Journal of Algebraic Combinatorics (2022) 56:271–277
https://doi.org/10.1007/s10801-021-01109-8

Equivalence of Butson-type Hadamard matrices

Patric R. J. Östergård[1]

Received: 20 April 2021 / Accepted: 3 December 2021 / Published online: 2 February 2022

Abstract
Two matrices H_1 and H_2 with entries from a multiplicative group G are said to be monomially equivalent, denoted by $H_1 \cong H_2$, if one of the matrices can be obtained from the other via a sequence of row and column permutations and, respectively, left- and right-multiplication of rows and columns with elements from G. One may further define matrices to be Hadamard equivalent if $H_1 \cong \phi(H_2)$ for some $\phi \in \mathrm{Aut}(G)$. For many classes of Hadamard and related matrices, it is straightforward to show that these are closed under Hadamard equivalence. It is here shown that also the set of Butson-type Hadamard matrices is closed under Hadamard equivalence.

Keywords Butson-type Hadamard matrix · Complex matrix · Hadamard equivalence · Monomial equivalence

1 Introduction

The concept of *equivalence*—or *isomorphism*, depending on the setting—is central in the study of mathematical structures. Equivalence is essentially about dealing with ambient symmetries and leads to a partitioning of structures into *equivalence classes*. For example, the aim of a classification of structures is to find a transversal of the equivalence classes. The equivalence mappings from a structure onto itself give the symmetries of the structure (and form a group under composition).

The definition of equivalence depends on the studied structures, whose main properties should be respected. For some structures, there is one obvious definition, but for others the situation may be more involved. In any case, it is generally desirable to have definitions that lead to as large equivalence classes as possible.

Hadamard and related matrices are considered in this paper; for more information about such structures, [2,4,7] can be consulted. See also [8,9,11–14] for specific classi-

✉ Patric R. J. Östergård
patric.ostergard@aalto.fi

[1] Department of Communications and Networking, Aalto University School of Electrical Engineering, P.O. Box 15400, 00076 Aalto, Finland

fication studies. Two types of equivalence are commonly considered for Hadamard and related matrices: monomial equivalence and Hadamard equivalence. It is not obvious whether the set of Butson-type Hadamard matrices is closed under Hadamard equivalence. We shall show in this paper that this is indeed the case.

Equivalence of Hadamard and related matrices is considered in Sect. 2, and the main proof regarding Hadamard equivalence of Butson-type matrices is given in Sect. 3. Throughout the paper, the group operation is identified with multiplication.

2 Equivalence of Hadamard matrices

A (real) *Hadamard matrix* of order n is an $n \times n$ matrix $H = (h_{i,j})$ with entries from the group $(\{-1, 1\}, \cdot)$ such that for any distinct $1 \leq a, b \leq n$, the multiset $\{h_{a,k}h_{b,k}^{-1} : 1 \leq k \leq n\}$ contains -1 and 1 equally often ($n/2$ times each). (Here, $h = h^{-1}$ for both elements of the group, but the definition is given in the particular form for the sake of a later generalization.) It is a classical result that a necessary condition for a Hadamard matrix of order n to exist is that $n = 1, 2$ or n is divisible by 4. It is further conjectured that this is also a sufficient condition; proving this conjecture is the main open question in the theory of Hadamard and related matrices.

A *generalized Hadamard matrix* of order $m\lambda$ and index λ is an $m\lambda \times m\lambda$ matrix $H = (h_{i,j})$ with entries from a group G of order m such that for any distinct $1 \leq a, b \leq m\lambda$, the multiset

$$\{h_{a,k}h_{b,k}^{-1} : 1 \leq k \leq m\lambda\} \tag{1}$$

contains each element of G equally often (λ times each). A comparison with the definition of real Hadamard matrices given earlier shows that real Hadamard matrices are generalized Hadamard matrices of order n and index $n/2$.

