

Quaternionic Perfect Sequences and Hadamard Matrices

Aidan Bennett^{*} Curtis Bright[†] Paul Colinot[‡]
Ashwin Nayak[§]

January 29, 2026

Abstract

A finite sequence of numbers is perfect if it has zero periodic autocorrelation after a nontrivial cyclic shift. In this work, we study quaternionic perfect sequences having a one-to-one correspondence with the binary sequences arising in Williamson’s construction of quaternion-type Hadamard matrices. Using this correspondence, we devise an enumeration algorithm that is significantly faster than previously used algorithms and does not require the sequences to be symmetric. We implement our algorithm and use it to enumerate all circulant and possibly non-symmetric Williamson-type matrices of orders up to 21; previously, the largest order exhaustively enumerated was 13. We

2020 *Mathematics subject classification*. Primary 05B20; Secondary 94A55, 15B33

Key words and phrases. Perfect sequences, Hadamard matrices, quaternions.

^{*}School of Computer Science, University of Windsor. 401 Sunset Ave. Windsor, Canada. Email: bennet43@uwindsor.ca. Research supported by an NSERC undergraduate research assistantship.

[†]School of Computer Science, University of Waterloo. 200 University Ave. W., Waterloo, Canada. Email: cbright@uwaterloo.ca, Webpage: www.curtisbright.com. Research supported in part by an NSERC Discovery Grant. Corresponding author.

[‡]Université Grenoble Alpes, G-SCOP, CNRS. 681 Rue de la Passerelle, Saint-Martin-d’Hères, France. Email: paul.colinot@grenoble-inp.org. Research conducted under the Mitacs Globalink research internship program.

[§]Department of Combinatorics and Optimization and Institute for Quantum Computing, University of Waterloo. 200 University Ave. W., Waterloo, Canada. Email: academic@ashwinnayak.info. Research supported in part by an NSERC Discovery Grant.

prove that when the blocks of a quaternion-type Hadamard matrix are circulant, the blocks are necessarily pairwise amicable. This dramatically improves the filtering power of our algorithm: in order 20, the number of block pairs needing consideration is reduced by a factor of over 25,000. We use our results to construct quaternionic Hadamard matrices of interest in quantum communication and prove they are not equivalent to those constructed by other means. We also study the properties of quaternionic Hadamard matrices analytically, and demonstrate the feasibility of characterizing quaternionic Hadamard matrices with a fixed pattern of entries. These results indicate a richer set of properties and suggest an abundance of quaternionic Hadamard matrices for sufficiently large orders.

1 Introduction

A finite sequence is called *perfect* if it has no correlation with itself after a nontrivial cyclic shift. A matrix $H \in \{\pm 1\}^{n \times n}$ is a (real) *Hadamard matrix* if it satisfies $HH^\top = nI_n$, and a matrix is *circulant* if every row is a cyclic shift of the previous row by one position to the right. When its entries are over an alphabet of ± 1 , a perfect sequence is equivalent to a Hadamard matrix that is circulant [35]. For example,

$$\begin{bmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{bmatrix}$$

is a circulant Hadamard matrix equivalent to the perfect sequence defining its first row $[1, -1, -1, -1]$.

Perfect sequences have long been studied for both their practical applications and their elegant mathematical properties. However, the condition of having *no* correlation with itself at all nontrivial cyclic shifts is in practice difficult to achieve for most alphabets. In fact, over the binary $\{\pm 1\}$ alphabet the longest known perfect sequence is the length 4 sequence given above, and it has been conjectured that this is the *only* nontrivial perfect binary sequence up to isomorphism [33].

By increasing the alphabet size one can find arbitrarily long perfect sequences. One of the first constructions for perfect sequences was in 1961 by R. C. Heimiller [22]. He gave a construction for perfect sequences of length p^2

over an alphabet consisting of the p th roots of unity when p is prime. In fact, R. L. Frank had discovered the same construction, without the restriction that the length be prime, in the 1950s while working as an aircraft engineer at the Sperry Gyroscope Company [17]. For example, Frank's construction produces perfect sequences of length $4^2 = 16$ over the quaternary (complex) alphabet $\{\pm 1, \pm \mathbf{i}\}$.

Perfect sequences over $\{\pm 1, \pm \mathbf{i}\}$ are equivalent to circulant complex Hadamard matrices, where a matrix $H \in \mathbb{C}^{n \times n}$ is a *complex Hadamard matrix* if all its entries have modulus one and $HH^* = nI_n$ where H^* denotes the conjugate transpose of H . For example, Frank's construction in length 4 generates a circulant 16×16 complex Hadamard matrix and it has been conjectured that this is the largest circulant complex Hadamard matrix [38].

Although it is unlikely that there are arbitrarily large circulant Hadamard matrices, there do exist arbitrarily large non-circulant Hadamard matrices. For example, in 1867, Sylvester [36] constructed Hadamard matrices in orders 2^k for all $k \geq 0$. In 1893, Hadamard [20] proved that if a Hadamard matrix exists of order $n > 2$ then n must be divisible by 4. The *Hadamard conjecture* is that this necessary condition is also sufficient. Computational evidence supports the conjecture that Hadamard matrices do exist in all orders that are multiples of four. Although this conjecture has not been proven, many infinite classes of Hadamard matrices have been discovered.

1.1 Quaternion-type Hadamard matrices

An important method of constructing Hadamard matrices was introduced by Williamson [43] in 1944. He considered Hadamard matrices of the form

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

Hadamard matrices of this form are known as *quaternion-type* [7], since the structure is based on the matrix representation of the fundamental quaternion units $1, \mathbf{i}, \mathbf{j}$, and $\mathbf{k}$ [39]. In Williamson's original paper, the block matrices A, B, C , and D were pairwise commuting symmetric $\{\pm 1\}$ -matrices of order n satisfying $A^2 + B^2 + C^2 + D^2 = 4nI_n$. Baumert and Hall [7] point out that Williamson's pairwise commuting condition can be replaced by the more

general condition

$$UV - VU + XY - YX = 0$$

for $(U, V, X, Y) \in \{(A, B, C, D), (A, C, B, D), (A, D, B, C)\}$. Additionally, the block matrices of a quaternion-type Hadamard matrix do not necessarily need to be symmetric, but if the block matrices are not symmetric then the equations defining a quaternion-type Hadamard matrix are given by

$$AA^\top + BB^\top + CC^\top + DD^\top = 4nI_n, \quad (1.1)$$

and

$$\begin{aligned} BA^\top - AB^\top + DC^\top - CD^\top &= 0, \\ CA^\top - AC^\top + BD^\top - DB^\top &= 0, \\ DA^\top - AD^\top + CB^\top - BC^\top &= 0. \end{aligned} \quad (1.2)$$

The blocks of Hadamard matrices satisfying (1.1) and (1.2) are sometimes called Williamson-type matrices, though we follow the more common convention of reserving the name *Williamson-type* for a somewhat more specific class of matrices, namely, those satisfying (1.1) but having (1.2) replaced by the stronger *pairwise amicability* condition of $XY^\top = YX^\top$ for all $X, Y \in \{A, B, C, D\}$ [42].

In this paper, like in Williamson's original paper, we also require that the block matrices A, B, C, D be circulant, in which case we can describe the matrices in terms of their initial row. In the case that the block matrices are circulant, we prove that the seemingly stronger condition of pairwise amicability is actually equivalent to the conditions (1.2) (see Theorem 9). That is, considering the first rows of circulant Williamson-type matrices as *Williamson-type sequences* and the first rows of circulant blocks of quaternion-type matrices as *QT sequences*, we prove the notions of QT sequences and Williamson-type sequences correspond exactly. We provide background for understanding our results and formally define QT sequences and Williamson-type sequences in terms of correlation in Section 2, with the equivalence of QT sequences and Williamson-type sequences proven in Section 2.4.

Prior work on circulant Williamson-type matrices also includes finding analytical constructions or obstructions. Using an analytical approach Fitzpatrick and O'Keeffe [16] proved that there are no Williamson-type sequences of lengths 35, 47, 53, and 59, though their result relies on computer-assisted

proofs that there are no circulant symmetric Williamson-type matrices of order 35 (as first shown by Đoković [13]) and no circulant symmetric Williamson-type matrices of orders 47, 53, and 59 (shown by Holzmann, Kharaghani, and Tayfeh-Rezaie [25]). Fitzpatrick and O’Keeffe use the amicability property of Williamson-type matrices in their proof, so quaternion-type Hadamard matrices with circulant blocks of orders 35, 47, 53, and 59 could conceivably exist. The equivalence we prove in Theorem 9 establishes that in fact such matrices do not.

1.2 Quaternionic perfect sequences

The work in this paper focuses on quaternion-type Hadamard matrices with circulant blocks, but such objects can be shown to be equivalent to perfect sequences over a quaternionic alphabet. The quaternions, first described by Sir William Rowan Hamilton [21] are an extension of the complex plane, adding two additional numbers $\mathbf{j}$ and $\mathbf{k}$ with $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{ij} = \mathbf{k}$. Hamilton discovered these numbers while attempting to discover ways to multiply points in three-dimensional space in an analogous way to how complex numbers (points in two-dimensional space) can be multiplied. Note that quaternions are not commutative in general, as $\mathbf{ji} = -\mathbf{k}$.

Kuznetsov [26] first studied perfect sequences of quaternions. He proved, among other results, that symmetries of the quaternion space preserve perfection of a sequence, and listed operations on sequences that preserve perfection. He was able to construct a perfect quaternion sequence of length 5,354,228,880, and extended many results of complex sequences to the quaternions. In a significant development, Barrera Acevedo and Hall [5] constructed perfect sequences over the alphabet $\{\pm 1, \pm \mathbf{i}, \mathbf{j}\}$ for all lengths $n = p^k + 1 \equiv 2 \pmod{4}$, where p is prime and $k \in \mathbb{N}$. For the first time this showed that perfect sequences over the basic quaternion alphabet $\mathcal{Q}_8 := \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$ could be found for unbounded lengths, despite the fact that only finitely many perfect sequences are expected over the alphabet $\{\pm 1, \pm \mathbf{i}\}$. Blake [8] ran an extensive search for perfect sequences over the alphabet $\mathcal{Q}_8$, and Bright, Kotsireas, and Ganesh [10] showed that perfect sequences of length 2^k over $\mathcal{Q}_8$ exist for all $k \in \mathbb{N}$. Barrera Acevedo and Dietrich [2] studied perfect quaternion sequences over $\mathcal{Q}_+ := \mathcal{Q}_8 \cup q\mathcal{Q}_8$ where $q := (1 + \mathbf{i} + \mathbf{j} + \mathbf{k})/2$, and built a one-to-one correspondence between perfect sequences over $\mathcal{Q}_+$ and quadruples of QT sequences.

In this paper we describe the results of exhaustive searches for QT se-

quences (and equivalently perfect sequences over $\mathcal{Q}_+$). The previous longest length exhaustively searched was $n = 13$, by Barrera Acevedo, Catháin, and Dietrich [6], using an amount of compute time estimated to be up to a week [1]. Our algorithm exhaustively completes lengths $n \leq 13$ in under 5 seconds. Barrera Acevedo, Catháin, and Dietrich were interested in searching for various kinds of sequences of prime length generating cocyclic Hadamard matrices (including QT sequences as a special case), but their search algorithm was unable to reach lengths 17 and 19. We are able to exhaustively enumerate QT sequences for lengths $n \leq 20$ in under 8 hours and for length $n = 21$ in under 40 hours (see Section 3 for our results). The equivalence between QT sequences and Williamson-type sequences mentioned in Section 1.1 plays a key role in the search, dramatically improving the amount of filtering possible in the enumeration algorithm described in Section 3. Applying this equivalence improves the amount of filtering performed by our algorithm by a factor of about 25,000 when enumerating QT sequences of length $n = 20$. Thus, the equivalence is not only of theoretical interest, but also of practical use.

Williamson-type matrices that are not necessarily symmetric have been studied for over fifty years [40, 41], but in stark contrast to the symmetric case we were surprised to find no enumerations specifically of circulant Williamson-type matrices *without* the assumption of symmetry. This may be due to the fact that the assumption of symmetry dramatically decreases the search space and simplifies the search, allowing more constraining properties to be exploited and more extensive enumerations to be performed (including all orders n up to 60 [9, 25]). For example, the conditions (1.2) become trivially satisfied when the blocks A, B, C, D are symmetric and circulant. The enumeration of Barrera Acevedo, Catháin, and Dietrich [6] of cocyclic Hadamard matrices of order $4p$ for primes $p \leq 13$ is the most extensive exhaustive enumeration we are aware of that does not rely on the assumption of symmetry. Since circulant Williamson-type matrices generate cocyclic Hadamard matrices, as a special case of their results they generated all Williamson-type sequences of lengths $p \leq 13$ for prime p . The efficiencies built into the computational search in Section 3 allow us to enumerate all Williamson-type sequences of length n for $n \leq 21$.

1.3 Quaternionic Hadamard matrices

A *quaternionic Hadamard matrix* (QHM) of order n is an $n \times n$ matrix G with unit quaternion entries such that $GG^* = nI$, where G^* is the conjugate

transpose of G . Farkas, Kaniewski, and Nayak [15] recently drew a connection between quaternionic Hadamard matrices and quantum information, rekindling interest in the construction of QHMs. In more detail, using an algebra isomorphism between quaternions and a subalgebra of the set of complex 2×2 matrices, they used QHMs to construct Hadamard matrices of *unitary operators*. The latter correspond to mutually unbiased measurements (MUMs), which are extensions of mutually unbiased bases (MUBs). Consequently, every order n quaternionic Hadamard matrix corresponds to an “ n -outcome” MUM. We refer the interested reader to [15] for the definitions of these concepts and their relevance in quantum information and communication.

Some MUMs can be derived from MUBs via a direct-sum construction. Farkas, Kaniewski, and Nayak [15] provided a complete proof of the characterization of MUMs that are direct sums of MUBs. This characterization was partially proven earlier by Tavakoli, Farkas, Rosset, Bancal, and Kaniewski [37]. The characterization implies that an MUM corresponding to a normalized quaternionic Hadamard matrix is a direct sum of MUBs if and only if all the elements of the quaternionic Hadamard matrix commute.

Farkas, Kaniewski, and Nayak showed that MUMs that are *not* direct sums of MUBs lead to novel quantum communication protocols for superdense coding. This connection led them to the construction of new such MUMs. They presented explicit such MUMs for several orders and showed how these may be used to derive such MUMs for infinitely many orders. The MUMs were either discovered earlier by an ad hoc computational search [37], or were derived more systematically from QHMs for a small set of orders [15]. This motivates the study of QHMs of arbitrary order in more depth.

Čhterental and Đoković [12] observed that QHMs of order up to three are all equivalent to complex Hadamard matrices. They characterized all QHMs of order four by showing that there are precisely two families of such matrices, each of uncountably infinite cardinality. They derived explicit expressions for the matrices in terms of a few parameters. Higginbotham and Worley [24] continued in similar vein, studying order five QHMs of specific types and also more general constructions of QHMs.

Barrera Acevedo, Dietrich, and Lionis [4] provided a number of constructions of quaternionic Hadamard matrices by generalizing methods for real and complex Hadamard matrices. These constructions lead to new normalized QHMs with noncommuting entries for infinitely many orders. The constructions also include infinite families of nonequivalent such matrices for a fixed order.

Unlike the real case, quaternionic Hadamard matrices of all orders exist. The complex Fourier matrices are well-known examples. The above works suggest the existence of multiple equivalence classes of QHMs of all orders greater than three, and even multiple infinite equivalence classes of normalized QHMs with noncommuting entries (and the corresponding MUMs) of a fixed order. Spurred by this, we continue the computational and analytical investigation of QHMs.

Circulant QHMs are equivalent to perfect quaternion sequences. The computational enumeration of QT sequences thus yields new perfect quaternionic sequences, and hence new quaternionic Hadamard matrices. The normalized matrices typically contain non-commuting entries, and hence lead to new MUMs of interest in quantum information. We list several examples of such QHMs in Section 4.1. This is in contrast to earlier computational search for non-trivial MUMs, which resulted in MUMs (those reported in [37]) for only a few small orders [14].

