
3	0	0	0	0
4	$-1 - 3i + j + k$	12	$-1 - i - j + k$	4
5	0	0	$-2j - 2k$	8

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 $t \in \{1, \ldots, n-1\}$.

$S = (i, j, -k, j, i, 1, k, -1, k, 1)$
$\mathrm{AC}_S^L = (10, 0, 0, 0, 0, 0, 0, 0, 0, 0)$
$\mathrm{AC}_S^R = (10, 0, 0, 0, 0, 0, 0, 0, 0, 0)$

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 Q_{24}.

At this point two main questions were stated: Are there perfect sequences of unbounded lengths over Q_{24}? If so, is it possible to restrict the alphabet size to a small one, say the basic quaternions $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$?

Theorem (Barrera Acevedo and Hall [4])

There exists a family of perfect sequences over Q_8 of length $n = p^a + 1 \equiv 2 \bmod 4$, where p is prime and $a \in \mathbb{N}$.

Symmetry type 1

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

Length 8: $(\mathbf{1}, 1, i, -1, \mathbf{1}, -1, i, 1)$

Length 10: $(\mathbf{1}, i, -1, -i, \boldsymbol{j}, -i, -1, i)$

Length 11: $(1, k, -j, -i, -1, \boldsymbol{q}, -1, -i, -j, k, 1)$

Length 16: $(\mathbf{1}, i, -1, i, j, k, -j, \boldsymbol{-i}, -j, k, j, i, -1, i)$

Symmetry type 2

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

Length 8: $(\underline{1, 1, i, -1}, \underline{1, -1, \quad i, \quad 1})$
$1, -1, \quad 1, -1$

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

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

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

[†] 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: $(\underline{1, i, -j, j, 1, -i, -k, -k}, \underline{1, i, \; j, -j, 1, -i, \; k, \; k})$
$1, 1, -1, -1, 1, \; 1, -1, -1)$

Length 48:
$(1, -qk, -j, j, -q, -i, -k, qj, 1, i, -qi, -j, 1, qk, k, k, -q, i, -j, -qi, 1, -i, qj, -k,$
$1, -qk, j, -j, -q, -i, k, -qj, 1, i, qi, j, 1, qk, -k, -k, -q, i, j, qi, 1, -i, -qj, k)$

Perfect sequences and relative difference sets

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 $\mathbb{Z}_2$.

RDS Definition

Hadamard matrices

A **Hadamard matrix** of order n is an $n \times n$ matrix H with entries in $\{-1, 1\}$ such that

$$HH^{\intercal} = nI_n,$$

where $H^{\intercal}$ is the transpose of H and I_n is the identity matrix of order n. A **Williamson (Hadamard) matrix** is a Hadamard matrix of order $4n$ of the form

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

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

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

and

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

Let G be a group of order n. A square matrix M of order n is called G-**invariant** if the rows and columns of $M = (m_{g,h})$ can be indexed with elements g, h of G such that

$$m_{gk,hk} = m_{g,h} \text{ for all } g, h, k \in G.$$

In particular, when $G = \mathbb{Z}_n$ the matrix M is called **circulant**.

We identify the element $S = \sum_{g \in G} s_g g \in \mathbb{Z}[G]$ with the G-invariant matrix $(m_{g,h})$ where $m_{g,h} = s_{gh^{-1}}$.

Williamson matrices

A Hadamard matrix H of order $4n$ is said to be a **Williamson matrix over an abelian group** G of order n if H is of the form Equation (1) and satisfies (in terms of the group ring)

$$AA^{(-1)} + BB^{(-1)} + CC^{(-1)} + DD^{(-1)} = 4n$$

and

$$UV^{(-1)} + XY^{(-1)} - VU^{(-1)} - YX^{(-1)} = 0,$$

for all $X, Y \in \{A, B, C, D\}$

Theorem (Schmidt [9] Theorem 2.1)

A Williamson matrix over an abelian group G of order n exists if and only if there is a $(4n, 2, 4n, 2n)$-relative difference set in $G \times Q_8$ relative to $\mathbb{Z}_2$.

Corollary

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 $\mathbf{G}_n \simeq Z_n \times Q_8$ relative to $\mathbb{Z}_2$.

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

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: 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

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

Theorem

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

Perfect sequences and Williamson matrices

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

$$\mathrm{R}(S) = \begin{pmatrix} -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & -1 \\ -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & 1 \end{pmatrix}$$

The circulant Williamson matrix with circulant components defined by

$$\mathsf{R}(M) = \begin{pmatrix} -1 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & 1 & -1 & -1 & 1 \\ -1 & -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & -1 & -1 \\ -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \end{pmatrix}$$

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),

$$1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, i = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, j = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

The original template consider 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 $WW^{\intercal} = 4nI_{4n}$ implies

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

and

$$XY^{\intercal} + UV^{\intercal} - YX^{\intercal} - VU^{\intercal} = 0,$$

for $X, Y, U, V \in \{A, B, C, D\}$.

