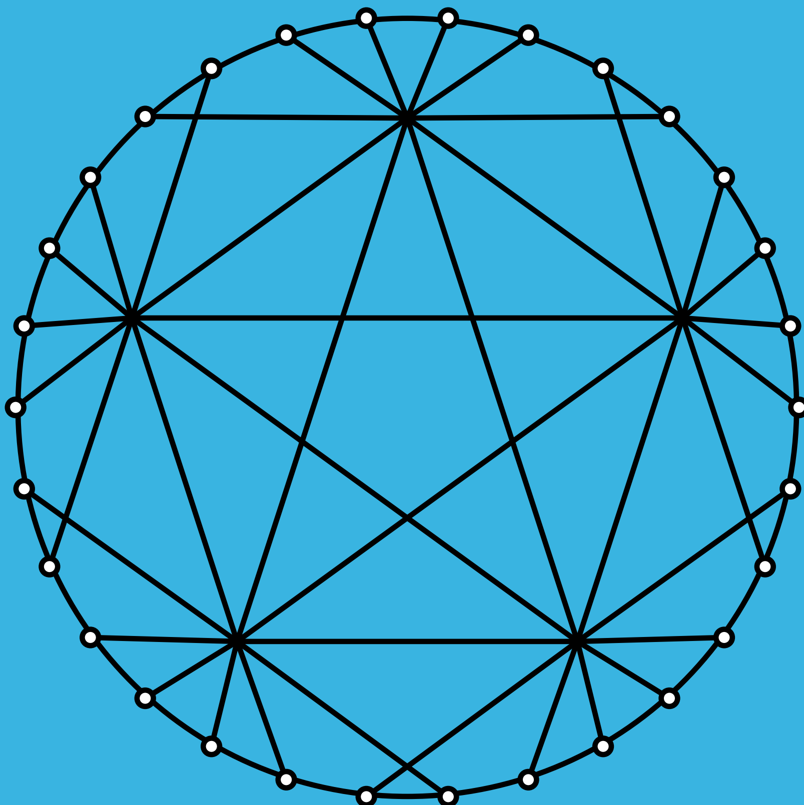
BULLETIN of The INSTITUTE of COMBINATORICS and its APPLICATIONS

Volume 90
October 2020



Boca Raton, FL, U.S.A.

ISSN: 2689-0674 (Online)
ISSN: 1183-1278 (Print)

BULLETIN OF THE ICA
Volume **90** (2020), 50–62

Morphisms of Skew Hadamard Matrices

Philip Heikoop, Guillermo Nuñez Ponasso*, Padraig Ó Catháin, and John Pugmire

Worcester Polytechnic Institute, Worcester, MA 01609, USA
ptheikoop@wpi.edu, gcnunez@wpi.edu,
pocathain@wpi.edu and pugmire@ucsb.edu

Abstract

Quaternary unit Hadamard (QUH) matrices were introduced by Fender, Kharaghani and Suda along with a method to construct them at prime power orders. We present a novel construction of real Hadamard matrices from QUH matrices. Our construction recovers the result by Mukhopadhyay on the existence of real Hadamard matrices of order $q^n + q^{n-1}$ for each prime power $q \equiv 3 \mod 4$, and $n \geq 1$. Furthermore we provide nonexistence conditions for QUH matrices.

1 Introduction

A celebrated theorem of Hadamard characterises the complex matrices with entries of norm at most one which have maximal determinant: they are precisely the solutions to the matrix equation $HH^* = nI_n$ satisfying $|h_{ij}| = 1$ for all $1 \leq i, j \leq n$. Equivalently, all entries of H have unit norm, and all rows are mutually orthogonal under the Hermitian inner product, [7]. Real

*Corresponding author.

Key words and phrases: Complex Hadamard Matrix, Skew Hadamard Matrix, Minimal Polynomial, Biquadratic Number Field, Ideal Decomposition

AMS (MOS) Subject Classifications: 15B34, 05B20

Received: 2 September 2019
Accepted: 22 January 2020

Hadamard matrices, having entries in $\{\pm 1\}$, have been extensively studied for a century, though the existence problem is far from settled. We refer the reader to the recent monographs of Horadam and of de Launey and Flannery for extensive discussion of Hadamard matrices, [8, 3].

In this paper we will study the problem of constructing real Hadamard matrices from complex Hadamard matrices (CHM). Suppose that X is a set of complex numbers of modulus 1. We define $\mathcal{H}(n, X)$ to be the set of $n \times n$ Hadamard matrices with entries drawn from X. In the special case that X is the set of k^{th} roots of unity, a CHM is called a *Butson Hadamard matrix*; the set of such matrices is denoted $\mathcal{BH}(n, k)$. Examples of Butson Hadamard matrices are furnished by the character tables of abelian groups of order n and exponent k. Cohn and Turyn proved independently that the existence of $H \in \mathcal{BH}(n, 4)$ implies the existence of a real Hadamard matrix of order $2n$, [1, 14]. More recently, Compton, Craigen and de Launey proved that an $n \times n$ matrix with entries in the *unreal* sixth roots of unity $\{\omega_6, \omega_6^2, \omega_6^4, \omega_6^5\}$ can be used to construct a real Hadamard matrix of order $4n$, [2].

