
Publisher's PDF, also known as Version of record

License (if available):
CC BY

Link to published version (if available):
10.1007/s11786-018-0382-0

Link to publication record in Explore Bristol Research
PDF-document

This is the final published version of the article (version of record). It first appeared online via Springer at https://link.springer.com/article/10.1007%2Fs11786-018-0382-0. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: http://www.bristol.ac.uk/pure/about/ebr-terms
Construction of the Outer Automorphism of $S_6$ via a Complex Hadamard Matrix

Neil I. Gillespie · Padraig Ó Catháin · Cheryl E. Praeger

Received: 15 December 2017 / Revised: 20 March 2018 / Accepted: 22 March 2018 / Published online: 26 September 2018 © The Author(s) 2018

Abstract We give a new construction of the outer automorphism of the symmetric group on six points. Our construction features a complex Hadamard matrix of order six containing third roots of unity and the algebra of split quaternions over the real numbers.

Keywords Complex hadamard matrix · Outer automorphism · Symmetric group

Mathematics Subject Classification Primary 20B25; Secondary 05B20 · 20B30

1 Introduction

Sylvester showed that the fifteen two-subsets of a six element set can be formed into 5 parallel classes in six different ways and that the action of $S_6$ on these synthematic totals is essentially different from its natural action on six points [13]. To our knowledge this was the first construction for the outer automorphism of $S_6$.

Miller attributes the result that for $n \neq 6$, $S_n$ has no outer automorphisms to Hölder, and Sylvester’s construction of the outer automorphism of $S_6$ to Burnside [11]. He also gives a by-hand construction of the outer automorphism. The papers of Janusz and Rotman, and of Ward provide easily readable accounts which are similar to Sylvester’s [10,14]. Cameron and van Lint devoted an entire chapter (their sixth!) to the outer automorphism of $S_6$ [2]. They build on Sylvester’s construction to construct the 5-(12, 6, 1) Witt design, the projective plane of order 4, and the Hoffman–Singleton graph.

Via consideration of the cube in $\mathbb{R}^3$, Fournelle gives a heuristic for the existence of an outer automorphism of $S_6$, and constructs it with the aid of a computer [7]. Howard, Millson, Snowden and Vakil give two constructions of
the outer automorphism of $S_6$, and use this to describe the invariant theory of six points in certain projective spaces [9].

In this note we give a construction which we believe has not previously been described, using a complex Hadamard matrix of order 6 and a representation of the triple cover of $A_6$ over the complex numbers. This note is inspired by a construction of Marshall Hall Jr [8] for the outer automorphism of $M_{12}$ via a real Hadamard matrix of order 12, and by Moorhouse’s classification of the complex Hadamard matrices with doubly transitive automorphism groups [12]. It was in the latter paper that we first became aware of the complex Hadamard matrix of order 6 discussed in this article, where it is described as corresponding to the distance transitive triple cover of the complete bipartite graph $K_{6,6}$.

2 Hadamard Matrices

Let $\omega$ be a primitive complex third root of unity. Then the matrix $H_6$ is complex Hadamard.

$$H_6 = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & \omega & \omega & \omega & \omega \\
1 & \omega & 1 & \omega & \omega & \omega \\
1 & \omega & \omega & 1 & \omega & \omega \\
1 & \omega & \omega & \omega & 1 & \omega \\
1 & \omega & \omega & \omega & \omega & 1
\end{pmatrix}$$

This means that $H_6$ satisfies the identity $H_6 H_6^\dagger = 6I_6$, where for an invertible complex matrix $A$, $A^\dagger$ is the complex conjugate transpose of $A$. Equivalently, $H_6$ reaches equality in Hadamard’s determinant bound. We refer the reader to [6] for a comprehensive discussion of Hadamard matrices and their generalisations.

