Perfect Sequences over the Quaternions and $(4n, 2, 4n, 2n)$-Relative Difference Sets in $C_n \times Q_8$

Santiago Barrera Acevedo[1⋆] and Heiko Dietrich[2⋆]

[1] Monash University, School of Mathematical Sciences, Clayton 3800 VIC, Australia
Santiago.Barrera.Acevedo@monash.edu
[2] Monash University, School of Mathematical Sciences, Clayton 3800 VIC, Australia
heiko.dietrich@monash.edu

Abstract. Perfect sequences over general quaternions were introduced in 2009 by Kuznetsov. The existence of perfect sequences of increasing lengths over the basic quaternions $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ was established in 2012 by Barrera Acevedo and Hall. The aim of this paper is to prove a 1–1 correspondence between perfect sequences of length n over $Q_8 \cup qQ_8$ with $q = (1+i+j+k)/2$, and $(4n, 2, 4n, 2n)$-relative difference sets in $C_n \times Q_8$ with forbidden subgroup C_2; here C_m is a cyclic group of order m. We show that if $n = p^a + 1$ for a prime p and integer $a \geq 0$ with $n \equiv 2 \bmod 4$, then there exists a $(4n, 2, 4n, 2n)$-relative different set in $C_n \times Q_8$ with forbidden subgroup C_2. Lastly, we show that every perfect sequence of length n over $Q_8 \cup qQ_8$ yields a Hadamard matrix of order $4n$ (and a quaternionic Hadamard matrix of order n over $Q_8 \cup qQ_8$).
The final publication is available at Springer via
http://link.springer.com/article/10.1007/s12095-017-0224-y

1 Introduction

The periodic autocorrelation of a sequence is a measure for how much the sequence differs from its cyclic shifts. If the autocorrelation values for all nontrivial cyclic shifts are 0, then the sequence is perfect. It is well known that 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. However, it is very difficult to construct perfect sequences over 2nd-, 4th-, and in general over n-th roots of unity. In fact, it is conjectured that perfect sequences over n-th roots of unity do not exist for lengths greater that n^2 [14].

Perfect sequences are closely related to relative difference sets and Hadamard matrices. Relative difference sets are important objects in combinatorial design theory and finite geometry, see [15, 16]. They have been studied extensively in abelian groups (see for example [5, 6] and their references). A Hadamard matrix H of order n is a an $n \times n$ matrix with entries in $\{\pm 1\}$ and $HH^\intercal = nI_n$. Hadamard matrices have significant applications, for example, in spectroscopy, object recognition, or coding of digital signals and encryption, see [9] for more details. Hadamard matrices exist for many orders, and it is the famous Hadamard Conjecture which claims that there is a Hadamard matrix

⋆ This research was partly funded by ARC DECRA projects DE140100088 and DE140101201.

of order $4n$ for all positive integers n. Starting 2001, Arasu, de Launey, and Ma [1, 3] established and studied a connection between perfect arrays of size $m \times n$ over 4th-roots of unity and $(2nm, 2, 2nm, nm)$-relative difference sets in $C_n \times C_m \times C_4$ with forbidden subgroup of size 2. Such relative difference sets are now related to Hadamard matrices: Jungnickel [11] proved that every $(n, 2, n, n/2)$-relative difference set with forbidden subgroup of size 2 yields a Hadamard matrix of order n. We note that for every n divisible by 4, Ito [10] constructed a group and conjectured that it contains an $(n, 2, n, n/2)$-relative difference set. This conjecture has been verified for all $n \leq 42$, see [18], and if it is true, then so is the Hadamard Conjecture.

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 [13], who defined perfect sequences over the quaternion algebra. In 2012, Barrera Acevedo and Hall [4] constructed the first infinite family of perfect sequences of increasing lengths over the basic quaternions $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. The aim of the present paper is to study such quaternionic sequences further and to exploit and establish relations with relative difference sets and Hadamard matrices.

In the following let $q = (1 + i + j + k)/2$. Motivated by the result of Arasu et al., our main result is a 1–1 correspondence between perfect sequences of length n over the alphabet $Q_8 \cup qQ_8$ and $(4n, 2, 4n, 2n)$-relative difference sets in $C_n \times Q_8$ with forbidden subgroup $C_2 \leq Q_8$. We discuss these relative difference sets in Section 3, and then prove the 1–1 correspondence in Section 4. In Section 5, we comment on the well known connections between relative difference sets and Hadamard matrices. We show that every perfect sequence of length n over the alphabet $Q_8 \cup qQ_8$ yields a quaternionic Hadamard matrix of order n and a Hadamard matrix of order $4n$. We conclude in Section 6 with a discussion of possible future work.

2 Notation

We denote by $\mathbb{R}$ and $\mathbb{C}$ the field of real and complex numbers, respectively. For a positive integer n we denote by C_n the cyclic group of order n. The **quaternion algebra** $\mathbb{H}$ is the 4-dimensional real algebra with $\mathbb{R}$-basis $\{1, i, j, k\}$ and non-commutative multiplication defined by $i^2 = j^2 = k^2 = -1$ and $ij = k$. It follows readily from these relations that $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, and $ik = -j$. The $\mathbb{R}$-linear complex conjugation on $\mathbb{H}$ is denoted $h \mapsto h^*$, and uniquely defined by $1^* = 1$, $i^* = -i$, $j^* = -j$, and $k^* = -k$. 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, it has size 24 and it is the unit group of the so-called Hurwitz quaternions. By abuse of notation, in this paper, we call it the **quaternion group** Q_{24}. Note that every element in Q_{24} has norm 1. If G is a multiplicatively written group and K is a ring with 1, then the **group**

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

$$\sum\nolimits_{g\in G} a_g g \sum\nolimits_{h\in G} b_h h = \sum\nolimits_{g,h\in G} a_g b_h gh.$$

We identify the multiplicative identities 1_G, 1_K, and $1_{K[G]}$, and denote them all by 1. Consequently, a positive integer n can be identified with the sum of n copies of 1_K in K, and with the sum of n copies of 1_G in $K[G]$. The following notation is also standard in the literature of relative difference sets, cf. Jungnickel and Pott [12].

