

DOUBLE CIRCULANT CODES FROM TWO CLASS ASSOCIATION SCHEMES

STEVEN T. DOUGHERTY

Department of Mathematics
University of Scranton, Scranton, PA 18518, USA

JON-LARK KIM

Department of Mathematics
University of Louisville, Louisville, KY 40292, USA

PATRICK SOLÉ

CNRS, I3S, ESSI, BP 145
Route des Colles, 06 903 Sophia Antipolis, France

(Communicated by Alexander Barg)

ABSTRACT. Two class association schemes consist of either strongly regular graphs (SRG) or doubly regular tournaments (DRT). We construct self-dual codes from the adjacency matrices of these schemes. This generalizes the construction of Pless ternary Symmetry codes, Karlin binary Double Circulant codes, Calderbank and Sloane quaternary double circulant codes, and Gaborit Quadratic Double Circulant codes (QDC). As new examples SRG's give 4 (resp. 5) new Type I (resp. Type II) [72, 36, 12] codes. We construct a [200, 100, 12] Type II code invariant under the Higman-Sims group, a [200, 100, 16] Type II code invariant under the Hall-Janko group, and more generally self-dual binary codes attached to rank three groups.

1. INTRODUCTION

Many classical constructions of double circulant self-dual codes use the Paley Hadamard matrix of order $p + 1$ based on the quadratic residues modulo p . To wit we have the Karlin binary double circulant codes [31, p.507], Pless ternary symmetry codes [33], Calderbank-Sloane quaternary double circulant codes [8], and more generally Gaborit Quadratic Double Circulant codes [15]. When -1 is a quadratic residue modulo p , this matrix is related to the adjacency matrix of a Strongly Regular Graph (SRG). When -1 is a quadratic non-residue modulo p , this matrix is related to the adjacency matrix of a Doubly Regular Tournament (DRT). A combinatorial structure that captures both cases is that of a two-class commutative association scheme, with adjacency matrices A_1 and A_2 . When the scheme is symmetric, that is $A_1 = A_1^T$, we see that A_1 is the adjacency matrix of a SRG. When the scheme is not symmetric, that is $A_2 = A_1^T$, we see that A_1 is the adjacency matrix of a DRT. The aim of the present research is to generalize Gaborit's QDC at that

2000 *Mathematics Subject Classification*: Primary: 94B60; Secondary: 05E30.

Key words and phrases: Self-dual code, 2-class association scheme, strongly regular graph, rank three groups, doubly regular tournament.

Dedicated to Vera Pless in honor of her retirement.

The first author is grateful to CNRS in Sophia Antipolis for their hospitality, where he stayed while this paper was written.

level of generality, thus unifying many classical constructions; and hopefully paving the way for new ones. In particular we will give very general self-duality conditions valid over any commutative alphabet ring; and will specialize them in the case of the four main alphabets of interest for self-dual codes $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{Z}_4$. Some of our examples are extremal self-dual codes (e.g. Golay code, two Conway Pless codes in length 32, Type III codes in lengths 40, 48, 64); others are conjecturally optimal (especially several non equivalent [72, 36, 12], both Type I and Type II); finally, some have very interesting automorphism groups (section on SRGs from rank three groups). We do find that the known constructions of our more general construction are in general the best examples produced by this construction. However, we are able to couch all of these constructions in a unified setting.

The article is organized in the following way. The next section collects definitions and notation from codes and association schemes. Section III contains the general self-duality conditions for the pure and bordered constructions and for SRG's and DRT's. Section IV specializes these conditions to the four said alphabets. Section V contains examples of codes constructed from SRG's and Section VI of codes constructed from DRTs. Section VII makes explicit the connection with QDC's.