We show that unlike in the case of real or complex Hadamard matrices, QHMs admit equivalence classes with uncountably many normalized matrices whenever they have at least one non-real entry in normalized form (Proposition 17). We also propose an approach for characterizing QHMs of small order and illustrate it for order five matrices (Section 4.3). Finally, we prove the order five QHMs generated by perfect $\mathcal{Q}_+$ -sequences produce QHMs not equivalent to those considered by Higginbotham and Worley [23], and similarly in order seven there are QHMs generated by perfect $\mathcal{Q}_+$ -sequences not equivalent to the QHMs generated by the perfect sequences listed by Kuznetsov [27] and Barrera Acevedo, Dietrich, and Lionis [4] (see Section 4.4). Consequently, there are at least three nonequivalent families of QHMs in orders five and seven; along with prior work, this leads us to conjecture there exist multiple nonequivalent quaternionic Hadamard matrices for all orders ≥ 4 . Our results imply this conjecture is not true if only *circulant* QHMs over $\mathcal{Q}_+$ are considered, though. The equivalence provided in Theorem 9, in conjunction with the results of Fitzpatrick and O’Keeffe [16], imply circulant quaternionic Hadamard matrices of orders 35, 47, 53, and 59 having entries in $\mathcal{Q}_+$ do not exist.

2 Background

In this section we provide the notations and the necessary background that we use. First, we introduce the quaternion algebra and the notation we use to denote important sets of quaternions in Section 2.1. We formally define Hadamard and quaternionic Hadamard matrices and the notion of equivalence between Hadamard matrices in Section 2.2. Next, we formally define the correlation of sequences as well as perfect sequences, QT sequences, and Williamson-type sequences in Section 2.3, including a one-to-one correspondence between certain quaternionic perfect sequences and QT sequences proven by Barrera Acevedo and Dietrich [2]. We then prove a one-to-one correspondence between QT sequences and Williamson-type sequences in Section 2.4. Finally, we define notions of equivalence of QT sequences in Section 2.5 that we later rely on to classify our QT sequence enumeration results.

2.1 Quaternions

The quaternions may be viewed as a noncommutative extension of the complex numbers. Formally, the real algebra of quaternions is represented as

$$\mathbb{H} := \{ \alpha + \beta \mathbf{i} + \gamma \mathbf{j} + \delta \mathbf{k} : \alpha, \beta, \gamma, \delta \in \mathbb{R} \},$$

where $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ are the *basic unit quaternions* satisfying the relations

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

The number α is the *real part* of the quaternion $\alpha + \beta \mathbf{i} + \gamma \mathbf{j} + \delta \mathbf{k}$, and $\beta \mathbf{i} + \gamma \mathbf{j} + \delta \mathbf{k}$ its *pure imaginary* part.

The algebra is endowed with a conjugation operation $x \mapsto x^*$ satisfying $\alpha^* = \alpha$ for real α along with $\mathbf{i}^* = -\mathbf{i}$, $\mathbf{j}^* = -\mathbf{j}$, and $\mathbf{k}^* = -\mathbf{k}$. The real part $\text{Re}(w)$ of a quaternion w can thus be expressed as $\text{Re}(w) = (w + w^*)/2$.

Conjugation distributes over addition and satisfies $(x_1 x_2)^* = x_2^* x_1^*$. The norm $\|x\|$ of a quaternion x is given by

$$\|x\| := \sqrt{x x^*} = \sqrt{x^* x},$$

and when $x \neq 0$, its multiplicative inverse x^{-1} is given by $x^{-1} := x^*/\|x\|$. The quaternions with norm 1 are the *unit quaternions*, and we denote the set of unit quaternions by

$$\mathbb{S}^3 := \{ w \in \mathbb{H} : \|w\| = 1 \}.$$

The unit quaternions form a non-abelian group under the multiplication operation. We denote the set of quaternionic square roots of -1 by S^2 . That is,

$$S^2 := \{ w \in \mathbb{H} : w^2 = -1 \},$$

and it can be shown that

$$S^2 = \{ w \in S^3 : \operatorname{Re}(w) = 0 \}.$$

So the elements of S^2 are pure imaginary quaternions.

We define $q := (1 + \mathbf{i} + \mathbf{j} + \mathbf{k})/2$. This is a unit quaternion that is a cube root of -1 . Three important sets of unit quaternions in this paper are

$$\mathcal{Q}_8 := \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}, \quad \mathcal{Q}_+ := \mathcal{Q}_8 \cup q\mathcal{Q}_8, \quad \text{and} \quad \mathcal{Q}_{24} := \mathcal{Q}_+ \cup q^2\mathcal{Q}_8.$$

The sets $\mathcal{Q}_8$ and $\mathcal{Q}_{24}$ are groups under multiplication, but $\mathcal{Q}_+$ is not since $q^2 = -q^* \notin \mathcal{Q}_+$.

Euler's formula $e^{it} = \cos t + \mathbf{i} \sin t$ generalizes to the quaternions via the power series expansion for the exponential function [11]. For $t \in \mathbb{R}$ and $w \in S^2$, we have

$$e^{wt} = \cos t + w \sin t.$$

2.2 Hadamard matrices

A square matrix H of order n is a (*real*) *Hadamard matrix* if H has ± 1 entries and $HH^\top = nI_n$. In other words, all the entries of the matrix have unit magnitude and the rows of the matrix are mutually orthogonal. This implies that the columns of the matrix are also mutually orthogonal.

For a quaternionic matrix G of order n , the matrix G^* denotes the conjugate transpose of G , i.e., $(G^*)_{ij} := (G_{ji})^*$ for all indices $i, j \in \{0, 1, \dots, n-1\}$. The matrix G is a *quaternionic Hadamard matrix* (QHM) if G has entries in S^3 and $GG^* = nI_n$. The latter condition requires the rows of the matrix to be orthogonal with respect to a sesquilinear form on the $\mathbb{H}$ -module $\mathbb{H}^n$ that is conjugate-linear in the second argument. We can show that this condition implies $G^*G = nI_n$, i.e., the columns of G are orthogonal with respect to a *different* sesquilinear form that is conjugate-linear in the *first* argument. Due to the non-commutativity of multiplication in $\mathbb{H}$, the use of the two different sesquilinear forms is important; orthogonality with respect to one does not necessarily imply orthogonality with respect to the other.

We may view the set of reals as a subset of quaternions with 0 pure imaginary part, and the set of complex numbers as a subset of quaternions generated by $\{1, \mathbf{i}\}$. So a complex Hadamard matrix may be viewed as a QHM with complex entries.

In the rest of the paper, we consider Hadamard matrices up to equivalence. Two real Hadamard matrices are considered to be equivalent if one can be obtained from the other by negating rows or columns, by interchanging rows, or by interchanging columns [30]. We extend this equivalence to QT sequences: two QT sequences are said to be *Hadamard equivalent* if they generate equivalent quaternion-type Hadamard matrices. Similarly, two quaternionic Hadamard matrices are said to be equivalent if one can be obtained from the other by multiplying rows *on the left* by unit quaternions, by multiplying columns *on the right* by unit quaternions, by interchanging rows, or by interchanging columns. Since the multiplication of quaternions is not commutative, the order of multiplication in these operations is important. The equivalence of two QHMs may be characterized as follows.

Lemma 1. *Two QHMs G, G' are equivalent if and only if there are permutation matrices P_1, P_2 and diagonal matrices D_1, D_2 of unit quaternions such that $G' = D_1 P_1 G P_2 D_2$.*

An analogous lemma holds for real or complex Hadamard matrices. In the real case, the diagonals of D_1 and D_2 are ± 1 , and in the complex case, they consist of unit complex numbers.

We say that a real, complex, or quaternionic Hadamard matrix is *normalized* if the entries in the first row and the first column are all ‘1’. Observe that every Hadamard matrix is equivalent to a normalized Hadamard matrix; we may multiply each row on the left by the conjugate of its first entry, and similarly multiply each column on the right by the conjugate of its first entry to achieve this. We refer to these operations as ‘dephasing’.

Given a quaternionic Hadamard matrix G and an algebra automorphism f of the quaternions, we may verify that the matrix $f(G)$ defined by $(f(G))_{ij} := f(G_{ij})$ for all indices $0 \leq i, j < n$ is also a quaternionic Hadamard matrix. It so happens that every automorphism of the quaternions corresponds to an *inner* automorphism.

Proposition 2 (Proposition 2.4.7, page 19, [32]). *Every automorphism of $\mathbb{H}$ is inner, i.e., if $f: \mathbb{H} \rightarrow \mathbb{H}$ is an automorphism, then there exists $a \in \mathbb{S}^2$ such that $f(x) = a^* x a$, for all $x \in \mathbb{H}$.*

Note that the application of an inner automorphism to every entry of a matrix may be achieved by an equivalence operation; we may multiply each row on the left by a^* and each column on the right by a . So the application of automorphisms results in equivalent QHMs.

Corollary 3. *Applying an automorphism of $\mathbb{H}$ to each entry of a quaternionic Hadamard matrix produces an equivalent quaternionic Hadamard matrix.*

2.3 Perfect, QT, and Williamson-type sequences

Let A and B be sequences of length n , with $A = [a_0, \dots, a_{n-1}]$ and $B = [b_0, \dots, b_{n-1}]$. For a *shift* $0 \leq t < n$, the *periodic crosscorrelation* $R_{A,B}(t)$ of A and B is defined as

$$R_{A,B}(t) := \sum_{r=0}^{n-1} a_r b_{r+t \bmod n}^*.$$

We further define the *right periodic autocorrelation* $R_A^R(t)$ of A and the *left periodic autocorrelation* $R_A^L(t)$ of A as

$$R_A^R(t) := \sum_{r=0}^{n-1} a_r a_{r+t \bmod n}^*, \quad \text{and} \quad R_A^L(t) := \sum_{r=0}^{n-1} a_r^* a_{r+t \bmod n},$$

respectively. A sequence S is called *right perfect* if its right periodic t -autocorrelation vanishes for all non-zero shifts t , i.e., for all t with $1 \leq t < n$, we have $R_S^R(t) = 0$. Left perfection of a sequence is defined in a similar way. Kuznetsov [26] proved that a quaternion sequence is right perfect if and only if it is left perfect. Thus without loss of generality, we define the *periodic autocorrelation* $R_A(t)$ of A as

$$R_A(t) := R_A^R(t) = R_{A,A}(t) = \sum_{r=0}^{n-1} a_r a_{r+t \bmod n}^*,$$

and call the sequence A *perfect* if its periodic autocorrelation values vanish for all non-zero t . A perfect sequence over $\mathbb{H}$ is called a *perfect quaternion sequence*.

We refer to sequences with $\{\pm 1\}$ entries as *binary* sequences. Let A , B , C , and D each be binary sequences of length n . Denote the Kronecker delta

by $\delta_{0,t}$ (note $\delta_{0,t}$ is 1 if $t = 0$ and 0 otherwise). We say that (A, B, C, D) is a quadruple of *QT sequences* if for all $0 \leq t < n$ we have

$$R_A(t) + R_B(t) + R_C(t) + R_D(t) = \delta_{0,t}4n, \quad (2.1)$$

$$R_{A,B}(t) - R_{B,A}(t) + R_{C,D}(t) - R_{D,C}(t) = 0, \quad (2.2)$$

$$R_{A,C}(t) - R_{C,A}(t) + R_{D,B}(t) - R_{B,D}(t) = 0, \quad (2.3)$$

$$R_{A,D}(t) - R_{D,A}(t) + R_{B,C}(t) - R_{C,B}(t) = 0. \quad (2.4)$$

We call (2.1) the *autocorrelation condition* and (2.2)–(2.4) the *crosscorrelation conditions*. If the crosscorrelation conditions are replaced by the conditions $R_{X,Y}(t) - R_{Y,X}(t) = 0$ for all $X, Y \in \{A, B, C, D\}$ then the sequences in the quadruple are known as *Williamson-type*. QT sequences are equivalent to quaternion-type Hadamard matrices with circulant blocks (as defined in the introduction) and similarly Williamson-type sequences are equivalent to the first rows of circulant Williamson-type matrices. If a quadruple of Williamson-type sequences generate *symmetric* circulant block matrices then they are called *Williamson sequences* [9]. Note a sequence $[a_0, \dots, a_{n-1}]$ generates a circulant symmetric matrix when $a_i = a_{n-i}$ for all $1 \leq i < n$.

Barrera Acevedo and Dietrich [2] showed that perfect quaternion sequences over $\mathcal{Q}_+$ of length n are equivalent to a certain kind of relative difference set in $C_n \times \mathcal{Q}_8$, where C_n denotes the cyclic group of order n . A result of Schmidt [34] shows this kind of relative difference set in $C_n \times \mathcal{Q}_8$ is equivalent to quaternion-type Hadamard matrices whose blocks are circulant (but not necessarily pairwise amicable or symmetric). Precisely, we have the following theorem.

Theorem 4 (cf. [3, Thm. 2.4]). *There is a one-to-one correspondence between quadruples of QT sequences of length n and perfect sequences of length n over $\mathcal{Q}_+$.*

This correspondence can be described by a map between the r th entry s_r of a perfect quaternion sequence S and the quadruple (a_r, b_r, c_r, d_r) of the r th entries of the QT sequences (A, B, C, D) . The following table specifies half of the mapping, with $+1$ and -1 abbreviated as ‘+’ and ‘−’, respectively.

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

The remaining half of the mapping is given by the rule that if (a_r, b_r, c_r, d_r) maps to s_r then $(-a_r, -b_r, -c_r, -d_r)$ maps to $-s_r$. Due to this correspondence, searching for perfect quaternion sequences over the alphabet $\mathcal{Q}_+$ is equivalent to searching for QT sequences.

We stress the equivalence established in Theorem 4 is *not* between Williamson-type sequences and perfect $\mathcal{Q}_+$ -sequences, but instead between QT sequences (that are conceivably not pairwise amicable) and perfect $\mathcal{Q}_+$ -sequences. Schmidt explicitly warns that he does *not* require pairwise amicability of the block matrices in the result used to prove Theorem 4:

We remark that this definition slightly differs from the usual one which requires that $XY^t = YX^t$ holds for all 2-subsets $\{X, Y\}$ of $\{A, B, C, D\}$. [34]

Thus, in order to complete an enumeration of perfect $\mathcal{Q}_+$ -sequences via this equivalence one could unfortunately *not* use the stronger pairwise amicability condition and would instead have to use the weaker quaternion-type conditions provided by (1.2). Fortunately, in the next section we show that the conditions (1.2) actually imply pairwise amicability, thereby rendering the above distinction irrelevant and providing the following.

Theorem 5. *There is a one-to-one correspondence between quadruples of Williamson-type sequences of length n and perfect sequences of length n over $\mathcal{Q}_+$.*

2.4 The equivalence of QT sequences and Williamson-type sequences

In order to show the equivalence of QT sequences and Williamson-type sequences we utilize the discrete Fourier transform (DFT). We denote by $\text{DFT}_A(t)$ the t -th value of the DFT of a sequence A of length n , i.e., $\text{DFT}_A(t) = \sum_{s=0}^{n-1} a_s \exp(2\pi i s t / n)$, and use $\text{DFT}(A)$ to denote the vector of DFT values, i.e., $\text{DFT}(A) = [\text{DFT}_A(0), \dots, \text{DFT}_A(n-1)]$. We also define the *power spectral density* of A by $\text{PSD}_A(t) := \text{DFT}_A(t) \text{DFT}_{A^*}(t) = |\text{DFT}_A(t)|^2$ and write PSD_A for the vector of $\text{PSD}_A(t)$ values for $t = 0$ to $n-1$. Here A^* is the conjugate transpose operation applied to a sequence; the k th entry of A^* is $(A_{-k \bmod n})^*$ where the mod operator gives the integer in $[0, n)$ congruent to its argument modulo n . The following equivalence is well-known but for completeness we provide a proof.

Proposition 6 (Power Spectral Density). *(A, B, C, D) is a quadruple of QT sequences of length n if and only if*

$$\text{PSD}_A(t) + \text{PSD}_B(t) + \text{PSD}_C(t) + \text{PSD}_D(t) = 4n \quad \text{for all } t \in \mathbb{Z}.$$

Proof. The autocorrelation condition is equivalent to the convolution equation

$$A * A^* + B * B^* + C * C^* + D * D^* = [4n, 0, \dots, 0] \quad (2.5)$$

where $X * Y$ denotes sequence convolution, i.e., the convolution of the sequences $[x_0, \dots, x_{n-1}]$ and $[y_0, \dots, y_{n-1}]$ has as its k th entry $\sum_{i=0}^{n-1} x_i y_{k-i \bmod n}$. From the DFT convolution theorem we have $\text{DFT}_{X * X^*}(t) = \text{DFT}_X(t) \text{DFT}_{X^*}(t) = \text{PSD}_X(t)$. Applying the DFT to both sides of (2.5), using the linearity of the DFT, and the fact that the DFT of $[4n, 0, \dots, 0]$ is $[4n, \dots, 4n]$, we have that (2.5) implies

$$\text{PSD}_A + \text{PSD}_B + \text{PSD}_C + \text{PSD}_D = [4n, \dots, 4n].$$

Applying the inverse DFT to this PSD equation shows it is equivalent to (2.5). $\square$

Similarly, the following proposition shows that we can also apply the DFT the crosscorrelation equations to derive an equivalent form of the equations in the frequency domain. Define the *cross power spectral density* by $\text{CPSD}_{X,Y}(t) = \text{DFT}_X(t) \text{DFT}_Y(t)^*$ and let $\text{CPSD}_{X,Y}$ be the vector of CPSD values from $t = 0$ to $n - 1$.