Definition 1. *Let $K[G]$ be as before, let $H \subseteq G$ be a subset and $A \in K[G]$.*

a) *We identify H with $\sum_{h\in H} h \in K[G]$, in particular, $G = \sum_{g\in G} g \in K[G]$.*

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

Notation 1. *Throughout this paper, n is a positive integer and $\boldsymbol{G}_n$ is the group*

$$\boldsymbol{G}_n = \langle w, x, y \mid w^n = x^4 = y^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1}, wx = xw, wy = yw\rangle.$$

We define $\boldsymbol{H} = \langle x, y\rangle$, $\boldsymbol{C}_n = \langle w\rangle$, and $\boldsymbol{N} = \langle x^2\rangle$ as subgroups of $\boldsymbol{G}_n$, so that $\boldsymbol{G}_n = \boldsymbol{C}_n \times \boldsymbol{H}$, and $\boldsymbol{C}_n$, $\boldsymbol{H}$, and $\boldsymbol{N}$ are isomorphic to C_n, Q_8, and C_2, respectively.

3 Relative difference sets

An (m, n, k, λ)-**relative difference set** R in a group G of order mn, relative to a forbidden normal subgroup N of order n, is a k-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, k, λ)-RDS, or simply RDS. For example, $R = \{x, y, wy, xy, x^2, wx^2, wx^3, wxy^3\} \subset \boldsymbol{G}_2$ is an $(8, 2, 8, 4)$-RDS in $\boldsymbol{G}_2$ with forbidden subgroup $\boldsymbol{N} = \langle x^2\rangle$. Note that $R \subseteq G$ is an (m, n, k, λ)-RDS if and only if in the real group ring $\mathbb{R}[G]$

$$RR^{(-1)} = k + \lambda(G - N).$$

Recall that every subset $R \subseteq \boldsymbol{G}_n$ is identified with $\sum_{r\in R} r \in \mathbb{R}[\boldsymbol{G}_n]$, and that the latter is a sum of elements of the form $w^d x^u y^v \in \boldsymbol{G}_n$, that is, R is identified with a *polynomial expression* in the generators $\{x, y, w\}$ of $\boldsymbol{G}_n$. It is useful to introduce the following characteristic functions. We comment on it in the subsequent remark.

Definition 2. *For a subset R of $\boldsymbol{G}_n$, we define*

a) $\chi_R \colon \boldsymbol{G}_n \to \{0, 1\}$ *by* $\chi_R(g) = 1$ *if* $g \in R$, *and* $\chi_R(g) = 0$ *otherwise,*

b) $\xi_R \colon \boldsymbol{G}_n \to \{-1, 1\}$ *by* $\xi_R(g) = -1$ *if* $g \in R$, *and* $\xi_R(g) = 1$ *otherwise,*

c) $P_R(w, x, y) = \sum_{w^d x^u y^v \in \boldsymbol{G}_n} \chi_R(w^d x^u y^u) w^d x^u y^v \in \mathbb{R}[\boldsymbol{G}_n]$,

d) $T_R(w, x, y) = \sum_{w^d x^u y^v \in \boldsymbol{G}_n} \xi_R(w^d x^u y^u) w^d x^u y^v \in \mathbb{R}[\boldsymbol{G}_n]$.

The main advantage of this notation is that it allows us to describe *evaluations*, that is, certain substitutions for the generators x and y, for example, we have

$$P_R(w,i,j) = \sum\nolimits_{w^d x^u y^v \in \boldsymbol{G}_n} \chi_R(w^d x^u y^u) w^d i^u j^v \in \mathbb{H}[\boldsymbol{C}_n], \tag{1}$$

which is an element in the quaternion group ring of $\boldsymbol{C}_n = \langle w \rangle$. Note that the coefficients of $P_R(w,i,j)$ are the original coefficients of $P_R(w,x,y)$; similarly, $T_R(w,i,j)$ is defined. The next remark lists further easy observations.

Remark 1. Let R be a subset of $\boldsymbol{G}_n$.

a) Since $\xi_R(g) = 1 - 2\chi_R(g)$ for all $g \in \boldsymbol{G}_n$, it follows that

$$T_R(w,x,y) = P_{\boldsymbol{G}_n}(w,x,y) - 2P_R(w,x,y) \in \mathbb{R}[\boldsymbol{G}_n].$$

Thus $P_R(w,x,y) = R$ and $T_R(w,x,y) = \boldsymbol{G}_n - 2R$ as elements in $\mathbb{R}[\boldsymbol{G}_n]$.

b) The map $\mathbb{R}[\boldsymbol{G}_n] \to \mathbb{H}[\boldsymbol{C}_n]$, $P_R(w,x,y) \mapsto P_R(w,i,j)$ is a surjective ring homomorphism whose kernel is the principal ideal of $\mathbb{R}[\boldsymbol{G}_n]$ generated by $1 + y^2$.

c) If R is a $(4n, 2, 4n, 2n)$-RDS in $\boldsymbol{G}_n$, then $RR^{(-1)} = 4n + 2n(\boldsymbol{G}_n - \boldsymbol{N})$ can be expressed as $P_R(w,x,y)P_{R^{(-1)}}(w,x,y) = 4n + 2n(P_{\boldsymbol{G}_n}(w,x,y) - P_{\boldsymbol{N}}(w,x,y))$.

d) Definition 2 is motivated by the work in [1], which, in a similar context, call P_R and T_R the $(0,1)$- and $(-1,1)$-characteristic polynomial of R, respectively. Here we also use the same names for P_R and T_R.

