Noname manuscript No.
(will be inserted by the editor)

Self-dual codes from 3-class association schemes

**M. Bilal · J. Borges · S.T. Dougherty ·
C. Fernández-Córdoba**

Received: date / Accepted: date

Abstract 3-class association schemes are used to construct binary self-dual codes. We use the pure and bordered construction to get self-dual codes starting from the adjacency matrices of symmetric and non-symmetric 3-class association schemes. In some specific cases, we also study constructions of self-dual codes over $\mathbb{Z}_k$. For symmetric 3-class association schemes, we focus on the rectangular scheme and association schemes derived from symmetric designs.

Keywords Non-symmetric association schemes, symmetric association schemes, self-dual codes, rectangular scheme, symmetric designs.

1 Introduction

Self-dual codes are an important class of codes over both fields and rings. There are numerous reasons for this. Not only they are interest in themselves as objects in coding theory but they have important connections to algebra, number theory and combinatorics. For example, self-dual codes over $\mathbb{Z}_k$ have interesting connections to invariant theory and also to unimodular lattices and modular forms, see [1] and [16] for complete descriptions of these connections. Additionally, self-dual codes have had many interesting connections to combinatorics. Most famously, self-dual codes were fundamental in proving the non-existence of the projective plane of order 10 [14]. A connection from

This work has been supported by the Spanish MEC grant TIN2013-40524-P and the Catalan AGAUR grant 2014 SGR691. This paper was presented in part at 3rd International Castle Meeting on Coding Theory and its Applications, and in VIII Jornadas de Matemática Discreta y Algorítmica.

M. Bilal, J. Borges and C. Fernández-Córdoba are with the Dept. of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra (Spain). E-mail: mbilal,jborges,cfernandez@deic.uab.cat · S.T. Dougherty is with the Dept. of Mathematics, University of Scranton, Scranton, PA 18510 (USA). E-mail: doughertys1@scranton.edu

self-dual codes to combinatorial designs has also been used in cryptography to construct secret sharing schemes [4].

Construction techniques for self-dual codes have always been of interest. Recently, several new ideas for constructing various types of self-dual codes have appeared. For example in [2], a construction was given to construct self-dual codes with a particular automorphism. In [13], a construction of self-dual codes over the family of rings R_k is given which is then used to construct binary self-dual codes. Very general versions of the building up construction of self-dual codes were given in [7] and [6]. New classification techniques have also been given in [3]. Additionally, combinatorial objects have been useful in the construction of self-dual codes. For example, in [5], a construction of self-dual codes from any symmetric design was given. In [8], self-dual codes were constructed from 2-class association schemes. In this paper, we extend it by constructing self-dual codes from 3-class association schemes.

We begin with some definitions from coding theory and then give some definitions from the theory of association schemes. In Section 2, we study how self-dual codes can be generated from the adjacency matrices of a 3-class association scheme. This can be done by using two different methods which we call pure and bordered constructions. In Section 3, we obtain the conditions under which we can get binary self-dual codes from non-symmetric 3-class association schemes. For a particular example, we also study the values of k such that we can obtain self-dual codes over $\mathbb{Z}_k$. Section 4 is devoted to binary self-dual codes from symmetric 3-class association schemes. Since the results are quite general, we focus on two kinds of important symmetric association schemes: the rectangular scheme and association schemes derived from symmetric designs. Again, we also mention conditions on k such that self-dual codes over $\mathbb{Z}_k$ can be obtained.

1.1 Self-dual codes

Let $\mathbb{Z}_k$ denote the ring of integers modulo k. A *code* of length n over $\mathbb{Z}_k$ is a subset of $\mathbb{Z}_k^n$ and the code is said to be *linear* if it is an additive subgroup of $\mathbb{Z}_k^n$. The Hamming weight of an element in $\mathbb{Z}_k$ is the number of non-zero coordinates and the minimum weight of a code is the smallest Hamming weight of all non-zero elements. For any undefined terms from coding theory see [15] or [10].

Given two elements, $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{Z}_k^n$, we consider the inner product

$$x \cdot y = \sum_{i=1}^{n} x_i y_i.$$

We define the *dual* code $C^\perp$ of a code C with respect to the above inner product, that is $C^\perp = \{w \mid w \cdot v = 0,\ \forall v \in C\}$. The code is said to be *self-dual* if it is equal to its dual and *self-orthogonal* if it is contained in its dual. A self-dual code is *Type II* if the weight of each of its elements is a multiple of $2k$. We refer the reader to [17] for a complete description of self-dual codes.

For a linear code C over $\mathbb{Z}_k$, we say that a matrix G, whose rows are codewords, generates C if C is equal to the linear span of the rows of G. Such a matrix is usually called a *generator matrix* if its number of rows is minimal.

In this paper we always consider linear codes and we are mainly interested in *binary* linear codes, that is, the case $k = 2$.

1.2 Association schemes

Let X be a finite set, $|X| = v$. Let R_i be a subset of $X \times X$, $\forall i \in \mathcal{I} = \{0, \ldots, d\}, d > 0$. We define $\Re = \{R_i\}_{i \in \mathcal{I}}$. We say that $(X, \Re)$ is a *d-class association scheme* if the following properties are satisfied:

(i) $R_0 = \{(x, x) : x \in X\}$ is the identity relation.
(ii) For every $x, y \in X$, $(x, y) \in R_i$ for exactly one i.
(iii) $\forall\, i \in \mathcal{I},\ \exists\, i' \in \mathcal{I}$ such that $R_i^T = R_{i'}$, where $R_i^T = \{(x, y) : (y, x) \in R_i\}$.
(iv) If $(x, y) \in R_k$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant p_{ij}^k.

The values p_{ij}^k are called *intersection numbers*. The elements $x, y \in X$ are called i^{th} *associates* if $(x, y) \in R_i$. If $i = i'$ for all i then the association scheme is said to be *symmetric*, otherwise it is *non-symmetric*. The association scheme $(X, \Re)$ is *commutative* if $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \mathcal{I}$. Note that a symmetric association scheme is always commutative but the converse is not true.

The adjacency matrix A_i for the relation R_i for $i \in \mathcal{I}$, is the $v \times v$ matrix with rows and columns labeled by the points of X and defined by

$$(A_i)_{x,y} = \begin{cases} 1, \ if\ (x, y) \in R_i, \\ 0, \quad otherwise. \end{cases}$$

The conditions (i)-(iv) in the definition of $(X, \Re)$ are equivalent to:

(i) $A_0 = I$ (the identity matrix).
(ii) $\sum_{i \in \mathcal{I}} A_i = J$ (the all-ones matrix).
(iii) $\forall\, i \in \mathcal{I}, \exists\, i' \in \mathcal{I}$, such that $A_i = A_{i'}^T$.
(iv) $\forall\, i, j \in \mathcal{I}, \quad A_i A_j = \sum\limits_{k \in \mathcal{I}} p_{ij}^k A_k$.

If the association scheme is symmetric, then $A_i = A_i^T$, for all $i \in \mathcal{I}$. If the association scheme is commutative, then $A_i A_j = A_j A_i$, for all $i, j \in \mathcal{I}$. The adjacency matrices generate an $(n+1)$-dimensional algebra $\mathbf{A}$ of symmetric matrices. This algebra is called the Bose-Mesner algebra.

Higman [9] proved that a d-class association scheme with $d \leq 4$ is always commutative, meaning that $p_{ij}^k = p_{ji}^k$, for all $i, j, k \in \mathcal{I}$.

2 3-class association schemes and self-dual codes

Let $(X, \Re)$ be a 3-class association scheme. The adjacency matrix for R_0 is I and the adjacency matrices for R_1, R_2 and R_3 are A_1, A_2 and $J - I - A_1 - A_2$, respectively.

Lemma 1 *If $(X, \Re)$ is a 3-class association scheme then the following equations hold:*

$$\begin{aligned}&A_1J = JA_1 = p^0_{11}J, A_2J = JA_2 = p^0_{22}J,\\ &A_1A_2 = A_2A_1 = p^0_{12}I + p^1_{12}A_1 + p^2_{12}A_2 + p^3_{12}\left(J - I - A_1 - A_2\right).\end{aligned}$$

Note that the number of ones per row (or column) in A_1 is p^0_{11}, A_2 is p^0_{22} and A_3 is p^0_{33}.

Let A_0, A_1, A_2, A_3 be the adjacency matrices. We describe the following construction which we shall use in our construction of self-dual codes. For arbitrary values of $r, s, t, u \in \mathbb{Z}_k$ let

$$\begin{aligned}Q\left(r, s, t, u\right) &= rA_0 + sA_1 + tA_2 + uA_3\\ &= rI + sA_1 + tA_2 + u\left(J - I - A_1 - A_2\right)\\ &= \left(r - u\right)I + \left(s - u\right)A_1 + \left(t - u\right)A_2 + uJ. \qquad (1)\end{aligned}$$

We write Q for $Q\left(r, s, t, u\right)$. We define two different methods of constructing self-dual codes, the pure and bordered construction. In both cases, the generator matrices are defined by using the matrix Q. In the *pure* construction, the generator matrix is

$$\mathcal{P}(r, s, t, u) = (I \mid Q).$$

In the *bordered* construction the generator matrix is

$$\mathcal{B}(r, s, t, u) = \left(\begin{array}{c|c|c|c} 1 & 0 \ldots 0 & a & b \ldots b \\ \hline 0 & & c & \\ \vdots & I & \vdots & Q \\ 0 & & c & \end{array}\right).$$

Codes generated by $\mathcal{P}(r, s, t, u)$ and $\mathcal{B}(r, s, t, u)$ have length $2v$ and $2v + 2$ respectively. Thus to construct a self-dual code we need only make it self-orthogonal.