Proposition 7 (Cross Power Spectral Density). *The crosscorrelation equation (2.2) holding for all integers t is equivalent to the condition*

$$\text{CPSD}_{A,B}(t) - \text{CPSD}_{B,A}(t) + \text{CPSD}_{C,D}(t) - \text{CPSD}_{D,C}(t) = 0 \quad \text{for all } t \in \mathbb{Z}.$$

Proof. The vector of crosscorrelations of X and Y is equal to the convolution vector $X * Y^*$, so the crosscorrelation condition (2.2) is equivalent to

$$A * B^* - B * A^* + C * D^* - D * C^* = [0, \dots, 0]. \quad (2.6)$$

By applying the DFT and using the DFT convolution theorem we have $\text{DFT}_{X * Y^*}(t) = \text{DFT}_X(t) \text{DFT}_{Y^*}(t) = \text{CPSD}_{X,Y}(t)$, so by applying the DFT to (2.2) and noting that the DFT of $[0, \dots, 0]$ is $[0, \dots, 0]$, we have that (2.6) is equivalent to

$$\text{CPSD}_{A,B} - \text{CPSD}_{B,A} + \text{CPSD}_{C,D} - \text{CPSD}_{D,C} = [0, \dots, 0]. \quad \square$$

Remark 8. A similar proof to that of Proposition 7 gives that (2.3) for all t is equivalent to $\text{CPSD}_{A,C} - \text{CPSD}_{C,A} = \text{CPSD}_{B,D} - \text{CPSD}_{D,B}$, and (2.4) for all t is equivalent to $\text{CPSD}_{A,D} - \text{CPSD}_{D,A} = \text{CPSD}_{C,B} - \text{CPSD}_{B,C}$.

Even though QT sequences and Williamson-type sequences are defined differently, we now prove these two notions are actually equivalent.

Theorem 9. (A, B, C, D) is a quadruple of QT sequences if and only if (A, B, C, D) is a quadruple of Williamson-type sequences.

Proof. If (A, B, C, D) is a set of Williamson-type sequences then $R_{X,Y}(t) - R_{Y,X}(t) = 0$ for all integers t and $X, Y \in \{A, B, C, D\}$. Adding together the conditions for $(X, Y) = (A, B)$ and $(X, Y) = (C, D)$ one derives (2.2). The conditions (2.3) and (2.4) are derived similarly.

Conversely, suppose (A, B, C, D) is a set of QT sequences. Take t to be a fixed integer, and let $a := \text{DFT}_A(t)$, $b := \text{DFT}_B(t)$, $c := \text{DFT}_C(t)$, and $d := \text{DFT}_D(t)$. By Proposition 7 we have

$$ab^* - ba^* + cd^* - dc^* = 0. \quad (2.7)$$

For $x \in \mathbb{C}$, write $x = r_x + i_x \mathbf{i}$ with $r_x, i_x \in \mathbb{R}$. Equivalently considering x as a row vector in $\mathbb{R}^2$, we write the determinant of the matrix $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} r_x & i_x \\ r_y & i_y \end{bmatrix}$ as $|x|_y| = r_x i_y - r_y i_x$, and note that $yx^* - xy^* = 2\mathbf{i}|x|_y|$. Thus (2.7) is equivalent to $|a|_b| + |c|_d| = 0$ or $|a|_b| = |c|_d|$. From the crosscorrelation equations in the frequency domain (cf. Remark 8) we have

$$\left| \begin{array}{c} a \\ b \end{array} \right| = \left| \begin{array}{c} d \\ c \end{array} \right|, \quad \left| \begin{array}{c} a \\ c \end{array} \right| = \left| \begin{array}{c} b \\ d \end{array} \right|, \quad \text{and} \quad \left| \begin{array}{c} a \\ d \end{array} \right| = \left| \begin{array}{c} c \\ b \end{array} \right|. \quad (2.8)$$

We now show this implies all these determinants are 0. Suppose not, and without loss of generality that $|a|_b| \neq 0$. Then $\{a, b\}$ form a basis of $\mathbb{R}^2$, so write $c = \alpha a + \beta b$ and $d = \gamma a + \delta b$ for $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. Now $|c|_d| = |\gamma a + \delta b|_{\alpha a + \beta b}| = |\gamma a|_{\alpha a + \beta b}| + |\delta b|_{\alpha a + \beta b}| = |\gamma a|_{\beta b}| + |\delta b|_{\alpha a}| = (\gamma\beta - \alpha\delta)|a|_b|$, $|a|_c| = \beta|a|_b|$, $|b|_d| = |b|_{\gamma a + \delta b}| = |b|_{\gamma a}| = -\gamma|a|_b|$, $|a|_d| = \delta|a|_b|$, and $|c|_b| = \alpha|a|_b|$. Using these expressions in (2.8), we have

$$\gamma\beta - \alpha\delta = 1, \quad \beta = -\gamma, \quad \text{and} \quad \delta = \alpha.$$

These imply $\alpha^2 + \beta^2 = -1$, a contradiction. Thus it must be the case that $|a|_b| = |a|_c| = |a|_d| = |b|_c| = |b|_d| = |c|_d| = 0$. From $|a|_b| = 0$ it follows $ab^* =$

ba^* . Since $a = \text{DFT}_A(t)$ and $b = \text{DFT}_B(t)$ and t was arbitrary, it follows $\text{CPSD}_{A,B} = \text{CPSD}_{B,A}$. Applying the inverse DFT, we have $R_{A,B}(t) = R_{B,A}(t)$ for all t . Similarly, we have $R_{X,Y}(t) = R_{Y,X}(t)$ for all t , so (A, B, C, D) is of Williamson-type. $\square$

Despite the one-to-one correspondence between Williamson-type sequences and QT sequences, we still find it useful to have separate terminology for both. In the next section we provide two different notions of equivalence of quadruples of QT sequences (one based on the definition of QT sequences and the other based on the definition of Williamson-type sequences) and describe the usefulness of having both kinds of equivalence available.

2.5 Sequence equivalence operations

QT sequences have a number of equivalence operations that can be used to define equivalence classes that in general are not the same as the equivalence classes formed by the Hadamard equivalence described in Section 2.2. Because we care about running exhaustive searches for QT sequences up to equivalence, we use these equivalence operations to effectively reduce the size of the search space without loss of generality. Each operation acts on a quadruple of QT sequences (A, B, C, D) and produces another quadruple of QT sequences.

QT equivalence operations

- NS: (Negate and Swap) Negate a single sequence of A, B, C, D and swap a single pair of sequences of A, B, C, D .
- AN: (Alternating negation) Multiply every other element of A, B, C and D simultaneously by -1 when the length n is even.
- DE: (Decimate) Apply an automorphism of the cyclic group C_n to the indices of each sequence A, B, C , and D simultaneously.
- CS: (Cyclic Shift) Cyclically shift all the entries of A, B, C , and D simultaneously by any amount.
- DH: (Double Half Shift) Shift the entries of two of A, B, C , and D by $n/2$ when the length n is even.

We call two quadruples of QT sequences *QT equivalent* if they are equivalent under these operations. For convenience, we also define the following two additional equivalence operations. They both can be derived from two applications of the NS operation.

- DN: (Double Negate) Negate two sequences of A , B , C , or D .
- DS: (Double Swap) Swap two pairs of A , B , C , D .

The NS equivalence operation preserves the autocorrelation condition since $R_X(t) = R_{-X}(t)$ for all t , and it preserves the crosscorrelation conditions because the action of applying a single negation and the action of applying a single swap has the effect of negating a single side of each of the three crosscorrelation conditions (as well as permuting two conditions amongst themselves in the case of a swap) when written in the form

$$\begin{aligned} R_{A,B}(t) - R_{B,A}(t) &= R_{D,C}(t) - R_{C,D}(t), \\ R_{A,C}(t) - R_{C,A}(t) &= R_{B,D}(t) - R_{D,B}(t), \\ R_{A,D}(t) - R_{D,A}(t) &= R_{C,B}(t) - R_{B,C}(t). \end{aligned}$$

Thus, the NS operation preserves the crosscorrelation conditions. The DE, AN, and both shift operations are well-known to preserve the sum of autocorrelation values [29] and they also preserve the sum of crosscorrelation values. For example, if $(-1) * X$ denotes the alternating negation of X , then $R_{(-1)*A, (-1)*B}(t) = (-1)^t R_{A,B}(t)$ (for even length sequences) and if $s(X)$ denotes a cyclic shift of X by 1 then $R_{s(A), s(B)}(t) = R_{A,B}(t)$ and

$$R_{s^{n/2}(A), B}(t) = R_{A, s^{n/2}(B)}(t) = R_{A,B}(t \pm n/2)$$

when n is even. Sequence reversal can also be considered an equivalence operation, but in this case it can be recovered by applying DE with the automorphism $x \mapsto -x$ followed by a cyclic shift to the left.

Note that the above equivalence operations do *not* make use of the one-to-one correspondence between QT sequences and Williamson-type sequences provided by Theorem 9. Incorporating Theorem 9, we could replace the negate-and-swap operation with a single-negate operation and a single-swap operation, and the double half shift with a single half shift:

- SN: (Single Negate) Negate one sequence of A , B , C , or D .

- SS: (Single Swap) Swap one pair of A, B, C, D .
- SH: (Single Half Shift) Shift the entries of one of A, B, C, D by $n/2$ when n is even.

This is because the SN, SS, and SH operations preserve the pairwise amicability condition $R_{X,Y}(t) = R_{Y,X}(t)$ satisfied by Williamson-type sequences. Consequently, we call two quadruples *Williamson-type equivalent* if they are equivalent under the QT equivalence operations with the NS operation replaced by SN and SS and the DH operation replaced by SH.

The primary reason why we define QT equivalence in a different way from Williamson-type equivalence is because QT equivalence relates better to Hadamard equivalence—in Theorem 10 we show that QT equivalence implies Hadamard equivalence, so to enumerate all QT sequences up to Hadamard equivalence one can enumerate all sequences up to QT equivalence and then filter by Hadamard equivalence. On the other hand, Williamson-type equivalence does *not* imply Hadamard equivalence in general. Thus, an enumeration of QT sequences up to Williamson-type equivalence is not guaranteed to produce an enumeration of QT sequences up to Hadamard equivalence. For simplicity, the algorithm we present will enumerate QT sequences up to Williamson-type equivalence, but in Section 3.4 we describe how to also ensure a complete enumeration up to both QT equivalence and Hadamard equivalence.

Theorem 10. *QT sequences that are QT equivalent are also Hadamard equivalent.*

Proof. We need to show that each equivalence operation NS, AN, DE, CS, and DH preserves Hadamard equivalence. Barrera Acevedo, Catháin, and Dietrich have shown that if two QT sequences are equivalent under NS equivalence then they are equivalent under Hadamard equivalence [6, Prop. 4.4(a,b)], so we have four remaining operations to consider. In each case we show that application of the operation to a quadruple of QT sequences produces a new quadruple which is Hadamard equivalent to the original. This is accomplished by showing that each equivalence operation (considered as an operation on quaternion-type Hadamard matrices) can be constructed out of the operations of negating or permuting rows or columns.

For the AN operation, suppose n is even. Consider the act of negating every second row and every second column of a quaternion-type Hadamard

matrix with circulant blocks. Because n is even, the resulting Hadamard matrix still has circulant blocks and the defining sequences of each circulant block have had AN applied to them. Thus, applying AN to a QT sequence quadruple produces a Hadamard equivalent quadruple.

The DE operation applies the same permutation ϕ over $\{0, \dots, n-1\}$ to the indices of all entries of a quadruple. Consider the act of using ϕ to permute both the columns and rows with indices in $[0, n)$, $[n, 2n)$, $[2n, 3n)$, and $[3n, 4n)$ of a quaternion-type Hadamard matrix with circulant blocks. (Here ϕ must be extended to be over $\{0, \dots, 4n-1\}$, e.g., via $\phi(i) = \phi(i-n) + n$ for $n \leq i < 4n$.) Because the same permutation was applied to both the rows and columns of each circulant block, the resulting Hadamard matrix still has circulant blocks (but their defining sequences have been permuted by ϕ and thus have had DE applied to them). Thus, the DE operation applied to a QT sequence quadruple produces a Hadamard equivalent quadruple.

The CS operation with a shift of c applies $s^c(i) = (i + c) \bmod n$ to the indices of all entries of a quadruple. Consider the act of using s^c to circularly shift the columns with indices in $[0, n)$, $[n, 2n)$, $[2n, 3n)$, and $[3n, 4n)$ of a quaternion-type Hadamard matrix with circulant blocks. Because a circular shift applied to the columns of a circulant matrix produces another circulant matrix, the resulting Hadamard matrix still has circulant blocks and those blocks have had the CS operation applied to their defining sequences. Thus, the CS operation applied to a QT sequence quadruple produces a Hadamard equivalent quadruple.

The DH operation applies a half-shift of $s^{n/2}$ to two sequences in a quadruple of QT sequences (without loss of generality, suppose DH is applied to the first two sequences in the quadruples). If X is a circulant matrix, denote by X' the columns of X circularly shifted by an offset of $n/2$. If A , B , C , and D denote the circulant blocks of a quaternion-type Hadamard matrix, after applying $s^{n/2}$ to the columns with indices in $[0, n)$ and $[n, 2n)$, the resulting Hadamard matrix has the form

$$\begin{bmatrix} A' & B' & C & D \\ -B' & A' & -D & C \\ -C' & D' & A & -B \\ -D' & -C' & B & A \end{bmatrix}.$$

Now, applying $s^{n/2}$ to the rows with indices in $[2n, 3n)$ and $[3n, 4n)$ we obtain

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

which is the Hadamard matrix generated by applying DH to the QT quadruple corresponding to (A, B, C, D) . $\square$

3 Exhaustive searches for QT sequences

In this section, we first describe previous work that has been done on exhaustive search for perfect quaternion sequences, QT sequences, and related problems (see Section 3.1). We then present an algorithm that we used to extend the search for QT sequences to longer lengths in Section 3.2, and explain the implementation and optimization of the algorithm in Section 3.3. After the enumeration is complete, we perform a postprocessing of the results by removing QT sequences that are equivalent up to QT, Williamson-type, and Hadamard equivalence (see Section 3.4). Finally, we summarize the results found by our enumeration in Section 3.5.

3.1 Previous work

In 2010, Kuznetsov [27] studied perfect sequences over $\mathcal{Q}_{24}$ and ran searches for perfect $\mathcal{Q}_{24}$ -sequences equivalent to sequences the form

$$[z, 1, \mathbf{j}, x_0, x_1, \dots, x_t, x_t, \dots, x_1, x_0, \mathbf{j}, 1]$$

where $z \in \mathcal{Q}_{24}$ and $x_0, \dots, x_t \in \mathcal{Q}_8$. Note such sequences are symmetric and this assumption allowed Kuznetsov's search to reach length 23 using a desktop computer for an unspecified amount of time. He discovered sequences of lengths 5, 7, 9, 11, 13, 17, 19, and 23, and used these sequences to create a perfect $\mathcal{Q}_{24}$ -sequence of length over 5 billion. In 2012, Barrera Acevedo and Hall [5] constructed perfect sequences over the alphabet $\{\pm 1, \pm \mathbf{i}, \mathbf{j}\}$ for all lengths of the form $q + 1$ where $q \equiv 1 \pmod{4}$, and q is a prime power. In 2017, Blake [8] ran extensive searches for perfect sequences over $\mathcal{Q}_8$.

In 2019, Barrera Acevedo, Catháin, and Dietrich [6] ran an exhaustive search to find cocyclic Hadamard matrices of prime order $p \leq 13$. One part of

their results include QT sequences directly, though their search also includes quadruples of other types that differ from QT sequences. Their algorithm enumerates the possibilities for three out of the four sequences, and then uses the first three sequences to generate all possibilities for the fourth sequence.

Also in 2019, Bright, Kotsireas, and Ganesh ran a search to find Williamson sequences. Their algorithm separates the four sequences into two pairs, enumerates all the possibilities for these pairs, and then combines the results from the enumeration of the pairs to generate all quadruples of Williamson sequences. We adapt this algorithm to work for QT sequences and show that this approach is more efficient than an approach that starts by enumerating the possibilities for three out of the four sequences.

