Discrete Mathematics 341 (2018) 1199–1209

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Orbit matrices of Hadamard matrices and related codes

Dean Crnković, Ronan Egan, Andrea Švob

Department of Mathematics, University of Rijeka, Radmile Matejčić 2, 51000 Rijeka, Croatia

ARTICLE INFO

Article history:
Received 26 September 2017
Accepted 23 January 2018
Available online 22 February 2018

Keywords:
Hadamard matrix
Orbit matrix
Self-orthogonal code

ABSTRACT

In this paper we introduce the notion of orbit matrices of Hadamard matrices with respect to their permutation automorphism groups and show that under certain conditions these orbit matrices yield self-orthogonal codes. As a case study, we construct codes from orbit matrices of some Paley type I and Paley type II Hadamard matrices. In addition, we construct four new symmetric (100,45,20) designs which correspond to regular Hadamard matrices, and construct codes from their orbit matrices. The codes constructed include optimal, near-optimal self-orthogonal and self-dual codes, over finite fields and over $\mathbb{Z}_4$.

1. Introduction

A *Hadamard matrix* of order n is a $n \times n$ $\{\pm 1\}$ matrix H such that $HH^\top = nI_n$. It is well known that a Hadamard matrix of order n can exist only if $n = 1, 2$ or $n \equiv 0 \mod 4$. The Hadamard conjecture states that these necessary conditions are also sufficient. Since the discovery of a Hadamard matrix of order 428, the smallest open case is $n = 668$ [22].

A *code* C of length n over the alphabet Q is a subset $C \subseteq Q^n$. Elements of a code are called *codewords*. A code C is called a q-ary *linear code* of dimension m if $Q = \mathbb{F}_q$, for a prime power q, and C is an m-dimensional subspace of a vector space $(\mathbb{F}_q)^n$. For $Q = \mathbb{F}_2$ a code is called *binary*.

Let $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$. The *Hamming distance* between words x and y is the number $d(x, y) = |\{i : x_i \neq y_i\}|$. The *minimum distance* of the code C is defined by $d = \min\{d(x, y) : x, y \in C,\ x \neq y\}$. The *weight* of a codeword x is $w(x) = d(x, 0) = |\{i : x_i \neq 0\}|$. For a *linear code* the minimum distance equals the minimum weight: $d = \min\{w(x) : x \in C, x \neq 0\}$.

A q-ary linear code of length n, dimension k, and distance d is called a $[n, k, d]_q$ code. A linear $[n, k, d]$ code can detect at most $d - 1$ errors in one codeword and correct at most $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ errors. An $[n, k]$ linear code C is said to be a *best known* linear $[n, k]$ code if C has the highest minimum weight among all known $[n, k]$ linear codes. An $[n, k]$ linear code C is said to be an *optimal* linear $[n, k]$ code if the minimum weight of C achieves the theoretical upper bound on the minimum weight of $[n, k]$ linear codes, and *near-optimal* if its minimum distance is at most 1 less than the largest possible value.

The *dual* code $C^\perp$ is the orthogonal complement under the standard inner product $(\cdot\,,\cdot)$, i.e. $C^\perp = \{v \in F^n | (v, c) = 0 \text{ for all } c \in C\}$. A code C is *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if equality is attained. Two linear codes are *isomorphic* if one can be obtained from the other by permuting the coordinate positions. An *automorphism* of the code C is an isomorphism from C to C. Two codes are *equivalent* if one of the codes can be obtained from the other by permuting the coordinates and permuting the symbols within one or more coordinate positions.

In this paper we introduce the notion of an orbit matrix of a Hadamard matrix with respect to a permutation automorphism group of the matrix. We use these orbit matrices to construct self-orthogonal codes. The orbit matrix of a Hadamard matrix H is defined in a way that the entry at the position (i, j) denotes the row (or column) sum of a submatrix of H determined by the ith row orbit and the jth column orbit. This definition of an orbit matrix of a Hadamard matrix is a

E-mail addresses: deanc@math.uniri.hr (D. Crnković), ronan.egan@math.uniri.hr (R. Egan), asvob@math.uniri.hr (A. Švob).

https://doi.org/10.1016/j.disc.2018.01.018
0012-365X/© 2018 Elsevier B.V. All rights reserved.

