Self-orthogonal codes over a non-unital ring and combinatorial matrices

Minjia Shi, Shukai Wang, Jon-Lark Kim, Patrick Solé

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

Self-orthogonal codes over a non-unital ring and combinatorial matrices

Minjia Shi · Shukai Wang · Jon-Lark Kim · Patrick Solé

Received: date / Accepted: date

Abstract There is a local ring E of order 4, without identity for the multiplication, defined by generators and relations as $E = \langle a, b \mid 2a = 2b = 0, a^2 = a, b^2 = b, ab = a, ba = b \rangle$. We study a special construction of self-orthogonal codes over E, based on combinatorial matrices related to two-class association schemes, Strongly Regular Graphs (SRG), and Doubly Regular Tournaments (DRT). We construct quasi self-dual codes over E, and Type IV codes, that is, quasi self-dual codes whose all codewords have even Hamming weight. All these codes can be represented as formally self-dual additive codes over $\mathbb{F}_4$. The classical invariant theory bound for the weight enumerators of this class of codes improves the known bound on the minimum distance of Type IV codes over E.

Keywords rings · codes · formally self-dual codes · Type IV codes.

1 Introduction

Since the the celebrated theorem of Gleason and Prange [2], formally self-dual codes over $\mathbb{F}_4$ with even weights, also known as Type IV codes have been studied extensively [10, Chap. 19], [11]. In [3] this notion was extended over the three rings of order four that are not a field, namely $\mathbb{Z}_4$, $\mathbb{F}_2 + u\mathbb{F}_2$, and $\mathbb{F}_2 + v\mathbb{F}_2$. Recently, a further extension was accomplished over a non commutative non-unital ring in [1].

M. Shi
Anhui University, Hefei, China
E-mail: smjwcl.good@163.com

S. Wang
Anhui University, Hefei, China
E-mail: wangshukai_2017@163.com

J.-L. Kim
Sogang University, Seoul, South Korea
E-mail: jlkim@sogang.ac.kr

P. Solé
Aix Marseille Univ, CNRS, Centrale Marseille, I2M, Marseille, France
E-mail: sole@enst.fr

The concept of self-dual code is replaced there by quasi self-dual (QSD) code that is self-orthogonal of length n, with 2^n codewords. Type IV codes are then defined as QSD codes, whose Hamming weights of all codewords are even. With every linear E-code is attached an additive $\mathbb{F}_4$-code obtained by forgetting the ring structure; this allows to use the additive codes package of [15] for numerical computations. Kim and Ohk [9] showed that quasi self-dual codes over that ring E can be applied to DNA codes in the sense that the GC-content concept can be described by a multiple of an element in the ring. They also improved the classification of QSD codes over E up to lengths 8. The Lee weight defined below is based on this DNA application.

In this paper, we study a special construction of QSD codes over E, based on combinatorial matrices related to two-class association schemes, Strongly Regular Graphs (SRG), and Doubly Regular Tournaments (DRT). This is a generalization from fields to rings of the approach of [4]. We construct QSD codes and Type IV codes over E. Along the way, we improve the upper bound on the minimum distance of Type IV codes from [1] by a multiplicative factor, by an application of the classical invariant bound for the minimum distance of extremal Type IV codes over $\mathbb{F}_4$. Some numerical results validate our approach.

The material is arranged in the following way. Section 2 collects the notions and notations required for the rest of the paper. Section 3 studies our special construction. Section 4 develops the needed theory of combinatorial matrices from designs, SRGs and DRTs. Section 5 concludes the article.

2 Background

2.1 Association schemes

An *association scheme* on a set X with s classes is a partition of the cartesian product $X \times X = \cup_{i=0}^{s} R_i$ with the following properties

1. $R_0 = \{(x, x) \mid x \in X\}$,
2. $(x, y) \in R_k$, if and only if $(y, x) \in R_k$,
3. $R_i^t = \{(y, x) \mid (x, y) \in R_i\} = R_j$ for some j,
4. 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 an integer p_{ij}^k that depends on i, j, k but not on the special choice of x and y.

Such a scheme is called an s-class association scheme. Let A_k denote the adjacency matrix of the relations R_k. Concretely A_k is indexed by X, and defined by

$$A_k(x, y) = \begin{cases} 1 & \text{if } xR_k y, \\ 0 & \text{else.} \end{cases}$$

It can be shown that the adjacency matrices A_k span a commutative algebra over the complex numbers [10, Chap. 21].

If $s = 2$ two cases may occur.

- $A_1 = A_1^T$ and $A_2 = A_2^T$. The undirected graph (X, R_1) is then strongly regular (SRG).
- $A_1 = A_2^T$. The directed graph (X, R_1) is then a doubly regular tournament (DRT).

For future use, we denote by I the identity matrix, and by J the all-one matrix, both of order $|X|$.