A general construction for mappings between sets of Butson Hadamard matrices is described by Egan and one of the present authors, [4]. A key ingredient in the construction is a matrix $H \in \mathcal{BH}(n, k)$ with minimal polynomial $\Phi_t(x)$ for some integer t. The construction of such matrices was considered further in collaboration with Eric Swartz, [5]. In all the examples considered previously, matrix entries are roots of unity, and all fields considered are cyclotomic. In this paper, we consider a family of complex Hadamard matrices with entries in the biquadratic extension $\mathbb{Q}[\sqrt{-q}, \sqrt{q+1}]$. When the matrix entries are all in the set $X_q = \{\frac{\pm 1 \pm \sqrt{-q}}{\sqrt{q+1}}\}$, such a matrix is called a *Quaternary Unit Hadamard matrix*, abbreviated QUH. Such matrices were first considered by Fender, Kharaghani and Suda, [6].

We will construct a morphism from QUH matrices onto real Hadamard matrices, using skew-Hadamard matrices. This provides a new construction for a family of Hadamard matrices of order $q^n + q^{n-1}$ for each prime power $q \equiv 3 \mod 4$ and each $n \geq 1$, previously constructed by Mukhopadhyay and studied further by Seberry, [12, 13]. We conclude the paper by studying the decomposition of prime ideals in the field $\mathbb{Q}[\sqrt{-q}, \sqrt{q+1}]$ to obtain non-existence results for QUH matrices in the style of Winterhof [15].

2 Morphisms of QUH matrices

In this section we construct an isomorphism of fields, which we lift to an isomorphism of matrix algebras. We prove that this isomorphism carries a QUH matrix in the set $\mathcal{H}(n, X_m)$ to a real Hadamard matrix of order $n(m+1)$; that is, the isomorphism is a *morphism* of complex Hadamard matrices. We will require some standard results in algebra, as discussed in, e.g., Chapters 17–19 of Isaacs' *Graduate Algebra*, [10]. An *extension field* k of $\mathbb{Q}$ is a field containing $\mathbb{Q}$ as a subfield; in this case k is a $\mathbb{Q}$-vector space and its *degree* is its dimension as a vector space. The degree of k over $\mathbb{Q}$ is denoted by $[k : \mathbb{Q}]$. In the ring $\mathbb{Q}[x]$ every ideal contains a unique monic polynomial of minimal degree, this polynomial is irreducible if and only if the ideal is maximal. For a polynomial $p(x)$ the quotient $\mathbb{Q}[x]/\left(p(x)\right)$ is a field if and only if the polynomial $p(x)$ is irreducible. An extension field k is the *splitting field* of a polynomial $p(x) \in \mathbb{Q}[x]$ if k is a field of minimal degree over $\mathbb{Q}$ which contains all the roots of $p(x)$. We apply these results to the polynomial $\mathfrak{m}(x) = x^4 + \frac{2(m-1)}{m+1}x^2 + 1$. By abuse of notation, a Hadamard matrix is *skew* if $H - I$ is a skew-symmetric matrix.

Proposition 2.1. *Let H be a skew-Hadamard matrix of order $m+1$, where $m+1$ is not a perfect square. The minimal polynomial of $\alpha_m = \frac{1+\sqrt{-m}}{\sqrt{m+1}}$ and the minimal polynomial of $\frac{1}{\sqrt{m+1}}H$ are both equal to*

$$\mathfrak{m}(x) = x^4 + \frac{2(m-1)}{m+1}x^2 + 1\,.$$

Proof. It is easily checked that α_m is a root of $\mathfrak{m}(x)$. Since $\mathfrak{m}(x)$ is even, $-\alpha_m$ is also a root. The coefficients of $\mathfrak{m}(x)$ are real, thus α_m^* and $-\alpha_m^*$ are roots. From the fact that $\mathfrak{m}(x)$ has degree 4, we conclude that these are all the possible roots. Therefore we obtain the factorisation

$$\mathfrak{m}(x) = (x - \alpha_m)(x - \alpha_m^*)(x + \alpha_m)(x + \alpha_m^*)\,.$$

Clearly $\mathfrak{m}(x)$ has no linear factors in $\mathbb{Q}[x]$. The only possible quadratic factors with real entries are $(x - \alpha_m)(x - \alpha_m^*) = x^2 - 2x/\sqrt{m+1} + 1$ and $(x + \alpha_m)(x + \alpha_m^*) = x^2 + 2x/\sqrt{m+1} + 1$. By hypothesis, $m+1$ is not a perfect square so these factors are not in $\mathbb{Q}[x]$. We have shown that $\mathfrak{m}(x)$ is irreducible. The field extension $\mathbb{Q}[\alpha_m]$ contains $\alpha^{-1} = \alpha_m^*$ and $-\alpha_m$, so it is the splitting field of $\mathfrak{m}(x)$.