To consider equivalence of Hadamard and related matrices, we define the monomial group $\mathcal{G}_n$ as the matrix group that is the subgroup of $\mathrm{GL}_n(\mathbb{Z}G)$ whose elements are the matrices in which each row and column contains exactly one element of G. We further let the group $\mathcal{G}_n \times \mathcal{G}_n$ act on an $n \times n$ matrix M by $(X, Y) \cdot M = XMY^{\mathrm{T}}$.

Definition 1 Two $n \times n$ matrices with entries from a group G, H_1 and H_2, are said to be *monomially equivalent*, denoted by $H_1 \cong H_2$, if $H_1 = XH_2Y^{\mathrm{T}}$ for some $(X, Y) \in \mathcal{G}_n \times \mathcal{G}_n$.

In other words, two matrices are monomially equivalent if one can be obtained from the other using row and column permutations and, respectively, left- and right-multiplication of rows and columns with elements from G. Such left- and right-multiplications permute the values in entries of individual rows and columns, respectively, and those permutions are called *local equivalence operations* in [5, Sect. 4.4.1]. If the group G is nonabelian, we get two different sets of permutations, but if the group G is abelian, the order of multiplication does not matter, and we get only one.

The set of generalized Hadamard matrices is closed under monomial equivalence; see [6, Theorem 1.16] for a proof.

In addition to local equivalence operations, one may also consider *global equivalence operations* [5, Sect. 4.4.3], which are permutations of the elements of the group (in all entries) under which a given class of matrices is closed. The term 'global equivalence operations' is used in [5] only for those permutations that are not local equivalence operations, but the author of the current paper finds it more natural to let the local equivalence operations form a subset of the global equivalence operations. As shown in [5, Theorem 4.4.10], for many classes of Hadamard and related matrices and with an abelian group G, the global equivalence operations are generated by the local equivalence operations and the group automorphisms, $\mathrm{Aut}(G)$.

We write $f(H)$ for the matrix obtained by applying the function f to each entry of H.

Definition 2 Two $n \times n$ matrices with entries from a group G, H_1 and H_2, are said to be *Hadamard equivalent* if $H_1 \cong \phi(H_2)$ for some $\phi \in \mathrm{Aut}(G)$, that is, $H_1 = \phi(XH_2Y^{\mathrm{T}})$ where $(X, Y) \in \mathcal{G}_n \times \mathcal{G}_n$.

Definition 2 is [7, Definition 4.12]. For some matrix classes, it is easy to show that they are closed under the mapping $\phi(H)$. For example, for generalized Hadamard matrices, the elements of (1) become

$$\phi(h_{a,k})\phi(h_{b,k})^{-1} = \phi(h_{a,k})\phi(h_{b,k}^{-1}) = \phi(h_{a,k}h_{b,k}^{-1}), \tag{2}$$

and because ϕ is a bijection, the multiset remains unchanged. In the real case, $|\mathrm{Aut}(G)| = 1$, and monomial and Hadamard equivalence coincide. Hence, there is no conflict between our definitions and the fact that both terms—and just *equivalence*—have been used for real Hadamard matrices in the literature.

Another generalization of real Hadamard matrices are complex Hadamard matrices. A *complex Hadamard matrix* of order n is an $n \times n$ matrix $H = (h_{i,j})$ with entries that are unit complex numbers, that is, lie on the unit circle in the complex plane, such that

$$HH^* = nI_n, \tag{3}$$

where H^* denotes the conjugate transpose of H, I_n is the $n \times n$ identity matrix, and operations are carried out in the field $\mathbb{C}$. This is the same as saying that for any distinct $1 \le a, b \le n$,

$$\sum_{k=1}^{n} h_{a,k}h_{b,k}^{-1} = 0, \tag{4}$$

which makes a comparison with (1) easier.

The set of entries of complex Hadamard matrices forms an *infinite* group that is isomorphic to the circle group S^1. General complex Hadamard matrices are of interest in physics [19], whereas in discrete mathematics, the main focus has been on matrices with entries from a *finite* subgroup. In fact, every finite subgroup of $\mathbb{C}^*$ is a (cyclic)

group of roots of unity. A *Butson-type Hadamard matrix* of order n over mth roots of unity is a complex Hadamard matrix of order n with $h^m = 1$ for every entry h.