2.2 Binary codes

Denote by $wt(x)$ the Hamming weight of $x \in \mathbb{F}_2^n$. The dual of a binary linear code C is denoted by $C^\perp$ and defined as

$$C^\perp = \{y \in \mathbb{F}_2^n \mid \forall x \in C,\, (x,y) = 0\},$$

where $(x,y) = \sum_{i=1}^n x_i y_i$, denotes the standard inner product. A code C is **self-orthogonal** if it is included in its dual: $C \subseteq C^\perp$. Two binary codes are **equivalent** if there is a permutation of coordinates that maps one to the other.

2.3 Quaternary codes

An **additive code** of length n over $\mathbb{F}_4$ is an additive subgroup of $\mathbb{F}_4^n$. It is a free $\mathbb{F}_2$ module with 4^k elements for some $k \leq n$ (here $2k$ is an integer, but k may be half-integral). Using a **generator matrix** G, such a code can be represented as the $\mathbb{F}_2$-span of its rows. With every linear E code C is attached an **additive** $\mathbb{F}_4$ code $\phi(C)$ by the substitution

$$0 \to 0, a \to \omega, b \to \omega^2, c \to 1,$$

where $\mathbb{F}_4 = \mathbb{F}_2[\omega]$. Note that the reverse substitution attaches to every additive $\mathbb{F}_4$ code an additive subgroup of E^n, which may or may not be linear.

Besides the Hamming weight of a vector, we might consider its Lee weight as follows:

$$wt_L(0) = 0, wt_L(a) = wt_L(b) = 1, wt_L(c) = 2.$$

2.4 Ring theory

Consider the ring of order 4 defined by two generators a and b by the relations

$$E = \langle a, b \mid 2a = 2b = 0,\, a^2 = a,\, b^2 = b,\, ab = a,\, ba = b\rangle.$$

The ring E is a non unital, non-commutative ring of order 4, of characteristic two[1, **?**]. Thus, E consists of four elements $E = \{0, a, b, c\}$, with $c = a + b$. Its multiplication table is as follows.

$\times$	0	a	b	c
0	0	0	0	0
a	0	a	a	0
b	0	b	b	0
c	0	c	c	0

From this table, we deduce that this ring is not commutative, and non-unital. It is local with maximal ideal $J = \{0, c\}$, and residue field $E/J = \mathbb{F}_2 = \{0, 1\}$, the finite field of order 2.

Denote by $\alpha : E \to E/J = \mathbb{F}_2$, the map of reduction modulo J. Thus $\alpha(0) = \alpha(c) = 0$, and $\alpha(a) = \alpha(b) = 1$. This map is extended in the natural way in a map from E^n to $\mathbb{F}_2^n$.

2.5 Codes over E

A **linear** E-code of length n is a one-sided E-submodule of E^n. Let C be a code of length n over E. With that code we associate two binary codes of length n :

(1) the **residue code** defined by $res(C) = \{\alpha(y) \mid y \in C\}$,
(2) the **torsion code** defined by $tor(C) = \{x \in \mathbb{F}_2^n \mid cx \in C\}$.

We equip E^n with the inner product (x, y) of $x, y \in E^n$ defined by the relation

$$(x, y) = \sum_{i=1}^{n} x_i y_i.$$

The **right dual** $C^{\perp_R}$ of C is the right module defined by

$$C^{\perp_R} = \{y \in E^n \mid \forall x \in C,\, (x, y) = 0\}.$$

The **left dual** $C^{\perp_L}$ of C is the left module defined by

$$C^{\perp_L} = \{y \in E^n \mid \forall x \in C,\, (y, x) = 0\}.$$

An E-code C is **self-orthogonal** if

$$\forall x, y \in C, (x, y) = 0.$$

Clearly, C is **self-orthogonal** if and only if $C \subseteq C^{\perp_L}$. Likewise, C is **self-orthogonal** if and only if $C \subseteq C^{\perp_R}$. Thus, for a self-orthogonal code C, we always have $C \subseteq C^{\perp_L} \cap C^{\perp_R}$. An E-code of length n is **Quasi Self-Dual** (QSD for short) if it is self-orthogonal and of size 2^n. A QSD code is **Type IV** if all its codewords have even weight.

The following result went unnoticed in [1], and improves on the previously known upper bound $d \leq 2\lfloor \frac{n+2}{4} \rfloor$ for the minimum Hamming distance d of a Type IV E-code of length n.

Theorem 1 *If C is a Type IV E-code of length n, then it is formally self-dual for the Hamming weight enumerator, and its minimum distance is $\leq 2(\lfloor \frac{n}{6} \rfloor + 1)$.*

Proof The first statement follows by specialization of variables in the MacWilliams relation for the joint weight enumerator of the residue and torsion code [1, Prop. 2]. The second statement follows by the standard argument used to prove the same bound for Type IV codes over $\mathbb{F}_4$ [10, Chap. 19, (69)]. Note that the Hamming weight enumerator of a Type IV code over E belongs to the same ring of invariants as that of a Type IV code over $\mathbb{F}_4$.

