Discrete Mathematics 339 (2016) 409–414

Contents lists available at ScienceDirect

Discrete Mathematics

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

Note

Self-dual codes from quotient matrices of symmetric divisible designs with the dual property

Dean Crnković*, Nina Mostarac, Sanja Rukavina

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

ARTICLE INFO

Article history:
Received 7 June 2015
Accepted 4 September 2015
Available online 1 October 2015

Keywords:
Self-dual code
Divisible design
Quotient matrix

ABSTRACT

In this paper we look at codes spanned by the rows of a quotient matrix of a symmetric (group) divisible design (SGDD) with the dual property. We define an extended quotient matrix and show that under certain conditions the rows of the extended quotient matrix span a self-dual code with respect to a certain scalar product. We also show that sometimes a chain of codes can be used to associate a self-dual code to a quotient matrix of a SGDD with the dual property.

1. Introduction

In this paper we introduce a construction of self-dual codes from extended quotient matrices of symmetric (group) divisible designs with the dual property. The results are obtained by developing the ideas presented in [7] and [9], and especially in [4] where a construction of self-dual codes from extended orbit matrices of symmetric designs with respect to the action of an automorphism group that acts with all orbits of the same length is given.

2. Background and terminology

In this section we give some basic definitions of coding theory and design theory. For further reading we refer the reader to [1,5] and [7].

2.1. Codes

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 p-ary *linear code* of dimension m if $Q = \mathbb{F}_p$, for a prime p, and C is an m-dimensional subspace of a vector space $\mathbb{F}_p^n$.

Let $C \subseteq \mathbb{F}_p^n$ be a linear code. Its *dual code* is the code $C^\perp = \{x \in \mathbb{F}_p^n | x \cdot c = 0,\ \forall c \in C\}$, where $\cdot$ is the standard inner product. The code C is called *self-orthogonal* if $C \subseteq C^\perp$, and C is called *self-dual* if $C = C^\perp$.

We may use a symmetric nonsingular matrix U over a field $\mathbb{F}_p$ to introduce a scalar product $\langle \cdot, \cdot \rangle_U$ for row vectors in $\mathbb{F}_p^n$: $\langle a, c \rangle_U = aUc^T$. The U-*dual code* of a linear code C is the code $C^U = \{a \in \mathbb{F}_p^n \mid \langle a, c \rangle_U = 0,\ \forall c \in C\}$. A code C is called *self-U-dual*, or self-dual with respect to U, if $C = C^U$.

* Corresponding author.
E-mail addresses: deanc@math.uniri.hr (D. Crnković), nmavrovic@math.uniri.hr (N. Mostarac), sanjar@math.uniri.hr (S. Rukavina).

http://dx.doi.org/10.1016/j.disc.2015.09.004
0012-365X/

2.2. Divisible designs

The definition of a divisible design (often also called group divisible design) varies. In this paper we use the definition given in Bose [2].

An incidence structure with v points, b blocks and constant block size k in which every point appears in exactly r blocks is a *(group) divisible design* (GDD) with parameters $(v, b, r, k, \lambda_1, \lambda_2, m, n)$ whenever the point set can be partitioned into m classes of size n, such that two points from the same class appear together in exactly λ_1 blocks, and two points from different classes appear together in exactly λ_2 blocks. Then the following holds:

$$v = mn, \qquad bk = vr, \qquad (n-1)\lambda_1 + n(m-1)\lambda_2 = r(k-1), \quad rk \geq v\lambda_2.$$

It follows from the definition that a divisible design is a block design if and only if either $n = 1$ or $\lambda_1 = \lambda_2$ [6]. If $n \neq 1$ and $\lambda_1 \neq \lambda_2$, then a divisible design is called *proper*.

For the incidence matrix N of a GDD, the determinant of NN^T is given by

$$det(NN^T) = rk(r-\lambda_1)^{m(n-1)}(rk - v\lambda_2)^{m-1},$$

and the eigenvalues of NN^T are rk, $r-\lambda_1$, $rk-v\lambda_2$ with multiplicities 1, $m(n-1)$ and $m-1$, respectively (see Raghavarao [8]).

Divisible designs were classified by Bose and Connor [3] into three types in terms of these eigenvalues:

1. *singular* if $r - \lambda_1 = 0$,
2. *nonsingular* if $r - \lambda_1 > 0$
   (a) *semi-regular* if $rk - v\lambda_2 = 0$,
   (b) *regular* if $rk - v\lambda_2 > 0$.

A GDD is called a *symmetric* GDD (SGDD) if $v = b$ (or, equivalently, $r = k$). It is then denoted by $D(v, k, \lambda_1, \lambda_2, m, n)$ and it follows that:

$$v = mn, \qquad (n-1)\lambda_1 + n(m-1)\lambda_2 = k(k-1), \quad k^2 \geq v\lambda_2.$$

A SGDD D is said to have the *dual property* if the dual of D (that is, the design with the transposed incidence matrix) is again a divisible design with the same parameters as D. This means that blocks of D can be divided into sets $S_1, \dots, S_m$, each set containing n blocks, such that any two blocks belonging to the same set intersect in λ_1 points, and any two blocks belonging to different sets intersect in λ_2 points.

We point out that what we call "with the dual property" is sometimes called "symmetric"; "symmetric" in our sense ($v = b$) is then called "square" (see for example Jungnickel [6]).

3. Codes from quotient matrices of SGDDs with the dual property

The vertex and the block partition from the definition of a SGDD with the dual property give us a partition (which will be called the *canonical partition*) of the incidence matrix

$$N = \begin{bmatrix} A_{11} & \cdots & A_{1m} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mm} \end{bmatrix},$$

where A_{ij}'s are square submatrices of order n.

Let us denote by I_n the $n \times n$ identity matrix, and by J_n the $n \times n$ all-ones matrix. Then the matrix NN^T can be written as follows:

$$NN^T = \begin{bmatrix} B_{11} & \cdots & B_{1m} \\ \vdots & \ddots & \vdots \\ B_{m1} & \cdots & B_{mm} \end{bmatrix},$$

where

$$B_{ij} = [(k-\lambda_1)I_n + (\lambda_1 - \lambda_2)J_n]\delta_{ij} + \lambda_2 J_n,$$

and δ_{ij} is the Kronecker delta.

Theorem 3.1. *Let $D(v, k, \lambda_1, \lambda_2, m, n)$ be a SGDD with the dual property, and let N be the incidence matrix of D. If p is a prime such that $p \mid \lambda_1$, $p \mid k$ and $p \mid \lambda_2$, then the rows of N span a self-orthogonal code of length v over $\mathbb{F}_p$.*

Proof. The statement follows from the fact that NN^T is a null-matrix modulo p, because its entries take values from the set $\{k, \lambda_1, \lambda_2\}$. $\square$