The next lemma follows directly from Definitions 1 and 2 and the fact that the inverse of $w^d x^u y^v$ in $\boldsymbol{G}_n$ is $w^{-d} x^{-u} y^{\alpha(u)v}$ where $\alpha(u) = (-1)^{u+1}$.

Lemma 1. *If $R \subseteq \boldsymbol{G}_n$, then $T_{R^{(-1)}}(w,i,j) = T_R(w^{-1},i,j)^*$, as elements of $\mathbb{H}[\boldsymbol{C}_n]$.*

A straightforward calculation yields the following result.

Lemma 2. *Let $R \subset \boldsymbol{G}_n$ be a $(4n, 2, 4n, 2n)$-RDS with forbidden group $\boldsymbol{N}$ and write $S = \boldsymbol{G}_n \setminus R$. Then $S = x^2 R$ and we have $RS^{(-1)} + SR^{(-1)} = 4n(\boldsymbol{G}_n - 1 + x^2)$ and*

$$RR^{(-1)} + RS^{(-1)} + SR^{(-1)} + SS^{(-1)} = 8n\boldsymbol{G}_n. \tag{2}$$

Another advantage of Definition 2 is that it allows us to formulate the main result of this section, namely a characterisation of certain $(4n, 2, 4n, 2n)$-RDS in $\boldsymbol{G}_n$.

Theorem 2. *Let $J = \{(0,0), (1,0), (0,1), (1,1)\}$. A subset $R \subseteq \boldsymbol{G}_n$ is a $(4n, 2, 4n, 2n)$-RDS with forbidden subgroup $\boldsymbol{N}$ if and only if*

$$T_R(w,x,y)T_{R^{(-1)}}(w,x,y) = 8n(1 - x^2)$$

and

$$T_R(w,x,y) = (1 - x^2) \sum\nolimits_{\substack{d \in \{0,\ldots,n-1\} \\ (u,v) \in J}} \xi_R(w^d x^u y^v) w^d x^u y^v.$$

Proof (of Theorem 2). To abbreviate notation, we write P_R and T_R for $P_R(w,x,y)$ and $T_R(w,x,y)$, respectively. For the first implication, let $R \subset \boldsymbol{G}_n$ be a $(4n,2,4n,2n)$-RDS with forbidden subgroup $\boldsymbol{N} = \langle x^2 \rangle$. This implies that at most one of $w^d x^u y^v$ and $w^d x^{u+2} y^v$ lies in R. If both lie in R, then $w^d x^u y^v (w^d x^{u+2} y^v)^{-1} = x^2 \in \boldsymbol{N}$, which is not allowed. Now $|R| = |G|/2$ implies that for $d \in \{0,\ldots,n-1\}$ and $(u,v) \in J$, exactly one of $w^d x^u y^v$ and $w^d x^{u+2} y^v$ lies in R. Recall from Definition 2 that

$$T_R = \sum\nolimits_{w^d x^u y^v \in \boldsymbol{G}_n} \xi_R(w^d x^u y^v) w^d x^u y^v$$

where $\xi_R(g) = -1$ if $g \in R$ and $\xi_R(g) = 1$ otherwise. This yields

$$\begin{aligned} &\xi_R(w^d x^u y^v) w^d x^u y^v + \xi_R(w^d x^{u+2} y^v) w^d x^{u+2} y^v \\ &= \begin{cases} (1-x^2)(-w^d x^u y^v) & \text{if } w^d x^u y^v \in R \\ (1-x^2)(w^d x^u y^v) & \text{if } w^d x^u y^v \notin R, \end{cases} \end{aligned}$$

which implies that

$$T_R = (1-x^2) \sum\nolimits_{\substack{d \in \{0,\ldots,n-1\} \\ (u,v) \in J}} \xi_R(w^d x^u y^v) w^d x^u y^v,$$

as claimed. Next, we prove $T_R T_{R^{(-1)}} = 8n(1-x^2)$. Recall from Remark 1 that T_R and $T_{R^{(-1)}}$ correspond to $\boldsymbol{G}_n - 2R$ and $\boldsymbol{G}_n - 2R^{(-1)}$ in $\mathbb{R}[\boldsymbol{G}_n]$, respectively, so it remains to show show that $(\boldsymbol{G}_n - 2R)(\boldsymbol{G}_n - 2R^{(-1)}) = 8n(1-x^2)$. Let $S = \boldsymbol{G}_n \setminus R$ be the set complement of R in $\boldsymbol{G}_n$, and note that $R + S = \boldsymbol{G}_n = \boldsymbol{G}_n^{(-1)} = R^{(-1)} + S^{(-1)}$. Using Equation (2) and Lemma 2, the claim follows from

$$\begin{aligned} (\boldsymbol{G}_n - 2R)(\boldsymbol{G}_n - 2R^{(-1)}) &= (S-R)(S^{(-1)} - R^{(-1)}) \\ &= SS^{(-1)} - SR^{(-1)} - RS^{(-1)} + RR^{(-1)} \\ &= 8n\boldsymbol{G}_n - 2(SR^{(-1)} + S^{(-1)}R) \\ &= 8n\boldsymbol{G}_n - 8n(\boldsymbol{G}_n - 1 + x^2) \\ &= 8n(1-x^2). \end{aligned}$$

For the second implication, let $R \subseteq \boldsymbol{G}_n$ with $T_R T_{R^{(-1)}} = 8n(1-x^2)$ and

$$T_R = (1-x^2) \sum\nolimits_{\substack{d \in \{0,\ldots,n-1\} \\ (u,v) \in J}} \xi_R(w^d x^u y^v) w^d x^u y^v.$$