Theorem 1 gives a construction of additive formally self-dual even codes over $\mathbb{F}_4$.

Corollary 1 *If C is Type IV then $\phi(C)$ is an additive formally self-dual even code.*

Proof The results follow by the fact that C and $\phi(C)$ have the same Hamming weight enumerator.

We now study the residue and torsion code of a QSD code over E.

Theorem 2 ([1]) *For any QSD E-linear code $\mathcal{C}$, we have*

(1) $res(\mathcal{C}) \subseteq res(\mathcal{C})^{\perp}$,
(2) $tor(\mathcal{C}) = res(\mathcal{C})^{\perp}$,
(3) $dim(\mathcal{C}) = dim(res(\mathcal{C})) + dim(tor(\mathcal{C}))$.

We can characterize QSD codes over E amongst linear codes over E as a function of their residue code in the following theorem.

Theorem 3 ([1]) *Let B be a self-orthogonal binary $[n, k_1]$ code, where $0 \leq k_1 \leq n/2$. The code $\mathcal{C}$ over the ring E defined by the relation*

$$\mathcal{C} = aB + cB^{\perp}$$

is a QSD code. Its residue code is B and its torsion code is $B^{\perp}$. Conversely, any QSD code C can be built in that way by taking for B the residue code of C.

By Theorem 3, we know that the classification of QSD E-codes is equivalent to the classification of their residue codes. Moreover, the following result is straightforward, but useful. The easy proof is ommitted.

Theorem 4 *The minimum distance $d(C)$ of a QSD code C defined by $\mathcal{C} = aB + cB^{\perp}$, where B is a self-orthogonal binary code, is less than or equal to* $\min\{d(B), d(B^{\perp})\}$. *If B is a self-dual binary code, then $d(C) = d(B)$.*

3 Construction

Consider the code $C(M)$ of length $2n$ with a generator matrix of the form

$$G = (xI, yM)$$

where $x, y \in E$, I is the identity matrix, and M is a binary matrix satisfying

$$MM^T = \lambda I + \mu J + \nu M \pmod 2,$$

where $\lambda, \mu, \nu \in \mathbb{F}_2$, and J is the all-one matrix.

Table 1: Conditions of self-orthogonal codes

n	λ	μ	ν
any	1	0	0
odd	1	1	0
any	0	0	1
even	0	1	1
odd	0	1	0
any	0	0	0

Theorem 5 *The code $C(M)$ is self-orthogonal if and only if either $x, y \in \{0, c\}$, or $y \in \{a, b\}$ and the three parameters λ, μ, ν are as in Table 1.*

Proof The code $C(M)$ is self-orthogonal if and only if $GG^{\mathrm{T}} = 0$.

If $y \in \{0, c\}$, $GG^{\mathrm{T}} = 0$ implies $x \in \{0, c\}$. It is trivial because the code only has a zero codeword.

If $y \in \{a, b\}$, then

$$\begin{aligned} GG^{\mathrm{T}} &= x^2 I + y^2 M M^{\mathrm{T}} \\ &= x^2 I + y(\lambda I + \mu J + \nu M) \\ &= x^2 I + y\lambda I + y\mu J + y\nu M. \end{aligned}$$

Therefore, $GG^{\mathrm{T}} = 0$ if and only if $-y\nu M = x^2 I + y\lambda I + y\mu J$.
Since

$$\begin{aligned} (-y\nu M)(-y\nu M)^{\mathrm{T}} &= y\nu M M^{\mathrm{T}} \\ [(x^2 + y\lambda)I + y\mu J][(x^2 + y\lambda)I + y\mu J]^{\mathrm{T}} &= y\nu(\lambda I + \mu J + \nu M) \\ (x^2 + y\lambda)I + ny\mu J &= y\nu\lambda I + y\nu\mu J + y\nu M \\ &= y\nu\lambda I + y\nu\mu J - (x^2 + y\lambda)I - y\mu J, \end{aligned}$$

then we have $(n + 1 - \nu)\mu y J = y\nu\lambda I$. Because J is the all-one matrix, and I is the identity matrix, then

$$\begin{cases} y\nu\lambda = 0 \\ (n + 1 - \nu)\mu y = 0. \end{cases} \tag{1}$$

Thus, $\lambda, \mu, \nu \in \mathbb{F}_2$ are as in Table 1.

The next two results give conditions for $C(M)$ to be QSD (resp. Type IV).

