Discrete Mathematics 327 (2014) 91–95

Contents lists available at ScienceDirect

Discrete Mathematics

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

Classes of self-orthogonal or self-dual codes from orbit matrices of Menon designs

Dean Crnković

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

ARTICLE INFO

Article history:
Received 15 February 2013
Received in revised form 11 February 2014
Accepted 13 February 2014
Available online 3 April 2014

Keywords:
Self-orthogonal code
Self-dual code
Pless symmetry code
Paley graph
Block design

ABSTRACT

For every prime power q, where $q \equiv 1 \pmod 4$, and p a prime dividing $\frac{q+1}{2}$, we construct a self-orthogonal $[2q, q-1]$ code and a self-dual $[2q+2, q+1]$ code over the field of order p. The construction involves Paley graphs and the constructed $[2q, q-1]$ and $[2q+2, q+1]$ codes admit an automorphism group $\Sigma(q)$ of the Paley graph of order q. If q is a prime and $q = 12m+5$, where m is a non-negative integer, then the self-dual $[2q+2, q+1]_3$ code is equivalent to a Pless symmetry code. In that sense we can view this class of codes as a generalization of Pless symmetry codes. For $q = 9$ and $p = 5$ we get a self-dual $[20, 10, 8]_5$ code whose words of minimum weight form a 3-(20, 8, 28) design.

1. Introduction

The terminology and notation in this paper for designs, codes and Hadamard matrices are as in [1,4,17].

In this paper we describe a method for constructing self-orthogonal or self-dual codes from orbit matrices of some Menon designs. For every prime power q, where $q \equiv 1 \pmod 4$ and p is a prime dividing $\frac{q+1}{2}$, we construct a self-orthogonal $[2q, q-1]$ code and a self-dual $[2q+2, q+1]$ code over the field of order p. If q is a prime and $q = 12m+5$, where m is a non-negative integer, then the self-dual $[2q+2, q+1]_3$ code is equivalent to a Pless symmetry code. For other values of q, to our knowledge, these codes do not belong to some previously known series of codes. For $q = 9$ and $p = 5$ we get a self-dual [20, 10, 8] code over $\mathbb{F}_5$, whose words of minimum weight form a 3-(20, 8, 28) design.

The class of self-orthogonal codes is important in coding theory from both theoretical and practical reasons. Self-dual codes, a special case of self-orthogonal codes, are in particular of interest because many of the best codes known are of this type. For example self-dual ternary codes include among others the ternary Golay code of length 12, the quadratic residue codes and the symmetry codes. Self-dual codes have been extensively studied. A comprehensive study of self-dual codes can be found in [14]. Some results on the classification of self-orthogonal codes over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_4$ have been obtained by Mallows, Pless and Sloane [13], Pless [16], Bouyukliev, Bouyuklieva, Gulliver and Östergård [2] and Bouyukliev and Östergård [3]. Some further results on self-orthogonal codes can be found in [18,19]. For basic definitions and properties of orbit matrices we refer the reader to [8,11].

The paper is organized as follows: in Sections 2 and 3 we present a construction of a series of self-orthogonal or self-dual codes using Paley graphs and orbit matrices of certain Menon designs, in Section 4 we show that some of the constructed self-dual codes belong to the series of Pless symmetry codes, while in Section 5 we describe a construction of a 3-(20,8,28) design from a self-dual [20, 10, 8] code over $\mathbb{F}_5$.

E-mail address: deanc@math.uniri.hr.

http://dx.doi.org/10.1016/j.disc.2014.02.012

2. Construction of self-orthogonal codes

Let q be a prime power, $q \equiv 1 \pmod 4$, and $A = (a_{ij})$ be a $(q \times q)$ matrix defined as follows:

$$a_{ij} = \begin{cases} 1, & \text{if } (i-j) \text{ is a non-zero square in } \mathbb{F}_q, \\ 0, & \text{otherwise.} \end{cases}$$

A is a symmetric matrix, since -1 is a square in $\mathbb{F}_q$. There are as many non-zero squares as non-squares in $\mathbb{F}_q$, so each row of A has $\frac{q-1}{2}$ elements equal to 1 and $\frac{q+1}{2}$ zeros. The set of non-zero squares in $\mathbb{F}_q$ is a partial difference set, called a Paley partial difference set (see [1, 10.15 Example, p. 231]), and the matrix A is the adjacency matrix of the Paley graph (see e.g. [4] and [17, Section 3.1]). Throughout the paper A will denote the above-defined matrix.