Since H is skew-Hadamard we have both $HH^\top = (m+1)I_{m+1}$ and $H^\top = 2I - H$. It follows that $H(2I - H) = (m+1)I$, or $H^2 = 2H - (m+1)I$.

Hence,

$$\left(\frac{1}{\sqrt{m+1}}H\right)^2 = \frac{2}{m+1}H - I\,.$$

We also compute that

$$\begin{aligned}\left(\frac{1}{\sqrt{m+1}}H\right)^4 &= \frac{4}{(m+1)}\left(\frac{1}{\sqrt{m+1}}H\right)^2 - \frac{4}{m+1}H + I \\ &= \frac{4}{(m+1)}\left(\frac{1}{\sqrt{m+1}}H\right)^2 - 2\left(\frac{2}{m+1}H - I\right) - I \\ &= \frac{4}{(m+1)}\left(\frac{1}{\sqrt{m+1}}H\right)^2 - 2\left(\frac{1}{\sqrt{m+1}}H\right)^2 - I \\ &= \frac{2-2m}{m+1}\left(\frac{1}{\sqrt{m+1}}H\right)^2 - I\end{aligned}$$

We conclude that the unitary matrix $\frac{1}{\sqrt{m+1}}H$ is a root of polynomial $\mathfrak{m}(x)$, which must be the minimal polynomial of $\frac{1}{\sqrt{m+1}}H$ by irreducibility. □

When $m+1$ is a perfect square, the polynomial $\mathfrak{m}(x)$ factors into two irreducible quadratic factors in $\mathbb{Q}[x]$, which correspond to the distinct minimal polynomials of α_m and $-\alpha_m$. In this case, the minimal polynomials of α_m and $\frac{1}{\sqrt{m+1}}H$ coincide, and also the minimal polynomials of $-\alpha_m$ and $\frac{1}{\sqrt{m+1}}(H-2I)$ coincide. The case that $m+1$ is a perfect square will be discussed after the proof of Theorem 2.4. From Proposition 2.1, the next result is immediate.

Proposition 2.2. *If H is a skew-Hadamard matrix of order m, then all of the following $\mathbb{Q}$-algebras are isomorphic:*

$$\mathbb{Q}[x]/(\mathfrak{m}(x)) \simeq \mathbb{Q}\left[\frac{1}{\sqrt{m+1}}H\right] \simeq \mathbb{Q}[\alpha_m]. \tag{1}$$

Definition 2.3. *A Quaternary Unit Hadamard (QUH) matrix is an element of $\mathcal{H}(n, X_m)$, where*

$$X_m = \left\{\frac{\pm 1 \pm \sqrt{-m}}{\sqrt{m+1}}\right\}.$$

Now we give the main result of this section.

Theorem 2.4. *If there exists a skew-Hadamard matrix H of order $m+1$, where $m+1$ is not a perfect square, there exists a morphism*

$$\mathcal{H}(n, X_m) \to BH(nm+n, 2).$$

Proof. Assume that there exists $M \in \mathcal{H}(n, X_m)$, since otherwise the claim is vacuous. By Proposition 2.2 that there exists an isomorphism $\mathbb{Q}(\alpha_m) \to \mathbb{Q}(\frac{1}{\sqrt{m+1}}H)$. We make this explicit:

$$\varphi : \alpha_m \mapsto \frac{1}{\sqrt{m+1}}H$$

and since α_m is a generator of $\mathbb{Q}(\alpha_m)$ the function φ extends uniquely to the whole field. Recalling that H is skew, we obtain

$$\varphi(-\alpha_m) = \frac{-1}{\sqrt{m+1}}H = \frac{1}{\sqrt{m+1}}(H - 2I)^\top, \;\; \varphi(\alpha_m^*) = \frac{1}{\sqrt{m+1}}H^\top .$$