Theorem 6 *A self-orthogonal code $C(M)$ is QSD if and only if either $x \in \{a, b\}$, or $x \in \{0, c\}, y \in \{a, b\}, \lambda = \mu = \nu = 0$ and M is a full rank matrix spanning a self-orthogonal binary code.*

Proof A self-orthogonal code C is QSD if and only if G has n linearly independent rows. If $x \in \{a, b\}$, C is QSD because of the form of G.

If $x \in \{0, c\}$, then we must let the determinant $|yM| \neq 0$ to make sure there are n linearly independent rows in G. From the proof of Theorem 5, $y \in \{a, b\}$ and $-y\nu M = y\lambda I + y\mu J$. Then, $\lambda = \mu = \nu = 0$, and M is a binary matrix such that

$$\begin{cases} |M| \neq 0, \\ MM^{\mathrm{T}} = 0. \end{cases} \tag{2}$$

This completes the proof.

Theorem 7 *A QSD code $C(M)$ is Type IV if either $x \in \{0, c\}$, or $x \in \{a, b\}$ and one of the following three conditions holds.*

(1) $\lambda = \mu = 0, \nu = 1$,
(2) $\lambda = 0, \mu = 1, \nu = 1$,
(3) $\lambda = 1, \mu = \nu = 0$.

Proof It easy to check that a QSD code is Type IV if the generator matrix G has all the rows of even weights. If $x \in \{0, c\}$, then $\lambda = \mu = \nu = 0$ because of Theorem 6. From $MM^{\mathrm{T}} = 0$ in Equation 2, it is clear that M has all the rows of even weights.

If $x \in \{a, b\}$, we just prove that M has all the rows of odd weights in the three cases. Now we have

$$\begin{cases} MM^{\mathrm{T}} = \lambda I + \mu J + \nu M, \\ y\nu M = (x + y\lambda)I + y\mu J. \end{cases} \tag{3}$$

(1) $\lambda = \mu = 0, \nu = 1$. In this case, we have $\begin{cases} MM^{\mathrm{T}} = M, \\ yM = xI. \end{cases}$ Therefore, $x = y$ and $M = I$ with all rows of odd weights.

(2) $\lambda = 0, \mu = 1, \nu = 1$. In this case, we have $\begin{cases} MM^{\mathrm{T}} = M + J, \\ yM = xI + yJ. \end{cases}$ Therefore, $x = y$ and $M = J - I$ with even n. So, M has all rows of odd weights.

(3) $\lambda = 1, \mu = \nu = 0$. In this case, we have $\begin{cases} MM^{\mathrm{T}} = I \\ (x + y)I = 0 \end{cases}$. Therefore, $x = y$ and M has all rows of odd weights.

This completes the proof.

Example 8 We describe the above constructions with two examples.

- If $M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, then $MM^T = 1I + 1J + 0M \pmod 2$, that is, $\lambda = 1, \mu = 1, \nu = 0$. Since $n = 3$ is odd, it follows from Table 1 of Theorem 5 that for any $x \in E$ and $y \in \{a, b\}$, the matrix $G = (xI, yM)$ generates a self-orthogonal code. In particular, if $x = a$ or b (with $y \in \{a, b\}$), then (xI, yM) generates a QSD code with minimum distance 3 by Theorem 6 but not Type IV since there is a codeword of weight 3.
- If $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, then $MM^T = 0I+0J+1M \pmod 2$ and $MM^T = 1I+0J+0M \pmod 2$, that is, $\lambda = 0, \mu = 0, \nu = 1$ or $\lambda = 1, \mu = 0, \nu = 0$. By Table 1 of Theorem 5, both of these two cases can generate self-orthogonal codes by using the matrix G. And if $x = a$ or b, then $G = (xI, xM)$ generates a Type IV code with minimum distance 2 from Theorem 7.

We now investigate the residue and torsion codes of $C(M)$.
From [1, Thm. 1], we write the generator matrix in the form

$$G = \begin{pmatrix} aI_{k_1} & X & Y \\ 0 & cI_{k_2} & cZ \end{pmatrix}.$$

For $x \neq 0$, we have the following cases depending on the values of $x \in E$.

- If $x = a$ or $x = b$, then $k_1 = n, k_2 = 0, (X, Y) = yM$. The generator matrix of the residue code is (I, M) if $y = a, b$ and $(I, \mathbf{0})$ if $y = c$.
- If $x = c$, then, $k_1 = 0, k_2 = n, y = c, Z = M$. The generator matrix of the torsion code is $G_2 = (I, M)$.

The (additive) generator matrix of the corresponding additive $\mathbb{F}_4$ code is

$$G' = \begin{pmatrix} \phi(aG) \\ \phi(bG) \end{pmatrix},$$

where ϕ is as defined in the preceding section.

Remarks:

- If $y = c$, then $C(M)$ has minimum distance 1. In the examples, we shall assume that $y = a$, or $y = b$.
- If $x = c$, then we find that $\phi(M)$ is a linear code over $\mathbb{F}_4$ given by $\phi(M) = \langle (0, M) \rangle$. We will avoid this case as well.
- Now if both x, y are in $\{a, b\}$, then we find that $\phi(M)$ is a linear code over $\mathbb{F}_4$ given by $\phi(M) = \langle (I, M) \rangle$.