2. DEFINITIONS AND NOTATION

2.1. CODES OVER RINGS. Let R be a finite commutative ring with identity. Let ϕ be a permutation of R . In this paper a **code** of length n over R is a subset of R^n and the code is said to be linear if it is an R -submodule of R^n . We equip R^n with the inner product

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

When ϕ is the identity we will call this the **Euclidean** inner product, and we call it the **Hermitian** inner product otherwise. In this paper, a **code** of length n over R is an R -submodule of R^n . The **dual** C^\perp of a code C is understood with respect to the above inner product. A code is **self-dual** if it is equal to its dual and **self-orthogonal** if it is contained in its dual. If $R = \mathbb{Z}_{2m}$ with m integral, then a self-dual code is **Type II** if the Euclidean weight of each of its elements is a multiple of $4m$. Here the **Euclidean weight** of $x = (x_1, \dots, x_n) \in \mathbb{Z}_{2m}^n$ is $w_E(x) = \sum_{i=1}^n w_E(x_i)$, where $w_E(a) = (\min(a, 2m - a))^2$, for $a \in \mathbb{Z}_{2m}$. For a complete description of self-dual codes see [34]. A linear code over R is free if it has rank r and $|R|^r$ elements. If R is a field then all linear codes are free. For any undefined terms from coding theory see [31] or [26].

2.2. ASSOCIATION SCHEMES. Let X be a set of size v . A **two class association scheme** on X is a partition of $X \times X$ into three relations R_0, R_1, R_2 such that

1. $R_0 = \{(x, x) \mid x \in X\}$
2. $R_i^T = R_j$ for some $j = 0, 1, 2$ and for all i
3. for any triple i, j, 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 which does not depend on the choice of x and y that satisfy $(x, y) \in R_k$.

Furthermore we recall that from [11] or [24] a two class scheme is **commutative** i.e. $p_{ij}^k = p_{ji}^k$ for any triple of indices i, j, k . With each such object we attach the algebra of matrices over the complex spanned by the adjacency matrices $A_0 = I, A_1, A_2$ of the relations R_i . We let J denote the all one matrix and I the identity matrix.

We observe that two cases may occur. Either $A_1^T = A_1, A_2^T = A_2$ and then the undirected graph (X, R_1) is a **strongly regular graph** with parameters $(v, \kappa := p_{11}^0, \lambda := p_{11}^1, \mu := p_{11}^2)$; or $A_1^T = A_2, A_2^T = A_1$ and the directed graph (X, R_1) is a **doubly regular tournament** with parameters $(v, \kappa, \lambda := p_{11}^1, \mu := p_{11}^2)$, where κ is the out-degree of any vertex. (Note that DRTs are equivalent to skew Hadamard matrices [35]). In both cases we have $A_2 = J - I - A_1 =: \overline{A_1}$, and the matrix $A := A_1$ satisfies the equation

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

and either

$$(1) \quad A^2 = \kappa I + \lambda A + \mu(J - I - A),$$

for SRGs, or

$$(2) \quad A^2 = \lambda A + \mu(J - I - A),$$

for DRTs. A classical construction of a SRG (the Paley graph) is constructed from quadratic residues in \mathbb{F}_q , when $q \equiv 1 \pmod{4}$, and $A = Q = Q^T$, where Q and N are defined in Section 7. The parameters are well-known to be $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ (see e.g. [17, p.183]).

A classical example of a DRT is Paley's tournament when $q \equiv -1 \pmod{4}$, and $A = Q = N^T$. Its parameters are $(q, \frac{q-1}{2}, \frac{q-3}{4}, \frac{q+1}{4})$. It should be noted that a DRT $(v, \kappa, \mu - 1, \mu)$ is a Doubly Regular Asymmetric Digraph, $DRAD(v, \kappa, k - \mu)$, in the sense of [27].

3. GENERAL CONSTRUCTIONS

Let A be the adjacency matrix of a graph G (first adjacency graph of a two class association scheme) with v vertices, degree κ , with parameters λ and μ .

We shall consider two cases, namely the first case, G is an SRG, is when $A^T = A$ and the second case, G is a DRT, is when $A^T = \overline{A}$.