Define M^φ to be the block matrix obtained from M by applying φ entry-wise. Then M^φ is a real matrix of size $n(m+1) \times n(m+1)$ with entries in the set $\{\pm 1/\sqrt{m+1}\}$. Since $M \in \mathcal{H}(n, X_m)$ the (Hermitian) inner product of columns c_i and c_j of M is $\langle c_i, c_j \rangle = n\delta_i^j$, where δ_i^j is the Kronecker δ function. Since φ is an isomorphism of $\mathbb{Q}$-algebras, $\varphi(0) = \mathbf{0}_{m+1}$ and $\varphi(1) = I_{m+1}$. It follows that

$$\begin{aligned}\sum_k \varphi(c_{i,k})\varphi(c_{j,k})^\top &= \sum_k \varphi(c_{i,k})\varphi(c_{j,k}^*) \\ &= \varphi\left(\sum_k c_{i,k}c_{j,k}^*\right) \\ &= \varphi(\langle c_i, c_j \rangle) \\ &= n\delta_i^j I_{m+1} .\end{aligned}$$

This shows that $M^\varphi \left(M^\varphi\right)^\top = nI_{n(m+1)}$. The entries of M^φ are in the set $\{\pm 1/\sqrt{m+1}\}$, so the entries of $\sqrt{m+1}M^\varphi$ are in the set $\{\pm 1\}$. We have shown that

$$\sqrt{m+1}M^\varphi \left(\sqrt{m+1}M^\varphi\right)^\top = n(m+1)I_{n(m+1)} ,$$

which establishes the theorem. □

A less technical method to prove the above theorem without assumptions on $m+1$ is as follows: Let $H \in \mathcal{H}(n, X_m)$, and let

$$H = \frac{1}{\sqrt{m+1}}A + \frac{\sqrt{-m}}{\sqrt{m+1}}B,$$

where A and B are ± 1 matrices of order n. Then

$$AB^\top = BA^\top \text{ and } AA^\top + BB^\top = n(m+1)I_n.$$

Let M be a skew Hadamard matrix of order $m+1$. Substituting A for the diagonal entries of M and $\pm B$ for the off-diagonal entries ± 1 of M, it can be verified that the resulting matrix will be a Hadamard matrix of order $n(m+1)$. Although this proof is simpler than that of Theorem 2.4, the morphism method gives additional insights into existence and non-existence of QUH matrices, as demonstrated in Section 3.

Let q be an odd prime power and $\mathbb{F}_q$ be a finite field with q elements. The element $a \in \mathbb{F}_q$ is a *quadratic residue* if there exists $y \in \mathbb{F}_q$ such that $y^2 = a$. Otherwise, a is a non-residue. The *quadratic character* is defined to be $\chi_q(a) = 1$ if $a \in \mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ is a quadratic residue in $\mathbb{F}_q$, $\chi_q(a) = -1$ if $a \in \mathbb{F}_q^*$ is a quadratic non-residue in $\mathbb{F}_q$ and $\chi_q(0) = 0$. In the case where $q = p$ is a prime number, the quadratic character $\chi_p(a)$ on $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$ can be identified with the *Legendre symbol* and is denoted (a/p). Later we will use the fact that for a fixed prime p and for every $a, b \in \mathbb{Z}$, $(ab/p) = (a/p)\,(b/p)$, [9, Proposition 5.1.2]. Let $\{g_0 = 0, g_1, \ldots, g_{q-1}\}$ be an enumeration of $\mathbb{F}_q$ then $Q = [\chi_q(g_i - g_j)]_{0 \le i,j \le q-1}$ is the *Jacobsthal matrix* of order q.

Theorem 2.5 (Section 3, [6])**.** *Let q be an odd prime power with $q \equiv 3 \pmod 4$. Define 1×1 matrices $A_0 = B_0 = 1$, let Q be the $q \times q$ Jacobsthal matrix and J_q the $q \times q$ all-ones matrix. For each $t \ge 1$, define*

$$A_t = J_q \otimes B_{t-1}, \;\; B_t = I_q \otimes A_{t-1} + Q \otimes B_{t-1}\,.$$

Then for each t the matrix $\frac{1}{\sqrt{q+1}} A_t + i\frac{\sqrt{q}}{\sqrt{q+1}} B_t$ is a matrix in $\mathcal{H}(q^t, X_q)$.

Hence there exist $\mathcal{H}(q^t, X_q)$ matrices for all prime powers $q \equiv 3 \mod 4$. Since the Paley matrix of order $q+1$ is skew, we can apply Theorem 2.4 to obtain the following result.

Corollary 2.6. *Let $q \equiv 3 \mod 4$ be a prime power. For any integer $n \ge 1$ there exists a (real) Hadamard matrix of order $q^n + q^{n-1}$.*

This result was first discovered by Mukhopadhyay, and later clarified and elaborated by Seberry, [12, 13]. Of course, it would be interesting to develop constructions of Hadamard matrices at previously unknown orders. As a first contribution in this direction, we investigate the non-existence of QUH matrices in the next section.