For the code generated by $\mathcal{P}(r, s, t, u)$ to be self-orthogonal we need

$$(I \mid Q)(I \mid Q)^T = \mathbf{0}.$$

Namely we need $QQ^T = -I$.

For the pure construction to give a Type II code we need the inner product of any row with itself to be $0 \pmod{2k}$, that is we need

$$1 + r^2 + s^2p^0_{11} + t^2p^0_{22} + u^2p^0_{33} \equiv 0 \pmod{2k}.$$

For the code generated by $\mathcal{B}(r,s,t,u)$ to be self-dual we need the following:

$$1 + a^2 + vb^2 = 0, \tag{2}$$

$$ac + b(r + sp^0_{11} + tp^0_{22} + up^0_{33} = 0, \tag{3}$$

$$I + c^2J + QQ^T = \mathbf{0}. \tag{4}$$

The first equation is the inner product of the top row with itself. The second is the inner product of the top row with any other row, and the third ensures that the other rows are orthogonal to each other.

We write $\mathcal{P}$ and $\mathcal{B}$ for $\mathcal{P}\,(r,s,t,u)$ and $\mathcal{B}\,(r,s,t,u)$, respectively.

3 Self-dual codes from non-symmetric 3-class association schemes

Let $(X,\Re)$ be a 3-class association scheme. If it is non-symmetric then we can order the relations such that $R_2 = R_1^T$ and R_3 is a symmetric relation. The association scheme is uniquely determined by R_1. If we denote the adjacency matrix for R_1 by A then the adjacency matrices for R_0, R_2 and R_3 are I, A^T and $J - I - A - A^T$, respectively.

The following lemma is well known, see [12] for example.

Lemma 2 *If $(X,\Re)$ is a non-symmetric 3-class association scheme then the following equations hold:*

$$\begin{aligned}&AJ = JA = \kappa J,\\ &AA^T = A^TA = \kappa I + \lambda\left(A + A^T\right) + \mu\left(J - I - A - A^T\right),\\ &A^2 = \alpha A + \beta A^T + \gamma\left(J - I - A - A^T\right),\end{aligned}$$

where $\kappa = p^0_{12} = p^0_{21}$, $\lambda = p^1_{12} = p^1_{21}$, $\mu = p^3_{12} = p^3_{21}$, $\alpha = p^1_{11}$, $\beta = p^2_{11}$ and $\gamma = p^3_{11}$. Moreover, $\alpha = \lambda$ and κ is the number of ones at each row and at each column of A.

Related to a non-symmetric 3-class association scheme $(X,\Re)$ we have the parameters $v = |X|$ and κ, λ, μ, α, β and γ as in the above lemma.

If $(X,\Re)$ is a non-symmetric 3-class association scheme then the matrix Q designed in Equation (1) can be written as

$$Q = (r-u)\,I + (s-u)\,A + (t-u)\,A^T + uJ. \tag{5}$$

3.1 Pure construction

Theorem 1 *Let C be the binary linear code generated by $\mathcal{P}$. The code C is self-dual if and only if one of the following holds:*

(i) $s \neq t$; $\kappa \neq \lambda = r + u + \mu$; $\mu = uv$.
(ii) $s = t$; $r = u$; $s = u$ *or* $\lambda = \beta$; $uv = 0$.

All of the operations are over $\mathbb{Z}_2$.

Proof From Equation (5) and Lemma 2

$$\begin{aligned} QQ^T &= [r+u+(s+t)(\kappa+\mu)]\,I \\ &+ [(s+t)(r+u+\lambda+\mu)+(s+u)(t+u)(\lambda+\beta)]\,(A+A^T) \\ &+ [(s+t)\mu+uv]\,J. \end{aligned}$$

It is clear that, for $x_0, x_1, x_2, x_3 \in \mathbb{Z}_2$, $x_0 I + x_1 A + x_2 A^T + x_3 J = I$ if and only if $x_0 = 1$ and $x_1 = x_2 = x_3 = 0$. C is self-dual if and only if $QQ^T = I$ which gives the following equations over $\mathbb{Z}_2$:

$$\begin{aligned} r+u+(s+t)(\kappa+\mu) &= 1, \\ (s+t)(r+u+\lambda+\mu)+(s+u)(t+u)(\lambda+\beta) &= 0, \\ (s+t)\mu+uv &= 0. \end{aligned}$$

If $s \neq t$, the equations reduce to condition (i). If $s = t$, then the equations reduce to condition (ii).

If we write $w = r + u \in \mathbb{Z}_2$, then we obtain the possible values of Q such that C is self-dual.

Corollary 1 *Let C be the binary linear code generated by $\mathcal{P}$. The code C is self-dual if and only if one of the following holds:*

(i) $Q = wI + B$, *with* $\mu = \lambda + w = 0$ *and* $\lambda \neq \kappa$*; or*
(ii) $Q = wI + B + J$, *with* $\mu = \lambda + w = v$ *and* $\lambda \neq \kappa$*; or*
(iii) $Q = I + A + A^T + uJ$ *with* $\lambda = \beta$ *and* $uv = 0$*; or*
(iv) $Q = I + uJ$ *with* $uv = 0$.

Where B stands for A or A^T and the equalities are over $\mathbb{Z}_2$.

Proof Cases (*i*) and (*ii*) correspond to case (*i*) in Theorem 1 and cases (*iii*) and (*iv*) correspond to case (*ii*) in Theorem 1.

Corollary 2 *Let C be the binary linear code generated by $\mathcal{P}$. The code C is Type II if and only if one of the following holds:*

(i) $Q = wI + B$, $\mu = \lambda + w = 0$, $\lambda \neq \kappa$ *and* $w + \kappa \equiv 3 \pmod 4$*; or*
(ii) $Q = wI + B + J$, $\mu = \lambda + w = v$, $\lambda \neq \kappa$ *and* $1 + v \equiv \kappa + w \pmod 4$*; or*
(iii) $Q = I + A + A^T$*;* $\lambda = \beta$ *and* κ *is odd; or*
(iv) $Q = I + A + A^T + J$*;* $\lambda = \beta$ *and* v *is even; or*
(v) $Q = I + J$ *and* $v \equiv 0 \pmod 4$.

Where B stands for A or A^T and the equalities are over $\mathbb{Z}_2$.

Proof The result is obtained by taking into account that a binary self-dual code is a Type II code if and only if all the rows of the generator matrix have doubly-even weight. Then, we compute the number of ones in any row of $\mathcal{P}$ for all different values of Q obtained in Corollary 1:

(i) $\mathcal{P}$ has $1 + w + \kappa$ ones per row.

(ii) $\mathcal{P}$ has $1+v-w-\kappa$ ones per row.

(iii) $\mathcal{P}$ has $1+1+2\kappa = 2(\kappa+1)$ ones per row. Note that $2(\kappa+1) \equiv 0 \pmod 4$ is equivalent to κ odd.

(iv) $\mathcal{P}$ has $1+v-2\kappa-1 = v-2\kappa$ ones per row. Note that v must be even if C is self-dual, hence the condition $v \equiv 2\kappa \pmod 4$ always holds.

(v) $\mathcal{P}$ has $1+v-1 = v$ ones per row.

Example 1 Let $v \equiv 0 \pmod 3$ and

$$\begin{aligned} X_0 &= \left\{0, 1, \ldots, \frac{v}{3} - 1\right\}, \\ X_1 &= \left\{\frac{v}{3}, \ldots, \frac{2v}{3} - 1\right\}, \\ X_2 &= \left\{\frac{2v}{3}, \ldots, v - 1\right\}. \end{aligned}$$

Let $X = X_0 \cup X_1 \cup X_2$, we define the following relations:

$$\begin{aligned} &R_0 = \{(x, x) \mid x \in X\}, \\ &R_1 = (X_0 \times X_1) \cup (X_1 \times X_2) \cup (X_2 \times X_0), R_2 = R_1^T, \\ &R_3 = \left[\bigcup_{i=0}^{2} (X_i \times X_i)\right] - R_0. \end{aligned}$$

Then, $(X, \Re)$ is a 3-class non-symmetric association scheme with parameters:

$$\kappa = \mu = \beta = \frac{v}{3}, \quad \gamma = 0 \quad \text{and} \quad \lambda = 0. \tag{6}$$

Proposition 1 *Consider the association scheme of Example 1. The binary linear code C generated by $\mathcal{P}$ is self-dual if and only if one of the following holds:*

(i) $Q = I + B + J$ *and* $v \equiv 3 \pmod 6$. *In this case C is not a Type II code.*

(ii) $Q = I + A + A^T + uJ$ *for some u and* $v \equiv 0 \pmod 6$. *Moreover C is a Type II code if and only if $u = 1$.*

(iii) $Q = I + uJ$ *for some u and* $v \equiv 0 \pmod 6$. *Moreover C is a Type II code if and only if $u = 1$ and $v \equiv 0 \pmod{12}$.*

Where B is A or A^T.

Proof We examine the different possible cases in Corollary 1.

If $Q = wI + B$ (where B is A or A^T) the construction does not give a self-dual code since we have $\mu = \kappa$ and $\lambda = 0$ in Equation (6) and for a code C generated by $Q = wI + B$ to be self-dual, Q has to satisfy case (i) in Corollary 1.