Lemma 1. *If G is an SRG we have*

$$(3) \quad AA^T = A^2 = \kappa I + \lambda A + \mu \overline{A}.$$

If G is a DRT we have

$$(4) \quad AA^T = \kappa I + (\kappa - 1 - \lambda)A + (\kappa - \mu)\overline{A}.$$

Proof. The first case follows from the known value of A^2 . The second case can be done by replacing $A^T = \overline{A}$ with $J - I - A$, and using the known value of AJ and A^2 . \square

For a DRT with parameters $(v, \kappa, \lambda, \mu)$, $AA^T = \kappa I + (\kappa - 1 - \lambda)A + (\kappa - \mu)\overline{A}$. Since $(AA^T)^T = AA^T$ and $A^T = \overline{A}$, we get $(\kappa - 1 - \lambda) = (\kappa - \mu)$, i.e. $p_{12}^1 = p_{12}^2$. Hence $\mu = \lambda + 1$. As a summary, we list relations among the parameters in the following lemma.

Lemma 2. *If G is a DRT with parameters $(v, \kappa, \lambda, \mu)$, then $v = 4\lambda + 3, \kappa = 2\lambda + 1$, and $\mu = \lambda + 1$.*

We describe the following constructions: for arbitrary scalars $r, s, t \in R$ let

$$(5) \quad Q_R(r, s, t) = (rI + sA + t\overline{A}).$$

The **pure** construction is

$$(6) \quad \mathcal{P}_R(r, s, t) = (I \mid Q_R(r, s, t)).$$

The **bordered** construction is

$$(7) \quad \mathcal{B}_R(r, s, t) = \left(\begin{array}{c|c|c|c} 1 & 0 \dots 0 & \alpha & \beta \dots \beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_R(r, s, t) \\ \hline 0 & & \gamma & \end{array} \right),$$

where α, β , and γ are scalars which will be determined according to specific cases.

Let $P_R(r, s, t)$ be the row span over R of $\mathcal{P}_R(r, s, t)$ and let $B_R(r, s, t)$ be the row span over R of $\mathcal{B}_R(r, s, t)$.

Fundamental Example: When A is the incidence matrix of the Paley graph or of the Paley tournament then the two families of codes above are the first two mentioned in [15].

The code $P_R(r, s, t)$ is a code over R of length $2v$ and the code $B_R(r, s, t)$ is a code over R of length $2v + 2$.

The code $P_R(r, s, t)$ is a free code over any ring R with $|R|^v$ elements and the code $B_R(r, s, t)$ is a free code over any ring R with $|R|^{v+1}$ elements. Hence to show that they are self-dual we need only show that they are self-orthogonal. We begin with the pure case.

For the code $\mathcal{P}_R(r, s, t)$ to be self-orthogonal we need $Q_R(r, s, t)Q_R(r, s, t)^T = -I$.

Lemma 3. *For SRGs we have*

$$\begin{aligned} Q_R(r, s, t)Q_R(r, s, t)^T &= (r^2 + s^2\kappa - t^2 - t^2\kappa + t^2v)I \\ &+ (2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2st\kappa + t^2v - 2t^2\kappa)A \\ &+ (2rt + s^2\mu - 2st\mu + t^2\mu + 2st\kappa + t^2v - 2t^2 - 2t^2\kappa)\bar{A}. \end{aligned}$$

For DRTs we have

$$\begin{aligned} Q_R(r, s, t)Q_R(r, s, t)^T &= (r^2 + (s^2 + t^2)\kappa)I \\ &+ (rt + sr + (s^2 + t^2)(\kappa - 1 - \lambda) + st\lambda + st\mu)A \\ &+ (rt + sr + (s^2 + t^2)(\kappa - \mu) + st\mu + st\lambda)\bar{A}. \end{aligned}$$

Proof. Follows from a straightforward computation using Lemma 1, and Equations 1 and 2. \square

The Euclidean weight of any row of $(I \mid Q_R(r, s, t))$ is $1 + r^2 + s^2\kappa + t^2(v - \kappa - 1)$. Hence if a self-dual $P_R(r, s, t)$ has $1 + r^2 + s^2\kappa + t^2(v - \kappa - 1) \equiv 0 \pmod{4m}$ for a code over \mathbb{Z}_{2m} then the code $P_R(r, s, t)$ is a Type II code.