3 Nonexistence of quaternary unit Hadamard matrices

The *Galois group* of an irreducible polynomial $p(x)$ is the group of field automorphisms of a splitting field of $p(x)$. Over $\mathbb{Q}$, the order of the Galois group and the degree of the splitting field coincide. The Galois correspondence gives an inclusion-reversing bijection between the lattice of subfields of $\mathbb{Q}[x]/\left(p(x)\right)$ and the subgroups of the Galois group.

An element $x \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic polynomial in $\mathbb{Z}[x]$. The ring of integers of a number field $k \subseteq \mathbb{C}$ is the largest subring of the algebraic integers contained in k, usually denoted $\mathcal{O}_k$. In the ring of integers of a number field, ideals factorise uniquely as a product of *prime ideals*, [11, Theorem 14]. Studying prime factorisations related to the determinant of a putative complex Hadamard matrix can sometimes yield nonexistence results. This argument is similar to one given by Winterhof for certain Butson Hadamard matrices, [15].

First, we introduce terminology for the factorisation of a prime ideal of $\mathbb{Z}$ in $\mathcal{O}_k$ for a number field k. As is customary we will denote prime ideals in k by the gothic letters $\mathfrak{p}$ and $\mathfrak{q}$ and rational primes by p and q.

Definition 3.1. *Let k be the splitting field of an irreducible polynomial, and q be a rational prime.*

- *q is inert in $\mathcal{O}_k$ if (q) is a prime ideal in $\mathcal{O}_k$.*
- *If q is not inert then it splits in $\mathcal{O}_k$. Let $(q) = \prod \mathfrak{q}_i^e$ be the prime ideal decomposition of (q). If $e \geq 1$ then q is ramified, otherwise it splits completely.*

The *discriminant* of a number field is an integer valued invariant that controls the factorisation of rational primes in that field. The following result is a special case of a more general result on the splitting of rational primes on number fields, see Theorems 21, 23 and 24 of Marcus' *Number Fields* for details, [11].

Theorem 3.2. *Let k be a number field. If a rational prime q is ramified in $\mathcal{O}_k$, then $q \mid \operatorname{disc}(k)$. Let k be the splitting field of some irreducible polynomial, where the degree of k over $\mathbb{Q}$ is $n = [k : \mathbb{Q}]$. If q is a rational prime such that $q \nmid \operatorname{disc}(k)$, then*

$$(q) = \mathfrak{q}_1 \dots \mathfrak{q}_r,$$

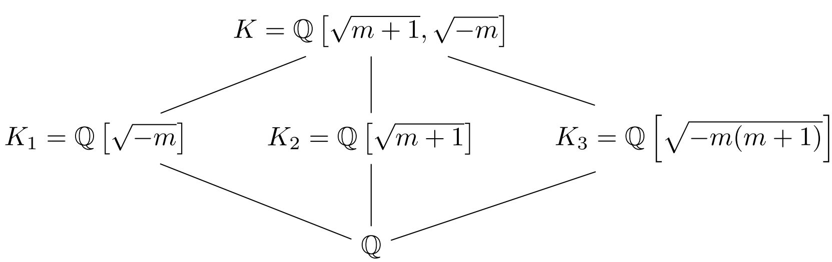
where $r|n$. Furthermore the action of the Galois group on $\{\mathfrak{q}_1, \dots, \mathfrak{q}_r\}$ is transitive.

In a quadratic extension of $\mathbb{Q}$, the Legendre symbol controls the splitting of prime ideals.

Theorem 3.3 (p.24, Theorem 25, [11])**.** *Let $k = \mathbb{Q}[\sqrt{d}]$ where d is a square-free integer. Then* $\operatorname{disc}(k) = d$ *if* $d \equiv 1 \mod 4$ *and* $\operatorname{disc}(k) = 4d$ *if* $d \equiv 2, 3 \mod 4$. *Suppose that q is an odd rational prime and* $q \nmid \operatorname{disc}(k)$. *Then*

- *q is inert in $\mathcal{O}_k$ if $(d/q) = -1$.*
- *q splits into distinct prime ideals in $\mathcal{O}_k$ if $(d/q) = 1$.*

We will study these concepts for the field $K = \mathbb{Q}[\alpha]$, which by Proposition 2.1 is the splitting field of $\mathfrak{m}(x)$. Since $2/(\alpha_m + \alpha_m^*) = \sqrt{m+1}$ and $(\sqrt{m+1})\alpha_m - 1 = \sqrt{-m}$ we have isomorphism $\mathbb{Q}[\alpha_m] \simeq \mathbb{Q}[\sqrt{-m}, \sqrt{m+1}]$. There are three intermediate subfields of K, as illustrated.



The lattice of subfields of K.

The discriminant of a biquadratic extension is given as an exercise by Marcus.