If $Q = wI + B + J$, then from case (ii) in Corollary 1 we know that $\mu \equiv \lambda + w \pmod 2$ and $\lambda \not\equiv \kappa \pmod 2$, combined with $\mu = \kappa$ in Equation (6) we get $w = 1$. Since $\lambda = 0$, we obtain

$$v \equiv \mu \equiv \beta \equiv v/3 \equiv 1 \pmod 2.$$

Since $v \equiv 0 \pmod 3$, the conclusion is that for $v \equiv 3 \pmod 6$, C is a self-dual code. Assume now that C is a Type II code, then $v \equiv \kappa \pmod 4$ by (ii) of Corollary 2. But $k = v/3$ in Equation (6) would imply $v \equiv v/3$ (mod 4), but this is impossible for $v \equiv 3 \pmod 6$, which corresponds to (i) in Proposition 1.

If $Q = I + A + A^T + uJ$, then from case (iii) in Corollary 1 we need $\lambda \equiv \beta \pmod 2$. Since $\lambda = 0$, by Equation (6), we obtain $v/3 \equiv 0 \pmod 2$. Combined with $v \equiv 0 \pmod 3$, we have $v \equiv 0 \pmod 6$. Note that now the condition $uv \equiv 0 \pmod 2$ in (iii) of Corollary 1 is always satisfied. If $u = 0$, then C would be self-dual for κ odd, but κ is even by Equation (6). If $u = 1$, then the condition v even is already satisfied. It corresponds to (ii) in Proposition 1.

$Q = I$ gives a trivial self-dual code, which is not of Type II.

If $Q = I + J$, then C is self-dual for v even, therefore $v \equiv 0 \pmod 6$. By Corollary 2, C is of Type II if $v \equiv 0 \pmod 4$, hence $v \equiv 0 \pmod{12}$, which corresponds to (iii) in Proposition 1.

Example 2 We take the specific case $v = 6$ from Example 1. The parameters are

$$\begin{array}{l}
p^0_{12} = p^0_{21} = p^3_{12} = p^3_{21} = p^2_{11} = p^1_{22} = \frac{v}{3} = 2, \\
p^1_{13} = p^1_{31} = p^2_{23} = p^2_{32} = p^0_{33} = \frac{v}{3} - 1 = 1, \\
p^3_{33} = \frac{v}{3} - 2 = 0, \\
p^k_{ko} = p^k_{0k} = 1\,(k = 0, 1, 2, 3)\,, \\
p^k_{ij} = 0 \quad \text{for the rest.}
\end{array}$$

So, for $v = 6$, $\kappa = \mu = \beta = 2$ and $\alpha = \lambda = 0$, the adjacency matrix for R_1 is

$$A = \begin{pmatrix} 0&1&0&1&0&0 \\ 0&0&1&0&1&0 \\ 0&0&0&1&0&1 \\ 0&0&0&0&1&1 \\ 1&0&1&0&0&0 \\ 1&1&0&0&0&0 \end{pmatrix}.$$

Take $Q = I + A + A^T$, then the generator matrix $\mathcal{P}$ is

$$\mathcal{P} = \left(\begin{array}{c|cccccc} & 1&1&0&1&1&1 \\ & 1&1&1&0&1&1 \\ & 0&1&1&1&1&1 \\ I & 1&0&1&1&1&1 \\ & 1&1&1&1&1&0 \\ & 1&1&1&1&0&1 \end{array} \right).$$

The code generated by $\mathcal{P}$ is a self-dual code but not a Type II code. The minimum weight of the code is 4.

Using the parameters given in Example 1, the equalities in Lemma 2 become:

$$\begin{array}{l} AJ = JA = \frac{v}{3}J, \\ AA^T = A^TA = \frac{v}{3}\left(J - A - A^T\right), \\ A^2 = \frac{v}{3}A^T, \left(A^T\right)^2 = \left(A^2\right)^T = \frac{v}{3}A, \\ A^2 + \left(A^2\right)^T = \frac{v}{3}\left(A + A^T\right). \end{array} \quad (7)$$

Following Example 1, we will now consider codes generated over rings $\mathbb{Z}_k$ with $k > 2$. Hence we need $QQ^T = -I$ so that the code generated by $\mathcal{P}$ is a self-dual code. From Equation (7) and Equation (5)

$$\begin{aligned} QQ^T = {} & (r-u)^2 I \\ & + \left[(r-u)(s+t-2u) + \frac{v}{3}\left[(s-u)(t-u) - (s-u)^2(t-u)^2\right]\right]\left(A + A^T\right) \\ & + \left[u\left[2(r-u) + 2\frac{v}{3}(s+t-2u) + uv\right] + \frac{v}{3}\left[(s-u)^2 + (t-u)^2\right]\right] J. \end{aligned}$$

We shall use the following classical result on number theory.

Lemma 3 *Let $k = 2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ be the prime factor decomposition of k. If -1 is a quadratic residue modulo k, then*

$$\alpha_0 \leq 1 \quad \textit{and} \quad p_i \equiv 1 \pmod 4 \;\; \forall i = 1, \ldots, r.$$

Proposition 2 *Following Example 1, let C be the code generated by $\mathcal{P}$ over $\mathbb{Z}_k$. If C is a self-dual code then*

$$\alpha_0 \leq 1 \quad \textit{and} \quad p_i \equiv 1 \pmod 4 \;\; \forall i = 1, \ldots, r;$$

where $k = 2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ is the prime factor decomposition of k.

Proof We have that $(r-u)^2 = -1$ over $\mathbb{Z}_k$. Thus, the result holds applying Lemma 3.

Therefore, the code C generated by $\mathcal{P}$ cannot be self-dual over, for example, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_7$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{11}$, $\mathbb{Z}_{12}$, $\mathbb{Z}_{14}$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{16}$.

3.2 Bordered construction

For $b = 0$ we will always have a code, generated by $\mathcal{B}$, with minimum weight 2 which does not lead to any interesting results, hence we confine ourselves to codes generated by $\mathcal{B}$ for $b = 1$.

Theorem 2 *Let C be the binary linear code generated by $\mathcal{B}$, with $b = 1$. The code C is self-dual if and only if $a = 0$, $c = v = 1$ and one of the following holds:*

(i) $s \neq t$; $r = \kappa \neq \lambda$, $\mu \neq u$.
(ii) $s = t$; $r = 0$, $u = 1$, $(t+u)(\lambda+\beta) = 0$.

All of the operations are over $\mathbb{Z}_2$.

Proof From Equation (5) and Lemma 2

$$\begin{aligned} QQ^T &= [r+u+(s+t)(\kappa+\mu)]\,I \\ &+ [(s+t)(r+u+\lambda+\mu)+(s+u)(t+u)(\lambda+\beta)]\,(A+A^T) \\ &+ [(s+t)\mu+uv]\,J. \end{aligned}$$

It is clear that, for $x_0, x_1, x_2, x_3 \in \mathbb{Z}_2$, $x_0 I + x_1 A + x_2 A^T + x_3 J = I + cJ$ if and only if $x_0 = 1$, $x_1 = x_2 = 0$ and $x_3 = c$. C is self-dual if and only if $QQ^T = -I - c^2 J$ which gives the following equations over $\mathbb{Z}_2$:

$$\begin{aligned} r+u+(s+t)(\kappa+\mu) &= 1, \\ (s+t)(r+u+\lambda+\mu)+(s+u)(t+u)(\lambda+\beta) &= 0, \\ (s+t)\mu+uv &= c. \end{aligned} \tag{8}$$

Also from Equations (2) and (3) we have

$$\begin{aligned} 1+a+vb &= 0, \\ ac+b(r+s\kappa+t\kappa+u(v-1)) &= 0. \end{aligned} \tag{9}$$

If $s \neq t$, then Equations (8) and (9) reduce to condition (i). If $s = t$, then the equations reduce to condition (ii).

Corollary 3 *Let C be a binary linear code generated by $\mathcal{B}$, with $b = 1$. The code C is self-dual if and only if one of the following conditions hold:*

(i) $Q = B$, *with* $a = 0$, $v \equiv 1$, $\kappa \equiv 0$, $\mu \equiv 1$, $c \equiv 1$ *and* $\lambda \equiv 1$; *or*
(ii) $Q = I + B + J$, *with* $a = 0$, $v \equiv 1$, $\kappa \equiv 0$, $\mu \equiv 0$, $c \equiv 1$ *and* $\lambda \equiv 1$; *or*
(iii) $Q = I + B$, *with* $a = 0$, $v \equiv 1$, $\kappa \equiv 1$, $\mu \equiv 1$, $c \equiv 1$ *and* $\lambda \equiv 0$; *or*
(iv) $Q = B + J$, *with* $a = 0$, $v \equiv 1$, $\kappa \equiv 1$, $\mu \equiv 0$, $c \equiv 1$ *and* $\lambda \equiv 0$; *or*
(v) $Q = I + A + A^T + J$ *with* $a = 0$, $v \equiv 1$, $c \equiv 1$ *and* $\lambda + \beta \equiv 0$; *or*
(vi) $Q = I + J$ *with* $a = 0$, $v \equiv 1$ *and* $c \equiv 1$.

Where B stands for A or A^T and the equalities are over $\mathbb{Z}_2$ and the congruences are modulo 2.

Proof The conditions are obtained for different values of r, s, t, u on Theorem 2.