Perfect sequences and Williamson matrices

$$\mathbf{XY}^\intercal + \mathbf{UV}^\intercal - \mathbf{YX}^\intercal - \mathbf{VU}^\intercal = \mathbf{0}, \text{ for } X, Y, U, V \in \{A, B, C, D\}$$

1. If the components A, B, C and D are circulant and symmetric, their respective Williamson matrix yields a perfect sequence with symmetry type 1.
2. If the components A, B, C and D are circulant and the matrix $XY^\intercal$ is symmetric for every $X, Y \in \{A, B, C, D\}$, their respective Williamson matrix yields a perfect sequence with symmetry type 2 or 3.
3. Example of the general case (yet to be found).

Bibliography

K. T. Arasu and W. de Launey. Two-dimensional Perfect Quaternary Arrays. IEEE Trans. Inf. Theory 47, 1482–1493 (2001).

K. T. Arausu, W. de Launey and S. L. Ma. On Circular Complex Hadamard Matrices Designs, Codes and Cryptography 25, 123–142 (2002).

S. Barrera Acevedo and H. Dietrich. Perfect Sequences over the Quaternions and $(4n, 2, 4n, 2n)$-Relative Difference Sets in $\mathbb{Z}_n \times Q_8$. Cryptography and Communications, (2017).

S. Barrera Acevedo and T. E. Hall. Perfect Sequences of Unbounded Lengths over the Basic Quaternions. In: Lect. Notes. Comput. Sci. SETA2012, 159–167 (2012).

O. Kuznetsov. Perfect sequences over the real quaternions. Signal Design and its Applications in Communications, 2009. IWSDA '09. Fourth Internat. Workshop 1, 17–20 (2010).

O. Kuznetsov. Perfect Sequences over the Real Quaternions of Longer Length. World Congress on Computer Science and Information Technology, The Online Journal on Mathematics and Statistics (OJMS), 1 (1), (2011).

S. L. Ma and W. S. Ng. On Non-existence of Perfect and Nearly Perfect Sequences. International Journal of Information and Coding Theory, 15–38 (2009).

J. Seberry. Some matrices of Williamson Type. Utilitas Mathematica, 4, 147–154 (1973).

B. Schmidt. Williamson Matrices and a Conjecture of Ito's. Design, Codes and Cryp. 17, 61–68 (1999).

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

An (m, n, l, λ)-**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 λ times and does not contain the elements of N.

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

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

$1i^{-1} = -i$	$i1^{-1} = i$	$j1^{-1} = j$	$k1^{-1} = k$
$1j^{-1} = -j$	$ij^{-1} = -k$	$ji^{-1} = k$	$ki^{-1} = -j$
$1k^{-1} = -k$	$ik^{-1} = j$	$jk^{-1} = -i$	$kj^{-1} = i$

Back

Bibliography

K. T. Arasu and W. de Launey. Two-dimensional Perfect Quaternary Arrays. IEEE Trans. Inf. Theory 47, 1482–1493 (2001).

K. T. Arausu, W. de Launey and S. L. Ma. On Circular Complex Hadamard Matrices Designs, Codes and Cryptography 25, 123–142 (2002).

S. Barrera Acevedo and H. Dietrich. Perfect Sequences over the Quaternions and $(4n, 2, 4n, 2n)$-Relative Difference Sets in $\mathbb{Z}_n \times Q_8$. Cryptography and Communications, (2017).

S. Barrera Acevedo and T. E. Hall. Perfect Sequences of Unbounded Lengths over the Basic Quaternions. In: Lect. Notes. Comput. Sci. SETA2012, 159–167 (2012).

O. Kuznetsov. Perfect sequences over the real quaternions. Signal Design and its Applications in Communications, 2009. IWSDA '09. Fourth Internat. Workshop 1, 17–20 (2010).

O. Kuznetsov. Perfect Sequences over the Real Quaternions of Longer Length. World Congress on Computer Science and Information Technology, The Online Journal on Mathematics and Statistics (OJMS), 1 (1), (2011).

S. L. Ma and W. S. Ng. On Non-existence of Perfect and Nearly Perfect Sequences. International Journal of Information and Coding Theory, 15–38 (2009).

J. Seberry. Some matrices of Williamson Type. Utilitas Mathematica, 4, 147–154 (1973).

B. Schmidt. Williamson Matrices and a Conjecture of Ito's. Design, Codes and Cryp. 17, 61–68 (1999).

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