Proposition 3.4 (p.36-37, [11]). *The discriminant of a biquadratic extension* $k = \mathbb{Q}[\sqrt{a}, \sqrt{b}]$ *where* $\gcd(a, b) = 1$ *is*

$$\mathrm{disc}(k) = \mathrm{disc}(k_1)\mathrm{disc}(k_2)\mathrm{disc}(k_3),$$

where $k_1 = \mathbb{Q}[\sqrt{a}]$, $k_2 = \mathbb{Q}[\sqrt{b}]$ *and* $k_3 = \mathbb{Q}[\sqrt{ab}]$.

Let $G = \mathrm{Gal}(K/\mathbb{Q})$ be the Galois group the splitting field of $\mathfrak{m}(x)$. By the Galois correspondence G has order 4, and has three distinct subgroups of order 2. So G is elementary abelian, generated by $\sigma : \sqrt{m+1} \mapsto -\sqrt{m+1}$ and $\tau : \sqrt{-m} \mapsto -\sqrt{-m}$. We identify τ with complex conjugation. Note that $K_1 = \mathrm{Fix}(\sigma)$ is the fixed field of σ, that $K_2 = \mathrm{Fix}(\tau)$ is the fixed field of τ and $K_3 = \mathrm{Fix}(\sigma\tau)$ is the fixed field of $\sigma\tau$.

From now on, let $m = p$ be a prime congruent to 3 modulo 4, and write s for the squarefree part of $p + 1$. Then $K \simeq \mathbb{Q}[\sqrt{-p}, \sqrt{s}]$, and applying Proposition 3.4 we have

$$\mathrm{disc}(K) = \begin{cases} s^2p^2 & \text{if } s \equiv 1 \mod 4 \\ 16s^2p^2 & \text{if } s \equiv 2, 3 \mod 4 \end{cases}.$$

Let q be a prime number. By Theorem 3.2, the prime q ramifies in $\mathcal{O}_K$ only if $q = p$ or $q|s$. Next we describe which non-ramified primes split in $\mathcal{O}_K$.

Proposition 3.5. *Let* q *be a rational prime not dividing* $\mathrm{disc}(k)$. *Then one of the following holds:*

- $(q) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$ *in* $\mathcal{O}_K$ *and* q *splits in every subfield of* K.
- $(q) = \mathfrak{q}_1\mathfrak{q}_2$ *in* $\mathcal{O}_K$ *and* q *splits in one proper subfield of* K, *being inert in the other two.*

Proof. By Theorem 3.3, the prime q splits in K_1 if and only if $(-p/q) = 1$, and q splits in K_2 if and only if $(s/q) = 1$. Suppose that $(-p/q) = (s/q) = -1$. Then $(-ps/q) = (-p/q)\,(s/q) = 1$, so q splits in K_3. We conclude that no rational prime is inert in K.

Since by assumption q does not ramify, Theorem 3.2 tells us that q splits in $\mathcal{O}_K$ into two or four prime ideals. Suppose that $(q) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$. Then up to a relabeling of the primes $\mathfrak{q}_i$ we can assume that

$$\begin{aligned} \mathfrak{q}_1^\sigma &= \mathfrak{q}_2, & \mathfrak{q}_3^\sigma &= \mathfrak{q}_4 \\ \mathfrak{q}_1^\tau &= \mathfrak{q}_3, & \mathfrak{q}_2^\tau &= \mathfrak{q}_4 \\ \mathfrak{q}_1^{\sigma\tau} &= \mathfrak{q}_4, & \mathfrak{q}_2^{\sigma\tau} &= \mathfrak{q}_3 \end{aligned}$$

This implies that $(\mathfrak{q}_1\mathfrak{q}_2)^\sigma = \mathfrak{q}_1\mathfrak{q}_2$ and $(\mathfrak{q}_3\mathfrak{q}_4)^\sigma = \mathfrak{q}_3\mathfrak{q}_4$, therefore $\mathfrak{q}_1\mathfrak{q}_2$ and $\mathfrak{q}_3\mathfrak{q}_4$ are ideals in the fixed field K_1 of σ and thus q splits as $(q) = (\mathfrak{q}_1\mathfrak{q}_2)(\mathfrak{q}_3\mathfrak{q}_4)$ in K_1. We can show analogously that q splits in K_2 and K_3. Suppose next that q splits in K as $\mathfrak{q}_1\mathfrak{q}_2$. Then the Galois group acts as in one of the following possibilities.

$\mathfrak{q}_1^\sigma$	$\mathfrak{q}_1^\tau$	$\mathfrak{q}_1^{\sigma\tau}$	Subfield containing $\mathfrak{q}_1$ and $\mathfrak{q}_2$
$\mathfrak{q}_1$	$\mathfrak{q}_2$	$\mathfrak{q}_2$	$K_1 = \mathrm{Fix}(\sigma)$
$\mathfrak{q}_2$	$\mathfrak{q}_1$	$\mathfrak{q}_2$	$K_2 = \mathrm{Fix}(\tau)$
$\mathfrak{q}_2$	$\mathfrak{q}_2$	$\mathfrak{q}_1$	$K_3 = \mathrm{Fix}(\sigma\tau)$

In each case, there is exactly one non-identity element $g \in G$ fixing both $\mathfrak{q}_1$ and $\mathfrak{q}_2$. So q splits in the fixed field of g, and is inert in the other two intermediate subfields. □

In our application to QUH matrices, we will require the following special case of Proposition 3.5.