Let $\overline{A} = [\overline{a}_{ij}]$ be $(q \times q)$ matrix such that $\overline{a}_{ij} = a_{ij} + 1 \pmod 2$. For $v \in N$ we denote by I_v the $(v \times v)$ identity matrix, by j_v the all-one column vector of length v, by J_v the all-one matrix of size $v \times v$, by 0_v the zero-vector of length v, and by $0_{v \times v}$ the zero-matrix of size $v \times v$. In [6, Lemma 2.2] we gave a construction of orbit matrices for Menon designs with parameters $(4p^2, 2p^2 - p, p^2 - p)$, whenever $q \equiv 1 \pmod 4$ is a prime power and $p = \frac{q+1}{2}$.

In [10] the authors presented a method of constructing self-orthogonal codes from orbit matrices induced by fixed-point-free and fixed-block-free action of an automorphism of prime order of a block design. That result was generalized in [7]. A direct consequence of [6, Lemma 2.2] and [7, Theorem 4] is the following theorem.

Theorem 1. *Let q be a prime power, $q \equiv 1 \pmod 4$, and $p = \frac{q+1}{2}$ be a prime. Then the rows of the matrix*

$$R = \left[\begin{array}{c|c} \frac{p-1}{2} J_q + \frac{p-1}{2} I_q & \frac{p-1}{2} A + \frac{p+1}{2} (\overline{A} - I_q) \\ \hline \frac{p+1}{2} A + \frac{p-1}{2} (\overline{A} - I_q) & \frac{p-1}{2} J_q + \frac{p-1}{2} I_q \end{array} \right]$$

span a self-orthogonal code over $\mathbb{F}_p$ of length $2q$.

In a similar way as in the case of Theorem 1, one can prove Corollary 1.

Corollary 1. *Let q be a prime power, $q \equiv 1 \pmod 4$, and p be a prime dividing $\frac{q+1}{2}$. Then the rows of the matrix*

$$R = \left[\begin{array}{c|c} \frac{q-1}{4} J_q + \frac{q-1}{4} I_q & \frac{q-1}{4} A + \frac{q+3}{4} (\overline{A} - I_q) \\ \hline \frac{q+3}{4} A + \frac{q-1}{4} (\overline{A} - I_q) & \frac{q-1}{4} J_q + \frac{q-1}{4} I_q \end{array} \right]$$

span a self-orthogonal code over $\mathbb{F}_p$ of length $2q$.

Remark 1. Let

$$R_1 = \left[\begin{array}{c|c} \frac{q-1}{4} J_q + \frac{q-1}{4} I_q & \frac{q-1}{4} A + \frac{q+3}{4} (\overline{A} - I_q) \end{array} \right].$$

Clearly, the code spanned by R_1 is also self-orthogonal. In all examples tested the submatrix R_1 spans the same code as the matrix R. Below we will study codes spanned by R_1.

In the following theorem we determine dimension of the codes spanned by R_1.

Theorem 2. *Let q be a prime power, $q \equiv 1 \pmod 4$, and p be a prime dividing $\frac{q+1}{2}$. Then rows of the matrix*

$$R_1 = \left[\frac{q-1}{4} J_q + \frac{q-1}{4} I_q \quad \frac{q-1}{4} A + \frac{q+3}{4} (\overline{A} - I_q) \right]$$

span a self-orthogonal code over $\mathbb{F}_p$ of length $2q$ and dimension $q - 1$.

Proof. The sum of all rows of the matrix R_1 equals $\frac{q+1}{2}(\frac{q-1}{2}, \frac{q-1}{2}, \ldots, \frac{q-1}{2})$, that is, the zero vector over $\mathbb{F}_p$, and thus the $\mathrm{rank}_p R_1 \leq q - 1$.

We will now take into consideration the first q columns of the matrix R_1, i.e., the submatrix $R_{1,1} = \frac{q-1}{4} J_q + \frac{q-1}{4} I_q$. Subtracting the $(i+1)$-th row from the ith row of $R_{1,1}$, for $i = 1, \ldots, q-1$, we obtain the matrix

$$M = \begin{bmatrix} \frac{q-1}{4} & \frac{1-q}{4} & 0 & \cdots & 0 & 0 \\ 0 & \frac{1-q}{4} & \frac{q-1}{4} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \frac{q-1}{4} & \frac{1-q}{4} \\ \frac{q-1}{4} & \frac{q-1}{4} & \frac{q-1}{4} & \cdots & \frac{q-1}{4} & \frac{q-1}{2} \end{bmatrix}$$

that means that the p-rank of the matrix $R_{1,1}$ and R_1 is at least $q - 1$. Therefore, the p-rank of R_1 is $q - 1$. $\square$