An automorphism of a complex Hadamard matrix is a pair of monomial matrices $(P, Q)$ such that $P^{-1}HQ = H$. The set of all automorphisms of $H$ forms a group under composition. In this note we will work with the subgroup of automorphisms $(P, Q)$ where all non-zero entries are third roots of unity, we denote this group Aut($H$). Consider now the projection maps $\rho_1(P, Q) \mapsto P$ and $\rho_2(P, Q) \mapsto Q$. Since $1/\sqrt{6}H_6$ is unitary, and for any automorphism $(P, Q)$ of $H$ the identity $HQH^{-1} = P$ holds, it follows that $\rho_1$ and $\rho_2$ are conjugate representations of Aut$(H)$. Note further that $\rho_1$ is a faithful representation, since $Q = I$ forces $P = I$. Thus Aut$(H)$ is isomorphic to a finite subgroup of monomial matrices of $GL_6(\mathbb{C})$. Furthermore, if Aut$(H)$ contains a subgroup isomorphic to $G$, then the projections $\rho_1$ and $\rho_2$ onto the first and second components of Aut$(H)$ give two conjugate representations of $G$ by monomial matrices.

Every monomial matrix has a unique factorisation $P = DK$ where $D$ is diagonal and $K$ is a permutation matrix. The projection $\pi : P \mapsto K$ is a homomorphism for any group of monomial matrices. In general, the representation Aut$(H)^{\rho_1\pi}$ is not linearly equivalent to the representation Aut$(H)^{\rho_2\pi}$. As mentioned above, this phenomenon was first observed by Hall, who showed that the automorphism group of a Hadamard matrix of order 12 is isomorphic to $2 \cdot M_{12}$, and that $\rho_1\pi$ and $\rho_2\pi$ realise the two inequivalent actions of $M_{12}$ on 12 points [8]. This interpretation of the outer automorphism of $M_{12}$ was also used by Elkies, Conway and Martin in their analysis of the Mathieu groupoid $M_{13}$ [4].

Throughout this note we use the following shorthand for monomial matrices: we list the elements of the diagonal matrix $D$, and give the cycle notation for $K$ as a permutation of the columns of the identity matrix (i.e. a right action).

Consider the following pairs of monomial matrices.

$\tau_1 := ([1, 1, 1, 1, 1, 1](2, 3, 4, 5, 6), [1, 1, 1, 1, 1, 1](2, 3, 4, 5, 6))$

$\tau_2 := ([1, 1, \omega, \omega, \omega, \omega](1, 2), [1, 1, \omega, \omega, \omega, \omega](1, 2)(3, 6)(4, 5))$.

We define $*$ to be the entry-wise complex conjugation map, and consider the group $X = \langle \tau_1, \tau_2, * \rangle$. 
Proposition 1 The group $X$ is of the form $3^{10} \cdot S_6 \cdot 2$.

Proof Since $\tau_1^* = \tau_1$ and $\tau_2^* = \tau_2^{-1}$, we have that $X_0 = \langle \tau_1, \tau_2 \rangle$ is normal in $X$. Hence $X = X_0 \rtimes \langle \tau \rangle$, with $X_0$ of index 2 in $X$.

The commutator $[\tau_2, \tau] = ([1, 1, \omega, \bar{\omega}, \omega], [1, \bar{\omega}, \omega, \omega, \omega])$ consists of diagonal matrices; furthermore $\tau_2' := [\tau_2, \tau]^{-1} = ((1, 2), (1, 2)(3, 6)(4, 5))$, a pair of permutation matrices. Recall that $\langle s, t \mid s^6 = t^2 = (st)^5 = [t, s^2] = [t, s^3]^2 = 1 \rangle$ is a presentation for $S_6$ (see [1], for example). A computation with $t = \tau_2'$ and $s = \tau_1^2$ shows that all the relations in this presentation hold for these elements $s, t$, and hence $Y = \langle \tau_1, \tau_2' \rangle$ is isomorphic to a quotient of $S_6$. On the other hand, $Y^\rho_\pi$ is easily seen to be isomorphic to $S_6$, so we conclude that $Y \cong S_6$.