Corollary 4 *Let C be a binary self-dual code generated by $\mathcal{B}$, with $b = 1$. The code C is Type II if and only if one of the following conditions hold:*

(i) $Q = B$, *with* $a = 0$, $v \equiv 3$, $\kappa \equiv 2$, $\mu \equiv 1$, $c = 1$ *and* $\lambda \equiv 1$; *or*
(ii) $Q = I + B + J$, *with* $a = 0$, $v \equiv 3$, $\kappa \equiv 0$, $\mu \equiv 0$, $c = 1$ *and* $\lambda \equiv 1$; *or*
(iii) $Q = I + B$, *with* $a = 0$, $v \equiv 3$, $\kappa \equiv 1$, $\mu \equiv 1$, $c = 1$ *and* $\lambda \equiv 0$; *or*
(iv) $Q = B + J$, *with* $a = 0$, $v \equiv 3$, $\kappa \equiv 3$, $\mu \equiv 0$, $c = 1$ *and* $\lambda \equiv 0$; *or*
(v) $Q = I + A + A^T + J$ *with* $a = 0$, $v \equiv 1$, κ *is even,* $c = 1$ *and* $\lambda + \beta \equiv 0$; *or*
(vi) $Q = I + J$ *with* $a = 0$, $v \equiv 1$ *and* $c = 1$.

Where B stands for A or A^T and the congruences are modulo 4.

Proof We know that a binary self-dual code is of Type II if and only if all the rows of generator matrices have doubly-even weight. Hence, we compute the number of ones in any row of $\mathcal{B}$ by considering the different cases of Q given in Corollary 3

(i) $\mathcal{B}$ has $1+v$ or $1+1+\kappa$ ones per row.
(ii) $\mathcal{B}$ has $1+v$ or $1+1-1-\kappa+v$ ones per row.
(iii) $\mathcal{B}$ has $1+v$ or $1+1+1+\kappa$ ones per row.
(iv) $\mathcal{B}$ has $1+v$ or $1+1-\kappa+v$ ones per row.
(v) $\mathcal{B}$ has $1+v$ or $1+1-1-\kappa-\kappa+v$ ones per row.
(vi) $\mathcal{B}$ has $1+v$ or $1+1-1+v$ ones per row.

Example 3 We take the specific value of v = 9 in Example 1.

The parameters are

$$\begin{aligned}
&p^0_{12}=p^0_{21}=p^3_{12}=p^3_{21}=p^2_{11}=p^1_{22}=\tfrac{v}{3}=3,\\
&p^1_{13}=p^1_{31}=p^2_{23}=p^2_{32}=p^0_{33}=\tfrac{v}{3}-1=2,\\
&p^3_{33}=\tfrac{v}{3}-2=1,\\
&p^k_{ko}=p^k_{0k}=1\,(k=0,1,2,3)\,,\\
&p^k_{ij}=0 \quad \text{for the rest.}
\end{aligned}$$

So, for $v=9$, $\kappa=\mu=\beta=3$ and $\alpha=\lambda=0$. The adjacency matrix for R_1 is

$$A=\begin{pmatrix}
0&1&0&0&1&0&0&1&0\\
0&0&1&0&0&1&0&0&1\\
1&0&0&1&0&0&1&0&0\\
0&1&0&0&1&0&0&1&0\\
0&0&1&0&0&1&0&0&1\\
1&0&0&1&0&0&1&0&0\\
0&1&0&0&1&0&0&1&0\\
0&0&1&0&0&1&0&0&1\\
1&0&0&1&0&0&1&0&0
\end{pmatrix},$$

Take $Q=I+A$, then the generator matrix $\mathcal{B}$ is:

$$\mathcal{B}=\left(\begin{array}{c|c|c|c}
1 & 0\ldots0 & 0 & 1\ldots1\\
\hline
0 & & 1 & \\
\vdots & I & \vdots & Q\\
0 & & 1 &
\end{array}\right).$$

The code generated by $\mathcal{B}$ is a self-dual code, but not a Type II code.

4 Self-dual codes from symmetric 3-class association schemes

Let $(X,\Re)$ be a 3-class association scheme. If it is symmetric then all adjacency matrices are symmetric. The theory presented for a general 3-class association scheme applies directly to a symmetric 3-class association scheme.

4.1 General results

Theorem 3 *Let C be the binary linear code generated by $\mathcal{P}$. The code C is self-dual if and only if the following holds:*

$$\begin{aligned} (r+u)+(s+u)\left(p_{11}^0+p_{11}^3\right)+(t+u)\left(p_{22}^0+p_{22}^3\right)&=1,\\ \left(p_{11}^0+p_{11}^3\right)(s+u)+\left(p_{22}^1+p_{22}^3\right)(t+u)&=0,\\ \left(p_{11}^2+p_{11}^3\right)(s+u)+\left(p_{22}^2+p_{22}^3\right)(t+u)&=0,\\ uv+(s+u)\,p_{11}^3+(t+u)\,p_{22}^3&=0. \end{aligned} \tag{10}$$

Proof From Equation (1) and Lemma 1, we have

$$\begin{aligned} Q^2 = {} & \left[(r+u)+(s+u)\left(p_{11}^0+p_{11}^3\right)+(t+u)\left(p_{22}^0+p_{22}^3\right)\right] I\\ & + \left[\left(p_{11}^0+p_{11}^3\right)(s+u)+\left(p_{22}^1+p_{22}^3\right)(t+u)\right] A_1\\ & + \left[\left(p_{11}^2+p_{11}^3\right)(s+u)+\left(p_{22}^2+p_{22}^3\right)(t+u)\right] A_2\\ & + \left(uv+(s+u)\,p_{11}^3+(t+u)\,p_{22}^3\right) J. \end{aligned}$$

It is clear that, for $x_0, x_1, x_2, x_3 \in \mathbb{Z}_2$, $x_0 I + x_1 A + x_2 A^T + x_3 J = I$ if and only if $x_0 = 1$ and $x_1 = x_2 = x_3 = 0$. C is self-dual if and only if $QQ^T = I$ which gives Equation (10) over $\mathbb{Z}_2$.

Corollary 5 *Let C be the binary self-dual generated by $\mathcal{P}$. The code C is Type II if and only if the following holds:*

(i) $Q = I + A_1 + A_2 + J$, $v - p_{11}^0 - p_{22}^0 \equiv 0$.
(ii) $Q = A_2$, $p_{22}^0 \equiv 3$.
(iii) $Q = I + A_1 + J$, $v - p_{11}^0 \equiv 0$.
(iv) $Q = A_1$, $p_{11}^0 \equiv 3$.
(v) $Q = I + A_2 + J$, $v - p_{22}^0 \equiv 0$.
(vi) $Q = A_1 + A_2$, $p_{11}^0 + p_{22}^0 \equiv 3$.
(vii) $Q = I + J$, $v \equiv 0$.
(viii) $Q = A_1 + A_2 + J$, $v - p_{11}^0 - p_{22}^0 \equiv 3$.
(ix) $Q = I + A_2$, $p_{22}^0 \equiv 2$.
(x) $Q = A_1 + J$, $v - p_{11}^0 \equiv 3$.
(xi) $Q = I + A_1$, $p_{11}^0 \equiv 2$.
(xii) $Q = A_2 + J$, $v - p_{22}^0 \equiv 3$.
(xiii) $Q = I + A_1 + A_2$, $p_{11}^0 + p_{22}^0 \equiv 2$.

All congruences are modulo 4.

Proof As mentioned before a binary self-dual code is of Type II if and only if all the rows of generator matrices have doubly-even weight. Hence, we compute the number of ones in any row of $\mathcal{P}$ by considering the different cases of Q.

(i) $\mathcal{P}$ has $1 - 1 - p_{11}^0 - p_{22}^0 + v$ ones per row.
(ii) $\mathcal{P}$ has $1 + p_{22}^0$ ones per row.
(iii) $\mathcal{P}$ has $1 - 1 - p_{11}^0 + v$ ones per row.

(iv) $\mathcal{P}$ has $1+p_{11}^0$ ones per row.
(v) $\mathcal{P}$ has $1-1-p_{22}^0+v$ ones per row.
(vi) $\mathcal{P}$ has $1+p_{11}^0+p_{22}^3$ ones per row.
(vii) $\mathcal{P}$ has $1-1+v$.
(viii) $\mathcal{P}$ has $1-p_{11}^0-p_{22}^0+v$ ones per row.
(ix) $\mathcal{P}$ has $1+1+p_{22}^0$ ones per row.
(x) $\mathcal{P}$ has $1-p_{11}^0+v$ ones per row.
(xi) $\mathcal{P}$ has $1+1+p_{11}^0$ ones per row.
(xii) $\mathcal{P}$ has $1-p_{22}^0+v$ ones per row.
(xiii) $\mathcal{P}$ has $1+1+p_{11}^0+p_{22}^0$ ones per row.

For the bordered construction, as earlier, we will confine ourselves to codes generated by $\mathcal{B}$ for $b=1$.

Theorem 4 *Let C be the binary linear code generated by $\mathcal{B}$, with $b=1$. The code C is self-dual if and only if following holds:*

$$\begin{aligned}
1+a+vb&=0,\\
ac+b(r+sp_{11}^0+tp_{22}^0+up_{33}^0)&=0,\\
(r+u)+(s+u)\left(p_{11}^0+p_{11}^3\right)+(t+u)\left(p_{22}^0+p_{22}^3\right)&=1,\\
\left(p_{11}^0+p_{11}^3\right)(s+u)+\left(p_{22}^1+p_{22}^3\right)(t+u)&=0,\\
\left(p_{11}^2+p_{11}^3\right)(s+u)+\left(p_{22}^2+p_{22}^3\right)(t+u)&=0,\\
uv+(s+u)\,p_{11}^3+(t+u)\,p_{22}^3&=c. \qquad (11)
\end{aligned}$$

All operations are over $\mathbb{Z}_2$.