3.2 An enumeration algorithm for QT sequences

We would like to search for a set of four binary sequences satisfying the autocorrelation and crosscorrelation conditions for QT sequences. The first step of the algorithm we present (Algorithm 1 below) is to look at the “rowsums” of the sequences. For a binary sequence $A = [a_0, \dots, a_{n-1}]$, we define $r_A := \sum_{i=0}^{n-1} a_i$ to be the *rowsum* of A . The following lemma is classic (cf. [43, eq. 15]).

Lemma 11 (Rowsum Decomposition). *If A, B, C, D are a quadruple of QT sequences of length n , then*

$$r_A^2 + r_B^2 + r_C^2 + r_D^2 = 4n.$$

This lemma means that for a given length n , we can limit our search to sequences whose rowsums satisfy a specific rowsum decomposition of $4n$. We compute all possible decompositions of $4n$ as the sum of four integer squares and enumerate the QT sequences for each possible decomposition.

The next part of the algorithm is to pick one decomposition and separate the four sequences into two pairs. Each pair can be used to check the part of the conditions they are required to satisfy as a whole. For example, for all shifts $t \neq 0$ the sum of the autocorrelations of the first pair is required to be the negation of the sum of the autocorrelations of the second pair (since they must add up to zero). We can also apply this reasoning to the crosscorrelation conditions, since once the first pair (say (A, B)) is known, Theorem 9 implies that $R_{A,B}(t) = R_{B,A}(t)$ for all t . Thus, if $R_{A,B}(t) \neq R_{B,A}(t)$ for some t then the pair (A, B) cannot be part of a QT sequence and can be ignored.

Therefore, we enumerate the set of pairs of sequences with rowsums (r_A, r_B) , separately enumerate the pairs of sequences with rowsums (r_C, r_D) , compute their auto- and crosscorrelations, and check if there are pairs of sequences from the first and second enumerations that have autocorrelations that exactly cancel out and crosscorrelations that do not change under a swap. If there are, then we would have found a quadruple of binary sequences satisfying (2.1) and (2.2) and therefore a potential quadruple of QT sequences. To ensure the four sequences are in fact a quadruple of QT sequences, we need to check if they satisfy the other two crosscorrelation conditions (2.3) and (2.4).

The pseudocode for this algorithm is given in Algorithm 1. Intuitively, the reason this algorithm is faster than enumerating triples of QT sequences is because enumerating pairs with rowsums (r_A, r_B) and (r_C, r_D) is faster than enumerating triples with rowsums (r_A, r_B, r_C) . Moreover, the step that finds matches in the correlation values (step 8) is fast in practice when implemented efficiently as described in Section 3.3. In order to shrink the search space and improve efficiency, Algorithm 1 enumerates QT sequences up to Williamson-type equivalence by using only certain decompositions of $4n$ into a sum of four squares that can be assumed without loss of generality (see Proposition 13 for justification). Although Algorithm 1 is guaranteed to enumerate all QT sequences of a given order up to Williamson-type equivalence, in general it generates the multiple quadruples in the same equivalence class. Thus, after running Algorithm 1 we run a postprocessing step (described in Section 3.4) to remove duplicate sequences up to equivalence.

3.3 Implementation and optimizations

One of the most important optimizations to speed up our search for QT sequences is to quickly remove unwanted sequences from consideration. A well-known “filtering” technique enabling the discarding of many sequences is based on the Discrete Fourier Transform (DFT) defined in Section 2.4. Proposition 6 says that if (A, B, C, D) is a quadruple of QT sequences of length n , then

$$\text{PSD}_A(t) + \text{PSD}_B(t) + \text{PSD}_C(t) + \text{PSD}_D(t) = 4n \quad \text{for all } t \in \mathbb{Z}.$$

This property was already used by Williamson [43, eq. 14], except written in the form $\text{DFT}_A(t)^2 + \text{DFT}_B(t)^2 + \text{DFT}_C(t)^2 + \text{DFT}_D(t)^2 = 4n$ because

Algorithm 1 Algorithm for enumerating QT sequences of a given order n up to Williamson-type equivalence.

```

1:  $\mathcal{L} := \emptyset$  // Set that will contain the QT sequences found
2: // Decompose  $4n$  as a sum of four nonnegative integer squares
    $\mathcal{D} := \{ (w, x, y, z) \in \mathbb{N}^4 : w^2 + x^2 + y^2 + z^2 = 4n \text{ and } w \geq x \geq y \geq z \}$ 
3: for  $(w, x, y, z) \in \mathcal{D}$  do
4:   Construct  $\mathcal{W}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$ , the sets of binary sequences with rowsums
     equal to  $w, x, y, z$ , respectively
5:    $\mathcal{L}_1 := \mathcal{W} \times \mathcal{Z}$  and  $\mathcal{L}_2 := \mathcal{X} \times \mathcal{Y}$ 
6:   // Compute autocorrelations of each candidate pair in  $\mathcal{L}_1$ 
     Compute  $[R_W(t) + R_Z(t) : 1 \leq t \leq n/2]$  for all  $(W, Z) \in \mathcal{L}_1$  with
      $R_{W,Z}(t) = R_{Z,W}(t)$  for all  $1 \leq t \leq n/2$  and store in a list  $C_1$ 
7:   // Compute negated autocorrelations of each candidate pair in  $\mathcal{L}_2$ 
     Compute  $[-R_X(t) - R_Y(t) : 1 \leq t \leq n/2]$  for all  $(X, Y) \in \mathcal{L}_2$  with
      $R_{X,Y}(t) = R_{Y,X}(t)$  for all  $1 \leq t \leq n/2$  and store in a list  $C_2$ 
     // Matching vectors in  $C_1$  and  $C_2$  provide solutions of (2.1) and (2.4)
8:   for each list of values  $v$  appearing in both  $C_1$  and  $C_2$  do
9:     Get the set  $\mathcal{S}$  of all the quadruples of sequences generating  $v$  in both
       lists  $C_1$  and  $C_2$ 
10:    for each quadruple  $(W, X, Y, Z)$  in  $\mathcal{S}$  do
11:      if  $(W, X, Y, Z)$  is a quadruple of QT sequences then
12:        Add  $(W, X, Y, Z)$  to  $\mathcal{L}$ 
13:      end if
14:    end for
15:  end for
16: end for
17: return  $\mathcal{L}$ 

```

Williamson assumed the symmetry of sequences (and if X is conjugate symmetric then $\text{PSD}_X(t) = \text{DFT}_X(t)^2$).

Corollary 12. *If (A, B, C, D) is a quadruple of QT sequences of length n , then*

$$\text{PSD}_A(t) + \text{PSD}_B(t) \leq 4n \text{ and } \text{PSD}_C(t) + \text{PSD}_D(t) \leq 4n.$$

Proof. Follows from Proposition 6 since PSDs are nonnegative. $\square$

Corollary 12 is applied as a filter on step 5 of Algorithm 1; if any pair has a PSD value sum that is larger than $4n$ it is not included in $\mathcal{L}_1$ or $\mathcal{L}_2$. Similarly, on step 4 any sequence that has a PSD value larger than $4n$ is not included in $\mathcal{W}$, $\mathcal{X}$, $\mathcal{Y}$, or $\mathcal{Z}$. In our implementation, the PSD values were computed using FFTW [18].

For step 2, finding all decompositions of $4n$ into a sum of four integer squares can be done with brute force, but not all decompositions are necessary. One immediate optimization is to only consider decompositions (w, x, y, z) where the parities of w , x , y , and z match the parity of n , because if $X \in \{\pm 1\}^n$ then $r_X \equiv n \pmod{2}$. The following proposition gives justification for why it is sufficient to only consider nonnegative decompositions in sorted order.

Proposition 13. *Every quadruple of QT sequences is Williamson-type equivalent to a quadruple whose rowsums are of the form (w, x, y, z) where $w \geq x \geq y \geq z \geq 0$.*

Proof. By applying the SN operation, every QT sequence can be made equivalent to one in which all rowsums are nonnegative. By then applying the SS operation those rowsums can then be sorted in descending order while preserving the nonnegativity of the rowsums. Thus, every QT sequence is equivalent to one with nonnegative rowsums sorted in descending order. $\square$

The following proposition provides a variant of Proposition 13 but in terms of QT equivalence instead of Williamson-type equivalence.

Proposition 14. *Every quadruple of QT sequences is QT equivalent to a quadruple whose rowsums are of the form $(\pm w, x, y, z)$ where $w \geq x \geq y \geq z \geq 0$. Furthermore, if $w = x$, $x = y$, $y = z$, or $z = 0$, then the sign of the first rowsum can additionally be taken to be positive.*

Proof. By applying appropriate DN and DS operations, every QT sequence can be made equivalent to one in which the last three rowsums are all nonnegative and sorted in decreasing order and the first rowsum is the largest or second largest rowsum in absolute value. By applying the NS operation, one can also sort the first two rowsums by absolute value (by swapping the first two sequences, if necessary, then negating them), so any QT sequence is equivalent to one with a rowsum decomposition of the form $(\pm w, x, y, z)$ where $w \geq x \geq y \geq z \geq 0$. Furthermore, in cases where $z = 0$ one can apply the DN operation to make the first rowsum positive while keeping the rowsums in sorted order (by negating the first and last sequences). Similarly, if at least two values in $\{w, x, y, z\}$ are equal, one can apply the NS operation to make the first rowsum positive while keeping the rowsums in sorted order (by negating the first sequence then swapping the sequences with equal rowsums). So if $z = 0$ or $w = x$ or $x = y$ or $y = z$, the decomposition $(-w, x, y, z)$ can be avoided. $\square$

In case one wants to modify Algorithm 1 to enumerate QT sequences up to QT equivalence (instead of Williamson-type equivalence), an efficient way to do this would be to modify step 12: after adding (W, X, Y, Z) to $\mathcal{L}$, also add $(-W, X, Y, Z)$ to $\mathcal{L}$, though this would only need to be done in cases when $z \neq 0$, $z \neq y$, $y \neq x$, and $x \neq w$. Proposition 14 guarantees in cases when $w = x$ or $x = y$ or $y = z$ or $z = 0$ that Algorithm 1 generates all QT sequences up to QT equivalence.

For step 5, we choose to generate the pairs so that the largest and smallest rowsums w and z belong to the same pair. We attempted all possible pairing combinations and found this to be the most efficient.

By Theorem 9, all QT sequences satisfy $R_{X,Y}(t) = R_{Y,X}(t)$ and $R_{W,Z}(t) = R_{Z,W}(t)$, so any pairs not satisfying these amicability conditions are not considered in steps 6 and 7. This filter dramatically reduces the number of pairs added to the lists C_1 and C_2 . For example, in length 20, over 16 billion pairs are generated without this filter, while only 625,896 are generated using it—reducing the number of pairs generated by a factor of about 26,000.

For steps 6 and 7, the reason one does not need to consider the correlation values at $t = 0$ is because the autocorrelation at $t = 0$ is the rowsum of the sequence (which has already been fixed by construction) and the crosscorrelation difference $R_{X,Y}(0) - R_{Y,X}(0)$ is always zero for real sequences X and Y . Similarly, the reason the correlation values for $n/2 < t < n$ do not need to be considered is because of the symmetries $R_X(t) = R_X(n - t)$ and

$R_{X,Y}(t) = R_{Y,X}(n-t)$ for real sequences X and Y .

For steps 6 and 7, we store the list of autocorrelation values generated by one pair as one line in a file, and we store the indices of the sequences used to generate those values at the end of the line. This way, we can quickly determine which pair the correlation values on each line was derived from, even after the lines of the files have been permuted.

In order to implement step 8 efficiently, we sort the lines of the files containing the correlation values by lexicographic order. This way, we iterate through the files simultaneously using a linear scan to efficiently find all matching correlation values from the file containing the list C_1 and the file containing the list C_2 . We test all matches and keep the ones that satisfy the three crosscorrelation conditions.

Computing the correlation vectors in steps 6 and 7 using the straightforward approach uses $O(n^2)$ arithmetic operations. An optimization is to match PSD values instead of matching correlation values. That is, instead of finding matches where

$$[R_W(t) + R_Z(t) : 1 \leq t \leq n/2] = [-R_X(t) - R_Y(t) : 1 \leq t \leq n/2],$$

by Proposition 6 it is sufficient to find matches where

$$[\text{PSD}_W(t) + \text{PSD}_Z(t) : 1 \leq t \leq n/2] = [4n - \text{PSD}_X(t) - \text{PSD}_Y(t) : 1 \leq t \leq n/2].$$

The PSD values were already computed as a part of the filtering used in step 4 and these values can be cached, so that they do not need to be recomputed. In general PSD values are real and not integers, so in order to write the value of $\text{PSD}_W(t) + \text{PSD}_Z(t)$ and $4n - \text{PSD}_X(t) - \text{PSD}_Y(t)$ to a file we round them to the nearest integer. This has the downside of potentially introducing spurious matches. However, in practice this is not a problem and once a match is found it can be checked easily if (2.1) holds or not.

Similarly, instead of verifying the conditions $R_{W,Z}(t) = R_{Z,W}(t)$ and $R_{X,Y}(t) = R_{Y,X}(t)$ in steps 6 and 7 it is sufficient to work in the frequency domain and instead verify

$$\text{CPSD}_{W,Z}(t) = \text{CPSD}_{Z,W}(t) \quad \text{and} \quad \text{CPSD}_{X,Y}(t) = \text{CPSD}_{Y,X}(t).$$

This is beneficial as the calculation of the CPSD values can be optimized by caching the values $\text{DFT}_W(t)$, $\text{DFT}_X(t)$, $\text{DFT}_Y(t)$, $\text{DFT}_Z(t)$ for $1 \leq t \leq n/2$

in step 4. In order to account for floating-point roundoff error we filter pairs (W, Z) for which there is some t with

$$|\text{CPSD}_{W,Z}(t) - \text{CPSD}_{Z,W}(t)| > 10^{-4},$$

since FFTW will compute the CPSD values many orders of magnitude more accurately than 10^{-4} . The $\text{CPSD}_{W,Z}(t) - \text{CPSD}_{Z,W}(t)$ values have no real component, because they are of the form $ab^* - ba^*$ for complex a, b and as noted in Section 2.4 such numbers have no real component.

3.4 Equivalence filtering

After enumerating all QT sequences of length n using Algorithm 1, we classify the sequences up to Hadamard equivalence (as described in Section 2.2) as well as QT and Williamson-type equivalence (as described in Section 2.5). Algorithm 1 will generate all QT sequences of length n whose rowsums are in a form given by Proposition 13. Because Proposition 13 was proven only using the SS and SN operations, Algorithm 1 will produce at least one quadruple of QT sequences from each Williamson-type equivalence class. However, if we also want to enumerate QT sequences up to Hadamard equivalence, we need to enumerate up to QT equivalence instead, because then Theorem 10 implies the list will be complete up to Hadamard equivalence. In Section 3.3, we describe how to modify Algorithm 1 to enumerate sequences up to QT equivalence (see the remark after Proposition 14). We now describe how to filter out any duplicates up to QT equivalence.

As a first step in the equivalence filtering process we take the output of Algorithm 1 and filter its output to keep exactly one “canonical” representative of every NS equivalence class. The canonical representative of an equivalence class will be its lexicographically minimal quadruple when the sequences in a quadruple of QT sequences are concatenated. In order to find the lexicographic minimum, we first use the NS operation to make the initial entry of each sequence in the quadruple -1 . Next, we use a DS operation to make the lexicographically least sequence appear first in the quadruple and the lexicographically second-least sequence appear second in the quadruple. If all sequences now appear in lexicographically ascending order, the quadruple of QT sequences is canonical. Otherwise, the last two sequences appear out of order. If there are two identical sequences in the quadruple then we use the DS operation to swap the identical sequences and swap the third and fourth

sequences, sorting the sequences in the quadruple in ascending order and making the quadruple canonical. If there are not two identical sequences in the quadruple we use the NS operation to swap the third and fourth sequences and finally negate the fourth sequence to make the quadruple canonical.

Using the above process we compute the canonical representative of each quadruple of QT sequences found by Algorithm 1 and discard quadruples whose canonical form have been seen before, thereby producing a complete list of QT sequences up to NS equivalence. Now, we want to filter this list up to the QT equivalences of Section 2.5. To do this, we adapt a filtering algorithm described by Lumsden, Kotsireas, and Bright [29, Alg. 7]. First, consider the symmetry group S generated by the AN, DE, CS, and DH operations (letting φ denote the Euler totient function, this group is of size $2^6 n \varphi(n)$ when n is even and not divisible by 4, of size $2^4 n \varphi(n)$ when n is divisible by 4, and of size $n \varphi(n)$ when n is odd). To find the lexicographically minimal representative of a quadruple of QT sequences (W, X, Y, Z) we apply all operations in S to (W, X, Y, Z) , thereby forming $|S|$ QT sequences, and use the above sorting process to lexicographically minimize each QT sequence using the NS operation. The global lexicographic minimum of these $|S|$ sequences becomes the minimal representative of the equivalence class generated by the operations in $\{\text{NS}, \text{AN}, \text{DE}, \text{CS}, \text{DH}\}$.