For $B_R(r, s, t)$ to be self-dual we need the following:

$$(8) \quad 1 + \alpha^2 + v\beta^2 = 0$$

$$(9) \quad \alpha\gamma + \beta(r + s\kappa + t(v - \kappa - 1)) = 0$$

$$(10) \quad I + \gamma^2 J + Q_R(r, s, t)Q_R(r, s, t)^T = \mathbf{0}.$$

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.

The third equation requires that

$$Q_R(r, s, t)Q_R(r, s, t)^T = -(1 + \gamma^2)I - \gamma^2 A - \gamma^2 \bar{A}.$$

When $R = \mathbb{Z}_{2m}$ for this code to be Type II we need the congruences

$$1 + \alpha^2 + v\beta^2 \equiv 0 \pmod{4m},$$

(inner product of top row with itself) and

$$1 + \gamma^2 + r^2 + s^2\kappa + t^2(v - k - 1) \equiv 0 \pmod{4m},$$

(inner product of any other row with itself). We summarize the results in this section with the following two theorems.

Theorem 1. *The code $P_R(r, s, t)$ formed from an SRG is Euclidean self-dual over R if and only if*

$$\begin{aligned} (r^2 + s^2\kappa - t^2 - t^2\kappa + t^2v) &= -1 \\ (2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2st\kappa + t^2v - 2t^2\kappa) &= 0 \\ (2rt + s^2\mu - 2st\mu + t^2\mu + 2st\kappa + t^2v - 2t^2 - 2t^2\kappa) &= 0. \end{aligned}$$

The code $P_R(r, s, t)$ formed from a DRT is Euclidean self-dual over R if and only if

$$\begin{aligned} (r^2 + (s^2 + t^2)\kappa) &= -1 \\ (rt + sr + (s^2 + t^2)(\kappa - 1 - \lambda) + st\lambda + st\mu) &= 0 \\ (rt + sr + (s^2 + t^2)(\kappa - \mu) + st\mu + st\lambda) &= 0. \end{aligned}$$

Furthermore, the self-dual code is Type II over \mathbb{Z}_{2m} if and only if $1 + r^2 + s^2\kappa + t^2(v - \kappa - 1) \equiv 0 \pmod{4m}$.

Theorem 2. *The code $B_R(r, s, t)$ formed from an SRG is Euclidean self-dual over R if and only if*

$$\begin{aligned} (r^2 + s^2\kappa - t^2 - t^2\kappa + t^2v) &= -(1 + \gamma^2) \\ (2rs + s^2\lambda - 2st - 2st\lambda + t^2\lambda + 2st\kappa + t^2v - 2t^2\kappa) &= -\gamma^2 \\ (2rt + s^2\mu - 2st\mu + t^2\mu + 2st\kappa + t^2v - 2t^2 - 2t^2\kappa) &= -\gamma^2 \\ 1 + \alpha^2 + v\beta^2 &= 0 \\ \alpha\gamma + \beta(r + s\kappa + t(v - \kappa - 1)) &= 0. \end{aligned}$$

The code $B_R(r, s, t)$ formed from a DRT is Euclidean self-dual over R if and only if

$$\begin{aligned} (r^2 + (s^2 + t^2)\kappa) &= -(1 + \gamma^2) \\ (rt + sr + (s^2 + t^2)(\kappa - 1 - \lambda) + st\lambda + st\mu) &= -\gamma^2 \\ (rt + sr + (s^2 + t^2)(\kappa - \mu) + st\mu + st\lambda) &= -\gamma^2 \\ 1 + \alpha^2 + v\beta^2 &= 0 \\ \alpha\gamma + \beta(r + s\kappa + t(v - \kappa - 1)) &= 0. \end{aligned}$$

