Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 308 (2008) 2910–2924
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

On the automorphisms of Paley's type II Hadamard matrix

Warwick de Launey, Richard M. Stafford

Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121, USA

Received 1 November 2006; accepted 17 July 2007
Available online 24 October 2007

Abstract

In this paper we determine the automorphism group of Paley's type II Hadamard matrix.

Keywords: Paley Hadamard matrix; Automorphism group; Doubly transitive groups; Designs

1. An overview

An automorphism of an $n \times m$ $(1, -1)$-matrix A is an ordered pair of monomial matrices (P, Q) such that $PAQ^{\mathrm{t}} = A$. These automorphisms form a group, denoted $\mathrm{Aut}(A)$, under the component-wise product: $(P_1, Q_1)(P_2, Q_2) = (P_1P_2, Q_1Q_2)$.

In this paper, we determine the full automorphism group Γ of the Paley Type II Hadamard matrix. The automorphism group of Paley's Type I matrix was determined three decades ago by Kantor [11]. Kantor's argument relied on deep results in permutation group theory and used a remarkable result of Carlitz of [4]. Our argument for the Paley Type II Hadamard involves a complicated combinatorial analysis of the Hadamard matrix, and uses the classification of the finite simple groups. In the next section, we will give a precise description of Γ. The automorphism group has a simple description as an abstract group. Let q denote an odd prime power. Let V denote the two-dimensional vector space over the Galois field $\mathrm{GF}(q)$, and let $\mathrm{G}\Gamma\mathrm{L}(2, q)$ denote the group of semilinear maps on V, see [15]. This group contains a subgroup denoted $\mathrm{GL}(2, q)$ comprised of the $\mathrm{GF}(q)$ linear invertible maps on V. The center of $\mathrm{GL}(2, q)$ is the group L of scalar maps $x \mapsto \lambda x$ where $\lambda \in \mathrm{GF}(q)^*$. Let Q denote the subgroup of index two in L comprised of the maps of the form $x \mapsto \lambda^2 x$ where $\lambda \in \mathrm{GF}(q)^*$. Since L and Q are normal in $\mathrm{G}\Gamma\mathrm{L}(2, q)$ (and since Q has index two in L), the quotient group L/Q is central in $\mathrm{G}\Gamma\mathrm{L}(2, q)/\mathrm{Q}$. A straightforward calculation shows that this is the entire center.

Theorem 1.1. *Let H be Paley's type* II *Hadamard matrix of order $2(q + 1)$. Then for $q > 5$, $\mathrm{Aut}(H)$ is obtained from $\mathrm{G}\Gamma\mathrm{L}(2, q)/\mathrm{Q}$ by adjoining a normalizing element ξ of order 4 and identifying ξ^2 with the generator of the center of $\mathrm{G}\Gamma\mathrm{L}(2, q)/\mathrm{Q}$. In particular, if $q = p^f$, where p is prime, then H has $4f\,q(q^2 - 1)$ distinct automorphisms.*

We remark that for $q = 5$, Paley's Type II Hadamard matrix is equivalent to the Hadamard matrix of order 12 first described by Hadamard. So in this case (see [10]), the automorphism group is a perfect central extension of the Mathieu group M_{12} by the cyclic group of order two.

E-mail addresses: warwick@ccrwest.org (W. de Launey), rmstaff@ccrwest.org (R.M. Stafford).

0012-365X/$ - see front matter © 2007 Published by Elsevier B.V.
doi:10.1016/j.disc.2007.07.118

This paper is organized as follows. In Section 2 we exhibit a large group Π of automorphisms of the Paley Type II Hadamard matrix. In Section 3 we show that for $q > 5$ the group Π is the full automorphism group Γ. This requires a detailed combinatorial analysis of the Hadamard matrix, and uses a novel counting argument for bounding the size of the automorphism group of any $(1, -1)$-matrix. The other main ingredient is a case by case discussion of the (at least) 2-transitive actions by "small" finite groups. Hence our proof of Theorem 1.1 depends on the classification of the 2-transitive permutation group actions. In Section 4 we show that a Paley type II matrix and a Paley type I matrix are equivalent if and only if they both have order equal to 12.

2. A large subgroup Π of the automorphism group

In this section, we identify a large group Π of automorphisms of the Paley type II Hadamard matrix. If x and y are elements of a group G, then we use the exponential notation y^x to denote the conjugate $x^{-1}yx$ of y by x. We will also use the notation $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ to denote the symmetric group and alternating group on n objects.