Now let $N$ be the subgroup of $X$ consisting of all elements for which each component is a diagonal matrix. Since $\tau_1^\rho$ and $\tau_2^\rho$ have determinants in $\{ \pm 1 \}$, every element of the projection $X_0^\rho$ also has determinant $\pm 1$. However all the elements of $N^\rho$ have third roots of unity along the diagonal, and so must have determinant 1. As a result, $X_0^\rho$ is isomorphic to a subgroup of $M \rtimes S_6$ where $M \cong 3^5$ is the group of unimodular diagonal matrices with entries from $(\omega)$, and $S_6$ acts as $Y^\rho_\pi$. The only non-trivial $S_6$-submodule of $M$ is the constant module of order 3.

Define $n_{i+1} : = [\tau_2, \tau]^{-1}$ for each $i \geq 1$. (We shift subscripts because the action of $\tau_1$ on $[\tau_2, \tau]$ gives elements of $N$ which have the non-initial rows of $H_6$ as the diagonal of the first component.) Since $[\tau_2, \tau] \in X_0$, we have $n_i \in X_0$ for $2 \leq i \leq 6$. Observe that

$$n_3 n_2 n_1^2 = ([1, 1, 1, 1, \omega, \bar{\omega}], [1, 1, 1, 1, \omega, \bar{\omega}])$$
$$n_3 n_2 n_1^2 = ([1, 1, 1, 1, \omega, \bar{\omega}], [1, 1, 1, 1, \omega, \bar{\omega}])$$

So neither of the projections $N^\rho_\rho$, $N^\rho_\pi$ are onto the constant module, and the kernel of $N^\rho_\pi$ is neither trivial nor the constant module. It follows that $N \cong M \rtimes M$. Finally, we observe that monomial matrices normalise diagonal matrices, and that $X_0$ acts as a group of monomial matrices in each component. It follows that $N \lhd X_0$, and that $Y$ is a complement of $N$ in $X_0$. Since $\tau$ acts on $N$ by inversion, $N \lhd X$.

The group $X$ has a natural action on $6 \times 6$ matrices over $\mathbb{C}$ where $(P, Q) \in X_0$ acts as $H^{(P, Q)} = P^{-1} H Q$, and $\tau$ acts by complex conjugation. We compute the stabiliser of $H_6$ under this action. We denote this group $\text{Aut}^\tau(H_6)$ to emphasise that this is a group of semi-linear transformations in its action on the normal subgroup $N$. We require the subgroups $X_0$, $Y$ and $N$ defined in Proposition 1 in the proof of the following.

Proposition 2 The group $\text{Aut}^\tau(H_6)$ is isomorphic to the nonsplit extension $3 \cdot S_6$, and $\text{Aut}^\tau(H_6)$ contains a $\mathbb{C}$-linear subgroup isomorphic to $3 \cdot A_6$.

Proof It is easily verified by hand that $H_6^{\nu_1} = H_6$ while $H_6^{\nu_2}$ is the complex conjugate $H_6^\tau$. Therefore both $\tau_1$ and the product $\tau_2^\tau$ fix $H_6$. We claim that $\text{Aut}^\tau(H_6) = \langle \tau_1, \tau_2^\tau \rangle$.

First, we show that the intersection $\text{Aut}^\tau(H_6) \cap N$ has order 3. To prove this, suppose that $(D, E) \in N$, and that $D^{-1} H_6 E = H_6$, or equivalently $D H_6 = H_6$. Since the first column of $H_6$ is constant, $D$ must be a scalar matrix. So $D$ commutes with $H_6$, and we have $D H_6 = H_6 D = H_6 E$. Hence $D = E$, so $(D, E) = (\omega^i I, \omega^i I)$ for some $i$. Since these elements do not leave $H_6$ invariant, the claim is proved.

We next claim that there is no element $(D, E)$ of $N$ such that $D H_6 = H_6 E$; suppose to the contrary that such a $(D, E)$ exists. Precisely the same argument as before shows that $D$ must be scalar. This implies that $H_6^\tau = H_6 E D^{-1}$, but this equation has no solution in diagonal matrices: since the first row of $H_6^\tau$ is equal to the first row of $H_6$, we would require $E D^{-1} = I_6$, from which we derive $H_6 = H_6^\tau$, a contradiction.