It is an easy exercise to show that the sets of complex and Butson-type Hadamard matrices are closed under monomial equivalence but what about Hadamard equivalence?

A basic fact for the circle group is that $\mathrm{Aut}(S^1)$ is isomorphic to the unique group of order 2 (cf. [1, Ch. 4, Problem 25]), and the nontrivial element of $\mathrm{Aut}(S^1)$ corresponds to complex conjugation here. Complex conjugation of H is denoted by $\overline{H}$. To verify that the set of complex Hadamard matrices is closed under conjugation, (3) can be used to get

$$\overline{H}\ \overline{H}^* = \overline{H}\ \overline{H^*} = \overline{HH^*} = \overline{nI_n} = nI_n.$$

So the only difference between monomial equivalence and Hadamard equivalence for complex Hadamard matrices is the inclusion of complex conjugation in the latter case. Complex conjugation indeed plays a central role in the study of complex Hadamard matrices [18].

For Butson-type Hadamard matrices over mth roots of unity, on the other hand, the entries are from a cyclic group of order m, that is, a group isomorphic to C_m. By letting $C_m = \langle g : g^m = e \rangle$, the elements of $\mathrm{Aut}(C_m)$ are given by the functions

$$f(x) = x^k, \quad \gcd(k, m) = 1, 1 \leq k \leq m. \tag{5}$$

Hence, $|\mathrm{Aut}(C_m)| = \varphi(m)$, where $\varphi(m)$ is Euler's totient function.

In the literature, studies of equivalence of Butson-type Hadamard matrices over mth roots of unity have mainly considered the case $m = 4$; see [13,14]. We have $|\mathrm{Aut}(C_4)| = 2$, and the only nontrivial element corresponds to complex conjugation. Butson-type Hadamard matrices form a subset of complex Hadamard matrices, and we have seen that the set of such matrices is closed under complex conjugation.

However, there are studies of equivalence of Butson-type Hadamard matrices over mth roots of unity for larger values of m. One such example is [12], co-authored by the current author, where Hadamard equivalence is used without justifications. Those missing justifications will now be provided.

3 Hadamard equivalence of Butson-type matrices

Everything would be straightforward if (5) would be automorphisms of $\mathbb{C}$ for all admissible values of k, but this is not the case as only $k = 1$ (identity) and $k = m - 1$ (conjugation) give such automorphisms. However, considering cyclotomic fields $\mathbb{Q}(\zeta)$, where ζ is a primitive mth root of unity, rather than $\mathbb{C}$ makes it possible to prove the main theorem in a direct manner.

Theorem 1 *The set of Butson-type Hadamard matrices is closed under Hadamard equivalence.*

Proof Because the set of Butson-type Hadamard matrices is closed under monomial equivalence, it remains to consider the case of applying a group automorphism to each entry of the matrix. Let $H = (h_{i,j})$ be a Butson-type Hadamard matrix of order n over mth roots of unity. By (2), we are done if we are able to show that $\sum_{k=1}^{n} h_{a,k}h_{b,k}^{-1} = 0$ implies that $\sum_{k=1}^{n} \phi(h_{a,k}h_{b,k}^{-1}) = 0$, for any ϕ given by (5).

Let ζ be a primitive mth root of unity. It is well known that $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ has order $\varphi(m)$ and that the automorphisms map the mth roots of unity by a function (5); see, for example, [20, Theorem 2.5]. A function ϕ given by (5) and whose domain is the mth roots of unity determines the entire automorphism ϕ' of $\mathbb{Q}(\zeta)$. So in $\mathbb{Q}(\zeta)$,

$$\sum_{k=1}^{n} \phi(h_{a,k}h_{b,k}^{-1}) = \sum_{k=1}^{n} \phi'(h_{a,k}h_{b,k}^{-1}) = \phi'\left(\sum_{k=1}^{n} h_{a,k}h_{b,k}^{-1}\right) = \phi'(0) = 0.$$

□

We shall next give another, longer but more constructive, proof of the same result. We will need a few lemmas and theorems, some of which—especially Lemma 1—are well known but proofs are included for completeness.