Proof From Equation (1) and Lemma 1, we have

$$\begin{aligned}
Q^2 = &\left[(r+u)+(s+u)\left(p_{11}^0+p_{11}^3\right)+(t+u)\left(p_{22}^0+p_{22}^3\right)\right] I\\
&+\left[\left(p_{11}^0+p_{11}^3\right)(s+u)+\left(p_{22}^1+p_{22}^3\right)(t+u)\right] A_1\\
&+\left[\left(p_{11}^2+p_{11}^3\right)(s+u)+\left(p_{22}^2+p_{22}^3\right)(t+u)\right] A_2\\
&+\left(uv+(s+u)\,p_{11}^3+(t+u)\,p_{22}^3\right) J.
\end{aligned}$$

It is clear that, for $x_0,x_1,x_2,x_3\in\mathbb{Z}_2$, $x_0I+x_1A+x_2A^T+x_3J=I+cJ$ if and only if $x_0=1$, $x_1=x_2=0$ and $x_3=c$. C is self-dual if and only if $QQ^T=-I-c^2J$ which along with Equation (2) and (3) gives Equation (11) over $\mathbb{Z}_2$.

Corollary 6 *Let C be the binary self-dual code generated by $\mathcal{B}$, with $b=1$. The code C is Type II if and only if the following holds:*

(i) $Q=I+A_1+A_2+J$, $a+v\equiv 3$, $c+v-p_{11}^0-p_{22}^0\equiv 0$.
(ii) $Q=A_2$, $a+v\equiv 3$, $c+p_{22}^0\equiv 3$.
(iii) $Q=I+A_1+J$, $a+v\equiv 3$, $c-p_{11}^0+v\equiv 0$.
(iv) $Q=A_1$, $a+v\equiv 3$, $c+p_{11}^0\equiv 3$.
(v) $Q=I+A_2+J$, $a+v\equiv 3$, $c-p_{22}^0+v\equiv 0$.

(vi) $Q = A_1 + A_2$, $a + v \equiv 3$, $c + p^0_{11} + p^0_{22} \equiv 3$.
(vii) $Q = I + J$, $a + v \equiv 3$, $c + v \equiv 0$.
(viii) $Q = A_1 + A_2 + J$, $a + v \equiv 3$, $c - p^0_{11} - p^0_{22} + v \equiv 3$.
(ix) $Q = I + A_2$, $a + v \equiv 3$, $c + p^0_{22} \equiv 2$.
(x) $Q = A_1 + J$, $a + v \equiv 3$, $c - p^0_{11} + v \equiv 3$.
(xi) $Q = I + A_1$, $a + v \equiv 3$, $c + p^0_{11} \equiv 2$.
(xii) $Q = A_2 + J$, $a + v \equiv 3$, $c - p^0_{22} + v \equiv 3$.
(xiii) $Q = I + A_1 + A_2$, $a + v \equiv 3$, $c + p^0_{11} + p^0_{22} \equiv 2$.

All congruences are modulo 4.

Proof A binary self-dual code is of Type II if and only if all the rows of generator matrices have doubly-even weight. We compute the number of ones in any row of $\mathcal{B}$ by considering the different cases of Q.

(i) $\mathcal{B}$ has $1 + a + v$ or $1 + c - 1 - p^0_{11} - p^0_{22} + v$ ones per row.
(ii) $\mathcal{B}$ has $1 + a + v$ or $1 + c + p^0_{22}$ ones per row.
(iii) $\mathcal{B}$ has $1 + a + v$ or $1 + c - 1 - p^0_{11} + v$ ones per row.
(iv) $\mathcal{B}$ has $1 + a + v$ or $1 + c + p^0_{11}$ ones per row.
(v) $\mathcal{B}$ has $1 + a + v$ or $1 + c - 1 - p^0_{22} + v$ ones per row.
(vi) $\mathcal{B}$ has $1 + a + v$ or $1 + c + p^0_{11} + p^3_{22}$ ones per row.
(vii) $\mathcal{B}$ has $1 + a + v$ or $1 + c - 1 + v$.
(viii) $\mathcal{B}$ has $1 + a + v$ or $1 + c - p^0_{11} - p^0_{22} + v$ ones per row.
(ix) $\mathcal{B}$ has $1 + a + v$ or $1 + c + 1 + p^0_{22}$ ones per row.
(x) $\mathcal{B}$ has $1 + a + v$ or $1 + c - p^0_{11} + v$ ones per row.
(xi) $\mathcal{B}$ has $1 + a + v$ or $1 + c + 1 + p^0_{11}$ ones per row.
(xii) $\mathcal{B}$ has $1 + a + v$ or $1 + c - p^0_{22} + v$ ones per row.
(xiii) $\mathcal{B}$ has $1 + a + v$ or $1 + c + 1 + p^0_{11} + p^0_{22}$ ones per row.

4.2 Self-dual codes from rectangular association schemes

Let us focus on the rectangular scheme $n \times m$ $(n, m \geq 2)$ which is defined as follows. Consider two sets A and B with $|A| = n \geq 2$ and $|B| = m \geq 2$. Let $X = A \times B$ and define the binary relations over X:

$$\begin{aligned}
R_0 &= \left\{ ((x,y),(x,y)) \in X^2 \right\};\\
R_1 &= \left\{ ((x,y),(x,y')) \in X^2 \middle| \, y \neq y' \right\};\\
R_2 &= \left\{ ((x,y),(x',y)) \in X^2 \middle| \, x \neq x' \right\};\\
R_3 &= \left\{ ((x,y),(x',y')) \in X^2 \middle| \, x \neq x' \, and \, y \neq y' \right\}.
\end{aligned}$$

$(X, \Re)$ is a symmetric 3-class association scheme with parameters:

$$\begin{array}{l}
v = nm, p^0_{11} = m - 1; p^0_{22} = n - 1; p^0_{33} = (m-1)(n-1);\\
p^1_{11} = m - 2; p^1_{23} = p^1_{32} = n - 1; p^1_{33} = (n-1)(m-2);\\
p^2_{13} = p^2_{31} = m - 1; p^2_{22} = n - 2; p^2_{33} = (n-2)(m-1);\\
p^3_{12} = p^3_{21} = 1; p^3_{31} = p^3_{13} = m - 2;\\
p^2_{23} = p^2_{32} = n - 2 = p^3_{33} = (n-2)(m-2);\\
\text{ and } \ p^k_{ij} = 0, \text{ for all other cases }.
\end{array}$$

Lemma 4 *If* $(X, \Re)$ *is a* $n \times m$ *symmetric rectangular association scheme, then the following equations hold:*

$$\begin{aligned}
&A_1 J = J A_1 = (m-1)\, J,\\
&A_2 J = J A_2 = (n-1)\, J,\\
&A_1^2 = (m-1)\, I + (m-2)\, A_1,\\
&A_2^2 = (n-1)\, I + (n-2)\, A_2,\\
&J^2 = nmJ,\\
&A_1 A_2 = A_2 A_1 = A_3 = J - I - A_1 - A_2.
\end{aligned}$$

Proof The proof follows by applying Lemma 1 to a rectangular symmetric association scheme.

Using Lemma 4 and Equation (1) we obtain:

$$\begin{aligned}
QQ^T &= Q^2\\
&= \Big[(r-u)^2 + (s-u)^2 (m-1) + (t-u)^2 (n-1) - 2\,(s-u)\,(t-u)\Big]\, I\\
&+ \Big[2\,(r-u)\,(s-u) + (s-u)^2 (m-2) - 2\,(s-u)\,(t-u)\Big]\, A_1\\
&+ \big[2(r-u)(t-u) + (t-u)^2(n-2) - 2(s-u)(t-u)\big]\, A_2\\
&+ \big[u\,[2(r-u) + 2(s-u)(m-1) + 2(t-u)(n-1) + unm]\\
&\quad +2(s-u)(t-u)\big]\, J.
\end{aligned} \tag{12}$$

4.2.1 Pure construction

Theorem 5 *Let* C *be a binary code generated by* $\mathcal{P}$ *using the rectangular association scheme* $n \times m$*. The code* C *is self-dual if* $r + s + t + u = 1$ *and*

(i) If m *is even and* n *is odd then* C *is self-dual whenever* $r \neq s$*.*
(ii) If n *is even and* m *is odd then* C *is self-dual whenever* $r \neq t$*.*
(iii) If m *and* n *are odd then* C *is self-dual whenever* $r = 1$*,* $s = t = u = 0$*.*

All of the operations are over $\mathbb{Z}_2$*.*

Proof From Equation (12) it is clear that, for $x_0, x_1, x_2, x_3 \in \mathbb{Z}_2$, $x_0 I + x_1 A + x_2 A^T + x_3 J = I$ if and only if $x_0 = 1$ and $x_1 = x_2 = x_3 = 0$. C is self-dual if and only if $QQ^T = I$ which gives the following equations over $\mathbb{Z}_2$:

$$\begin{aligned}
&(r+u) + (s+u)\,(m+1) + (t+u)\,(n+1) = 1,\\
&(s+u)\, m = 0,\\
&(t+u)\, n = 0,\\
&unm = 0.
\end{aligned}$$

Checking different cases for m and n, even or odd, we obtain the conditions given above.

Corollary 7 *Let* C *be a binary code generated by* $\mathcal{P}$*, using the rectangular association scheme* $n \times m$*. The code is self-dual if one of the following conditions hold:*

(i) $Q = A_1$ *or* $Q = A_1 + J$ *and* m *is even.*
(ii) $Q = A_2$ *or* $Q = A_2 + J$ *and* n *is even.*
(iii) $Q = I + A_1 + A_2$ *or* $Q = I + A_1 + A_2 + J$ *and* m*,* n *are even.*
(iv) $Q = I + J$ *and* m *or* n *is even.*
(v) $Q = I$*.*

Proof Results are derived from Theorem 5 and Equation (1).