We also filter the list up to Hadamard equivalence. By Theorem 10, we know that the filtered list computed above contains at least one representative from every Hadamard equivalence class. However, more filtering may be necessary to remove duplicates up to Hadamard equivalence. Starting from the complete list of quadruples up to QT equivalence we convert each quadruple of QT sequences into a Hadamard matrix and reduce the matrix to its graph representation as described by McKay [30]. Then we use the program NAUTY [31] to convert each graph into a canonical form. Two graphs have the same canonical form if and only if they are isomorphic, so we filter any QT sequence that results in a graph whose canonical form has been seen before.

The process for filtering up to QT equivalence described above can also be used to filter up to Williamson-type equivalence, except we use single-swap (SS) and single-negate (SN) operations instead of negate-and-swap (NS) operations, and similarly use the single half shift (SH) instead of the double half shift (DS). In this case the canonical representative found with the $\{\text{SS}, \text{SN}\}$ operations will always have each sequence sorted in lexicographically decreasing order and the initial entry of each sequence will be -1 .

In practice, to enumerate QT sequences up to each of Williamson-type

equivalence, QT equivalence, and Hadamard equivalence we do the following.

1. Enumerate sequences up to Williamson-type equivalence using Algorithm 1 and place them in a list.
2. Filter the list by Williamson-type equivalence to remove duplicate quadruples up to equivalence.
3. For each (W, X, Y, Z) in the list, add $(-W, X, Y, Z)$ to the list. Following this, if n is even, for each (W, X, Y, Z) in the list, add $(s^{n/2}(W), X, Y, Z)$ to the list.
4. Filter the list up to QT equivalence. This list will be exhaustive up to QT equivalence because each NS equivalence class splits into at most two classes under $\{SS, SN\}$ equivalence, and when it does split (W, X, Y, Z) and $(-W, X, Y, Z)$ will be in separate classes. Similarly, each DH equivalence class splits into at most two classes under SH equivalence, and when it does split (W, X, Y, Z) and $(s^{n/2}(W), X, Y, Z)$ will be in separate classes.
5. Filter the list up to Hadamard equivalence.

3.5 Results

We implemented the algorithm in Rust 1.91.0 and Bash shell scripts. The algorithm was run on a machine with an AMD EPYC CPU running at 2.7 GHz and configured to use no more than 4 GiB of RAM. Sorting was done using the GNU sort utility. The code and the results for the algorithm can be found at <https://github.com/colinotp/quaternion-sequences>. A summary of the results found by the algorithm is provided in Table 1.

In the appendix we provide the complete enumeration of all 124 sets of QT sequences (up to Williamson-type equivalence) for lengths $n \leq 21$ found by our implementation. By combining the enumerations of Holzmann, Kharaghani, and Tayfeh-Rezaie [25] and Bright, Kotsireas, and Ganesh [10] all sets of Williamson sequences (i.e., *symmetric* QT sequences) are known for $n \leq 60$. Up to Williamson-type equivalence, it was previously determined that there are exactly 94 sets of Williamson sequences for $n \leq 21$ and our search confirms this amount. Moreover, it determines there are an additional 30 sets of QT sequences for lengths $n \leq 21$ that are *not* equivalent to Williamson

Table 1: Table of results for Algorithm 1 by length n . W_{equ} , Q_{equ} , and H_{equ} indicate the total number of QT sequences found up to Williamson-type, QT, and Hadamard equivalence, respectively. “Time” is the total enumeration runtime in seconds, “Pairs” is the total number of pairs generated in step 5 (generating these is the bottleneck of the algorithm), and “Space” is the amount of disk space used in MiB.

n	W_{equ}	Q_{equ}	H_{equ}	Time (s)	Pairs	Space
1	1	1	1	0.16	2	0.0
2	1	1	1	0.08	4	0.0
3	1	1	1	0.08	6	0.0
4	2	3	2	0.19	46	0.0
5	1	1	1	0.08	20	0.0
6	1	1	1	0.16	48	0.0
7	2	3	3	0.15	182	0.0
8	3	4	3	0.08	384	0.0
9	4	7	7	0.31	999	0.0
10	2	4	2	0.23	770	0.0
11	1	2	2	0.15	715	0.0
12	5	10	6	0.80	6288	0.2
13	4	6	6	3.14	8216	0.4
14	5	12	10	3.15	5334	0.3
15	4	7	7	23.46	15732	1.0
16	18	44	19	121.20	206480	7.9
17	4	5	5	361.36	39372	3.6
18	28	88	82	2001.79	275184	17.5
19	6	11	11	7753.85	200526	22.0
20	24	84	54	17632.48	625896	46.1
21	7	13	13	141267.63	561519	86.1

sequences because they are only equivalent to sets of sequences that are non-symmetric.

Interestingly, Fitzpatrick and O’Keeffe [16] prove that for certain odd lengths n (when n is prime or of the form $n = pq$ for distinct odd primes p and q with each a generator of the other) that *all* sets of Williamson-type sequences of length n must be Williamson-type equivalent to a set of symmetric sequences. For $n \leq 21$, the only odd lengths not covered by their theorem are $n = 9$ and $n = 21 = 3 \cdot 7$ (because 7 is not a generator modulo 3). Our search reveals that their theorem also holds for $n = 21$, because we find no non-symmetric QT sequences of length 21. For $n = 9$, a set of non-symmetric QT sequences exists; an example was already known to Fitzpatrick and O’Keeffe, and our enumeration shows up to Williamson-type equivalence this is the *only* set of non-symmetric QT sequences of length 9. This is currently the only known set of Williamson-type sequences of odd length that is not equivalent to a set of symmetric sequences, though we find 29 examples of sets of Williamson-type sequences of even length that are not equivalent to a set of symmetric sequences.

Fitzpatrick and O’Keeffe’s result combined with the exhaustive search for Williamson sequences of length $n = 23$ by Baumert and Hall [7] implies that there is exactly one set of QT sequences of length 23 up to Williamson-type equivalence. We found this set generates two inequivalent sets of QT sequences up to QT equivalence and Hadamard equivalence.

4 Construction of quaternionic Hadamard matrices

Perfect sequences correspond in a straightforward manner to Hadamard matrices. As explained in Section 1.3, such matrices are of interest in communication and information theory. This further motivates a deeper study of quaternionic Hadamard matrices (QHMs). The new sequences discovered through the computational search in Section 3 yield new quaternionic Hadamard matrices. We provide examples of such matrices of interest in quantum communication in Section 4.1. In contrast to the real and complex cases, these matrices may be used to generate uncountably many (equivalent) QHMs; see Section 4.2. In Section 4.3, we propose an approach for characterizing QHMs and illustrate it in the case of order five matrices. In Section 4.4, we formally establish

the nonequivalence of matrices resulting from the computational search for perfect sequences.

4.1 Hadamard matrices from perfect sequences

Perfect quaternion sequences can be used to generate quaternionic Hadamard matrices in a straightforward manner. Given such a sequence S of length n , we may construct an $n \times n$ circulant quaternionic Hadamard matrix M by taking the first row of the matrix to be the sequence S , and the rest of the rows to be successive cyclic shifts of the first row. Formally, we define $M_{ij} := S_{j-i}$ for $0 \leq i, j < n$, where we take the indices to be modulo n .

As explained in Section 3.5, our computational search produces numerous examples of perfect quaternion sequences that are of interest in quantum information and communication. Consider the quaternionic Hadamard matrices derived from these sequences as described above, and the equivalent normalized matrices. (Recall that normalization is the process of transforming their first row and column to all 1s via equivalence operations.) We obtain normalized quaternionic Hadamard matrices with non-commuting entries for all lengths n with $3 < n \leq 21$ in the search described in Section 3.5.

Below we list a few examples of the matrices we find. The entries are described using symbols given by the mapping

$$\begin{bmatrix} + & - & \mathbf{i} & \mathbf{j} & \mathbf{k} & \mathbf{q} & \mathbf{x} & \mathbf{y} & \mathbf{z} & \mathbf{s} & \mathbf{u} & \mathbf{v} & \mathbf{w} \\ 1 & -1 & \mathbf{i} & \mathbf{j} & \mathbf{k} & \mathbf{q} & \mathbf{qi} & \mathbf{qj} & \mathbf{qk} & \mathbf{q}^* & \mathbf{q}^*\mathbf{i} & \mathbf{q}^*\mathbf{j} & \mathbf{q}^*\mathbf{k} \end{bmatrix}, \quad (4.1)$$

with a capital letter standing for the negation of the quaternion represented by the same letter in lower case. For example, $\mathbf{X}$ denotes $-\mathbf{qi}$. Normalized

quaternionic Hadamard matrices for orders 6, 8, 10, and 12 are given by

$$\begin{aligned}
& \begin{bmatrix} + & + & + & + & + & + \\ + & s & Q & k & S & x \\ + & z & S & + & Q & U \\ + & - & + & - & + & - \\ + & S & Q & K & S & X \\ + & Z & S & - & Q & u \end{bmatrix}, \quad \begin{bmatrix} + & + & + & + & + & + & + \\ + & Y & I & q & - & y & i & Q \\ + & I & - & i & + & I & - & i \\ + & q & i & Y & - & Q & I & y \\ + & - & + & - & + & - & + & - \\ + & y & I & Q & - & Y & i & q \\ + & i & - & I & + & i & - & I \\ + & Q & i & y & - & q & I & Y \end{bmatrix}, \\
& \begin{bmatrix} + & + & + & + & + & + & + & + & + & + \\ + & J & + & Y & U & - & j & - & y & u \\ + & Q & q & W & y & + & Q & q & W & y \\ + & w & J & Z & + & - & W & j & z & - \\ + & j & U & z & J & + & j & U & z & J \\ + & - & - & j & - & - & + & + & J & + \\ + & J & - & y & v & + & J & - & y & v \\ + & Y & y & V & q & - & y & Y & v & Q \\ + & S & J & Z & - & + & S & J & Z & - \\ + & j & v & z & J & - & J & V & Z & j \end{bmatrix}, \quad \begin{bmatrix} + & + & + & + & + & + & + & + & + & + \\ + & W & Y & - & W & y & - & w & y & + & w & Y \\ + & Y & W & - & y & w & + & Y & W & - & y & w \\ + & - & - & + & + & - & - & + & + & - & - & + \\ + & W & y & + & W & y & + & W & y & + & W & y \\ + & y & w & - & y & W & - & Y & W & + & Y & w \\ + & - & + & - & + & - & + & - & + & - & + & - \\ + & w & Y & + & W & Y & - & W & y & - & w & y \\ + & y & W & + & y & W & + & y & W & + & y & W \\ + & + & - & - & + & + & - & - & + & + & - & - \\ + & w & y & - & W & Y & + & w & y & - & W & Y \\ + & Y & w & + & y & w & - & y & W & - & Y & W \end{bmatrix}.
\end{aligned}$$

These matrices may be used to generate infinite families of Hadamard matrices via algebra automorphisms of the quaternions, as explained in more detail in Section 4.2. They may also be used to characterize matrices with the same pattern of entries as in Section 4.3. However, the matrices so generated may not include all the quaternionic Hadamard matrices of a given order. We examine this possibility later in the section.

4.2 Infinite families of fixed order

For a fixed real or complex Hadamard matrix M , there are only a finite number of distinct normalized matrices equivalent to M .

Lemma 15. *Suppose M is a real (or complex) Hadamard matrix. The number of normalized real (respectively, complex) Hadamard matrices which are equivalent to M is finite.*

Proof. By Lemma 1 and the note following it, any matrix M' equivalent to M may be written as $D_1 P_1 M P_2 D_2$, where P_1 and P_2 are permutation matrices, and D_1 and D_2 are diagonal matrices of unit real or complex numbers. The lemma is immediate for real matrices, as the number of matrices D_1 , D_2 , P_1 , and P_2 as above is finite. We prove the lemma for complex matrices.

Let $M'' := P_1 M P_2$. There are a finite number of such matrices M'' obtained by permuting row and columns of M . Suppose $M'' = (x_{ij} : 0 \leq i, j < n)$. Then normalizing M'' gives us the matrix $N'' := (x_{i0}^* x_{ij} x_{0j}^* : 0 \leq i, j < n)$.

Suppose $D_1 = \text{diag}(a)$ and $D_2 = \text{diag}(b)$. Then $M' = (a_i x_{ij} b_j : 0 \leq i, j < n)$, and normalizing M' gives us the matrix $N' := (b_0^* x_{i0}^* x_{ij} x_{0j}^* a_0^* : 0 \leq i, j < n)$. Since the first row of N' is all 1, we have $b_0^* x_{00}^* a_0^* = 1$, i.e., $b_0^* = a_0 x_{00}$. So $N' = (a_0 x_{00} x_{i0}^* x_{ij} x_{0j}^* a_0^* : 0 \leq i, j < n)$. As complex multiplication is commutative, the entries of N' simplify: $N' = (x_{00} x_{i0}^* x_{ij} x_{0j}^* : 0 \leq i, j < n) = x_{00} N''$. Since the number of distinct matrices M'' (and therefore N'') is finite and x_{00} is an entry of M'' , the number of matrices N' is also finite. $\square$

We now show that uncountably infinite families of normalized QHM of order n exist whenever there is a normalized QHM of order n with a nonreal entry. We begin with a characterization of automorphisms of the quaternions. Any such automorphism corresponds to an orthogonal transformation (more specifically, a rotation) in the real vector space spanned by the basic unit quaternions $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$.

Theorem 16 (Theorem 2.4.4, page 17, [32]). *The group of automorphisms of the quaternions is isomorphic to $\text{SO}(3)$, the Special Orthogonal Group in three dimensions (i.e., rotations of the two-sphere).*

This implies that for any pair of pure imaginary quaternions a, b of the same norm, there is an automorphism that maps a to b . This property helps show the following.

Proposition 17. *Suppose G is a normalized QHM of order n with at least one non-real entry. There are an uncountably infinite number of normalized QHM of order n that are equivalent to G .*

Proof. Let $\alpha + w$ be an entry of G with real part α and non-zero pure imaginary part w .

Let S be the set of all normalized quaternionic Hadamard matrices that are equivalent to G . Suppose for the sake of contradiction that S is countable. Let Q be the set of quaternions x such that x is an entry of some matrix

in S . The set Q is also countable. The set of pure imaginary quaternions with the same norm as w form a sphere of radius $\|w\|$ in $\text{span}\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$. Thus there is a pure imaginary quaternion y with $\|y\| = \|w\|$ that is different from the imaginary part of any quaternion in Q . By Theorem 16, there is an automorphism f of $\mathbb{H}$ that maps w to y . By Proposition 2, there is a pure imaginary unit quaternion a such that $f(x) = a^*xa$ for every x . So $f(G)$ is a QHM that is equivalent to G . By construction, the matrix $f(G)$ has an entry which is not contained in Q , so $f(G) \notin S$. This is a contradiction, hence S is uncountably infinite. $\square$

Thus the Hadamard matrices listed in Section 4.1 lead to infinite families of (equivalent) quaternionic Hadamard matrices. The appendix lists the perfect quaternion sequences corresponding to nonequivalent QT sequences of length up to 21. The normalized QHMs derived from perfect sequences found by our computational search typically contain non-real entries, and hence also lead to infinite equivalence classes of QHMs. As illustrated by the examples in Section 4.1, the normalized matrices typically also have noncommuting entries. Such QHMs lead to MUMs of interest in quantum communication theory [15].

4.3 Quaternionic Hadamard matrices of order five

Chterental and Đoković [12] identified all quaternionic Hadamard matrices of order four, characterizing them in terms of two parametrized families of QHMs. They posed the characterization of quaternionic Hadamard matrices of order five as an open problem. Higginbotham and Worley [24] make progress on this problem by studying a specific type of normalized order five QHMs with a circulant core, where the *core* of a normalized matrix is obtained by deleting its first row and column.

Since characterizing all 5×5 quaternionic Hadamard matrices appears to be challenging, a natural approach to take is to study matrices with a fixed pattern of entries. This approach appears to be feasible, and we illustrate it with an example. Our analysis of this example will ultimately allow us to prove (see Section 4.4) that the infinite family of QHMs produced by the single (up to QT equivalence) quadruple of QT sequences of order five is *not* equivalent to the QHMs considered by Higginbotham and Worley [24].