4 Combinatorial matrices

4.1 Two-class association schemes

From now on, we can discuss two-class association schemes which will play an important role in M.

There are two kinds of two-class association schemes. One is a Strongly Regular Graph (SRG), where the two adjacency matrices satisfy $A_i = A_i^T$ for $i = 1, 2$. Here, A_2 satisfies $A_2 = J - I - A_1 := \overline{A_1}$. An important database of SRGs is [14].

A classical construction of a SRG is the Paley graph. It is constructed from quadratic residues in $\mathbb{F}_q$, where $q \equiv 1 \pmod 4$ and $A = Q = N$. The parameters are $(q, \frac{q-1}{2}, \frac{q-3}{4}, \frac{q+1}{4})$. The example of $q = 5$ is the pentagon graph.

Another class is a Doubly Regular Tournament (DRT), which is equivalent to a skew Hadamard matrix [12]. The adjacency matrix A_2 satisfies $A_2 = J - I - A_1 := \overline{A_1}$. Note that $A_1^T = \overline{A_1}$.

From now on, let $A = A_1$.

Lemma 1 ([4]) *If G is an SRG, then we have*

$$AA^T = A^2 = \kappa I + \Lambda A + \mathcal{M}\overline{A}.$$

If G is a DRT, then we have

$$AA^T = \kappa I + (\kappa - 1 - \Lambda)A + (\kappa - \mathcal{M})\overline{A}.$$

Using the same parameters in the above lemma, both of them satisfy the equation

$$AJ = JA = \kappa J,$$

and for SRGs, we have

$$A^2 = \kappa I + \Lambda A + \mathcal{M}(J - I - A), \tag{4}$$

for DRTs, we have

$$A^2 = \Lambda A + \mathcal{M}(J - I - A). \tag{5}$$

We connect these parameters to that of the matrix M of the preceding section. The trivial proof is omitted.

Proposition 1 *Keep the notation of Lemma* 1. *If M is the adjacency matrix of G with parameters $(n, \kappa, \Lambda, \mathcal{M})$ then*

- *in the SRG case $\lambda = \kappa - \mathcal{M}, \mu = \mathcal{M}$, $\nu = \Lambda - \mathcal{M}$,*
- *in the DRT case $\lambda = \mathcal{M}, \mu = \kappa - \mathcal{M}$, $\nu = \mathcal{M} - \Lambda - 1$.*

We can use the database of two class association schemes from Hanaki and Miyamoto's database [7]. In particular there is a classification of DRT of sizes up to 40.

4.2 Pure and double circulant codes from two-class association schemes

We can also follow the construction method from [4]. Let $Q_E(r, s, t) = rI + sA + t\overline{A}$, where $r, s, t \in E$, where A is an adjacency matrix of a SRG or a DRT. Let $C(Q_E(r, s, t))$ be a code of length $2n$ with a generator matrix of the form

$$G = (aI, Q_E(r, s, t)) = (aI, rI + sA + t\overline{A}).$$

This construction can be called the *pure* construction.

First we consider $r = 0$ and $s, t \in \{a, b\}$. The code $C(Q_E(0, s, t))$ of length $2n$ has generator matrix of the form

$$G = (aI, Q_E(0, s, t)) = (aI, sA + t\overline{A}),$$

where A is an adjacency matrix of a SRG or a DRT.

Theorem 9 *Suppose A is an adjacency matrix of a SRG or a DRT.*

(1) *If $n \geq 7$, then the minimum distance of $C(Q_E(0, s, t))$ is exactly* 4.
(2) *If $3 \leq n < 7$, then the minimum distance of $C(Q_E(0, s, t))$ is* 2 *or* 3.

Proof Due to symmetry between A and $\overline{A}$, we may assume $s = a$ and $t = b$, or $s = t = a$. We only consider the case $s = a$ and $t = b$ because the other case $s = t = a$ can be done similarly. Note that $aG = a(aI, aA + b\overline{A}) = (aI, aA + a\overline{A}) = (aI, a(A + \overline{A}))$. Since $A + \overline{A} = J - I$, $aG = (aI, a(J - I))$. It is easy to see that the minimum distance of the code generated by $(aI, a(J - I))$ is 4 if $n \geq 3$. Hence G generates a codeword of weight 4 if $n \geq 3$. Each row of G and aG has weight at least 4 if $n \geq 7$. Hence the first statement of the theorem follows. If $3 \leq n < 7$, then G has weight 2 or 3. Hence the second statement follows.

Similarly, we have the following theorem.