Furthermore, this self-dual code is Type II over \mathbb{Z}_{2m} if and only if

$$1 + \gamma^2 + r^2 + s^2\kappa + t^2(v - \kappa - 1) \equiv 0 \pmod{4m}$$

and

$$1 + \alpha^2 + v\beta^2 \equiv 0 \pmod{4m}.$$

4. SELF-DUALITY CONDITIONS BY ALPHABET

We simplify the preceding conditions for self-duality in characteristic 2, 3, and 4.

4.1. $R = \mathbb{F}_2$.

4.1.1. *SRGs.* Over \mathbb{F}_2 the equations in Lemma 3 for SRG reduce to

$$Q_{\mathbb{F}_2}(r, s, t)Q_{\mathbb{F}_2}(r, s, t)^T = (r^2 + s^2\kappa + t^2 + t^2\kappa + t^2v)I + (s^2\lambda + t^2\lambda + t^2v)A + (s^2\mu + t^2\mu + t^2v)\bar{A},$$

and then noticing that $a^2 = a$ for all a we have

$$Q_{\mathbb{F}_2}(r, s, t)Q_{\mathbb{F}_2}(r, s, t)^T = (r + s\kappa + t + t\kappa + tv)I + (s\lambda + t\lambda + tv)A + (s\mu + t\mu + tv)\bar{A}.$$

We use these to examine when the constructions give self-dual codes. In Table 1 and 2, all equalities are given in \mathbb{F}_2 and congruences are given modulo 4. In the columns we give the conditions necessary for the results. For the bordered we only give the conditions on v, κ, λ, μ and γ . Additionally it must satisfy the necessary conditions given for α and β .

TABLE 1. SRG binary self-dual codes

r	s	t	Pure self-dual	Pure Type II	Bordered self-dual	Bordered Type II
0	0	1	$\lambda = v = \mu = \kappa$	$v \equiv \kappa$	$\lambda = \mu = \kappa, \gamma = \kappa + v$	$v - \kappa + \gamma \equiv 0$
0	1	0	$\kappa = 1, \lambda = \mu = 0$	$\kappa \equiv 3$	$\lambda = \mu = \gamma = \kappa + 1$	$\gamma + \kappa \equiv 3$
0	1	1	$v = 0$	$v \equiv 0$	$v = \gamma$	$\gamma \equiv -v$
1	0	0	Always	Never	$\gamma = 0$	Never
1	0	1	$\lambda = \mu = v = \kappa + 1$	$v \equiv \kappa + 3$	$\kappa + 1 = v + \gamma = \lambda = \mu$	$\kappa + 3 \equiv v + \gamma$
1	1	0	$\lambda = \mu = \kappa = 0$	$\kappa \equiv 2$	$\kappa = \gamma = \lambda = \mu$	$\gamma + \kappa \equiv 2$
1	1	1	$v = 1$	$v \equiv 3$	Never	Never

4.1.2. *DRTs.* Over \mathbb{F}_2 the equations for DRT do not reduce except that as before each element is equal to its square.

We recall from Lemma 2 that the parameters of a DRT satisfy, $v = 4\lambda + 3$, $\kappa = 2\lambda + 1$, $\mu = \lambda + 1$. This gives that $P(1, 1, 0)$ and $P(1, 0, 1)$ are never self-dual codes since the equations would imply that κ must be 0 in this case which contradicts that $\kappa = 2\lambda + 1$ which is always 1 modulo 2. It also gives that $B(1, 1, 1)$ is never self-dual since it requires $\mu = \lambda$ which is also a contradiction.