Corollary 8 *Let* C *be the binary self-dual generated by* $\mathcal{P}$*. The code* C *is Type II if and only if the following holds:*

(i) $Q = A_1$*,* $m \equiv 0$*.*
(ii) $Q = A_1 + J$*,* $mn - m \equiv 2$*.*
(iii) $Q = A_2$*,* $n \equiv 0$*.*
(iv) $Q = A_2 + J$*,* $mn - n \equiv 2$*.*
(v) $Q = I + A_1 + A_2$*,* $m + n \equiv 0$*.*
(vi) $Q = I + A_1 + A_2 + J$*,* $mn - m - n \equiv 0$*.*
(vii) $Q = I + J$*,* $mn \equiv 0$*.*

All congruences are modulo 4*.*

Proof The code C generated by $\mathcal{P}$ is of Type II if and only if all the rows of generator matrices have doubly-even weight. Hence, we compute the number of ones in any row of $\mathcal{P}$ by considering the different cases of Q.

(i) $\mathcal{P}$ has $1 + m - 1$ ones per row.
(ii) $\mathcal{P}$ has $1 - m + 1 + mn$ ones per row.
(iii) $\mathcal{P}$ has $1 + n - 1$ ones per row.
(iv) $\mathcal{P}$ has $1 - n + 1 + mn$ ones per row.
(v) $\mathcal{P}$ has $1 + 1 + m - 1 + n - 1$ ones per row.
(vi) $\mathcal{P}$ has $1 - 1 - m + 1 - n + 1 + mn$ ones per row.
(vii) $\mathcal{P}$ has $1 - 1 + mn$.

Example 4 Consider a 3-class rectangular association scheme with $n = 2$ and $m = 3$. The parameters are:

$$\begin{array}{l}
p^0_{11} = 3; p^0_{22} = 1; p^0_{33} = 2;\\
p^1_{11} = 2; p^1_{23} = p^1_{32} = 1; p^1_{33} = 1;\\
p^2_{13} = p^2_{31} = 1; p^2_{22} = 0; p^2_{33} = 0;\\
p^3_{12} = p^3_{21} = 1; p^3_{31} = p^3_{13} = 1; p^2_{23} = p^2_{32} = 0 = p^3_{33} = 0;\\
\text{ and } \; p^k_{ij} = 0 \text{ for all other cases .}
\end{array}$$

The adjacency matrices are: $A_0 = I$,

$$A_1 = \begin{bmatrix} 0\,1\,1\,0\,0\,0\\ 1\,0\,1\,0\,0\,0\\ 1\,1\,0\,0\,0\,0\\ 0\,0\,0\,0\,1\,1\\ 0\,0\,0\,1\,0\,1\\ 0\,0\,0\,1\,1\,0 \end{bmatrix}, A_2 = \begin{bmatrix} 0\,0\,0\,1\,0\,0\\ 0\,0\,0\,0\,1\,0\\ 0\,0\,0\,0\,0\,1\\ 1\,0\,0\,0\,0\,0\\ 0\,1\,0\,0\,0\,0\\ 0\,0\,1\,0\,0\,0 \end{bmatrix}, A_3 = \begin{bmatrix} 0\,0\,0\,0\,1\,1\\ 0\,0\,0\,1\,0\,1\\ 0\,0\,0\,1\,1\,0\\ 0\,1\,1\,0\,0\,0\\ 1\,0\,1\,0\,0\,0\\ 1\,1\,0\,0\,0\,0 \end{bmatrix}.$$

The generator matrix for code C is $\mathcal{P}$, where Q can be taken from condition (ii) and (iv) from Corollary 7. The code generated by matrix $\mathcal{P}$ is a self-dual code.

4.2.2 Bordered construction

Theorem 6 *Let C be a binary linear code generated by $\mathcal{B}$, with $b = 1$, using the rectangular association scheme $n \times m$. The code C is self-dual if and only if*

$$Q = I + J, a = 0, c = 1,$$

with m and n odd. Moreover the code C is Type II if and only if $nm \equiv 3 \pmod 4$.

Proof From Equation (12) it is clear that, for $x_0, x_1, x_2, x_3 \in \mathbb{Z}_2$, $x_0 I + x_1 A + x_2 A^T + x_3 J = I + cJ$ if and only if $x_0 = 1$, $x_1 = x_2 = 0$ and $x_3 = c$. C is self-dual if and only if $QQ^T = -I - c^2 J$ which gives the following equations over $\mathbb{Z}_2$:

$$\begin{aligned} (r+u) + (s+u)(m+1) + (t+u)(n+1) &= 1, \qquad (13)\\ (s+u)\,m &= 0,\\ (t+u)\,n &= 0,\\ unm &= c. \end{aligned}$$

Also from Equation (2) and (3) for a rectangular 3-class symmetric association scheme we have

$$\begin{aligned} 1 + a + mn &= 0,\\ ac + r + s(m+1) + t(n+1) + u(m+1)(n+1) &= 0. \end{aligned} \qquad (14)$$

where $nm = v$. Since $(s+u)\,m = 0$ and $(t+u)\,n = 0$, Equations (13) and (14) can be reduced to

$$\begin{aligned} r + s + t + u &= 1,\\ aunm + unm + 1 &= 0. \end{aligned} \qquad (15)$$

We observe that $a = 1$ does not satisfy Equation (15) thus for $a = 0$ the above equations give us $c = 1$, $nm = 1$, $s = t = u = 1$ and $r = 0$. Therefore by using the values of r, s, t, u we get $Q = I + J$.

Let $\rho = r - u$, $\sigma = s - u$ and $\tau = t - u$. We can write Equation (12) as

$$\begin{aligned} Q^2 = &\left[\rho^2 + \sigma^2(m-1) + \tau^2(n-1) - 2\sigma\tau\right] I\\ &+ \left[2\rho\sigma + \sigma^2(m-2) - 2\sigma\tau\right] A_1\\ &+ \left[2\rho\tau + \tau^2(n-2) - 2\sigma\tau\right] A_1\\ &+ \left[u\left[2\rho + 2\sigma(m-1) + 2\tau(n-1) + unm\right]\right.\\ &\quad \left. + 2\sigma\tau\right] J. \end{aligned}$$

For the code generated by $\mathcal{P}$ to be self-orthogonal we need

$$\begin{aligned} \rho^2 + \sigma^2 (m-1) + \tau^2 (n-1) - 2\sigma\tau &= -1, \\ 2\rho\sigma + \sigma^2 (m-2) - 2\sigma\tau &= 0, \\ 2\rho\tau + \tau^2 (n-2) - 2\sigma\tau &= 0, \\ u\left[2\rho + 2\sigma (m-1) + 2\tau (n-1) + unm\right] + 2\sigma\tau &= 0. \end{aligned} \tag{16}$$

For a code generated by $\mathcal{B}$ to be self-orthogonal, along with Equations (2) and (3), we need

$$\begin{aligned} \rho^2 + \sigma^2 (m-1) + \tau^2 (n-1) - 2\sigma\tau &= -1; \\ 2\rho\sigma + \sigma^2 (m-2) - 2\sigma\tau &= 0; \\ 2\rho\tau + \tau^2 (n-2) - 2\sigma\tau &= 0; \\ u\left[2\rho + 2\sigma (m-1) + 2\tau (n-1) + unm\right] + 2\sigma\tau &= -c^2. \end{aligned} \tag{17}$$

Theorem 7 *Let C be a code generated from a $n \times m$ rectangular association scheme over $\mathbb{Z}_k$ by using the pure or the bordered construction. Let $k = 2^{\alpha_0} p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factor decomposition of k. If C is a self-dual code, then*

$$\alpha_0 \le 1 \quad \textit{and} \quad p_i \equiv 1 \pmod 4 \ \ \forall i = 1, \ldots, r. \tag{18}$$

Moreover, if (18) is satisfied, then there exist values of n and m such that C is a self-dual code.

Proof Assume that C is a self-dual code. Thus, Equations (16) or (17) are satisfied over $\mathbb{Z}_k$. Note that the first three equations are the same in both cases. From these three equations, it is easy to obtain $(\rho - \sigma - \tau)^2 \equiv -1 \pmod k$. Hence, -1 is a quadratic residue modulo k and, using Lemma 3, it follows (18).

If (18) is satisfied, then we can take the following values:

$$\begin{aligned} m &\equiv \ \ 1 \pmod k; \\ n &\equiv \ \ 2 \pmod k; \\ \rho^2 &\equiv -1 \pmod k; \\ \tau &\equiv \ \ 0 \pmod k; \\ \sigma &\equiv \ \ 2\rho \pmod k. \end{aligned}$$

With these values, the first three equations in (16) or (17) are satisfied. The fourth equation becomes:

$$2u(\rho+u) \equiv 0 \pmod k, \quad \text{or} \quad 2u(\rho+u) \equiv -c^2 \pmod k;$$

respectively in (16) or (17). Clearly, the equation has solutions in both cases. It is also straightforward to find solutions for the Equations (2) and (3), as we can see in the following example.