Lemma 1 *Let $m \geq 2$. If ζ is a primitive mth root of unity, then $\sum_{i=0}^{m-1} \zeta^i = 0$.*

Proof As ζ is an mth root of unity, $\zeta^m = 1$, that is, $\zeta^m - 1 = 0$. We may now write

$$0 = \zeta^m - 1 = (\zeta - 1)(1 + \zeta + \zeta^2 + \cdots + \zeta^{m-1}),$$

and the result follows as 1 is not a primitive mth root of unity, so $\zeta \neq 1$. □

Lemma 2 *The function (5) maps a qth root of unity to a qth root of unity, for any q.*

Proof If $z^q = 1$, then $(z^k)^q = (z^q)^k = 1^k = 1$. □

Lemma 3 *Let G be the group of mth roots of unity ($m \geq 2$), let $\phi \in \mathrm{Aut}(G)$, let p be a prime factor of m, and let ζ be a primitive mth root of unity. Then, $\sum_{i=0}^{p-1} \phi(\zeta^{im/p+j}) = 0$ for any integer j.*

Proof We get

$$\begin{aligned}\sum_{i=0}^{p-1} \phi(\zeta^{im/p+j}) &= \sum_{i=0}^{p-1} \phi(\zeta^j \zeta^{im/p}) = \sum_{i=0}^{p-1} \phi(\zeta^j)\phi(\zeta^{im/p}) \\ &= \phi(\zeta^j) \sum_{i=0}^{p-1} \phi(\zeta^{im/p}) = \phi(\zeta^j) \sum_{i=0}^{p-1} \phi((\zeta^{m/p})^i) \\ &= \phi(\zeta^j) \sum_{i=0}^{p-1} \phi((\zeta^r)^i)\end{aligned}$$

by substituting $r = m/p$. Hence, ζ^r is a pth root of unity, which must be primitive as p is a prime (and $\zeta^r \neq 1$ as ζ is a primitive mth root of unity). Then, $(\zeta^r)^i, 0 \leq i \leq p-1$ are precisely the p pth roots of unity. By Lemma 2 and the fact that automorphisms are bijections, the values of $\phi((\zeta^r)^i)$ for $0 \leq i \leq p-1$ are also the pth roots of unity. Therefore, $\sum_{i=0}^{p-1} \phi((\zeta^r)^i) = 0$ by Lemma 1. □

We need one more result, which has been proved in several different ways in the literature [3,10,15–17].

Theorem 2 *Let ζ be a primitive mth root of unity, and, for $1 \leq i \leq n$, let z_i be an mth root of unity. Every relation of the form $\sum_{i=1}^{n} a_i z_i = 0$ can be obtained as a $\mathbb{Z}$-linear combination of relations, where each relation is of the form $\sum_{i=0}^{p-1} \zeta^{im/p+j} = 0$ for some prime factor p of m and integer j.*

We are now ready for an alternative proof of the main theorem.

Proof of Theorem 1 As in the earlier proof, we show that $\sum_{k=1}^{n} h_{a,k} h_{b,k}^{-1} = 0$ implies that $\sum_{k=1}^{n} \phi(h_{a,k} h_{b,k}^{-1}) = 0$, for any ϕ given by (5).