Theorem 10 *Suppose A is an adjacency matrix of a SRG or a DRT. If $r \neq 0$, and $s, t \in \{a, b\}$, then the following statements hold.*

(1) *If $n \geq 7$ and $r = c$, then the minimum distance of $C(Q_E(r, s, t))$ is exactly* 4.
(2) *If r is either a or b, then the minimum distance of $C(Q_E(r, s, t))$ is* 2.

Therefore if $n \geq 7$, it is reasonable to consider the following three constructions (i) $C(Q_E(0,a,0))$, (ii) $C(Q_E(a,a,0))$, or (iii) $C(Q_E(c,a,0))$, where replacing a into b gives the same result.

Note that Case (i) and Case (ii) are the same construction as $C(M)$ with $x = a$ and $y = a$ in Section 3 by taking $M = A$ and $M = A + I$, respectively. Therefore, we can apply these two cases to various SRGs and DRTs.

Next we can consider the *bordered* construction as follows.

$$B_E(r,s,t) = \left(\begin{array}{c|ccc|c|ccc} a & 0 & \dots & 0 & 0 & a & \dots & a \\ \hline 0 & & & & a & & & \\ \vdots & & aI & & \vdots & & Q_E(r,s,t) & \\ 0 & & & & a & & & \end{array}\right).$$

Just like for the pure construction, we can distinguish three cases (i) $Q_E(0,a,0)$, (ii) $Q_E(a,a,0)$, or (iii) $Q_E(c,a,0)$.

Lemma 2 *The codes in these two constructions with Case* (i) *and Case* (iii) *are the same.*

Proof In Case (i), $Q_E(0,a,0) = aA$, and the generator matrix $G_{(\mathrm{i})} = (aI|aA)$ in pure construction. So, the code $C_{(\mathrm{i})} = \{\mathbf{x}G_{(\mathrm{i})} | \mathbf{x} \in E^n\}$. In Case (iii), $Q_E(c,a,0) = cI + aA$, and the generator matrix $G_{(\mathrm{iii})} = (aI|cI + aA)$ in pure construction. So, the code $C_{(\mathrm{iii})} = \{\mathbf{x}G_{(\mathrm{iii})} | \mathbf{x} \in E^n\}$. Since

$$\begin{aligned} \mathbf{x}G_{(\mathrm{iii})} &= \mathbf{x}(G_{(\mathrm{i})} + (\mathbf{0}|cI)) \\ &= \mathbf{x}G_{(\mathrm{i})} + \mathbf{x}(\mathbf{0}|cI) \\ &= \mathbf{x}G_{(\mathrm{i})}, \end{aligned}$$

we have $C_{(\mathrm{i})} = C_{(\mathrm{iii})}$.

For bordered construction in Case (i), we have $C'_{(\mathrm{i})} = \{\mathbf{y}G'_{(\mathrm{i})} | \mathbf{y} \in E^{n+1}\}$, where

$$G'_{(\mathrm{i})} = \left(\begin{array}{c|ccc|c|ccc} a & 0 & \dots & 0 & 0 & a & \dots & a \\ \hline 0 & & & & a & & & \\ \vdots & & aI & & \vdots & & aA & \\ 0 & & & & a & & & \end{array}\right),$$

and in Case (iii), we have $C'_{(\mathrm{iii})} = \{\mathbf{y}G'_{(\mathrm{iii})} | \mathbf{y} \in E^{n+1}\}$, where

$$G'_{(\mathrm{iii})} = \left(\begin{array}{c|ccc|c|ccc} a & 0 & \dots & 0 & 0 & a & \dots & a \\ \hline 0 & & & & a & & & \\ \vdots & & aI & & \vdots & & cI + aA & \\ 0 & & & & a & & & \end{array}\right).$$

Let

$$A' = \left(\begin{array}{c|ccc|c|ccc} 0 & 0 & \dots & 0 & 0 & 0 & \dots & 0 \\ \hline 0 & & & & 0 & & & \\ \vdots & & \mathbf{0} & & \vdots & & cI & \\ 0 & & & & 0 & & & \end{array}\right),$$

then

$$\begin{aligned}\mathbf{y}G'_{(\mathrm{iii})} &= \mathbf{y}(G'_{(\mathrm{i})} + A') \\ &= \mathbf{y}G'_{(\mathrm{i})} + \mathbf{y}A' \\ &= \mathbf{y}G'_{(\mathrm{i})}.\end{aligned}$$

Therefore, $C'_{(\mathrm{i})} = C'_{(\mathrm{iii})}$.

Example 11 It is well known that there is unique DRT of order 11. The pure construction with $Q_E(0, a, 0)$ gives a QSD $[22, 11, 6]$ code over E. The bordered construction with $Q_E(a, a, 0)$ gives a QSD $[24, 12, 8]$ code over E. The minimum distances of these codes are justified by Theorem 4.