Consider the 5×5 quaternionic Hadamard matrix

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & c\mathbf{j} + s\mathbf{i} & c\mathbf{j} - s\mathbf{i} & \mathbf{j} \\ 1 & c\mathbf{j} + s\mathbf{i} & -1 & \mathbf{j} & c\mathbf{j} - s\mathbf{i} \\ 1 & c\mathbf{j} - s\mathbf{i} & \mathbf{j} & -1 & c\mathbf{j} + s\mathbf{i} \\ 1 & \mathbf{j} & c\mathbf{j} - s\mathbf{i} & c\mathbf{j} + s\mathbf{i} & -1 \end{bmatrix} \quad (4.2)$$

with $c := \cos(\frac{2\pi}{3})$ and $s := \sin(\frac{2\pi}{3})$. This corresponds to the 5×5 Hadamard matrix of 2×2 unitary operators reported by Tavakoli *et al.* [37], via the $\mathbb{R}$ -linear extension of the anti-homomorphism mapping

$$1 \leftrightarrow I, \quad \mathbf{i} \leftrightarrow -i\sigma_x, \quad \mathbf{j} \leftrightarrow -i\sigma_y, \quad \mathbf{k} \leftrightarrow i\sigma_z, \quad (4.3)$$

where $I, \sigma_x, \sigma_y, \sigma_z$ are the 2×2 Pauli operators

$$I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \text{and} \quad \sigma_z := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

and $i := \sqrt{-1}$ is the complex square root of -1 (see [15, Section II.D] for the details). A similar QHM was presented by Higginbotham and Worley [24, Example 3] as an example of an order five QHM with a non-circulant core. In fact, it follows from Theorem 19 below that the QHM in [24, Example 3] is equivalent to (4.2).

The matrix (4.2) has the same pattern of entries as in the matrix

$$G(a, b, c) := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & a & b & c \\ 1 & a & -1 & c & b \\ 1 & b & c & -1 & a \\ 1 & c & b & a & -1 \end{bmatrix}, \quad (4.4)$$

where $a, b, c \in \mathbb{S}^3$ are unit quaternions. We would like to characterize a, b , and c such that $G(a, b, c)$ a Hadamard matrix. We begin with a simple property of quaternions.

Lemma 18. *Let $a, b \in \mathbb{S}^3$ be unit quaternions such that*

$$1 + a + b = 0. \quad (4.5)$$

Then there is a quaternionic square root w of -1 , i.e., $w \in \mathbb{S}^2$, such that $a = e^{\frac{2\pi}{3}w}$ and $b = e^{\frac{4\pi}{3}w}$. In other words, a and b are non-trivial quaternionic cube-roots of 1 and $b = a^2$.

Proof. Let us write $a = a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}$ and $b = b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}$. Eq. (4.5) is equivalent to

$$\begin{aligned} a_1 + b_1 &= -1 \quad \text{and} \\ a_i &= -b_i \quad \text{for } i \in \{2, 3, 4\}. \end{aligned} \tag{4.6}$$

Furthermore, since a and b are unit quaternions, we have $1 = \|a\| = \|b\|$, i.e., $1 = a_1^2 + a_2^2 + a_3^2 + a_4^2 = b_1^2 + b_2^2 + b_3^2 + b_4^2$. Since $a_i^2 = b_i^2$ for $i > 1$ by (4.6), we have $a_1^2 = b_1^2$. Thus $a_1 = b_1 = -\frac{1}{2}$ and $b = a^*$. Define $w := \frac{2}{\sqrt{3}}(a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k})$. We see that $\|w\|^2 = \frac{4}{3}(a_2^2 + a_3^2 + a_4^2) = \frac{4}{3}(1 - a_1^2) = 1$. So $w \in \mathbf{S}^2$. Moreover, according to the Euler formula for quaternions, $e^{\frac{2\pi}{3}w} = \cos(\frac{2\pi}{3}) + w \sin(\frac{2\pi}{3}) = a$. Similarly, $b = e^{\frac{4\pi}{3}w}$. $\square$

We may verify that the converse also holds. That is, for any non-trivial quaternionic cube-root a of 1 ($a^3 = 1$ and $a \neq 1$) we have $1 + a + a^2 = 0$. Using this property, we determine precisely when $G(a, b, c)$ is a Hadamard matrix.

Theorem 19. *Consider the matrix $G(a, b, c)$ defined in Eq. (4.4), where a, b, c are unit quaternions. Suppose $G(a, b, c)$ is a Hadamard matrix. Then up to an automorphism of $\mathbb{H}$, it equals*

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & \mathbf{i} & \mathbf{i}e^{\frac{2\pi}{3}\mathbf{j}} & \mathbf{i}e^{\frac{4\pi}{3}\mathbf{j}} \\ 1 & \mathbf{i} & -1 & \mathbf{i}e^{\frac{4\pi}{3}\mathbf{j}} & \mathbf{i}e^{\frac{2\pi}{3}\mathbf{j}} \\ 1 & \mathbf{i}e^{\frac{2\pi}{3}\mathbf{j}} & \mathbf{i}e^{\frac{4\pi}{3}\mathbf{j}} & -1 & \mathbf{i} \\ 1 & \mathbf{i}e^{\frac{4\pi}{3}\mathbf{j}} & \mathbf{i}e^{\frac{2\pi}{3}\mathbf{j}} & \mathbf{i} & -1 \end{bmatrix}, \tag{4.7}$$

i.e., $G(a, b, c)$ is equivalent to the matrix (4.7).

Proof. For ease of notation, we abbreviate $G(a, b, c)$ by M . Suppose M is a Hadamard matrix. Let M_i denote the i th row of M for $0 \leq i < 5$. The condition $MM^* = 5I_5$ is equivalent to the row-orthogonality conditions $M_i M_j^* = 5\delta_{ij}$, for all $0 \leq i, j < 5$.

From $M_2 M_1^* = 0$, we get $a + b + c = 0$, i.e., $a(1 + a^*b + a^*c) = 0$. According to Lemma 18, there is a quaternionic square-root of -1 , $w \in \mathbf{S}^2$, such that $b = a e^{\frac{2\pi}{3}w}$ and $c = a e^{\frac{4\pi}{3}w}$. The orthogonality of rows M_2 and M_3 along with

the relationship between a , b , and c gives

$$\begin{aligned}
& 1 - a^* - a + bc^* + cb^* &= 0 \\
\iff & 1 - 2\operatorname{Re}(a) + a e^{-\frac{2\pi}{3}w} a^* + a e^{\frac{2\pi}{3}w} a^* &= 0 \\
\iff & 1 - 2\operatorname{Re}(a) + a(2\cos(\frac{2\pi}{3}))a^* &= 0 \\
\iff & 1 - 2\operatorname{Re}(a) - \|a\|^2 &= 0 \\
\iff & \operatorname{Re}(a) &= 0.
\end{aligned}$$

Therefore, $a \in \mathbb{S}^2$.

From $M_2 M_4^* = 0$, which is the same as $M_3 M_5^* = 0$, we get

$$\begin{aligned}
& 1 - b^* - ac^* - b + ca^* &= 0 \\
\iff & 1 - 2\operatorname{Re}(b) + a e^{-\frac{4\pi}{3}w} a^* + a e^{\frac{4\pi}{3}w} a^* &= 0 \\
\iff & 1 - 2\operatorname{Re}(b) - aa^* &= 0 \\
\iff & \operatorname{Re}(a e^{\frac{2\pi}{3}w}) &= 0 \\
\iff & \operatorname{Re}(a(-\frac{1}{2} + \frac{\sqrt{3}}{2}w)) &= 0 \\
\iff & \operatorname{Re}(aw) &= 0,
\end{aligned}$$

since $\operatorname{Re}(a) = 0$.

Define $x := aw$. The above derivation shows that $x \in \mathbb{S}^2$, so $x^* = -x = -aw$. Since $a, w \in \mathbb{S}^2$, we also have $-aw = x^* = w^* a^* = (-w)(-a) = wa$. That is, a and w are pure imaginary unit quaternions that anticommute. In other words, a , w , and x satisfy the same relations as $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$, and there is an automorphism f of $\mathbb{H}$ given by the mapping

$$a \leftrightarrow \mathbf{i}, \quad w \leftrightarrow \mathbf{j}, \quad \text{and} \quad x \leftrightarrow \mathbf{k}.$$

Up to the automorphism f , the matrix M equals (4.7). We may verify that the matrix (4.7) satisfies all the remaining row orthogonality conditions, and is therefore a Hadamard matrix. $\square$

Thus, all quaternionic Hadamard matrices of the form $G(a, b, c)$ are generated from the matrix $G(\mathbf{i}, \mathbf{i} e^{\frac{2\pi}{3}\mathbf{j}}, \mathbf{i} e^{\frac{4\pi}{3}\mathbf{j}})$ by automorphisms of the quaternions. By Corollary 3, automorphisms of the quaternions preserve QHM equivalence, so all QHMs of the form $G(a, b, c)$ are equivalent. Since $G(a, b, c)$ is equivalent to the QHM in [24, Example 3] (by swapping the second row with the second-last row and the middle row with the last row), the family of QHMs of order five with non-circulant core considered by Higginbotham and Worley [24] are also equivalent to QHMs of the form $G(a, b, c)$. This kind of analysis may be a good starting point for a complete characterization of order five QHMs.

4.4 Nonequivalent QHMs of small order

The QHMs constructed from perfect sequences can lead to matrices not equivalent to those obtained from other constructions. We now prove that the QHMs constructed from the length five perfect sequence $\mathbf{x}+\mathbf{JJ}+$ are not equivalent to matrices of the form (4.4) or to the other order five QHMs considered by Higginbotham and Worley [24].

Consider the length five perfect sequence $\mathbf{x}+\mathbf{JJ}+$ listed in the appendix and the QHM obtained from this sequence. For ease of comparison, we work with the equivalent circulant matrix

$$M := \begin{bmatrix} 1 & q\mathbf{i} & 1 & -\mathbf{j} & -\mathbf{j} \\ -\mathbf{j} & 1 & q\mathbf{i} & 1 & -\mathbf{j} \\ -\mathbf{j} & -\mathbf{j} & 1 & q\mathbf{i} & 1 \\ 1 & -\mathbf{j} & -\mathbf{j} & 1 & q\mathbf{i} \\ q\mathbf{i} & 1 & -\mathbf{j} & -\mathbf{j} & 1 \end{bmatrix}. \quad (4.8)$$

having $+\mathbf{x}+\mathbf{JJ}$ as the first row. We begin by showing that M is not equivalent to the order five matrices of the form $G(a, b, c)$ studied in Section 4.3. In what follows, we assume the indices are taken to be modulo n , where n is the length of the perfect sequence or order of the corresponding QHM.

Lemma 20. *Let H be a cyclic QHM of order n with first row h . Let $\tilde{H}$ denote the QHM obtained by dephasing the first column of H , i.e., $\tilde{H} := \text{diag}(c)^* H$, where c is the first column of H . Any normalized QHM equivalent to H may be expressed as $\alpha h_k Q_1 \tilde{H} \text{diag}(g(k))^* Q_2 \alpha^*$, for some unit quaternion α , $k \in [0, n)$, and permutation matrices Q_1, Q_2 , where $g(k)$ is the vector given by the cyclic permutation of the entries of h by k places to the left.*

Proof. Let h denote the first row of H , so that $g(k)_i = h_{i+k}$, $H = (h_{j-i} : 0 \leq i, j < n)$ and $\tilde{H} = (h_{-i}^* h_{j-i} : 0 \leq i, j < n)$.

Suppose H' is a normalized QHM equivalent to H . By Lemma 1, we have $H' = D_1 P_1 H P_2 D_2$ for some diagonal matrices D_1, D_2 with unit quaternions on the diagonals and some permutation matrices P_1, P_2 . We may write $H' = P_1 D'_1 H D'_2 P_2$, where $D'_1 := P_1^* D_1 P_1$ and $D'_2 := P_2 D_2 P_2^*$. Note that D'_1, D'_2 are also diagonal matrices with unit quaternions on the diagonals.

Let $K := D'_1 H D'_2$. It suffices to prove that K is of the form stated in the lemma, i.e., $K = \alpha h_k Q'_1 \tilde{H} \text{diag}(g(k))^* Q'_2 \alpha^*$ for some permutation matrices Q'_1, Q'_2 and $\alpha, k, g(k)$ as in the lemma.

Let $D'_1 = \text{diag}(a)$, and $D'_2 = \text{diag}(b)$ so that $K = (a_i h_{j-i} b_j : 0 \leq i, j < n)$. Suppose P_1 maps the $(r+1)$ th row of K to the first row of H' , and P_2 maps the $(s+1)$ th column of K to the first column of H' . Since H' is normalized, all entries of the $(r+1)$ th row of H' and its $(s+1)$ th column are 1. So $a_r h_{j-r} b_j = 1 = a_i h_{s-i} b_s$ for all $0 \leq i, j < n$. Solving these equations, we get $b_j = h_{j-r}^* a_r^*$ and $a_i = b_s^* h_{s-i}^* = a_r h_{s-r} h_{s-i}^*$. So

$$K = (a_r h_{s-r} h_{s-i}^* h_{j-i} h_{j-r}^* a_r^* : 0 \leq i, j < n) = a_r h_{s-r} K' a_r^*,$$

where $K' = (h_{s-i}^* h_{j-i} h_{j-r}^* : 0 \leq i, j < n)$. Note that the (i, j) th entry of K' is the $(i-s, j-s)$ th entry of $\tilde{H} \text{diag}(g(k))^*$, with $k := s-r$. The lemma follows. $\square$

The lemma helps us prove that the matrix M is not equivalent to the QHM $G(\mathbf{i}, \mathbf{i} e^{\frac{2\pi}{3}\mathbf{j}}, \mathbf{i} e^{\frac{4\pi}{3}\mathbf{j}})$, and therefore to any QHM of the form $G(a, b, c)$.

Proposition 21. *The QHM M in Eq. (4.8) is not equivalent to the QHM $G(\mathbf{i}, \mathbf{i} e^{\frac{2\pi}{3}\mathbf{j}}, \mathbf{i} e^{\frac{4\pi}{3}\mathbf{j}})$ as defined in Section 4.3.*

Proof. Observe that every column of $G(\mathbf{i}, \mathbf{i} e^{\frac{2\pi}{3}\mathbf{j}}, \mathbf{i} e^{\frac{4\pi}{3}\mathbf{j}})$ other than the first contains exactly three pure imaginary quaternions. We argue that for any normalized QHM equivalent to M , there is some column different from the first that does not have this property.

By Lemma 20, any normalized matrix equivalent to M has the form

$$\alpha h_k Q_1 \tilde{H} \text{diag}(g(k))^* Q_2 \alpha^*$$

for α , h , k , Q_1 , $\tilde{H}$, $g(k)$, and Q_2 as in the lemma. Every inner automorphism $x \mapsto \alpha x \alpha^*$ preserves pure imaginary quaternions, and the permutation of rows of a matrix preserves the number of pure imaginary quaternions in each of the columns. The permutation Q_2 maps some column of the matrix $L := h_k \tilde{H} \text{diag}(g(k))^*$ to the first and permutes the rest. So it suffices to prove that there is some other column of L that does not contain exactly three pure imaginary quaternions.

Consider the third column of L . Depending on the value of k , this column

is given in the table

k	0	1	2	3	4	
$h_k h_0^* h_2 h_{2+k}^*$	1	$q\mathbf{k}$	$\mathbf{j}$	$-\mathbf{j}$	$-\mathbf{k}q^*$	(4.9)
$h_k h_4^* h_1 h_{2+k}^*$	$\mathbf{j}q\mathbf{i}$	$(q\mathbf{k})^2$	$\mathbf{j}q\mathbf{k}$	$q\mathbf{i}$	1	
$h_k h_3^* h_0 h_{2+k}^*$	$\mathbf{j}$	$-q\mathbf{i}$	-1	1	$-\mathbf{i}q^*$	
$h_k h_2^* h_4 h_{2+k}^*$	$-\mathbf{j}$	$q\mathbf{i}$	1	-1	$\mathbf{i}q^*$	
$h_k h_1^* h_3 h_{2+k}^*$	$\mathbf{i}q^*\mathbf{j}$	1	$-\mathbf{i}q^*$	$\mathbf{k}q^*\mathbf{j}$	$(\mathbf{k}q^*)^2$	

Since none of the possible columns is all 1, the permutation Q_2 does not map the third column of L to the first. We may verify that none of the above column vectors have exactly three pure imaginary quaternions. The claim follows. $\square$

Recall that the order n complex Fourier matrix F_n is given by $F_n(i, j) := \omega^{ij}$, $0 \leq i, j < n$, where $\omega := \exp(2\pi\mathbf{i}/n)$. The matrix F_n is a quaternionic Hadamard matrix for all $n \geq 1$. The complex Fourier matrix F_5 has a circulant core and is contained in a class of order five QHMs with a circulant core characterized by Higginbotham and Worley [24, Theorem 6]. We now prove the matrix M is not equivalent to this class of QHMs.