We show that R is a $(4n,2,4n,2n)$-RDS in $\boldsymbol{G}_n$ with forbidden subgroup $\boldsymbol{N} = \{1, x^2\}$, which is equivalent to $P_R P_R^{(-1)} = 4n + 2n(\boldsymbol{G}_n - \boldsymbol{N})$. It follows from $(1-x^2)P_{\boldsymbol{G}_n} = P_{\boldsymbol{G}_n} - x^2 P_{\boldsymbol{G}_n} = P_{\boldsymbol{G}_n} - P_{\boldsymbol{G}_n} = 0$ that

$$\begin{aligned} T_R P_{\boldsymbol{G}_n} &= (1-x^2) \sum\nolimits_{\substack{d \in \{0,\ldots,n-1\} \\ (u,v) \in J}} \xi_R(w^d x^u y^v) w^d x^u y^v P_{\boldsymbol{G}_n} \\ &= \sum\nolimits_{\substack{d \in \{0,\ldots,n-1\} \\ (u,v) \in J}} \xi_R(w^d x^u y^v) w^d x^u y^v (1-x^2) P_{\boldsymbol{G}_n} = 0, \end{aligned}$$

and, similarly, $P_{\boldsymbol{G}_n} T_{R^{(-1)}} = 0$. Since $T_R = P_{\boldsymbol{G}_n} - 2P_R$, we have $2P_R = P_{\boldsymbol{G}_n} - T_R$. Recall from the proof of Lemma 2 that $\boldsymbol{G}_n \boldsymbol{G}_n = 8n\boldsymbol{G}_n$, so we obtain

$$\begin{aligned} 2P_R 2P_{R^{(-1)}} &= (P_{\boldsymbol{G}_n} - T_R)(P_{\boldsymbol{G}_n} - T_{R^{(-1)}}) \\ &= P_{\boldsymbol{G}_n} P_{\boldsymbol{G}_n} - T_R P_{\boldsymbol{G}_n} - P_{\boldsymbol{G}_n} T_{R^{(-1)}} + T_R T_{R^{(-1)}} \\ &= P_{\boldsymbol{G}_n} P_{\boldsymbol{G}_n} + T_R T_{R^{(-1)}} \\ &= 8nP_{\boldsymbol{G}_n} + 8n(1 - x^2). \end{aligned}$$

From this, we deduce the claim:

$$P_R P_{R^{(-1)}} = 2nP_{\boldsymbol{G}_n} + 2n(1-x^2) = 4n + 2n(P_{\boldsymbol{G}_n} - 1 - x^2) = 4n + 2n(P_{\boldsymbol{G}_n} - P_{\boldsymbol{N}}).$$

4 Perfect sequences

The aim of this section is to prove the aforementioned 1–1 correspondence between certain perfect sequences over Q_{24} and certain RDS. We start with the relevant notation for perfect sequences; recall also the definition of Q_8 and Q_{24} in Section 2.

4.1 Notation

A sequence of length n over an alphabet $\mathcal{A} \subseteq \mathbb{C}$ is a list $S = (s_0, \ldots, s_{n-1})$ of elements in $\mathcal{A}$. We use the convention that $s_m = s_{m \bmod n}$ for every integer m, and sometimes abbreviate $S = (s_i)$ if there is no confusion about the length of S. Using this convention, the **periodic t-autocorrelation value** of S is

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

and the **autocorrelation sequence** of S is $\mathrm{AC}_S = (\mathrm{AC}_S(0), \ldots, \mathrm{AC}_S(n-1))$, 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.

In this paper we are interested in finite sequences over a quaternion alphabet $\mathcal{A} \subseteq \mathbb{H}$, and the non-commutativity of $\mathbb{H}$ requires to adjust the above definitions slightly: if $S = (s_0, \ldots, s_{n-1})$ is a finite sequence over $\mathcal{A}$, then for every integer t, the **right** and **left periodic t-autocorrelation** of S are defined as

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

respectively. The sequence S is **right (left) perfect** if its right (left) periodic autocorrelation is equal to zero for all $t \in \{1, \ldots, n-1\}$. Kuznetsov [13, Lemma 1] proved that right perfection and left perfection are equivalent, so we can call S perfect if it is right (or left) perfect. For example, $S = (1, -i, j, k, -1, k, j, -i, 1, i)$ is a perfect sequence of length 10 over Q_8, with peak-value 10.

Notation 3. *We identify a sequence $S = (s_0, \ldots, s_{n-1})$ over $\mathbb{H}$ with*

$$S(w) = \sum\nolimits_{d=0}^{n-1} s_d w^d \in \mathbb{H}[\boldsymbol{C}_n],$$

and define $S^*(w) = \sum_{d=0}^{n-1} s_d^* w^d$ and $S(w)^{-1} = \sum_{d=0}^{n-1} s_d w^{-d}$. Considering $S(w)$ as a polynomial expression in w, we have $S(w)^{-1} = S(w^{-1})$.

If S is a sequence of length n over $\mathbb{H}$, then a short calculation shows that

$$S(w)S^*(w)^{-1} = \mathrm{AC}_S^{\mathrm{R}}(0) + \mathrm{AC}_S^{\mathrm{R}}(n-1)w + \mathrm{AC}^{\mathrm{R}}(n-2)w^2 + \ldots + \mathrm{AC}_S^{\mathrm{R}}(1)w^{n-1}.$$

This implies the following lemma.

Lemma 3. *Let S be a sequence of length n over quaternions with norm 1. Then S is a perfect sequence if and only if $S(w)S^*(w)^{-1} = n$.*

4.2 The correspondence

We present the main theorem of this section; throughout, let $q = (1 + i + j + k)/2$.