Example 5 Consider the 3-class rectangular association scheme with $n = 2$ and $m = 6$. The parameters are:

$$\begin{array}{l}
p^0_{11} = 5; p^0_{22} = 1; p^0_{33} = 5;\\
p^1_{11} = 4; p^1_{23} = p^1_{32} = 1; p^1_{33} = 4;\\
p^2_{13} = p^2_{31} = 5; p^2_{22} = 0; p^2_{33} = 0;\\
p^3_{12} = p^3_{21} = 1; p^3_{31} = p^3_{13} = 4; p^2_{23} = p^2_{32} = 0 = p^3_{33} = 0;\\
\text{ and } p^k_{ij} = 0 \text{ for all other cases.}
\end{array}$$

The adjacency matrix for R_1 is:

$$A_1 = \begin{bmatrix}
0&1&1&1&1&1&0&0&0&0&0&0\\
1&0&1&1&1&1&0&0&0&0&0&0\\
1&1&0&1&1&1&0&0&0&0&0&0\\
1&1&1&0&1&1&0&0&0&0&0&0\\
1&1&1&1&0&1&0&0&0&0&0&0\\
1&1&1&1&1&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&1&1&1\\
0&0&0&0&0&0&1&0&1&1&1&1\\
0&0&0&0&0&0&1&1&0&1&1&1\\
0&0&0&0&0&0&1&1&1&0&1&1\\
0&0&0&0&0&0&1&1&1&1&0&1\\
0&0&0&0&0&0&1&1&1&1&1&0
\end{bmatrix}.$$

The code C generated by $\mathcal{P}$, with $Q = 2I + 4A_1$, is a self-dual code over $\mathbb{Z}_5$.

We can generate two self-dual codes over $\mathbb{Z}_5$ with $\mathcal{B}$, using $Q = 2I + 4A_1$ with $a \equiv 2 \pmod 5$ or $a \equiv 3 \pmod 5$ along with $b \equiv c \equiv 0 \pmod 5$.

Note that $\rho^2 \equiv -1 \pmod k$, $\tau \equiv 0 \pmod k$ and $\sigma \equiv 2\rho \pmod k$ in this example.

4.3 Self-dual codes from symmetric designs

A $t-(v,k,\lambda)$ design is a pair $D = (P, B)$ where P is a set of points, $|P| = v$, and B is a collection of k-subsets of elements in P called blocks, $|B| = b$, satisfying that every t-subset of elements of P is contained in exactly λ blocks of B $(0 \leq t \leq k \leq v)$. It is well known that $b \geq v$ (Fisher's inequality) and we say that D is symmetric if the number of points and blocks coincide; that is, $v = b$.

Let D be a $t-(v,k,\lambda)$ design. The incidence matrix of D is a $v \times b$ matrix A whose rows are indexed by the points of P, whose columns are indexed by the blocks of B, and with entries $A_{p,b}$, for $p \in P, b \in B$, equals 1 if $p \in b$, and 0 otherwise. Note that if D is symmetric, then A is a square $v \times v$ matrix.

Denote by I_m and J_m the identity and the square all-one $m \times m$ matrices, respectively. If the size is not indicated, we shall assume that they are $v \times v$ matrices. The following property is well known and can be found, for instance, in [11].

Lemma 5 *Let D be a symmetric $t-(v,k,\lambda)$ design with incidence matrix A. Then,*

1. $AA^T = (k-\lambda)I + \lambda J$;
2. $AJ = JA = kJ$.

Let $D=(P,B)$ be a symmetric $t-(v,k,\lambda)$ design. Consider $X_D = P \cup B$ and $\mathcal{R}_D$ the relations over X:

$$\begin{aligned}
R_0 &= \{(x,x)|x \in X\};\\
R_1 &= \{(p,b)|p \in P, b \in B, p \in b\} \cup \{(b,p)|p \in P, b \in B, p \in b\};\\
R_2 &= \{(p,p')|p,p' \in P, p \neq p'\} \cup \{(b,b')|b,b' \in B, b \neq b'\};\\
R_3 &= \{(p,b)|p \in P, b \in B, p \notin b\} \cup \{(b,p)|p \in P, b \in B, p \notin b\}.
\end{aligned}$$

From the previous definitions, it follows directly the following proposition.

Proposition 3 *If $D=(P,B)$ is a symmetric $t-(v,k,\lambda)$ design, then $(X_D,\mathcal{R}_D)$ is a symmetric 3-class association scheme with adjacency matrices:*

$$A_0 = I_{2v} \qquad A_1 = \left(\begin{array}{c|c} 0 & A \\ \hline A^T & 0 \end{array}\right)$$
$$A_2 = \left(\begin{array}{c|c} J-I & 0 \\ \hline 0 & J-I \end{array}\right) \; A_3 = \left(\begin{array}{c|c} 0 & J-A \\ \hline J-A^T & 0 \end{array}\right)$$

Obtaining self-dual codes from symmetric designs is not a new topic. For example in [18], binary self-dual codes are obtained from $I+A$ under certain conditions. However, our technique is quite different, since we use pure and bordered construction from the association scheme $(X_D,\mathcal{R}_D)$.

4.3.1 Pure construction

Theorem 8 *Let C be the binary code generated by $\mathcal{P}$ using the association scheme $(X_D,\mathcal{R}_D)$. The code C is self-dual if and only if one of the following holds:*

(i) $Q = I_{2v}$ *or* $Q = I_{2v} + J_{2v}$.
(ii) $Q = A_1$ *or* $Q = A_1 + J_{2v}$; $k \equiv 1$, *and* $\lambda \equiv 0 \pmod 2$.
(iii) $Q = A_2$ *or* $Q = A_2 + J_{2v}$; $v \equiv 0 \pmod 2$.
(iv) $Q = A_3$ *or* $Q = A_3 + J_{2v}$; $k \not\equiv \lambda \equiv v \pmod 2$.
(v) $Q = I_{2v} + A_1$ *or* $Q = I_{2v} + A_1 + J_{2v}$; $k \equiv \lambda \equiv 0 \pmod 2$.
(vi) $Q = I_{2v} + A_3$ *or* $Q = I_{2v} + A_3 + J_{2v}$; $k \equiv \lambda \equiv v \pmod 2$.

Proof The binary code C is self-dual if and only if $QQ^T = Q^2 = I_{2v}$ (note, from Proposition 3, that Q is a symmetric matrix). Since $J_{2v}^2 = 2vJ_{2v} = 0$ over $\mathbb{Z}_2$, we have that if $Q^2 = I_{2v}$, then $Q + J_{2v}$ also satisfies $(Q+J_{2v})^2 = I_{2v}$ over $\mathbb{Z}_2$.

(i) If $Q = I_{2v}$, clearly $Q^2 = I_{2v}$.

(ii) If $Q = A_1$, $Q^2 = \left(\begin{array}{c|c} (k+\lambda)I+\lambda J & 0 \\ \hline 0 & (k+\lambda)I+\lambda J \end{array}\right) = I_{2v}$ if and only if λ is even, and k is odd.

(iii) If $Q = A_2$, $Q^2 = \left(\begin{array}{c|c} (I+J)^2 & 0 \\ \hline 0 & (I+J)^2 \end{array}\right) = \left(\begin{array}{c|c} I+vJ & 0 \\ \hline 0 & I+vJ \end{array}\right) = I_{2v}$ if and only if v is even.

(iv) If $Q = A_3$,$Q^2 = \left(\begin{array}{c|c} (J+A)(J+A^T) & 0 \\ \hline 0 & (J+A)(J+A^T) \end{array}\right) =$ $\left(\begin{array}{c|c} (k+\lambda)I+(v+\lambda)J & 0 \\ \hline 0 & (k+\lambda)I+(v+\lambda)J \end{array}\right) = I$ if and only if $k \not\equiv \lambda \equiv v \pmod 2$.

(v) If $Q = I_{2v} + A_1$, $Q^2 = \left(\begin{array}{c|c} (k+\lambda+1)I+\lambda J & 0 \\ \hline 0 & (k+\lambda+1)I+\lambda J \end{array}\right) = I_{2v}$ if and only if k and λ are even.

(vi) If $Q = I_{2v}+A_3$, $Q^2 = \left(\begin{array}{c|c} (k+\lambda+1)I+(v+\lambda)J & 0 \\ \hline 0 & (k+\lambda+1)I+(v+\lambda)J \end{array}\right) =$ I if and only if $k \equiv \lambda \equiv v \pmod 2$.

In the case $Q = I_{2v} + A_2$, we have $Q^2 = \left(\begin{array}{c|c} vJ & 0 \\ \hline 0 & vJ \end{array}\right) \neq I_{2v}$. Moreover, since $I_{2v} + A_1 + A_2 + A_3 = J_{2v}$ we have all the possible values of Q in $(i) - (vi)$.

We remark that in (i), the minimum distance of the code is $d = 2$. In the rest of the cases, the minimum distance is $d = 2j$, for some $j \geq 2$.

As corollaries, we shall determine the matrices Q for which we obtain a binary self-dual code by the pure construction for a certain well-known symmetric designs such as projective planes, Hadamard designs, biplanes, and projective geometry hyperplanes.

Corollary 9 *Let D be a projective plane of order n and let $v = n^2+n+1$. Let C be the binary code generated by $\mathcal{P}$ using the association scheme $(X_D, \mathcal{R}_D)$. The code C is self-dual if and only if one of the following holds:*

(i) $Q = I_{2v}$ *or* $Q = I_{2v} + J_{2v}$.
(ii) $Q = A_3$ *or* $Q = A_3 + J_{2v}$, $n \equiv 1 \pmod 2$.
(iii) $Q = I_{2v} + A_3$ *or* $Q = I_{2v} + A_3 + J_{2v}$, $n \equiv 0 \pmod 2$.

Proof A projective plane of order n is a $2-(n^2+n+1, n+1, 1)$ design [11]. Then, the only possible matrices Q are those obtained from items (i), (iv) and (vi) in Theorem 8.