Consider the subgroup $K := \langle \tau_1, \tau_2^\tau, N \rangle$ of $X$. Since $X = \langle K, \tau \rangle$ and $\tau \notin K$, we have $|X : K| = 2$ and $X = K \cup (K \tau)$. It follows, moreover, from the previous arguments that no element of $K$ sends $H_6 - H_6^\tau$, and hence
no element of the right coset \( K \) can fix \( H_6 \). Therefore, \( \text{Aut}^\circ(H_6) \subseteq K \), and from the first paragraph of the proof we also have \( \text{Aut}^\circ(H_6) \sim N = K \). The quotient \( \text{Aut}^\circ(H_6)/(\text{Aut}^\circ(H_6) \cap N) \) is isomorphic to \( K/N \), an index 2 subgroup of \( X/N \sim S_6 \). In particular \( K/N \) contains \( A_6 \) as a normal subgroup of index 2. Since the element \( N\tau_2 \) does not lie in \( A_6 \) and does not centralise \( A_6 \) it follows that \( K/N \sim S_6 \).

We have shown that \( \text{Aut}^\circ(H_6) \) has a normal subgroup of order 3 with quotient isomorphic to \( S_6 \). The elements \((\tau_2)^{3i}\) for \( 0 \leq i \leq 4 \) project onto a set of Coxeter generators for \( S_6 \). With these generators, it is straightforward to construct a Sylow 3-subgroup of \( \text{Aut}^\circ(H_6) \). One such subgroup is generated by

\[
x := ([\bar{\omega}, 1, \omega, 1, \bar{\omega}](1, 2, 3), \quad [\omega, 1, \omega, 1, \bar{\omega}](1, 4, 6)(2, 3, 5))
\]

\[
y := ([\omega, \bar{\omega}, 1, 1, \bar{\omega}, \omega](4, 5, 6), \quad [\omega, \omega, \omega, \omega, \omega, \omega](1, 4, 6)(2, 5, 3))
\]

A computation shows that \( [x, y] = ([\omega, \omega, \omega, \omega, \omega], [\omega, \omega, \omega, \omega, \omega]) \). This shows that the commutator subgroup contains the normal subgroup of order 3, hence the extension is non-split. Elements of \( \text{Aut}^\circ(H) \) which map onto odd permutations act on \( [X, Y] \) by inversion. So the centraliser of this normal subgroup is of index 2 in \( \text{Aut}^\circ(H) \): this is necessarily a non-split central extension \( 3 \cdot A_6 \).

A perfect group \( S \) has a largest non-split central extension \( \hat{S} \) which is unique up to isomorphism. The center of \( \hat{S} \) is the Schur multiplier of \( S \), and every non-split central extension of \( S \) is a quotient of \( \hat{S} \). The number of generators of the Schur multiplier is bounded by \( g - r \) where \( g \) is the number of generators in a presentation of \( S \) and \( r \) is the number of relations. We refer the reader to Wiegold’s survey on the Schur multiplier for proofs of all these results [15]. Since \( A_6 \) is shown in [3] to have the presentation

\[
\langle a, b | a^4, b^5, abab^{-1}abab^{-1}a^{-1}b^{-1} \rangle,
\]

it follows that the Schur multiplier of \( A_6 \) is cyclic. Hence the non-split extension \( 3.A_6 \) is unique up to isomorphism.