TABLE 2. DRT binary self-dual codes

r	s	t	Pure self-dual	Pure Type II	Bordered self-dual	Bordered Type II
0	0	1	$\lambda + 1 = \kappa = 1$	$v \equiv \kappa$	$\lambda = 0, \kappa = \gamma + 1$	$v - \kappa + \gamma \equiv 0$
0	1	0	$1 = \kappa = \lambda + 1$	$\kappa \equiv 3$	$\lambda = 0, \kappa = \gamma + 1$	$\gamma + \kappa \equiv 3$
0	1	1	Never	Never	$\lambda + \mu = \gamma = 1$	$\gamma + v \equiv 0$
1	0	0	Always	Never	$\gamma = 0$	Never
1	0	1	Never	Never	$\kappa = \gamma, \mu = 1, \lambda = 0$	$\kappa + 3 \equiv v + \gamma$
1	1	0	Never	Never	$\kappa = \gamma, \mu = 1, \lambda = 0$	$\gamma + \kappa \equiv 2$
1	1	1	$\kappa = \lambda$	$v \equiv 3$	Never	Never

The case when $r = 0, s = t = 1$ gives an interesting result in the pure case. The construction gives the matrix $(I \mid J - I)$ which would only be self-dual if the order of the matrices is even. However, the result gives that there are no self-dual codes from which we recover the known result that a DRT must have $v \equiv 1 \pmod{2}$.

4.2. $R = \mathbb{F}_4$. For \mathbb{F}_4 we shall use the Hermitian inner-product. Hence we need to compute an analog of the computation in Lemma 3:

Lemma 4. *Over \mathbb{F}_4 with involution ϕ for SRGs we have*

$$\begin{aligned} Q(r, s, t)\phi(Q(r, s, t)) &= (r^3 + s^3\kappa + t^3 + t^3\kappa + t^3v)I \\ &+ (rs^2 + sr^2 + s^3\lambda + ts^2 + st^2 \\ &+ t^3\lambda + (ts^2 + st^2)\kappa + t^3v)A \\ &+ (rt^2 + tr^2 + s^3\mu + (ts^2 + st^2)\mu + t^3\mu \\ &+ (ts^2 + st^2)\kappa + t^3v)\bar{A}. \end{aligned}$$

Over \mathbb{F}_4 with involution ϕ for DRTs we have

$$\begin{aligned} Q(r, s, t)\phi(Q(r, s, t)) &= (r^3 + (s^3 + t^3)\kappa)I \\ &+ (rt^2 + sr^2 + (s^3 + t^3)(\kappa + 1 + \lambda) + st^2\lambda + ts^2\mu)A \\ &+ (rs^2 + tr^2 + (s^3 + t^3)(\kappa + \mu) + st^2\mu + ts^2\lambda)\bar{A}. \end{aligned}$$

Proof. If the involution of \mathbb{F}_4 is ϕ then we have

$$\begin{aligned} Q(r, s, t)\phi(Q(r, s, t)) &= (rI + sA + t\bar{A})(\phi(r)\phi(I) + \phi(s)\phi(A) + \phi(t)\phi(\bar{A})) \\ &= (rI + sA + t\bar{A})(\phi(r)I + \phi(s)A + \phi(t)\bar{A}). \end{aligned}$$

Then we notice that in \mathbb{F}_4 we have $\phi(a) = a^2$ and then using that the characteristic is 2, the computation follows. \square

4.2.1. *Pure case.* We determine now when codes obtained from SRGs in the pure construction over \mathbb{F}_4 are self-dual. If s and t are non-zero then

$$\begin{aligned} r^3 &= v \\ (rt^2 + sr^2 + ts^2 + st^2) &= (st^2 + ts^2)\kappa + v \\ (rt^2 + tr^2) &= (st^2 + ts^2)(\mu + \kappa) + v. \end{aligned}$$

If $s = 0, t \neq 0$ then

$$\begin{aligned} r^3 &= \kappa + v \\ \lambda &= v \\ (rt^2 + tr^2) &= \mu + v. \end{aligned}$$

If $s \neq 0, t = 0$ then

$$\begin{aligned} r^3 &= \kappa + 1 \\ (rs^2 + sr^2) &= \lambda \\ \mu &= 0. \end{aligned}$$

We determine now when codes obtained from DRTs in the pure construction over \mathbb{F}_4 are self-dual.