Corollary 10 *Let D be a Hadamard 2-design of order $\lambda+1$ and let $v = 4\lambda+3$. Let C be the binary code generated by $\mathcal{P}$ using the association scheme $(X_D, \mathcal{R}_D)$. The code C is self-dual if and only if one of the following holds:*

(i) $Q = I_{2v}$ *or* $Q = I_{2v} + J_{2v}$.
(ii) $Q = A_1$ *or* $Q = A_1 + J_{2v}$, $\lambda \equiv 0 \pmod 2$.
(iii) $Q = I_{2v} + A_3$ *or* $Q = I_{2v} + A_3 + J_{2v}$, $\lambda \equiv 1 \pmod 2$.

Proof A Hadamard 2-design is a $2-(4\lambda+3, 2\lambda+1, \lambda)$ design [11]. Then, the only possible matrices Q are the obtained from items (i), (ii) and (vi) in Theorem 8.

One example of an infinite family of Hadamard 2-designs with odd λ is the family of $2-(2^{n+1}-1, 2^n-1, 2^{n-1}-1)$ designs called Paley designs. ([11]).

Corollary 11 *Let D be a biplane of order n and let $v = \frac{n^2+3n+4}{2}$. Let C be the binary code generated by $\mathcal{P}$ using the association scheme $(X_D, \mathcal{R}_D)$. The code C is self-dual if and only if one of the following holds:*

(i) $Q = I_{2v}$ *or* $Q = I_{2v} + J_{2v}$.
(ii) $Q = A_1$ *or* $Q = A_1 + J_{2v}$, $n \equiv 1 \pmod 2$.
(iii) $Q = A_2$ *or* $Q = A_2 + J_{2v}$, *n is a square.*
(iv) $Q = A_3$ *or* $Q = A_3 + J_{2v}$, *n is an odd square.*
(v) $Q = I_{2v} + A_1$ *or* $Q = I_{2v} + A_1 + J_{2v}$, $n \equiv 0 \pmod 2$.
(vi) $Q = I_{2v} + A_3$ *or* $Q = I_{2v} + A_3 + J_{2v}$, *$n$ is an even square.*

Proof A biplane is a $2-(\frac{n^2+3n+4}{2}, n+2, 2)$ design [11]. Then, the only possible matrices Q are those obtained from items (i) to (vi) in Theorem 8. In items (iii), (iv) and (vi) we obtain $n \equiv 0$ or $1 \pmod 4$, $n \equiv 1 \pmod 4$ and $n \equiv 0 \pmod 4$, respectively. But in these cases, v is even, hence n must be a square according to the Bruck-Ryser-Chowla Theorem (see [11], for example).

Corollary 12 *Let D be the design defined by the hyperplanes of dimension $n-1$ from an n-dimensional finite projective geometry $PG(n,q)$. Let $v = \frac{q^{n+1}-1}{q-1}$. Let C be the binary code generated by $\mathcal{P}$ using the association scheme $(X_D, \mathcal{R}_D)$. The code C is self-dual if and only if one of the following holds:*

(i) $Q = I_{2v}$ *or* $Q = I_{2v} + J_{2v}$.
(ii) $Q = A_1$ *or* $Q = A_1 + J_{2v}$, $n \equiv q \equiv 1 \pmod 2$.
(iii) $Q = A_2$ *or* $Q = A_2 + J_{2v}$, $n \equiv q \equiv 1 \pmod 2$.
(iv) $Q = A_3$ *or* $Q = A_3 + J_{2v}$, $q \equiv 1 \pmod 2$.
(v) $Q = I_{2v} + A_3$ *or* $Q = I_{2v} + A_3 + J_{2v}$, $q \equiv 0 \pmod 2$.

Proof The desing D is a $2-(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1})$ design [11]. Then, the only possible matrices Q are those obtained from items (i), (ii), (iii), (iv) and (vi) in Theorem 8.

4.3.2 Bordered construction

Using the bordered construction, recall that we require $1 + a^2 + 2vb = 0$ (in order that the first row be self-orthogonal). This reduces to $a = 1$ over $\mathbb{Z}_2$. Since the first row must be orthogonal to any other, we get $ac + b\chi = c + b\chi = 0$, where χ denotes the number of ones per row (column) in Q. So, if $b = 0$ then $c = 0$ and the matrix $\mathcal{B}$ becomes

$$\mathcal{B} = \left(\begin{array}{c|c|c|c} 1 & 0\ldots0 & 1 & 0\ldots0 \\ \hline 0 & & 0 & \\ \vdots & I & \vdots & Q \\ 0 & & 0 & \end{array}\right), \tag{19}$$

and it would be a trivial generalization of the previous pure construction. So, we assume that $b = 1$ and hence $c + \chi = 0$. In order to have the remaining rows orthogonal, we must have $I_{2v} + cJ_{2v} + QQ^T = 0$. For $c = 1$, this reduces to $QQ^T = Q^2 = I_{2v} + J_{2v}$. But we have seen in the pure construction that

$$Q^2 = \left(\begin{array}{c|c} M & 0 \\ \hline 0 & M \end{array}\right),$$

for some matrix M. Therefore, it is not possible $Q^2 = I_{2v} + J_{2v}$. We conclude that $c = 0$ and χ must be even.

Lemma 6 *In all the cases (i)–(vi) of Theorem 8, the number of ones per row χ in Q is odd.*

Proof Computing χ in all the cases, we have:

(i) If $Q = I_{2v}$, then $\chi = 1$.
(ii) If $Q = A_1$, then $\chi = k$ and k is odd.
(iii) If $Q = A_2$, then $\chi = v - 1$ and v is even.
(iv) If $Q = A_3$, then $\chi = v - k$ and $v \not\equiv k \pmod 2$.
(v) If $Q = I_{2v} + A_1$, then $\chi = k + 1$, and k is even.
(vi) If $Q = I_{2v} + A_3$, then $\chi = v - k + 1$, and $v \equiv k \pmod 2$.

Note that the number of ones per row of $Q + J_{2v}$ is $2v - \chi$ and therefore has the same parity as χ.

Hence, we cannot obtain self-dual codes using the bordered construction with $b = 1$.

Theorem 9 *Let C be the binary code generated by $\mathcal{B}$ with $b = 1$ using the association scheme $(X_D, \mathcal{R}_D)$. Then, C is not self-dual.*

Proof From the previous discussion, we deduce that $a = 1$, $c = 0$ and Q should have an even number of ones per row, for C to be self-dual. In such situation, we also had that $Q^2 = I$. Therefore, we should be in one of the cases of Theorem 8 but, by the previous lemma, this is not possible.

References

1. E. Bannai, S. T. Dougherty, M. Harada and M. Oura: Type II codes, even unimodular lattices, and invariant rings. IEEE Trans. Inform. Theory 45 (1999), no. 4, 1194-1205.
2. S. Bouyuklieva: A method for constructing self-dual codes with an automorphism of order 2. IEEE Trans. Inform. Theory 46 (2000), no. 2, 496-504.

3. S. Bouyuklieva and I. Bouyukliev: An algorithm for classification of binary self-dual codes. IEEE Trans. Inform. Theory 58 (2012), no. 6, 3933-3940.
4. S. Bouyuklieva and Z. Varbanov: Some connections between self-dual codes, combinatorial designs and secret sharing schemes. Adv. Math. Commun. 5 (2011), no. 2, 191-198.
5. S. T. Dougherty, T. A. Gulliver and R. Ramadurai: Symmetric designs and self-dual codes over rings. Ars Combin. 85 (2007), 193-209.
6. S. T. Dougherty, J. L. Kim and H. Kulosman: Liu, Hongwei Self-dual codes over commutative Frobenius rings. Finite Fields Appl. 16 (2010), no. 1, 14-26.
7. S. T. Dougherty, J. L. Kim and H. Liu: Constructions of self-dual codes over finite commutative chain rings. Int. J. Inf. Coding Theory 1 (2010), no. 2, 171-190.
8. S. T. Dougherty, J. L. Kim, and P. Solé: Double Circulant Codes from Two Class Association Schemes. AMC, vol. 1, no. 1, pp. 45-64, 2007.
9. D. G. Higman: Coherent Configurations. Geom.Dedicata, Vol. 4, pp. 1-32, 1975.
10. W. C. Huffman and V. S. Pless: Fundamentals of Error-correcting Codes. Cambridge University Press, 2003.
11. D. R. Hughes and F. C. Piper: Design Theory. Cambridge University Press, 1985.
12. L. K. Jørgensen: Non-symmetric 3-class association schemes: Research Report Series; R-2005-13 Aalborg Universitetsforlag. 2005.
13. S. Karadeniz and B. Yildiz: Double-circulant and bordered-double-circulant constructions for self-dual codes over R2. Adv. Math. Commun. 6 (2012), no. 2, 193-202.
14. C. W. H. Lam: The search for a finite projective plane of order 10 [MR1103185 (92b:51013)]. Organic mathematics (Burnaby, BC, 1995), 335-355, CMS Conf. Proc., 20, Amer. Math. Soc., Providence, RI, 1997.
15. F. J. MacWilliams and N. J. A. Sloane: The theory of error correcting codes. North Holland, 1981.
16. G. Nebe, E. M. Rains and N. J. Sloane: Self-dual codes and invariant theory. Algorithms and Computation in Mathematics, 17. Springer-Verlag, Berlin, 2006. xxviii+430 pp. ISBN: 978-3-540-30729-7; 3-540-30729-X
17. E. Rains and N. J. A. Sloane: Self-dual codes in the Handbook of Coding Theory, V.S. Pless and W.C. Huffman. Elsevier, Amsterdam, pp. 177-294, 1998.
18. P. Solé: Self-dual codes and self-dual designs. IMA volumes, 20, pp. 188-192, Springer-Verlag, 1990.