2.1. Some actions of classical groups

The group $\mathrm{GL}(2, q)$: Let V be the two-dimensional vector space obtained by regarding the finite field $\mathrm{GF}(q^2)$ as a vector space over its subfield $\mathrm{GF}(q)$ of order q. Let $\mathrm{GL}(2, q)$ denote the group of invertible linear transformations on V. This group acts transitively on the set V^* of non-zero elements of V: the linear transformation $A \in \mathrm{GL}(2, q)$ moves the point $x \in V^*$ to the point Ax.[1] This is the usual action of $\mathrm{GL}(2, q)$ on V^*. $\mathrm{GL}(2, q)$ can also act as follows on V^*: A moves x to $\det(A)Ax$. Under this action $AB(x) = \det(AB)(AB)x = \det(A)A(\det(B)Bx) = A(B(x))$. We will call this the *non-standard action* of $\mathrm{GL}(2, q)$ on V^*.

The group $\mathrm{G}\Gamma\mathrm{L}(2, q)$: Now fix a basis $\{b_1, b_2\}$ of V. Then any element $x \in V$ may be written as (x_1, x_2) where $x = x_1b_1 + x_2b_2$. Next write q as a prime power p^f, and let σ denote the map $\sigma : (x_1, x_2) \mapsto (x_1^p, x_2^p)$. Since, $\sigma(\lambda(x_1, x_2)) = \lambda^p(x_1^p, x_2^p) = \lambda(\sigma(x_1, x_2))$ if and only if $\lambda^p = \lambda$ for all $\lambda \in \mathrm{GF}(q)$, this map is in $\mathrm{GL}(2, q)$ if and only if $f = 1$. In any case, we can form the classical group $\mathrm{G}\Gamma\mathrm{L}(2, q)$ of semi-linear maps on V by adjoining σ to $\mathrm{GL}(2, q)$. To see this, observe that for some elements $a_{11}, a_{12}, a_{21}, a_{22} \in \mathrm{GF}(q)$, the Frobenius map $x \mapsto x^p$ is

$$x_1b_1 + x_2b_2 \mapsto (x_1b_1 + x_2b_2)^p = x_1^p b_1^p + x_2^p b_2^p = (x_1^p a_{11} + x_2^p a_{21})b_1 + (x_1^p a_{12} + x_2^p a_{22})b_2.$$

Therefore, the Frobenius map is σ followed by a linear map. Since the group $\mathrm{G}\Gamma\mathrm{L}(2, q)$ is obtained by adjoining the Frobenius map to $\mathrm{GL}(2, q)$, adjoining σ to $\mathrm{GL}(2, q)$ gives $\mathrm{G}\Gamma\mathrm{L}(2, q)$. Indeed, any element of $\mathrm{G}\Gamma\mathrm{L}(2, q)$ may be written uniquely in the form $A\sigma^k$ where $A \in \mathrm{GL}(2, q)$ and $k \in \{0, 1, \ldots, f - 1\}$.

With the above action of σ, each of the actions of $\mathrm{GL}(2, q)$ described in the previous paragraph extends to an action of $\mathrm{G}\Gamma\mathrm{L}(2, q)$ on V^*. The easiest way to see that the non-standard action extends is to recall that an action of a group G on a set Ω is simply a homomorphism from G to the symmetric group, $\mathrm{Sym}(\Omega)$. The non-standard action corresponds to the endomorphism $\phi :\to \mathrm{Sym}(V^*)$ defined so that for all $k \in \mathbb{Z}$, $A \in \mathrm{GL}(2, q)$ and $x \in V^*$,

$$\phi(A\sigma^k)(x) = \det(A)A\sigma^k(x).$$

If

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix},$$

then

$$\sigma^k A \sigma^{-k} = \begin{bmatrix} a_{11}^{p^k} & a_{12}^{p^k} \\ a_{21}^{p^k} & a_{22}^{p^k} \end{bmatrix}.$$

[1] A word of caution. For group action on the rows and columns of a design we prefer to use the functional rather than exponential notation. Under the exponential notation $x^{\alpha\beta}$, the group element α first acts on the row indexed by x, and then the group element β acts on the row x^α. Under the functional notation this is equivalent to $\beta\alpha(x)$.