Theorem 4. *There is a 1–1 correspondence between the $(4n, 2, 4n, 2n)$-RDS in $\boldsymbol{G}_n$ with forbidden subgroup $\boldsymbol{N}$ and the perfect sequences of length n over $Q_8 \cup qQ_8$.*

Note that $Q_{24} = Q_8 \cup qQ_8 \cup q^*Q_8$ is a partition into cosets. If S is a perfect sequence of length n over $q^*Q_8 \cup qQ_8$, then q^*S is a perfect sequence of length n over $Q_8 \cup qQ_8$; note that $(q^*)^2Q_8 = qQ_8$. Similarly, if S is over $Q_8 \cup q^*Q_8$, then S^* is over $Q_8 \cup qQ_8$. This shows that Theorem 4 also associates a perfect sequence of length n over the alphabet $Q_8 \cup qQ_8$ or $Q_8 \cup q^*Q_8$ or $qQ_8 \cup q^*Q_8$ with a $(4n, 2, 4n, 2n)$-RDS in $\boldsymbol{G}_n$. We collect these observations in a lemma. Its proof is a straightforward calculation in the finite group Q_{24}.

Lemma 4. *Let $A = qQ_8$ and $B = q^*Q_8$. If $a \in A$ and $b \in B$, then $a^* \in B$, $a^2 \in B$, $b^* \in A$, $b^2 \in A$, and $A = aQ_8$ and $B = bQ_8$, and $a(A \cup B) = B \cup Q_8$ and $b(A \cup B) = Q_8 \cup A$.*

Proof (of Theorem 4). First, let R be a $(4n, 2, 4n, 2n)$-RDS in $\boldsymbol{G}_n$ with forbidden subgroup $\boldsymbol{N}$. We have to construct a perfect sequence S corresponding to R. Recall from Theorem 2 that

$$T_R(w, x, y) = (1 - x^2) \sum\nolimits_{\substack{d \in \{0,\ldots,n-1\} \\ (u,v) \in J}} \xi_R(w^d x^u y^v) w^d x^u y^v$$

with $J = \{(0,0), (1,0), (0,1), (1,1)\}$ and $T_R(w, x, y)T_{R^{(-1)}}(w, x, y) = 8n(1 - x^2)$. This shows that the substitution $T_R(w, i, j) \in \mathbb{H}[\boldsymbol{C}_n]$ as defined in Equation 1 has the form

$$T_R(w, i, j) = \sum\nolimits_{d \in \{0,\ldots,n-1\}} 2(\xi_R(w^d) + \xi_R(w^d x)i + \xi_R(x^d y)j + \xi_R(w^d xy)k)w^d.$$

In particular, the coefficients of $\frac{1}{4}T_R(w,i,j)$ and of $\frac{1}{4}q^*T_R(w,i,j)$ lie in Q_{24}, and hence there is a unique sequence S of length n over Q_{24} such that

$$S(w) = \tfrac{1}{4}q^*T_R(w,i,j).$$

Note that $S^*(w)^{-1} = \frac{1}{4}T_R(w^{-1},i,j)^*q$, and $S^*(w)^{-1} = \frac{1}{4}T_{R^{(-1)}}(w,i,j)q$ by Lemma 1. Together with our assumption $T_R(w,i,j)T_{R^{(-1)}}(w,i,j) = 8n(1-i^2) = 16n$, we deduce that $S(w)S^*(w)^{-1} = n$, and now Lemma 3 proves that S is perfect. Recall that $Q_{24} = Q_8 \cup qQ_8 \cup q^*Q_8$, and note that the coefficients of $\frac{1}{4}T_R(w,i,j)$ lie in q^*Q_8, in qQ_8, or in $qQ_8 \cup q^*Q_8$. Using Lemma 4 and noting that $(q^*)^2Q_8 = qQ_8$, it follows that the coefficients of $S(w)$ and hence the alphabet of S is one of qQ_8, Q_8, or $Q_8 \cup qQ_8$. In any case, the alphabet is contained in $Q_8 \cup qQ_8$, as claimed.

Second, let S be a perfect sequence of length n over $Q_8 \cup qQ_8$, and define

$$\hat{S} = 2qS.$$

The coefficients of $\hat{S}(w)$ lie in $2qQ_8 \cup 2q^*Q_8$, so we can factor out i,j,k and decompose

$$\hat{S}(w) = 2qS(w) = S_1(w) + iS_2(w) + jS_3(w) + kS_4(w) \tag{3}$$

such that each $S_u(w) \in \mathbb{R}[\boldsymbol{C}_n]$ has coefficients in $\{\pm 1\}$. This allows us to define

$$\begin{aligned} T(w,x,y) &= (1-x^2)(S_1(w) + xS_2(w) + yS_3(w) + xyS_4(w)) \\ &= (1-x^2)\sum\nolimits_{\substack{d\in\{0,\ldots,n-1\}\\(u,v)\in J}} \alpha_{d,u,v} w^d x^u y^v \in \mathbb{R}[\boldsymbol{G}_n], \end{aligned}$$

where $J = \{(0,0),(1,0),(0,1),(1,1)\}$ and each $\alpha_{d,u,v} \in \{\pm 1\}$. In particular, we have $T(w,x,y) = \sum_{g\in\boldsymbol{G}_n} \alpha_g g$ where each $\alpha_g \in \{\pm 1\}$. Now $R = \{g \in G \mid \alpha_g = -1\}$ is a subset of G which satisfies

$$T(w,x,y) = T_R(w,x,y) = (1-x^2)\sum\nolimits_{\substack{d\in\{0,\ldots,n-1\}\\(u,v)\in J}} \xi_R(w^d x^u y^v) w^d x^u y^v.$$