Corollary 3.6. *Let q be an odd rational prime q, coprime to both p and s. In $\mathcal{O}_K$, we have $(q) = \mathfrak{q}_1\mathfrak{q}_2$ with $\mathfrak{q}_1^\tau = \mathfrak{q}_1$ and $\mathfrak{q}_2^\tau = \mathfrak{q}_2$ if and only if $(-p/q) = -1$ and $(s/q) = 1$.*

Proof. Since $\mathfrak{q}_1^\tau = \mathfrak{q}_1$ it must be the case that $\mathfrak{q}_1^\sigma = \mathfrak{q}_2$ and, by Proposition 3.5, q splits in K_2 as $\mathfrak{q}_1\mathfrak{q}_2$. So by Theorem 3.3, we must have $(s/q) = 1$. Furthermore, (q) must be inert in K_1, from which we obtain $(-p/q) = -1$ as required. The converse follows from Theorem 3.3 and Proposition 3.5. □

Recall that the action of τ on K corresponds to the action of complex conjugation on K. Therefore the case above is equivalent to $(q) = \mathfrak{q}_1\mathfrak{q}_2$ with $\mathfrak{q}_1^* = \mathfrak{q}_1$ and $\mathfrak{q}_2^* = \mathfrak{q}_2$. We can now formulate our main nonexistence theorem.

Theorem 3.7. *Let n be an odd integer, with squarefree part t. Let $p \equiv 3 \mod 4$ be a prime number such that the squarefree part of $p+1$ is $s > 1$. If there exists an odd prime q such that*

- *q divides t,*
- *$(s/q) = 1$, and*
- *$(-p/q) = -1$,*

then $\mathcal{H}(n, X_p)$ is empty.

Proof. Let $M \in \mathcal{H}(n, X_p)$ and set $D = (p+1)^n \det M$. Then $D \in \mathcal{O}_K$, since $(p+1)\alpha \in \mathcal{O}_K$ for every $\alpha \in X_p$. The matrix H is complex Hadamard, therefore $DD^* = (p+1)^{2n} n^n = a^2 t^n$, for some $a \in \mathbb{Z}$. By Corollary 3.6, $(q) = \mathfrak{q}_1 \mathfrak{q}_2$ in $\mathcal{O}_K$ with $\mathfrak{q}_1 = \mathfrak{q}_1^*$. We have that $q|t$, so since n is odd the prime ideal $\mathfrak{q}_1$ appears with odd multiplicity in the decomposition of $(p+1)^{2n} n^n$ in $\mathcal{O}_K$. Since $\mathfrak{q}_1$ is prime and divides the product $(D)(D^*)$, it divides one of the factors; without loss of generality, suppose that $\mathfrak{q}_1$ divides (D). So (D) factors into prime ideals uniquely as

$$(D) = \mathfrak{q}_1^{\ell} \prod_j \mathfrak{p}_j^{\ell_j},$$

Then $(D^*) = (D)^* = \mathfrak{q}_1^{\ell} \prod_j (\mathfrak{p}_j^*)^{\ell_j}$. But implies that $\mathfrak{q}_1$ appears with even multiplicity in $(D)(D^*)$, contradicting its odd multiplicity in $(p+1)^{2n} n^n$. □

The only prime of the form $n^2 - 1$ is 3. In this case the matrices $\mathcal{H}(n, X_3)$ coincide with the unreal $BH(n, 6)$ matrices of Compton, Craigen and de Launey. The set $\mathcal{H}(n, X_3)$ is empty if there exists a prime $q \equiv 5 \pmod 6$ which divides the square-free part of n (see Theorem 2 of [2] or Theorem 5 of [15] for a proof).