Lemma 3 (1) *For SRGs we have*

$$Q_E(r,s,t)Q_E(r,s,t)^T = \omega_1 I + \omega_2 A + \omega_3 \overline{A},$$

where $\omega_1 = (r^2+s^2\kappa-t^2-t^2\kappa+t^2v)$, $\omega_2 = (rs+sr+s^2\Lambda-st-ts-st\Lambda-ts\Lambda+t^2\Lambda+st\kappa+ts\kappa+t^2v-2t^2\kappa)$, $\omega_3 = (rt+tr+s^2\mathcal{M}-st\mathcal{M}-ts\mathcal{M}+t^2\mathcal{M}+st\kappa+ts\kappa+t^2v)$.

(2) *For DRTs we have*

$$Q_E(r,s,t)Q_E(r,s,t)^T = \omega'_1 I + \omega'_2 A + \omega'_3 \overline{A},$$

where $\omega'_1 = (r^2+(s^2+t^2)\kappa)$, $\omega'_2 = (rt+sr+s^2(\kappa-1-\Lambda)+t^2(\kappa-\mathcal{M})+st\Lambda+st\mathcal{M})$, $\omega'_3 = (tr + rs + s^2(\kappa - \mathcal{M}) + t^2(\kappa - 1 - \Lambda) + st\mathcal{M} + st\Lambda)$.

Proof It is straightforward by Equations 4 and 5 and Lemma 1.

We will discuss the weight of rows of generator matrices in Case (i) and Case (ii). Then, the conditions of QSD and Type IV can be confirmed. By the form of generator matrices in pure construction and bordered construction, the code is QSD if it is self-orthogonal. The following remark gives when the code is self-orthogonal and Type IV.

Remark 1 For Cases (i) and (ii), we have the following observations.

- pure construction with SRGs
  For the code $P_E(r, s, t)$ to be self-orthogonal, we need

  $$(aI|Q_E(r,s,t))(aI|Q_E(r,s,t))^T = \mathbf{0}.$$

  That is we need $Q_E(r,s,t)Q_E(r,s,t)^T = -aI$. By Lemma 3 (1), we compute the parameters $\kappa, \Lambda, \mathcal{M}$ of self-orthogonal (QSD) codes in Table 2.
  The weight of any row of $Q_E(r, s, t)$ is related to the coefficient of I, where I is in Lemma 3 (1). So, the weight of any row of $(aI|Q_E(r, s, t))$ is

  $$1 + \alpha(r^2) + \alpha(s^2)\kappa + \alpha(t^2)(n - \kappa - 1),$$

  that is, $1 + \kappa$ in Case (i) and $2 + \kappa$ in Case (ii). Therefore, a QSD code is Type IV if

  $$1 + \alpha(r^2) + \alpha(s^2)\kappa + \alpha(t^2)(n - \kappa - 1) = 0 \pmod 2,$$

  that is, $1 + \kappa = 0 \pmod 2$ in Case (i) and $2 + \kappa = 0 \pmod 2$ in Case (ii). Then we have the conditions of Type IV in Table 2.

- bordered construction with SRGs
  Similar to the pure construction, we need

$$B_E(r,s,t)B_E(r,s,t)^T = \mathbf{0}.$$

  Then we have

$$\begin{aligned} a(1+n) &= 0 \\ a(r+s\kappa+t(n-\kappa-1)) &= 0 \\ aI + aJ + Q_E(r,s,t)Q_E(r,s,t)^T &= \mathbf{0}. \end{aligned}$$

  The first equation is the product of the top row with itself. The second equation is the product of the top row with any other row, and the third equation ensures that the other rows are orthogonal to each other. The results of the calculation by Lemma 3 (1) are in Table 2.
  And this code is Type IV if

$$\begin{aligned} \alpha(a)(1+n) &= 0 \pmod 2, \\ \alpha(r)+\alpha(s)\kappa+\alpha(t)(n-\kappa-1) &= 0 \pmod 2. \end{aligned}$$

  We also have the results in Table 2.

Table 2: Conditions of QSD and Type IV with SRGs

r	s	t	Pure		Bordered	
			QSD	Type IV	QSD	Type IV
0	a	0	$\kappa=1, \Lambda=\mathcal{M}=0$	Always	$\kappa=0, n=\Lambda=\mathcal{M}=1$	Always
a	a	0	$\kappa=\Lambda=\mathcal{M}=0$	Always	$n=\Lambda=\mathcal{M}=\kappa=1$	Always

- pure and bordered construction with DRTs
  By using the same arguments as these two constructions with SRGs and Lemma 3 (2), then we have the results in Table 3.