If both s and t are non-zero then

$$\begin{aligned} rt^2 + sr^2 &= st^2\lambda + ts^2\mu \\ rs^2 + tr^2 &= st^2\mu + ts^2\lambda. \end{aligned}$$

If one of s and t are non-zero then $r^3 = 1 + \kappa$ that is r is non-zero if and only if $\kappa \equiv 0 \pmod{2}$.

If $s = 0, t \neq 0$ then

$$\begin{aligned} rt^2 &= \kappa + 1 + \lambda \\ tr^2 &= \kappa + \mu. \end{aligned}$$

If $s \neq 0, t = 0$ then

$$\begin{aligned} sr^2 &= \kappa + 1 + \lambda \\ rs^2 &= \kappa + \mu. \end{aligned}$$

Then using that $\mu = \lambda + 1$ and that $s \neq 0$ we have $r^2 = rs$. Hence if r is non-zero then $r = s$.

4.2.2. *Bordered case.* We determine now when codes obtained from SRGs in the bordered construction over \mathbb{F}_4 are self-dual. If s and t are non-zero then

$$\begin{aligned} r^3 + v &= \gamma^2 \\ rs^2 + sr^2 + ts^2 + st^2 &= (ts^2 + st^2)\kappa + v + \gamma^2 \\ rt^2 + tr^2 &= (ts^2 + st^2)\mu + (ts^2 + st^2)\kappa + v + \gamma^2. \end{aligned}$$

If $s = 0, t \neq 0$ then

$$\begin{aligned} r^3 + \kappa + v &= \gamma^2 \\ \lambda + v &= \gamma^2 \\ (rt^2 + tr^2)\mu + v &= \gamma^2 \end{aligned}$$

If $s \neq 0, t = 0$ then

$$\begin{aligned} r^3 + \kappa &= 1 + \gamma^2 \\ (rs^2 + sr^2) + \lambda &= \gamma^2 \\ \mu &= \gamma^2. \end{aligned}$$

We determine now when codes obtained from DRTs in the bordered construction over \mathbb{F}_4 are self-dual.

If both s and t are non-zero then

$$\begin{aligned} r^3 &= 1 + \gamma^2 \\ rt^2 + sr^2 + st^2\lambda + t^2\mu &= \gamma^2 \\ rs^2 + tr^2 + st^2\mu + ts^2\lambda &= \gamma^2. \end{aligned}$$

If one of s and t are non-zero then $r^3 = 1 + \kappa$ that is r is non-zero if and only if $\kappa \equiv 0 \pmod{2}$.

If $s = 0, t \neq 0$ then

$$\begin{aligned} r^3 + \kappa &= 1 + \gamma^2 \\ rt^2 + \kappa + 1 + \lambda &= \gamma^2 \\ tr^2 + \kappa + \mu &= \gamma^2. \end{aligned}$$

If $s \neq 0, t = 0$ then

$$\begin{aligned} r^3 + \kappa &= 1 + \gamma^2 \\ sr^2 + \kappa + 1 + \lambda &= \gamma^2 \\ rs^2 + \kappa + \mu &= \gamma^2. \end{aligned}$$

4.3. $R = \mathbb{F}_3$. Over \mathbb{F}_3 we see that we cannot have $s = t = 0$.
The equalities in Table 3,4,5, and 6 are all in the field \mathbb{F}_3 .