Recall that $T_R(w,x,y) = \boldsymbol{G}_n - 2R$, which also implies $T_{R^{(-1)}} = \boldsymbol{G}_n - 2R^{(-1)} = \boldsymbol{G}_n^{(-1)} - 2R^{(-1)} = T_R^{(-1)}$, and so

$$T_{R^{(-1)}}(w,x,y) = (1-x^2)(S_1(w^{-1}) + x^3S_2(w^{-1}) + y^3S_3(w^{-1}) + xy^3S_4(w^{-1})).$$

It remains to show that $T_R(w,x,y)T_{R^{(-1)}}(w,x,y) = 8n(1-x^2)$. Once this is proved, Theorem 2 shows that R is a $(4n,2,4n,2n)$-RDS in $\boldsymbol{G}_n$ with forbidden group $\boldsymbol{N}$, as required. We now prove this claim. Since S and $\hat{S}$ are perfect and $qq^* = 1$, it follows from Lemma 3 that that $\hat{S}(w)\hat{S}^*(w^{-1}) = 4n$. On the other hand, using the decomposition in Equation 3 yields

$$\begin{aligned} &\hat{S}(w)\hat{S}^*(w^{-1}) = \\ &\quad S_1(w)S_1(w^{-1}) + S_2(w)S_2(w^{-1}) + S_3(w)S_3(w^{-1}) + S_4(w)S_4(w^{-1}) + \\ &+i\left[(S_2(w)S_1(w^{-1}) + S_4(w)S_3(w^{-1})) + i^2(S_1(w)S_2(w^{-1}) + S_3(w)S_4(w^{-1}))\right] \\ &+j\left[(S_2(w)S_4(w^{-1}) + S_3(w)S_1(w^{-1})) + j^2(S_1(w)S_3(w^{-1}) + S_4(w)S_2(w^{-1}))\right] \\ &+k\left[(S_3(w)S_2(w^{-1}) + S_4(w)S_1(w^{-1})) + k^2(S_1(w)S_4(w^{-1}) + S_2(w)S_3(w^{-1}))\right], \end{aligned}$$

which implies that

$$4n = S_1(w)S_1(w^{-1}) + S_2(w)S_2(w^{-1}) + S_3(w)S_3(w^{-1}) + S_4(w)S_4(w^{-1})$$

and

$$\begin{aligned}
S_2(w)S_1(w^{-1}) + S_4(w)S_3(w^{-1}) &= S_1(w)S_2(w^{-1}) + S_3(w)S_4(w^{-1}),\\
S_2(w)S_4(w^{-1}) + S_3(w)S_1(w^{-1}) &= S_1(w)S_3(w^{-1}) + S_4(w)S_2(w^{-1}),\\
S_3(w)S_2(w^{-1}) + S_4(w)S_1(w^{-1}) &= S_1(w)S_4(w^{-1}) + S_2(w)S_3(w^{-1}).
\end{aligned}$$

These equations and $(1-x^2)(x+x^3) = (1-x^2)(y+y^3) = (1-x^2)(xy+xy^3) = 0$ allow us to deduce that

$$\begin{aligned}
&T_R(w,x,y)T_{R^{-1}}(w,x,y) =\\
&\quad 2(1-x^2)\Big\{S_1(w)S_1(w^{-1}) + S_2(w)S_2(w^{-1}) + S_3(w)S_3(w^{-1}) + S_4(w)S_4(w^{-1}))\\
&+x\big[S_2(w)S_1(w^{-1}) + S_4(w)S_3(w^{-1})\big] + x^3\big[S_1(w)S_2(w^{-1}) + S_3(w)S_4(w^{-1})\big]\\
&+y\big[S_2(w)S_4(w^{-1}) + S_3(w)S_1(w^{-1})\big] + y^3\big[S_1(w)S_3(w^{-1}) + S_4(w)S_2(w^{-1})\big]\\
&+xy\big[S_3(w)S_2(w^{-1}) + S_4(w)S_1(w^{-1})\big] + xy^3\big[S_1(w)S_4(w^{-1}) + S_2(w)S_3(w^{-1})\big]\Big\}\\
&= 8n(1-x^2).
\end{aligned}$$

Note that $(1-x^2)$ lies in the centre of $\mathbb{R}[\boldsymbol{G}_n]$, and $(1-x^2)^2 = 2(1-x^2)$. Since $T_R(w,x,y)T_{R^{(-1)}}(w,x,y) = 8n(1-x^2)$, it follows that R is an RDS.

We have described how to map a $(4n, 2, 4n, 2n)$-RDS in $\boldsymbol{G}_n$ with forbidden subgroup $\boldsymbol{N}$ to a perfect sequence of length n over $Q_8 \cup qQ_8$, and vice versa. It follows from our constructions that these maps are mutually inverse to each other. This completes the proof of Theorem 4.

Example 1. The set $R = \{1, x^3, y^3, xy^3, w, wx, wy, wxy, w^2, w^2x, w^2y, w^2xy\}$ is a $(12, 2, 12, 6)$-RDS in $\boldsymbol{G}_3$ with forbidden subgroup $\boldsymbol{N}$. Following the construction in the proof of Theorem 4, the corresponding sequence is $S = (q, -1, -1)$. This sequence is perfect and has length 3 over $Q_8 \cup qQ_8$. Conversely, the sequence $S = (1, i)$ is perfect of length 2. The construction in the proof of Theorem 4 associates S with the $(8, 2, 8, 4)$-RDS $R = \{w, wxy, y^2, xy^2, wxy^2, y^3, wy^3, xy^3\}$ in $\boldsymbol{G}_2$.

An immediate consequence of Theorem 4 is the following corollary, which proves the existence of an infinite family of RDS.

Corollary 1. *Let $n = p^a + 1$ for a prime p and integer $a > 0$ with $n \equiv 2 \bmod 4$. Then there exists a $(4n, 2, 4n, 2n)$-RDS in $\boldsymbol{G}_n$ with forbidden subgroup $\boldsymbol{N}$.*

Proof. It is shown in [4] that there exists a perfect sequence over Q_8 of length n; now Theorem 4 proves the claim.