We conclude this paper by discussing some consequences of Theorem 3.7. Suppose first that $p = 7$. Then a prime q satisfying both $(q/7) = -1$ and $(2/q) = 1$ cannot divide the square-free part of n. By quadratic reciprocity, these are the primes which satisfy both $q \equiv 3, 5, 6 \mod 7$ and $q \equiv 1, 7 \mod 8$. By Dirichlet's Theorem on primes in arithmetic progressions, there are infinitely many such primes. Similar results hold for each prime p, as illustrated in the table below.

p	n
7	$17, 31, 41, 47, 51, 73, 85, 89, 93, 97, 103, 119, 123, 141, \ldots$
11	$13, 39, 61, 65, 73, 83, 91, 107, 109, 117, 131, 143, 167, \ldots$
19	$29, 31, 41, 59, 71, 79, 87, 89, 93, 109, 123, 145, 151, \ldots$
23	$5, 15, 19, 35, 43, 45, 53, 55, 57, 65, 67, 85, 95, 97, 105, \ldots$
31	$17, 23, 51, 69, 73, 79, 85, 89, 115, 119, 127, 137, 151, \ldots$
43	$5, 7, 15, 19, 21, 35, 37, 45, 55, 57, 63, 65, 77, 85, 89, 91, \ldots$

Pairs (n, p) such that $\mathcal{H}(n, p)$ is empty.

In fact, it is a consequence of the Chebotarev Density Theorem that the proportion of primes $q \leq N$ to which the conditions of Theorem 3.7 apply tends to 1/4 as N tends to infinity. In particular, there are infinitely many primes which obstruct the existence of matrices in $\mathcal{H}(n, X_p)$ for any fixed p.

To illustrate Theorem 3.7 in a case where not all ideals are principal, we consider $p = 43$ and $q = 5$, then $s = 11$. We have $(5/43) = -1$, thus the prime 5 should be inert in $\mathcal{O}_{K_1}$. By Proposition 3.5, (5) splits in $\mathcal{O}_K$ as the product of two prime ideals in $\mathcal{O}_{K_2}$, indeed $(5) = (5, 1+\sqrt{11})(5, 1-\sqrt{11})$ in $\mathcal{O}_K$. If there exists $H \in \mathcal{H}(5, X_{43})$ then $D = 11^5 \det H$ and $DD^* = 11^{10} \cdot 5^5$. Thus in $\mathcal{O}_K$ this means

$$(D)(D)^* = (11^5)^2(5, 1 + \sqrt{11})^5(5, 1 - \sqrt{11})^5.$$

The ideal $(5, 1+\sqrt{11}) = (5, 1+\sqrt{11})^*$ appears with even multiplicity on the left hand side and odd multiplicity on the right hand side. Hence $\mathcal{H}(5, X_{43})$ is empty.

Acknowledgements

This research was completed while JP and PH were undergraduates and GNP was a doctoral student at Worcester Polytechnic Institute. JP was supported by a Student Undergraduate Research Fellowship sponsored by the office of the Dean of Arts and Sciences. PH and GNP were supported by PÓC's startup funds. The authors acknowledge the anonymous referees for many helpful suggestions which improved the exposition of the paper.

References

[1] J. H. E. Cohn, Hadamard matrices and some generalisations, *Amer. Math. Monthly*, **72** (1965), 515–518.

[2] B. Compton, R. Craigen, and W. de Launey, Unreal $BH(n, 6)$'s and Hadamard matrices, *Des. Codes Cryptogr.*, **79(2)** (2016), 219–229.

[3] W. de Launey and D. Flannery, *Algebraic design theory*, Mathematical Surveys and Monographs, vol. 175. American Mathematical Society, Providence, RI, 2011.

[4] R. Egan and P. Ó Catháin, Morphisms of Butson classes, *Linear Algebra Appl.*, **577** (2019), 78–93.

[5] R. Egan, P. Ó Catháin, and E. Swartz, Spectra of Hadamard matrices, *Australas. J. Combin.*, **73** (2019), 501–512.

[6] K. Fender, H. Kharaghani, and S. Suda, On a class of quaternary complex Hadamard matrices, *Discrete Math.*, **341(2)** (2018), 421–426.

[7] J. Hadamard, Résolution d'une question relative aux déterminants, *Bull. Sci. Math.*, **17** (1893), 240–246.

[8] K. J. Horadam, *Hadamard matrices and their applications*, Princeton University Press, Princeton, NJ, 2007.

[9] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition, 1990.

[10] I. M. Isaacs, *Algebra: a graduate course*, volume 100 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, RI, 2009, Reprint of the 1994 original.

[11] D. A. Marcus, *Number fields*, Universitext. Springer, Cham, 2018.

[12] A. C. Mukhopadhyay, Some infinite classes of Hadamard matrices, *J. Combin. Theory Ser. A*, **25(2)** (1978), 128–141.

[13] J. Seberry, Some infinite classes of Hadamard matrices, *J. Austral. Math. Soc. Ser. A*, **29(2)** (1980), 235–242.

[14] R. J. Turyn, Complex Hadamard matrices, In *Combinatorial Structures and their Applications (Proc, Calgary Internat. Conf., Calgary, Alta., 1969)*, pages 435–437, Gordon and Breach, New York, 1970.

[15] A. Winterhof, On the non-existence of generalized Hadamard matrices, *J. Statist. Plann. Inference*, **84(1-2)** (2000), 337–342.