Proposition 22. *The QHM M in Eq. (4.8) is not equivalent to QHMs with a circulant core and with two complex entries in the core.*

Proof. By [24, Theorem 6], any order five QHM with a circulant core and with two complex entries in the core is either equivalent to the complex Fourier matrix F_5 , or has two pairs of non-real conjugate quaternions (β, β^*) , (γ, γ^*) in every column other than the first. Moreover, in the latter case, the inner product of the vectors of coefficients of the pure imaginary parts of β and γ is $\pm 5/16$.

Every inner automorphism $x \mapsto \alpha x \alpha^*$ preserves the conjugacy relation. By Theorem 16, it also preserves the inner products of the vectors of coefficients of the pure imaginary parts of every pair of quaternions. Similarly, two quaternions θ, ω commute if and only if $\alpha\theta\alpha^*$ and $\alpha\omega\alpha^*$ commute. Also note that two quaternions commute if and only if their pure imaginary parts are real multiples of the same quaternion.

Consider the nonequivalence of M to the complex Fourier matrix F_5 . Note that all the entries of the complex Fourier matrix commute. By following the same arguments as in the proof of Proposition 21, it suffices to show

that the pure imaginary parts of the third column of the QHM L are not all real multiples of the same quaternion. By inspecting the possibilities for this column in Eq. (4.9), we see that this is indeed the case.

Consider the nonequivalence of M to the other class of order five QHM described above. Inspecting the possibilities for the third column of L in Eq. (4.9), we see that only the possibility with $k = 0$ has two pairs of non-real conjugate quaternions. However, the inner product of the vectors of coefficients of the pure imaginary parts of the non-conjugate quaternions is $\pm 1/2$. The claim follows. $\square$

Next, we show there are at least three nonequivalent QHMs of order seven. Consider the order seven QHM R obtained from the sequence $+JYJ+--$ reported in the appendix (up to a shift),

$$R := \begin{bmatrix} 1 & -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} & 1 & -1 & -1 \\ -1 & 1 & -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} & 1 & -1 \\ -1 & -1 & 1 & -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} & 1 \\ 1 & -1 & -1 & 1 & -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} \\ -\mathbf{j} & 1 & -1 & -1 & 1 & -\mathbf{j} & -q\mathbf{j} \\ -q\mathbf{j} & -\mathbf{j} & 1 & -1 & -1 & 1 & -\mathbf{j} \\ -\mathbf{j} & -q\mathbf{j} & -\mathbf{j} & 1 & -1 & -1 & 1 \end{bmatrix}. \quad (4.10)$$

We compare R to the QHMs corresponding to $\mathcal{Q}_{24}$ -sequences reported in prior works, viz. $+jIIj+W$ [27, Example 7.3] and $qJIKKIJ$ [28] (see [4, Table 1]). The former sequence cannot be directly converted into a set of QT sequences because of the presence of the W entry, since $q^*\mathbf{k} \notin \mathcal{Q}_+$. The application of conjugation converts $+jIIj+W$ into a perfect $\mathcal{Q}_+$ -sequence whose corresponding set of QT sequences is QT equivalent to the set of QT sequences corresponding to $qJIKKIJ$. However, conjugation is not an automorphism of $\mathbb{H}$ (it is an *anti*-automorphism, i.e., $(xy)^* = y^*x^*$), so conjugation does not in general preserve the property of being a QHM and is not an equivalence operation of QHMs. Thus, below we prove that R is not equivalent to both the normalized

form of the QHM obtained from $+jIIj+W$,

$$S := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -kqj & -kqk & kq & kqk & kqj & (kq)^2 \\ 1 & -q^*i & i & -k & k & -i & iq \\ 1 & -1 & jq^*j & k & -j & -k & q \\ 1 & i & -1 & -iq^*j & -k & k & kq \\ 1 & -j & j & -1 & -iq^*i & i & -q \\ 1 & -i & -j & i & -1 & jq^*k & -iq \end{bmatrix}, \quad (4.11)$$

and the normalized form of the QHM obtained from $jQjikki$ (a shift and negation of $qJIKKIJ$),

$$T := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & iq^* & kqj & -1 & -i & k & i \\ 1 & -q^* & -i & -iqi & -1 & -k & k \\ 1 & -jq^* & -j & j & -iqk & -1 & -i \\ 1 & q^* & j & k & -j & kqk & -1 \\ 1 & -iq^* & i & -j & j & -i & qi \\ 1 & (jq^*)^2 & jq^*k & jq^*j & -jq^* & -jq^*j & -jq^*k \end{bmatrix}. \quad (4.12)$$

In order to prove nonequivalence of R to S and T , we follow the approach taken for order five matrices.

Proposition 23. *The QHM R in Eq. (4.10) is neither equivalent to the QHM S defined in Eq. (4.11) nor to the QHM T defined in Eq. (4.12).*

Proof. By Lemma 20, any normalized matrix equivalent to R has the form

$$\alpha h_k Q_1 \tilde{H} \text{diag}(g(k))^* Q_2 \alpha^*$$

for α , h , k , Q_1 , $\tilde{H}$, $g(k)$, and Q_2 as in the lemma. Let $L := h_k \tilde{H} \text{diag}(g(k))^*$. It suffices to prove that there is some column of L that does not correspond to any column of S or T (after the application of the permutations Q_1, Q_2 and automorphism $x \mapsto \alpha x \alpha^*$ as in the above expression).

Consider the second column of L . Depending on the value of k , this

column equals one of the columns of the table

k	0	1	2	3	4	5	6
$h_k h_0^* h_1 h_{1+k}^*$	1	$-\mathbf{j}q^*$	$-q\mathbf{j}$	-1	$\mathbf{j}$	$-\mathbf{j}$	$\mathbf{j}$
$h_k h_6^* h_0 h_{1+k}^*$	$-\mathbf{j}$	$-q^*$	$-q$	$\mathbf{j}$	1	-1	1
$h_k h_5^* h_6 h_{1+k}^*$	$\mathbf{j}$	q^*	q	$-\mathbf{j}$	-1	1	-1
$h_k h_4^* h_5 h_{1+k}^*$	$-\mathbf{j}$	$-q^*$	$-q$	$\mathbf{j}$	1	-1	1
$h_k h_3^* h_4 h_{1+k}^*$	-1	$\mathbf{j}q^*$	$q\mathbf{j}$	1	$-\mathbf{j}$	$\mathbf{j}$	$-\mathbf{j}$
$h_k h_2^* h_3 h_{1+k}^*$	$\mathbf{j}q^*$	$(q^*)^2$	1	$-q^*\mathbf{j}$	$\mathbf{j}q^*\mathbf{j}$	$-\mathbf{j}q^*\mathbf{j}$	$\mathbf{j}q^*\mathbf{j}$
$h_k h_1^* h_2 h_{1+k}^*$	$\mathbf{j}q$	1	q^2	$-q\mathbf{j}$	$\mathbf{j}q\mathbf{j}$	$-\mathbf{j}q\mathbf{j}$	$\mathbf{j}q\mathbf{j}$

since the i th entry of the column for $k \in [0, 7)$ is $h_k h_{-i}^* h_{1-i} h_{1+k}^*$. The column is not all 1, and has one of the following types depending on the value of k .

1. It has two elements in $\{\pm 1\}$ and three elements in $\{\pm\beta\}$, where $\beta \in \mathcal{Q}_8$ is some pure imaginary quaternion.
2. It has three elements in $\{\pm 1\}$ and two elements in $\{\pm\beta\}$, where $\beta \in \mathcal{Q}_8$ is some pure imaginary quaternion.
3. It has two distinct pairs of quaternions of the form $(\beta, -\beta)$ for some $\beta \in \mathcal{Q}_{24} \setminus \mathcal{Q}_8$, and one pair of quaternions (γ, γ^2) where $\gamma \in \mathcal{Q}_{24} \setminus \mathcal{Q}_8$ is a cube root of -1 .

All elements of R, S, T are in $\mathcal{Q}_{24}$, but the rest of the proof only uses the property that the elements of $\mathcal{Q}_{24} \setminus \mathcal{Q}_8$ have non-zero real and imaginary parts. Suppose R is equivalent to S or T . Then the automorphism $f: x \mapsto \alpha x \alpha^*$ (and the permutations Q_1, Q_2) preserves the properties of the three types of columns described above. However, none of the columns of S or T are of types 1 or 2. Only the last column of S and the second column of T are of type 3. So the second column of L may only be mapped to these columns, and with $k \in \{1, 2\}$ (cf. Eq. (4.13)). We argue next that this too is not possible.

We present the argument for the last column of S and $k = 1$. The other cases follow along the same lines. The only pairs of the form $(\beta, -\beta)$ in the last column of S are $(q, -q)$ and $(\mathbf{i}q, -\mathbf{i}q)$, and in the second column of L with $k = 1$ are $(q^*, -q^*)$ and $(\mathbf{j}q^*, -\mathbf{j}q^*)$. Since $\text{Re}(q) = \text{Re}(-\mathbf{i}q) = \text{Re}(q^*) = \text{Re}(\mathbf{j}q^*) = 1/2$, the equivalence operations may only map $(q^* \mapsto q, \mathbf{j}q^* \mapsto -\mathbf{i}q)$ or $(q^* \mapsto -\mathbf{i}q, \mathbf{j}q^* \mapsto q)$. Further, we have $-q^* \mapsto \mathbf{k}q$ or $-q^* \mapsto (\mathbf{k}q)^2$. However, the two sets of conditions are not consistent as they map q^* to distinct quaternions, so the required equivalence operations do not exist. $\square$

Using similar arguments as above, we show that the QHMs R and S are not equivalent to the complex Fourier matrix F_7 .

Proposition 24. *Neither the QHM R in Eq. (4.10) nor the QHM S defined in Eq. (4.11) is equivalent to the order seven Fourier matrix F_7 .*

Proof. As in the proof of Proposition 23, to show that R is not equivalent to F_7 , it suffices to show that none of the columns in (4.13) equal a column of F_7 after some permutation of rows and the application of an automorphism. All the entries of F_7 commute. However, every column in (4.13) has at least two entries whose pure imaginary parts are not real multiples of the same quaternion, and this property is preserved by the permutation of rows and the application of an automorphism. The claim for R follows.

We may repeat this argument for the nonequivalence of S to F_7 . Let $L' := h_k \tilde{H} \text{diag}(g(k))^*$, where the parameters $h, \tilde{H}, g(k)$ now correspond to the QHM generated by the perfect sequence $+jIIj+W$, and k is determined by a putative sequence of equivalence operations. Consider the second column of L' . Depending on the value of k , this column equals one of the columns of the table

k	0	1	2	3	4	5	6
$h_k h_0^* h_1 h_{1+k}^*$	1	$-\mathbf{i}$	$-\mathbf{j}$	$-\mathbf{i}$	-1	$-\mathbf{i}q$	$-q^*\mathbf{i}$
$h_k h_6^* h_0 h_{1+k}^*$	$\mathbf{k}q\mathbf{j}$	$-\mathbf{i}q\mathbf{i}$	$-\mathbf{j}q\mathbf{i}$	$\mathbf{j}q\mathbf{j}$	$-\mathbf{i}q$	$(\mathbf{k}q)^2$	1
$h_k h_5^* h_6 h_{1+k}^*$	$q^*\mathbf{i}$	$\mathbf{j}q^*\mathbf{j}$	$-\mathbf{i}q^*\mathbf{j}$	$-\mathbf{i}q^*\mathbf{i}$	$\mathbf{j}q^*\mathbf{k}$	1	$(q^*\mathbf{k})^2$
$h_k h_4^* h_5 h_{1+k}^*$	-1	$\mathbf{i}$	$\mathbf{j}$	$\mathbf{i}$	1	$\mathbf{i}q$	$q^*\mathbf{i}$
$h_k h_3^* h_4 h_{1+k}^*$	$\mathbf{i}$	-1	$-\mathbf{k}$	1	$\mathbf{i}$	q	$-q^*$
$h_k h_2^* h_3 h_{1+k}^*$	$-\mathbf{j}$	$-\mathbf{k}$	1	$\mathbf{k}$	$\mathbf{j}$	$-\mathbf{k}q$	$q^*\mathbf{k}$
$h_k h_1^* h_2 h_{1+k}^*$	$-\mathbf{i}$	1	$\mathbf{k}$	-1	$-\mathbf{i}$	$-q$	q^*

(4.14)

Again, every column in (4.14) has at least two entries whose pure imaginary parts are not real multiples of the same quaternion. The claim for S also follows. $\square$

The results in this section suggest that the multiplicity of equivalence classes of QHMs extends to larger orders as well and we conjecture that this is the case for all orders ≥ 4 .

5 Conclusion

We have enumerated perfect quaternion sequences over $\mathcal{Q}_+$ of lengths $n \leq 21$. In the process, we derived new properties of quaternion-type Hadamard matrices with circulant blocks, formalized three different types of equivalence of such objects, and developed methods ensuring a complete enumeration up to each notion of equivalence. In particular, the natural notion of equivalence of quadruples of Williamson-type sequences does not preserve the natural notion of equivalence of Hadamard matrices, but introducing a third notion of equivalence allowed us to classify all quaternion-type Hadamard matrices with circulant blocks up to equivalence of Hadamard matrices. Ultimately, we classify all quaternion-type Hadamard matrices with circulant blocks of orders $n \leq 21$ up to each type of equivalence we consider (see Table 1).

We also proved and exploited a one-to-one correspondence between quadruples of circulant Williamson-type matrices and quaternion-type Hadamard matrices with circulant blocks. Both these kinds of Hadamard matrices have long been studied [19, 40]. It is immediate that circulant Williamson-type matrices produce Hadamard matrices of quaternion-type, but surprisingly it was not previously known that quaternion-type Hadamard matrices with circulant blocks necessarily have blocks that are of Williamson-type. We prove this in Theorem 9. This property allows our search for quaternion-type Hadamard matrices defined by QT sequences to filter the vast majority of pairs of sequences from consideration early.

Our computational enumeration of QT sequences helps construct new quaternion-type Hadamard matrices with circulant blocks and provably nonequivalent quaternionic Hadamard matrices. We also study properties of quaternionic Hadamard matrices analytically, and demonstrate the feasibility of characterizing quaternionic Hadamard matrices with a fixed pattern of entries. Perfect sequences give us quaternionic Hadamard matrices that are provably not equivalent to those constructed by other means, as we show in Section 4.4. These results indicate a larger abundance of quaternionic Hadamard matrices exist than known about in previous works, including matrices studied for their application to quantum communication protocols [15].

References

- [1] Santiago Barrera Acevedo. Personal communication, July 25, 2023.