5 Hadamard Matrices

Hadamard matrices are important not only because they have various applications in engineering and other sciences, but also because the Hadamard Conjecture is one of the great unsolved problems in mathematics. Semi-regular RDS (like the $(4n, 2, 4n, 2n)$-RDS we have considered) are closely related to Hadamard matrices and, by the 1–1 correspondence proved in the previous section, so are perfect sequences over the quaternions. For example, it follows that a Hadamard matrix of order $4n$ can be constructed from a perfect sequence of length n over $Q_8 \cup qQ_8$, where $q = (1+i+j+k)/2$. Consequently, the Hadamard Conjecture can be phrased in terms of perfect sequences over quaternions. As a generalisation of complex Hadamard matrices, we introduce quaternionic Hadamard matrices defined over $Q_8 \cup qQ_8$. We show that there exists an infinite family of circulant quaternionic Hadamard matrices of increasing size, which is in contrast to the Circulant Hadamard and Circulant Quaternary Complex Hadamard Conjecture: the latter claim that there are no circulant Hadamard matrices of order greater than 4, and no circulant quaternary complex Hadamard matrices of order greater than 16, see [9, Research Problems 5 & 20].

5.1 Hadamard Matrices

A **Hadamard matrix** of order n is a square $n \times n$ 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 $n \times n$ identity matrix. Jungnickel [11] showed that a $(n, 2, n, n/2)$-relative difference set in a group G relative to a normal subgroup of size 2 yields a Hadamard matrix H of size n. Together with Theorem 4 and Corollary 1, the next result follows.

Theorem 5. a) *Every perfect sequence of length n over $Q_8 \cup qQ_8$ yields a Hadamard matrix of order $4n$.*

b) *Let $n = p^a + 1$ with p a prime and $a \geq 0$ such that $n \equiv 2 \bmod 4$. Then exists a Hadamard matrix of order $4n$.*

In view of Theorem 5a), if for every n there exists a perfect sequence of length n over $Q_8 \cup qQ_8$, then the Hadamard Conjecture is proved. We note that the Hadamard matrices in Theorem 5b) are part of the known class of Paley Hadamard matrices: these are constructed from the quadratic residue character of the multiplicative group $\mathrm{GF}(p^a)^*$, in combination with tensor products of Hadamard matrices, see [9] for details.

5.2 Hadamard Matrices over quaternions

The definition of Hadamard matrices has been generalised to non-binary alphabets, such as the quaternary complex alphabet $\{\pm 1, \pm i\}$, and to higher dimensional arrays. Hadamard matrices have also been considered over certain quaternion alphabets and the generalised quaternion groups $Q_{2^{n+1}}$, see [17, 19]. Recall that a square $n \times n$ matrix H

with entries from an alphabet $\mathcal{A} \subseteq \mathbb{H}$ is a **quaternionic Hadamard matrix** of order n over $\mathcal{A}$ if

$$HH^* = nI_n,$$

where H^* is the conjugate-transpose of H. If no confusion arises, then we also write $H = (h_{r,c})$, where $h_{r,c}$ with $0 \leq r, c \leq n-1$ is the entry of H in row r and column c. For arbitrary integers u, v, we define $h_{u,v} = h_{u \bmod n, v \bmod n}$. A quaternionic Hadamard matrix $H = (h_{r,c})$ over an alphabet $\mathcal{A}$ 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.

The next lemma is an easy observation.

Lemma 5. *There exists a circulant quaternionic Hadamard matrix of order n over $\mathcal{A}$ if and only if there exists a perfect sequence of length n over $\mathcal{A}$.*

Proof. Given a perfect sequence $S = (s_0, s_1, \ldots, s_{n-1})$ over an alphabet $\mathcal{A}$, we define a circulant matrix H over $\mathcal{A}$ by specifying its first row as $h_{0,t} = s_t$ for $0 \leq t \leq n-1$. Let A denote the matrix HH^*. The entry $a_{u,v}$ of A is equal to $\mathrm{AC}_S(v-u \bmod n)$. Thus, $a_{u,v} = n$ if $u = v$, and $a_{u,v} = 0$ otherwise, that is, H is a quaternionic Hadamard matrix over $\mathcal{A}$. Conversely, given a quaternionic Hadamard matrix H over $\mathcal{A}$, we define $S = (h_{0,0}, h_{0,1}, \ldots, h_{0,n-1})$. Since $\mathrm{AC}_S(u) = \sum_{t=0}^{n-1} h_{0,t} h_{0,t+u}^*$ is the scalar product of the 0-th row of H and the u-th column of H^*, it follows that S is perfect.

The results of the previous section imply the following theorem.

Theorem 6. a) *There exists a $(4n, 2, 4n, 2n)$-RDS in $\boldsymbol{G}_n$ with forbidden subgroup $\boldsymbol{N}$ if and only if there exists a circulant quaternionic Hadamard matrix of order n over $Q_8 \cup qQ_8$.*

b) *Let $n = p^a + 1$ for a prime p and integer $a \geq 0$ such that $n \equiv 2 \bmod 4$. There exists a circulant quaternionic Hadamard matrix over Q_8 of order n.*

c) *There is no circulant quaternionic Hadamard matrix over Q_8 of odd order.*

Proof. This follows from Theorem 4, Corollary 1, and Lemma 5. For part c) note that every perfect sequence S over Q_8 must have even length: this is an easy consequence of the property $\mathrm{AC}_S(t) = 0$ for $1 \leq t \leq n-1$.