Now, since \( \text{Aut}^\circ(H) \) splits over \( 3.A_6 \), we have that \( 3.A_6 < \text{Aut}^\circ(H) < \text{Aut}(3.A_6) \). Suppose that \( \xi \in \text{Aut}(3.A_6) \) such that the image of \( \xi \) in \( \text{Aut}(A_6) \) is the trivial automorphism. Let \( \sigma \in 3.A_6 \) be an element of order 15, projecting onto a 5-cycle in \( A_6 \). Then \( \sigma^5 \) generates the central subgroup of order 3. Each coset of \( \langle \sigma^5 \rangle \) contains a unique element of order 5, which is fixed by hypothesis. So either \( (\sigma) \) is fixed element-wise, or \( \xi = \ast \). Moreover, any two subgroups of order 15 intersect in \( \langle \sigma^5 \rangle \), so the action of \( \xi \) is identical on all 5-cycles. Since the 5-cycles generate \( A_6 \), the action of \( \xi \) is completely determined.

So each choice of actions on 3 and on \( A_6 \) determines at most one isomorphism class of groups. It follows that \( \text{Aut}^\circ(H) \) is uniquely described as the group of shape \( 3.S_6 \) with trivial center.

The projection of \( \rho_1 (\text{Aut}^\circ(H) \cap X_0) \) is clearly a faithful linear representation of \( 3.A_6 \) over the complex numbers, completing the proof.

\[ \square \]

In fact, \( 3.A_6 \) is the largest subgroup of \( \text{Aut}^\circ(H_6) \) admitting a faithful 6-dimensional representation over \( \mathbb{C} \). So this is \( \text{Aut}(H_6) \). A useful way to understand the actions of \( X \) and of \( \text{Aut}^\circ(H_6) \) is via a permutation action on 18 points, which we now describe. Let \( P_1 = \tau_1^{\rho_1} \) and \( P_2 = \tau_2^{\rho_1} \), and define the following \( 18 \times 6 \) matrices:

\[
M_1 = \begin{pmatrix} H & \omega H \\ \omega^2 H & \omega H^{\ast} \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} H^{\ast} & \omega H^{\ast} \\ \omega^2 H^{\ast} & \omega H^{\ast} \end{pmatrix}.
\]

For \( 1 \leq i \leq 18 \), let \( \text{Row}_i(M_j) \) denote the \( i \)th row of \( M_j \) (where \( j = 1, 2 \)). Let \( P_1 \) act on the rows of \( M_1 \), and similarly the rows of \( M_2 \), as follows:

\[
P_1 \cdot M_1 = \begin{pmatrix} P_1 H \\ \omega P_1 H \\ \omega^2 P_1 H \end{pmatrix}.
\]

By letting \( P_2 \) act on the rows of \( M_1 \) and \( M_2 \) in a similar manner, we find that \( P_1 \) and \( P_2 \) act in the same way on the rows of \( M_1 \) and the rows of \( M_2 \), and hence act on the set \( \Omega(18) := \{ \text{Row}_i(M_1), \text{Row}_i(M_2) \} | i = 1, \ldots, 18 \}. \)

Also, letting \( \ast \) act as complex conjugation on \( M_1 \) and \( M_2 \), we see that \( \ast \) also induces a permutation of \( \Omega(18) \). Thus
$\tau_1$, $\tau_2$, and $*$ all induce permutations of $\Omega(18)$ and, identifying $\{\text{Row}_i(M_1), \text{Row}_i(M_2)\}$ with $i$, for each $i$, we get a permutation representation of $X$ on 18 points with the following generating permutations:

$\tau_1 = (2, 3, 4, 5, 6)(8, 9, 10, 11, 12)(14, 15, 16, 17, 18),$
$\tau_2 = (1, 2)(3, 15, 9)(4, 10, 16)(5, 11, 17)(6, 18, 12)(7, 8)(13, 14),$

The kernel of $X$ in this action is the subgroup of $N$ of order $3^5$ consisting of pairs with trivial first component. The restriction to $\text{Aut}^3(H_6)$ is faithful, however. One could construct a faithful action of $X$ by taking the permutation action induced by its action on the rows of $H_6$ together with the induced action on columns.