Table 3: Conditions of QSD and Type IV with DRTs

r	s	t	Pure		Bordered	
			QSD	Type IV	QSD	Type IV
0	a	0	$\kappa=\mathcal{M}=1, \Lambda=0$	Always	$\kappa=\Lambda=0, n=\mathcal{M}=1$	Always
a	a	0	$\kappa=\Lambda=0, \mathcal{M}=1$	Always	$n=\mathcal{M}=\kappa=1, \Lambda=0$	Always

We computed the Hamming weight and Lee weight of some codes. These examples are from [7,14] and MAGMA databases of SRGs [15].

Theorem 12 *There are QSD codes over E with the following parameters.*

(1) *Based on SRGs, there are QSD codes with parameters $(2n, d)$, where $2n$ is the length of the code, and d is the minimum distance.*

$$(32,8),(56,8),(70,10),(72,12),(80,12),(92,12).$$

Table 4: Weights of some QSD codes of SRGs

Construction	Cases	$(n-\kappa-\Lambda-\mathcal{M})$	Code Length	Hamming	Lee
Pure	(i)	$(36-15-6-6)$	72	12	12
	(ii)	$(16-6-2-2)$	32	8	8
		$(28-12-6-4)$	56	8	8
		$(35-16-6-8)$	70	10	10
		$(36-14-4-6)$	72	12	12
		$(40-12-2-4)$	80	12	12
Bordered	(i)	$(15-6-1-3)$	32	8	8
		$(27-10-1-5)$	56	8	8
		$(45-12-3-3)$	92	12	12

Table 5: Weights of QSD some codes of DRTs

Construction	n	Length		Hamming	Lee		Hamming	Lee
Pure	11	22	Case (i)	6	6	Case (ii)	7	7
	19	38		8	8		7	7
Bordered	11	24		7	7		8	8
	19	40		8	8		8	8

(2) *Based on DRTs, there are QSD codes with parameters* $(2n, d)$*, where* $2n$ *is the length of the code, and* d *is the minimum distance.*

$$(22, 7), (24, 8), (38, 8), (40, 8).$$

We display these results in Table 4 and Table 5.

The images by $\phi()$ of these codes are formally self-dual additive codes over $\mathbb{F}_4$ in [6].

5 Conclusion

In this work, we have constructed QSD and Type IV codes over the ring E in the sense of [1]. The construction method is based on the adjacency matrices of two-class association schemes, in an analogue over E of [4] over finite fields. Formally self-dual additive codes over $\mathbb{F}_4$ were introduced in [6]. This little-known class of codes deserves further exploration. In another direction, the construction methods we used can be explored over the rings H and I of the Raghavendran classification [5].

References

1. A. Alahmadi, A. Altassan, W. Basaffar, A. Bonnecaze, H. Shoaib, P. Solé. Type IV codes over a non-unital ring. Journal of Algebra and Its Applications, to appear. Available from `https://hal.archives-ouvertes.fr/hal-02433480/document`
2. E. F. Assmus, H. F. Mattson, R. J. Turyn, Research to develop the algebraic theory of codes AFCRL-67-365, Air Force Cambridge Research labs, (1967). `https://apps.dtic.mil/dtic/tr/fulltext/u2/656783.pdf`
3. S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, P. Solé, Type IV self-dual codes over rings. IEEE Trans. Information Theory, 1999, 45(7): 2345-2360.

4. S. T. Dougherty, J.-L. Kim, P. Solé, Double circulant codes from two-class association schemes, Advances in Math. of Comm., 2007, 1(1): 45–64. https://www.researchgate.net/publication /243116174_Double_circulant_codes_from_two_class_association_schemes
5. B. Fine, Classification of finite rings of order p^2, Mathematics Magazine, 1993, 66(4): 248–252.
6. S. Han, J-L. Kim, Formally self-dual additive codes over $\mathbb{F}_4$, J. of Sym-bolic Comp., **45**, (2010): 787–799.
7. A. Hanaki, I. Miyamoto, http://math.shinshu-u.ac.jp/h̃anaki/as/
8. Y.J. Ionin and M.S. Shrikhande, *Combinatorics of Symmetric Designs*, Cambridge University Press, (2009), Cambridge.
9. J.-L. Kim and D. E. Ohk, *DNA codes over noncommutative rings of order four*, preprint.
10. F.J. MacWilliams, N.J. A. Sloane, *The theory of Error Correcting Codes*, North-Holland, Amsterdam (1981).
11. G. Nebe, E. M. Rains, N. J. A. Sloane, *Self-dual codes and invariant theory*, ACM 17, Springer (2006) Berlin, Heidelberg.
12. K. B. Reid, E. Brown, Doubly regular tournaments are equivalent to skew Hadamard matrices. J. of Comb. Th. (A), 1972, 12(3): 332–338.
13. E. Spence http://www.maths.gla.ac.uk/ẽs/symmdes/2designs.php
14. T. Spence http://www.maths.gla.ac.uk/ẽs/srgraphs.php
15. http://magma.maths.usyd.edu.au/magma/handbook/text/1799#20143