- [2] Santiago Barrera Acevedo and Heiko Dietrich. Perfect sequences over the quaternions and $(4n, 2, 4n, 2n)$ -relative difference sets in $C_n \times Q_8$. *Cryptography and Communications*, 10(2):357–368, 2018. doi:[10.1007/s12095-017-0224-y](https://doi.org/10.1007/s12095-017-0224-y).
- [3] Santiago Barrera Acevedo and Heiko Dietrich. New infinite families of Williamson Hadamard matrices. *Australasian Journal of Combinatorics*, 73(1):207–219, January 2019. URL: https://ajc.maths.uq.edu.au/pdf/73/ajc_v73_p207.pdf.
- [4] Santiago Barrera Acevedo, Heiko Dietrich, and Corey Lionis. New families of quaternionic Hadamard matrices. *Designs, Codes and Cryptography*, 92(9):2511–2525, June 2024. doi:[10.1007/s10623-024-01401-1](https://doi.org/10.1007/s10623-024-01401-1).
- [5] Santiago Barrera Acevedo and Thomas E. Hall. Perfect sequences of unbounded lengths over the basic quaternions. In Tor Helleseht and Jonathan Jedwab, editors, *Sequences and Their Applications - SETA 2012 - 7th International Conference, Waterloo, ON, Canada, June 4-8, 2012. Proceedings*, volume 7280 of *Lecture Notes in Computer Science*, pages 159–167. Springer, 2012. doi:[10.1007/978-3-642-30615-0_15](https://doi.org/10.1007/978-3-642-30615-0_15).
- [6] Santiago Barrera Acevedo, Padraig Ó. Catháin, and Heiko Dietrich. Constructing cocyclic Hadamard matrices of order $4p$. *Journal of Combinatorial Designs*, 27(11):627–642, August 2019. doi:[10.1002/jcd.21664](https://doi.org/10.1002/jcd.21664).
- [7] L. D. Baumert and Marshall Hall. Hadamard matrices of the Williamson type. *Mathematics of Computation*, 19(91):442–447, 1965. doi:[10.1090/s0025-5718-1965-0179093-2](https://doi.org/10.1090/s0025-5718-1965-0179093-2).
- [8] Samuel Thomas Blake. *Constructions for Perfect Autocorrelation Sequences and Multi-Dimensional Arrays*. PhD thesis, Monash University, 2017. doi:[10.4225/03/58FD558C6A8E5](https://doi.org/10.4225/03/58FD558C6A8E5).
- [9] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. Applying computer algebra systems with SAT solvers to the Williamson conjecture. *Journal of Symbolic Computation*, 100:187–209, September 2020. doi:[10.1016/j.jsc.2019.07.024](https://doi.org/10.1016/j.jsc.2019.07.024).
- [10] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. New infinite families of perfect quaternion sequences and Williamson sequences. *IEEE*

- Transactions on Information Theory*, 66(12):7739–7751, December 2020. doi:[10.1109/TIT.2020.3016510](https://doi.org/10.1109/TIT.2020.3016510).
- [11] E. Cho. De Moivre’s formula for quaternions. *Applied Mathematics Letters*, 11(6):33–35, 1998. doi:[10.1016/S0893-9659\(98\)00098-6](https://doi.org/10.1016/S0893-9659(98)00098-6).
 - [12] Oleg Chterental and Dragomir Ž. Đoković. On orthostochastic, unistochastic and qustochastic matrices. *Linear Algebra and its Applications*, 428(4):1178–1201, 2008. doi:[10.1016/j.laa.2007.09.022](https://doi.org/10.1016/j.laa.2007.09.022).
 - [13] Dragomir Ž. Đoković. Williamson matrices of order $4n$ for $n = 33, 35, 39$. *Discrete Mathematics*, 115(1–3):267–271, May 1993. doi:[10.1016/0012-365x\(93\)90495-f](https://doi.org/10.1016/0012-365x(93)90495-f).
 - [14] Máté Farkas. Personal communication, January 2021.
 - [15] Máté Farkas, Jędrzej Kaniewski, and Ashwin Nayak. Mutually unbiased measurements, Hadamard matrices, and superdense coding. *IEEE Transactions on Information Theory*, 69(6):3814–3824, June 2023. doi:[10.1109/TIT.2023.3269524](https://doi.org/10.1109/TIT.2023.3269524).
 - [16] Patrick Fitzpatrick and Henry O’Keeffe. Williamson type Hadamard matrices with circulant components. *Discrete Mathematics*, 346(12):113615, December 2023. doi:[10.1016/j.disc.2023.113615](https://doi.org/10.1016/j.disc.2023.113615).
 - [17] R. L. Frank, S. A. Zadoff, and R. C. Heimiller. Phase shift pulse codes with good periodic correlation properties (corresp.). *IRE Transactions on Information Theory*, 8(6):381–382, 1962. doi:[10.1109/TIT.1962.1057786](https://doi.org/10.1109/TIT.1962.1057786).
 - [18] M. Frigo and S. G. Johnson. The design and implementation of FFTW3. *Proceedings of the IEEE*, 93(2):216–231, February 2005. doi:[10.1109/jproc.2004.840301](https://doi.org/10.1109/jproc.2004.840301).
 - [19] Solomon W. Golomb and Leonard D. Baumert. The search for Hadamard matrices. *The American Mathematical Monthly*, 70(1):12–17, January 1963. doi:[10.1080/00029890.1963.11990035](https://doi.org/10.1080/00029890.1963.11990035).
 - [20] Jacques Hadamard. Résolution d’une question relative aux déterminants. *Bull. des sciences math.*, 2:240–246, 1893.

- [21] William Rowan Hamilton. On quaternions; or on a new system of imaginaries in algebra. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 25(163):10–13, July 1844. doi:[10.1080/14786444408644923](https://doi.org/10.1080/14786444408644923).
- [22] R. Heimiller. Phase shift pulse codes with good periodic correlation properties. *IRE Transactions on Information Theory*, 7(4):254–257, October 1961. doi:[10.1109/tit.1961.1057655](https://doi.org/10.1109/tit.1961.1057655).
- [23] Logan M. Higginbotham and Chase T. Worley. On some quaternionic Hadamard matrices of small order. 2021. arXiv:2112.09613v2 [math.CO]. doi:[10.48550/ARXIV.2112.09613](https://doi.org/10.48550/ARXIV.2112.09613).
- [24] Logan M. Higginbotham and Chase T. Worley. On some quaternionic Hadamard matrices of small order. Technical Report arXiv:2112.09613v2 [math.CO], arXiv, 2022. doi:[10.48550/ARXIV.2112.09613](https://doi.org/10.48550/ARXIV.2112.09613).
- [25] W. H. Holzmann, H. Kharaghani, and B. Tayfeh-Rezaie. Williamson matrices up to order 59. *Designs, Codes and Cryptography*, 46(3):343–352, January 2008. doi:[10.1007/s10623-007-9163-5](https://doi.org/10.1007/s10623-007-9163-5).
- [26] Oleg Kuznetsov. Perfect sequences over the real quaternions. In *2009 Fourth International Workshop on Signal Design and its Applications in Communications*, page 8–11. IEEE, October 2009. doi:[10.1109/iwsda.2009.5346443](https://doi.org/10.1109/iwsda.2009.5346443).
- [27] Oleg Kuznetsov. *Perfect sequences over the real quaternions*. PhD thesis, Monash University, Melbourne, Australia, 2010. doi:[10.4225/03/5927d7a6284be](https://doi.org/10.4225/03/5927d7a6284be).
- [28] Wolfgang Lang and Ekkehard Schneider. Turyn type Williamson matrices up to order 99. *Designs, Codes and Cryptography*, 62(1):79–84, March 2011. doi:[10.1007/s10623-011-9492-2](https://doi.org/10.1007/s10623-011-9492-2).
- [29] Tyler Lumsden, Ilias Kotsireas, and Curtis Bright. New results on periodic Golay pairs. *Mathematics of Computation*, April 2025. doi:[10.1090/mcom/4096](https://doi.org/10.1090/mcom/4096).
- [30] Brendan D. McKay. Hadamard equivalence via graph isomorphism. *Discrete Mathematics*, 27(2):213–214, 1979. doi:[10.1016/0012-365x\(79\)90113-4](https://doi.org/10.1016/0012-365x(79)90113-4).

- [31] Brendan D. McKay and Adolfo Piperno. Practical graph isomorphism, II. *Journal of Symbolic Computation*, 60:94–112, January 2014. doi:[10.1016/j.jsc.2013.09.003](https://doi.org/10.1016/j.jsc.2013.09.003).
- [32] Leiba Rodman. *Topics in Quaternion Linear Algebra*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, New Jersey, USA, August 24, 2014. doi:[10.2307/j.ctt6wpz0p](https://doi.org/10.2307/j.ctt6wpz0p).
- [33] Herbert John Ryser. *Combinatorial mathematics*. Number 14 in The Carus Mathematical Monographs. The Mathematical Association of America, 1963.
- [34] Bernhard Schmidt. Williamson matrices and a conjecture of Ito’s. *Designs, Codes and Cryptography*, 17(1–3):61–68, September 1999. doi:[10.1023/a:1008398319853](https://doi.org/10.1023/a:1008398319853).
- [35] Kai-Uwe Schmidt. Sequences with small correlation. *Designs, Codes and Cryptography*, 78(1):237–267, 2016. doi:[10.1007/s10623-015-0154-7](https://doi.org/10.1007/s10623-015-0154-7).
- [36] J.J. 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, December 1867. doi:[10.1080/14786446708639914](https://doi.org/10.1080/14786446708639914).
- [37] Armin Tavakoli, Máté Farkas, Denis Rosset, Jean-Daniel Bancal, and Jędrzej Kaniewski. Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments. *Science Advances*, 7(7), 2021. doi:[10.1126/sciadv.abc3847](https://doi.org/10.1126/sciadv.abc3847).
- [38] Richard J. Turyn. Complex hadamard matrices. *Combinatorial structures and their applications*, pages 435–437, 1970.
- [39] B. L. van der Waerden. Hamilton’s discovery of quaternions. *Mathematics Magazine*, 49(5):227–234, 1976. doi:[10.2307/2689449](https://doi.org/10.2307/2689449).
- [40] Jennifer Seberry Wallis. Some matrices of Williamson type. *Utilitas Mathematica*, 4:147–154, 1973.

- [41] Jennifer Seberry Wallis. *Williamson matrices of even order*, page 132–142. Springer Berlin Heidelberg, 1974. [doi:10.1007/bfb0057387](https://doi.org/10.1007/bfb0057387).
- [42] Jennifer Seberry Wallis. Construction of Williamson type matrices. *Linear and Multilinear Algebra*, 3(3):197–207, January 1975. [doi:10.1080/03081087508817111](https://doi.org/10.1080/03081087508817111).
- [43] John Williamson. Hadamard’s determinant theorem and the sum of four squares. *Duke Mathematical Journal*, 11(1), March 1944. [doi:10.1215/s0012-7094-44-01108-7](https://doi.org/10.1215/s0012-7094-44-01108-7).

Appendix: List of QT sequences

Here we provide an exhaustive list of all QT sequences up to Williamson-type equivalence for all lengths $n \leq 21$. The sequences are classified as either symmetric (such sequences are also known as *Williamson sequences*) or non-symmetric. Each set of QT sequences is encoded as a perfect quaternion sequence using the correspondence from Theorem 4, as described in Section 2.3. The symbols + and - denote 1 and -1 , respectively; q, i, j, k denote the quaternions $q = \frac{1+i+j+k}{2}$, **i**, **j**, **k**, respectively; x, y, z denote qi , qj , qk , respectively; and capitalization corresponds to the negation of the quaternion denoted by the same letter in lower case. For example, X denotes $-qi$.

Length 1 (1 total; 1 symmetric, 0 non-symmetric)

+

Length 2 (1 total; 1 symmetric, 0 non-symmetric)

+J

Length 3 (1 total; 1 symmetric, 0 non-symmetric)

Q++

Length 4 (2 total; 1 symmetric, 1 non-symmetric)

1 Symmetric:

++-+

1 Nonsymmetric:

+YIQ

Length 5 (1 total; 1 symmetric, 0 non-symmetric)

x+JJ+

Length 6 (1 total; 1 symmetric, 0 non-symmetric)

KJ+j+J

Length 7 (2 total; 2 symmetric, 0 non-symmetric)

YJ+--+J, y+JKKJ+

Length 8 (3 total; 1 symmetric, 2 non-symmetric)

1 Symmetric:

J++-J-++

2 Nonsymmetric:

+YYIiqq-, +JYZikqx

Length 9 (4 total; 3 symmetric, 1 non-symmetric)

3 Symmetric:

yi+JKKJ+i, XKJ+jj+JK, Z+J+--+J+

1 Nonsymmetric:

+YQJYZikx

Length 10 (2 total; 2 symmetric, 0 non-symmetric)

KJ+ikIki+J, K+J+j-j+J+

Length 11 (1 total; 1 symmetric, 0 non-symmetric)

z-+JKIIKJ+-

Length 12 (5 total; 3 symmetric, 2 non-symmetric)

3 Symmetric:

Y++y-+y+-y++, YQ++-QyQ-++Q, JIIY+-j-+YII

2 Nonsymmetric:

+++Yy++-+yy-, +++YQ++-+yQ-

Length 13 (4 total; 4 symmetric, 0 non-symmetric)

x-+JK+II+KJ+-, XKJ+jK--Kj+JK, QJ++jJjjJj++J, X-k+JKIIKJ+k-

Length 14 (5 total; 5 symmetric, 0 non-symmetric)

KJ+J+j-J-j+J+J, QQ+J+jzYzj+J+Q, +QY+kzxJxzk+YQ, YKJ+j-iQi-j+JK,
QJ++iIkxkIi++J

Length 15 (4 total; 4 symmetric, 0 non-symmetric)

XIij+JKJJKJ+jiI, QjJKj+JJJJ+jKJj, XIKJ+kKjjKk+JKI,
Q+J+jj+--+jj+J+

Length 16 (18 total; 6 symmetric, 12 non-symmetric)

6 Symmetric:

-J+++-+j-j+-+++J, QJ++q-+jQj+-q++J, KJ++k-+jKj+-k++J,
JJ++j-j+jj+-j++J, YJ++y-+jYj+-y++J, +J+--+j+j+--+J

12 Nonsymmetric:

+Y+JYZ+qIxJkqQjy, ++JJ+J+j+-jJ+j-j, ++JY+J+y+-jY+j-y,
++J++J+-+j++j--, ++JK+J+k+-jK+j-k, +++J+J-++-+j+j--,
++YJ+Jy++-Yj+jy-, ++JK+Kj++-Jk+kj-, ++JJ+Jj++-Jj+jj-,
+Q++JQYqKXJjixxz, ++YJIIJQ++-YjIjQ-, ++YIIIIQ++-YiIiQ-

Length 17 (4 total; 4 symmetric, 0 non-symmetric)

ZK+J+i-kKKk-i+J+K, yjKJ-+J+KK+J+-JKj, xkKI+JJKKJJ+kIKk,
y-+Kk+JJKKJJ+kK+-

Length 18 (28 total; 23 symmetric, 5 non-symmetric)

23 Symmetric:

ZXY+i-KZyYyZK-i+YX, Z+J+i-KIjYjIK-i+J+, YJ++xyKiIZIiKyx++J,
YJY+yxJZkXkZJxy+YJ, Q+++i-IiIXIiI-i+++, I+Y+yqIQiJiQIQy+Y+,
K+J+jKiIkIkIKij+J+, ZKJ++jKk-Y-kKj++JK, KIJY+jQi-J-iQj+YJI,
YQJ++jJiyXyiJj++JQ, YJQ++jJxkXkxJj++QJ, QKJ++jJIjzjIJj++JK,
+QY+-JJZyjjZJJ-+YQ, KJ++yZijkJkjiZy++J, KZJ++kKiyIyiKk++JZ,
ZKJ++kKi-X-iKk++JK, QIYJ+iIXjxjXIi+JYI, QY++yXKIzxxIKXy++Y,
Z+J+xQKIkkIKQx+J+, ZKJ++kKI-q-IKk++JK, XXY+-KkzqZqzkK-+YX,
ZKJ+j+j-iXi-j+j+JK, QJ++jikKiyiKkij++J

5 Nonsymmetric:

+YXXXQY+kKqQyyXqK-, +YJXXIY+zKqIyyJqKy, ++YXXQ+KkJqxYyyJ-,
++YJXIQ+JjJqiYjyJ-, ++YQJY+jqiIzxxZikx

Length 19 (6 total; 6 symmetric, 0 non-symmetric)

Qj-J-++JKIiKJ+-J-j, YKk-Kj+J+JJ+J+jK-kK, Y+-kJj+JKKKKJ+jJk-+,
ZIKJJ+-kiIIik-+JJKI, ZIKJ+kJj-JJ-jJk+JKI, ZJJJ+j+-jJJj-+jJJJ

Length 20 (24 total; 17 symmetric, 7 non-symmetric)

17 Symmetric:

JQ+Y+k+x-XjX-x+k+Y+Q, JIY++xKkzJjJzkKx++YI, IJY++xKkzIiIzkKx++YJ,
IIYJ+xkiQKiKQikx+JYI, YJXY+yjQz+y+zQjy+YXJ, XJ+Y+y-ZkXjJkZ-y+Y+J,
QJ+Y+jkY-IqI-Ykj+Y+J, +KJ++kKJi-iIKjk++JK, JQJ++xkKKzjzKKkx++JQ,
JKJ++xKjkJjJkjKx++JK, KKJ++zjJK-k-KJjz++JK, IJXY+q-ZX-i-XZ-q+YXJ,
QKJ++y-+jKqKj+-y++JK, YJ++jxJ+-JyJ-+Jxj++J, QJJ++x-+jJqJj+-x++JJ,
QKJ++z-+jKqKj+-z++JK, YJ++jyJ+-JyJ-+Jy++J

7 Nonsymmetric:

+++JKQzJK+-+jKqzjK-, ++JQQ+Jj+j-+jQq+jj-j, ++JKJQ+Ky+-JkJq+ky-,
++JJJQ+Jx+-JjJq+jx-, ++JKJQ+Kx+-JkJq+kx-, +++JKQyJK+-+jKqyjK-,
++YJ+Jj+Jy-+yJ-JJ+jy

Length 21 (7 total; 7 symmetric, 0 non-symmetric)

ZiIIk-+JKK++KKJ+-kIIi, x+iJ--+JK+II+KJ+--Ji+,
zK+ikj+JKJIIJKJ+jki+K, zK+jki+JKIJIKJ+ikj+K,

Z++J+-jjJ-++-Jjj-+J++, XK+J+kj+I-ii-I+jk+J+K,
ZIKJ+j-kKiKKiKk-j+JKI