Example 2. Choosing $p = 109$ and $a = 1$, we obtain a circulant quaternionic Hadamard matrix of order 110 over $\{\pm 1, \pm i, j\}$ whose first row has entries

$$\begin{aligned}
&j, i, -1, i, 1, i, -1, i, -1, -i, 1, i, -1, -i, 1, i, -1, -i, 1, -i, 1, -i, -1, -i, -1, i,\\
&1, i, -1, -i, 1, -i, 1, i, 1, i, 1, -i, 1, i, -1, i, 1, -i, 1, -i, 1, -i, -1, -i, -1, i, 1, i,\\
&1, i, 1, i, 1, i, -1, -i, -1, -i, 1, -i, 1, -i, 1, i, -1, i, 1, -i, 1, i, 1, i, 1, -i, 1, -i, -1,\\
&i, 1, i, -1, -i, -1, -i, 1, -i, 1, -i, -1, i, 1, -i, -1, i, 1, -i, -1, i, -1, i, 1, i, -1, i.
\end{aligned}$$

Theorem 6b) is in contrast to the Circulant Hadamard and Circulant Quaternary Complex Hadamard Conjectures. Moreover, in contrast to Theorem 6c), there exist circulant

quaternionic Hadamard matrices of certain odd lengths over $Q_8 \cup qQ_8$: the perfect sequence $(q, -1, -1)$ yields such a circulant quaternionic Hadamard matrix of odd order.

The next theorem follows from Theorems 5 and 6, the well-known tensor-product constructions of Hadamard matrices. The matrices in Theorem 7a) are part of the known class of Paley Hadamard matrices.

Theorem 7. *Let $m \geq 0$ be an integer, and for $r = 1, \ldots, m$ let $n_r = p_r^{a_r} + 1$ with p_r a prime and $a_r \geq 0$ such that $n_r \equiv 2 \bmod 4$.*

a) *There exists a Hadamard matrix of order $n = \prod_{r=1}^{m} 4n_r^{t_r}$ for all $t_1, \ldots, t_m \in \mathbb{N}$.*
b) *There exists a quaternionic Hadamard matrix over Q_8 of order $n = \prod_{r=1}^{m} n_r^{t_r}$.*

6 Outlook and future work

The proven 1–1 correspondence relates perfect sequences over quaternion alphabets with relative difference sets in non-abelian groups, which in turn are related to Williamson and cocyclic Hadamard matrices. These relations provide a new approach to study the existence and properties of such combinatorial objects.

A relatively new feature in the research discipline is the study of non-abelian relative difference sets in generalised quaternion groups or dicyclic groups, which are also related to Williamson matrices and Ito's Conjecture. We plan to investigate all these connections further. We also plan to investigate possible connections between our perfect sequences and other plug-in constructions for Hadamard matrices, see for example [7, 9].

Our systematic computer search for perfect sequences over $Q_8 \cup qQ_8$ and Q_{24} revealed surprising patterns of symmetry. We aim to prove that these patterns exist for sequences of increasing lengths. Currently there exists only one infinite family of perfect sequences over the quaternions (of magnitude one), and this family exhibits one of the observed patterns. Constructing infinite families of perfect sequences over the quaternions, with other types of symmetry patterns, will have the potential to lead to new non-abelian relative difference sets and Hadamard matrices.

References

1. K. T. Arasu and W. de Launey. Two-dimensional Perfect Quaternary Arrays. IEEE Trans. Inf. Theory 47, 1482–1493 (2001).
2. K. T. Arasu, Y. Q. Cheng and A. Pott. Hadamard and Conference Matrices Journal of Algebraic Combinatorics 14, 103–107 (2001).
3. K. T. Arausu, W. de Launey and S. L. Ma. On Circular Complex Hadamard Matrices Designs, Codes and Cryptography 25, 123–142 (2002).
4. 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).
5. J. A. Davis and J. Jedwab. A Unifying Construction of Difference Sets. Journal of Combinatorial Theory, Series A, 80, 13–78 (1997).

6. J. A. Davis, J. Jedwab and M. Mowbray. New Families of Semi-Regular Relative Difference Sets. Designs, Codes and Cryptography 13, 131–146 (1998).
7. W. de Launey and D. Flannery. Algebraic Design Theory. Mathematical Surveys and Monographs, 175. AMS, Providence, RI, (2011).
8. J. E. H. Elliott and A. T. Butson. Relative Difference Sets. Illinois J. Math. 10, 517–531 (1966).
9. K. J. Horadam. Hadamard Matrices and Their Applications. Princeton Uni. Press (2007).
10. N. Ito. On Hadamard Groups III. Kysushu. J. Math. 1, 369–379 (1997).
11. D. Jungnickel. On Automorphism Groups of Divisible Designs. Canad. J. Math. 24, 257–297 (1982).
12. D. Jungnickel and A. Pott. Difference Sets: An Introduction. Difference Sets, Sequences and their Correlation Properties, 259–295, Springer Netherlands (1999).
13. 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).
14. 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).
15. A. Pott. Finite Geometry and Character Theory. Lecture Notes in Math. 1601, Springer-Verlag, Berling-Heidelberg-New York (1995).
16. A. Pott. A survey on Relative Difference Sets. Groups, Difference Sets, and the Monster. Proc. of a Special Research Quarter at Ohio State Uni., Spring 1993, K. T. Arasu, J. Dillon, K. Harada, S. Sehgal, and R. Solomon Eds., Berlin, Walter de Gruyter, 195–232 (1996).
17. W. A. Rutledge. Quaternions and Hadamard Matrices. Proceedings of the American Mathematical Society 3, 625–630 (1952).
18. B. Schmidt. Williamson matrices and a Conjecture of Ito's. Design, Codes and Cryp. 17, 61–68 (1999).
19. M. Yamada. Hadamard Matrices of Generalised Quaternion Type. Discr. Math. 87, 187–196 (1991).