By Theorem 2, we may write

$$0 = \sum_{k=1}^{n} h_{a,k} h_{b,k}^{-1} = \sum_{s=1}^{N} \left(T_s \sum_{i=0}^{p_s-1} \zeta^{im/p_s+j_s} \right),$$

where ζ is a primitive mth root of unity and, for $1 \leq s \leq N$, T_s are integers, p_s are (not necessarily distinct) prime factors of m, and j_s are integers. Now consider the linear combination obtained by substituting $h_{a,k} h_{b,k}^{-1}$ with $\phi(h_{a,k} h_{b,k}^{-1})$ for all $1 \leq k \leq n$:

$$\sum_{k=1}^{n} \phi(h_{a,k} h_{b,k}^{-1}) = \sum_{s=1}^{N} \left(T_s \sum_{i=0}^{p_s-1} \phi(\zeta^{im/p_s+j_s}) \right) = \sum_{s=1}^{N} (T_s \cdot 0) = 0,$$

utilizing Lemma 3. □

Acknowledgements The author is grateful to Mikhail Ganzhinov and Padraig Ó Catháin for valuable discussions on various algebraic structures and to the referees for helpful comments.

Funding Open Access funding provided by Aalto University.

Data availability The study has no associated data.

References

1. Armstrong, M.A.: Basic Topology. Springer, New York (1983)
2. Craigen, R., Kharaghani, H.: Hadamard matrices and Hadamard designs. In: Colbourn, C.J., Dinitz, J.H. (eds.) Handbook of Combinatorial Designs, 2nd edn., pp. 273–280. Chapman & Hall/CRC, Boca Raton (2007)
3. de Bruijn, N.G.: On the factorization of cyclic groups. Indagationes Math. **15**, 370–377 (1953)
4. de Launey, W.: Generalized Hadamard matrices. In: Colbourn, C.J., Dinitz, J.H. (eds.) Handbook of Combinatorial Designs, 2nd edn., pp. 301–306. Chapman & Hall/CRC, Boca Raton (2007)
5. de Launey, W., Flannery, D.: Algebraic Design Theory. American Mathematical Society, Providence (2011)
6. Evans, A.B.: Orthogonal Latin Squares Based on Groups. Springer, Cham (2018)
7. Horadam, K.J.: Hadamard Matrices and Their Applications. Princeton University Press, Princeton (2007)
8. Kharaghani, H., Tayfeh-Rezaie, B.: On the classification of Hadamard matrices of order 32. J. Combin. Des. **18**, 328–336 (2010)
9. Kharaghani, H., Tayfeh-Rezaie, B.: Hadamard matrices of order 32. J. Combin. Des. **21**, 212–221 (2013)
10. Lam, T.Y., Leung, K.H.: On vanishing sums of roots of unity. J. Algebra **224**, 91–109 (2000)
11. Lampio, P.H.J., Östergård, P.R.J.: Classification of difference matrices over cyclic groups. J. Statist. Plann. Inference **141**, 1194–1207 (2011)
12. Lampio, P.H.J., Östergård, P.R.J., Szöllősi, F.: Orderly generation of Butson Hadamard matrices. Math. Comp. **89**, 313–331 (2020)
13. Lampio, P.H.J., Szöllősi, F., Östergård, P.R.J.: The quaternary complex Hadamard matrices of orders 10, 12, and 14. Discrete Math. **313**, 189–206 (2013)
14. Östergård, P.R.J., Paavola, W.T.: Quaternary complex Hadamard matrices of order 18. J. Combin. Des. **29**, 129–140 (2021)
15. Rédei, L.: Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen. Acta Math. Acad. Sci. Hungar. **1**, 197–207 (1950)
16. Rédei, L.: Über das Kreisteilungspolynom. Acta Math. Acad. Sci. Hungar. **5**, 27–28 (1954)
17. Schoenberg, I.J.: A note on the cyclotomic polynomial. Mathematika **11**, 131–136 (1964)
18. Szöllősi, F.: Construction, classification and parametrization of complex Hadamard matrices, PhD thesis, Central European University, Budapest, 2011
19. Tadej, W., Życzkowski, K.: A concise guide to complex Hadamard matrices. Open Syst. Inf. Dyn. **13**, 133–177 (2006)
20. Washington, L.C.: Introduction to Cyclotomic Fields, 2nd edn. Springer, New York (1997)