Remark 3 The matrix $H_6$ and the group $3 \cdot A_6$ can be realised over any field $k$ for which $k^\times$ has a subgroup of order 3. In the case that $k$ is the finite field of order 4, the rows of $H_6$ span the Hadamard code, introduced by Conway as part of a construction for the group $M_{12}$. It is discussed in detail in Sect. 11.2 of [5]. In particular, this code is the extended quadratic residue code with parameters $(6, 3, 4)$. Uniqueness can easily be verified by hand: observe that the punctured code is the Hamming $(5, 3, 3)$ code, which is unique, and that any pair of one-bit extensions which increase the minimum distance are isomorphic. The 6-dimensional $\mathbb{C}$-representation of $3 \cdot A_6$ has been previously described in the literature, normally via its action on a set of vectors in $\mathbb{C}^6$ derived from the hexacode. In particular, Wilson gives the action of $3 \cdot A_6$ on certain vectors of weight 4 in Sect. 2.7.4 of [16].

3 The Outer Automorphism of $S_6$

Finally we construct the outer automorphism of $S_6$ over the split-quaternions. Recall that the split-quaternions are a 4-dimensional $\mathbb{R}$-algebra with basis $\{1, i, \beta, \beta i\}$ where $\{1, i\}$ generates the usual algebra of complex numbers and $\beta^2 = 1, i\beta = -i$. We denote the split quaternions by $\mathbb{B}$. They admit an $\mathbb{R}$-linear representation generated by

$i \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \beta \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$

Observe that $\text{Aut}^\circ(H_6)$ admits a $\mathbb{B}$-linear representation if and only if $*$ does, and that the latter is realised by $(\beta I_6, \beta I_6)$.

Since $H_6$ is invertible over $\mathbb{C}$, it is invertible over $\mathbb{B}$. Now, rearranging the matrix equation $H_6^{\tau_2*} = H_6$, and using the same notation as before for monomial matrices, we obtain that

$H_6[[\beta, \beta, \beta\bar{\omega}, \beta\omega, \beta\bar{\omega}, \beta\bar{\omega}](1, 2)(3, 6)(4, 5)] H_6^{-1} = [[\beta, \beta, \beta\omega, \beta\bar{\omega}, \beta\bar{\omega}, \beta\omega](1, 2)].$

Note that $(\beta\omega)^2 = (\beta\bar{\omega})^2 = 1$ so that the matrix on the right hand side of the above equation is an involution.

As was the case over the complex numbers, $H_6$ intertwines the projections $\rho_1$ and $\rho_2$. We observe that for any $g \in \text{Aut}^\circ(H)$, we have that $g^{\rho_1} = H_6 g^{\rho_2} H_6^{-1}$. But, as illustrated above, $\tau_2^{\rho_1 \pi}$ is a 2-cycle, while the projection $\tau_2^{\rho_2 \pi}$ is a product of 3 disjoint 2-cycles. We conclude that the representations $\rho_1 \pi$ and $\rho_2 \pi$ of $S_6$ cannot be conjugate. Thus whereas the permutation representations of $S_6$ on 6 points are not equivalent, and the monomial representations of $3 \cdot A_6$ are not equivalent, we have constructed two explicit $\mathbb{B}$-linear representations of $3 \cdot S_6$ which are equivalent under conjugation by $H_6$. Moreover, although the representation is not defined over $\mathbb{C}$, the intertwiner $H_6$ is.

Theorem 4 There exists an irreducible 6-dimensional monomial representation of $3 \cdot S_6$ over the split-quaternions. Two conjugate representations of $3 \cdot S_6$ intertwined by the complex Hadamard matrix $H_6$ give an explicit construction for the outer automorphism of $S_6$.

Acknowledgements Work on this paper was begun while the second author was visiting the Centre for the Mathematics of Symmetry and Computation at the University of Western Australia in March 2012. The hospitality of the CMSC is gratefully acknowledged, and in particular support from the ARC Federation Fellowship Grant FF0776186 of the third author, which also supported the first author. The second author acknowledges the support of the Australian Research Council via grant DP120103067, and Monash University where much of this work was completed. This research was partially supported by the Academy of Finland (Grants #276031, #282938, #283262 and #283437). The support from the European Science Foundation under the COST Action IC1104 is also gratefully acknowledged.
References