generalization of the definition of an orbit matrix of an incidence structure. For a Hadamard matrix H, the matrix $B = \frac{1}{2}(H+J)$, where J denotes the all-one matrix, is called the binary Hadamard matrix associated to H. In comparison to the usual orbit matrices of the binary Hadamard matrix B associated to a Hadamard matrix H (i.e. orbit matrices obtained by considering B as the incidence matrix of an incidence structure), with this approach we have a wider range of choices for an automorphism group G in the construction of orbit matrices of H from which we obtain self-orthogonal codes. Another advantage of this generalization of the definition of orbit matrices is that it can be applied to a wider range of matrices, not just to $\{0, 1\}$ matrices (incidence matrices of incidence structures). This allows us to construct orbit matrices of the matrices $H + kI$ in Section 3, where H is a Hadamard matrix, and obtain the corresponding self-dual codes.

The codes constructed in this paper have been constructed and examined using Magma [2]. Minimum distances are compared to known codes and bounds at [12].

2. Orbit matrices of Hadamard matrices

P. Dembowski introduced the notion of a tactical decomposition of an incidence structure and showed that the orbits of an automorphism group acting on an incidence structure $\mathcal{I}$ induce a tactical decomposition of $\mathcal{I}$ (see [9]). Tactical decompositions induced by the action of an automorphism group leads us to orbit matrices of incidence structures, which have been successfully used for a construction of block designs since the 1980s (see [5,18]). Construction of self-orthogonal codes from orbit matrices of block designs was introduced in [15] and further developed in [4]. In this paper we define orbit matrices of Hadamard matrices and show that under certain conditions these orbit matrices yield self-orthogonal codes.

M. Hall defined an *automorphism* of a Hadamard matrix H of order n as a pair (P, Q) of $n \times n$ monomial matrices such that $PHQ = H$ (see [13]). A *permutation automorphism* of a $\{\pm 1\}$-matrix H is defined to be a permutation g of rows and columns of H that maps H to itself, i.e. $Hg = H$. The permutations g can be considered as an ordered pair $g = (\alpha, \beta)$, where α is a permutation of rows of H and β is a permutation of columns of H. To these permutations α and β we can associate a pair of permutation matrices (P, Q) such that $PHQ^\top = H$. We transpose the righthand component so that the product $(P, Q)(R, S) = (PR, QS)$ of automorphisms (P, Q) and (R, S) is an automorphism.

The next three theorems follow from Theorems 3.1, 3.2 and 3.3 of [23] on orbits of points and blocks of a symmetric design under the action of an automorphism. For completeness we include proofs specific to Hadamard matrices.

Theorem 2.1. *A permutation automorphism g of a Hadamard matrix fixes an equal number of rows and columns.*

Proof. If g is an automorphism of a Hadamard matrix H, then there exist permutation matrices P and Q such that $PHQ^\top = H$. Since the matrix H is regular and since the inverse of a permutation matrix is its transpose, then $HQH^{-1} = P$. Thus the matrices Q and P are similar and $tr(P) = tr(Q)$.

Since the number of fixed points of a permutation is equal to the trace of the associated permutation matrix, it follows that g fixes an equal number of rows and columns. □

The Möbius function μ is defined by

$$\mu(n) = \begin{cases} 0, & \text{if } n \text{ has one or more repeated prime factors}, \\ 1, & \text{if } n = 1, \\ (-1)^k, & \text{if } n \text{ is a product of } k \text{ distinct primes}, \end{cases}$$

for a positive integer n. So $\mu(n) \neq 0$ if and only if n is squarefree. The Möbius inversion formula states that if f and g are functions that map positive integers to complex numbers, satisfying

$$g(n) = \sum_{d|n} f(d),$$

for every positive integer n, then

$$f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d}),$$

where μ is the Möbius function and the sums run over all positive divisors d of n.

Theorem 2.2. *Let $g = (\alpha, \beta)$ be a permutation automorphism of a Hadamard matrix H, where α is a permutation of rows and β is a permutation of columns of H. Then the permutations α and β have the same cycle structure.*

Proof. Let $f_\alpha(d)$ and $f_\beta(d)$ be the number of cycles of length d in the cycle decomposition of α and β, respectively. For every positive integer m the number of fixed points of α^m is $\sum_{d|m} f_\alpha(d)$, and the number of fixed points of β^m is $\sum_{d|m} f_\beta(d)$. By Theorem 2.1

$$\sum_{d|m} f_\alpha(d) = \sum_{d|m} f_\beta(d)$$

for all positive integers m. By applying the Möbius inversion formula we get $f_\alpha(d) = f_\beta(d)$ for all d. □