TABLE 3. SRG ternary self-dual codes: pure case

r	s	t	Pure self-dual
$\neq 0$	$\neq 0$	0	$rs = \lambda, \mu = 0, \kappa = 1$
$\neq 0$	0	$\neq 0$	$2 = v - \kappa, \kappa = \lambda + 2 = 2rt + \mu$
0	$\neq 0$	0	$\kappa = 2, \lambda = \mu = 0$
0	0	$\neq 0$	$v = \kappa = \lambda = \mu + 1$
0	$\neq 0$	$\neq 0$	$v = 0, \lambda - \kappa = st(1 + \lambda - \kappa), \mu - \kappa = st(\mu - \kappa)$

TABLE 4. SRG ternary self-dual codes: bordered case

r	s	t	Bordered self-dual
$\neq 0$	$\neq 0$	0	$2rs + \lambda = \mu = 2 + \kappa, \gamma^2 = 1 + 2\kappa,$
$\neq 0$	0	$\neq 0$	$\lambda = 1 + \kappa, 2rt + \mu = \kappa, \gamma^2 = 2 + 2v + \kappa$
0	$\neq 0$	0	$\lambda = 1 + \kappa = \mu, \gamma^2 = 2 + 2\kappa$
0	0	$\neq 0$	$\lambda = \kappa = \mu + 1, \gamma^2 = \kappa + 2v$
0	$\neq 0$	$\neq 0$	$v = -\gamma^2, \lambda - \kappa = st(1 + \lambda - \kappa), \mu - \kappa - 1 = st(\mu - \kappa)$

TABLE 5. DRT ternary self-dual codes: pure case

r	s	t	Pure self-dual
$\neq 0$	$\neq 0$	0	$\lambda = rs, \kappa = 1$
$\neq 0$	0	$\neq 0$	$\lambda = rt, \kappa = 1$
0	$\neq 0$	0	$\lambda = 1, \kappa = 2$
0	0	$\neq 0$	$\lambda + 1 = \kappa = 2$
0	$\neq 0$	$\neq 0$	$\kappa = 1, (\kappa - 1 - \lambda) = st(\lambda + \mu)$

4.4. $R = \mathbb{Z}_4$. All the codes we constructed over \mathbb{Z}_4 are free. We recover several known constructions. The general case of DRT is in [9, p.41] via the equivalence with skew Hadamard matrices. For instance, equation (40) in [9, p.41] is a $B_{\mathbb{Z}_4}(0, 1, 3)$. Similarly, the matrices in [8, eq. (3.1),(3.2)] are equivalent (up to top row reduction) to our bordered case $B_{\mathbb{Z}_4}(b, b, 0)$, and $B_{\mathbb{Z}_4}(1, 3, 2)$, respectively, for suitable α, β, γ . The $B_{\mathbb{Z}_4}(2, 1, 3)$ with $\alpha = 2, \beta = 1, \gamma = 3$ was used by Chapman to derive a computer free construction of the Leech lattice [7].

TABLE 6. DRT ternary self-dual codes: bordered case

r	s	t	Bordered self-dual
$\neq 0$	$\neq 0$	0	$sr = \lambda, \gamma^2 = 1 + 2\kappa$
$\neq 0$	0	$\neq 0$	$rt = \lambda = 0, \gamma^2 = 1 + 2\kappa$
0	$\neq 0$	0	$\lambda = 1, \gamma^2 = 2 + 2\kappa$
0	0	$\neq 0$	$\lambda = 1, \gamma^2 = 2 + 2\kappa$
0	$\neq 0$	$\neq 0$	$\kappa + 2 = \gamma^2, st(\lambda + \mu) = 1 - \kappa - 2(\kappa - 1 - \lambda)$

4.4.1. *Pure Case.* We determine now when codes obtained from SRGs in the pure construction over \mathbb{Z}_4 are self-dual. If s and t are both non units then $r^3 = 3$, an equation without a solution. So we assume that at least one of s or t is a unit. If s is a unit, and t a non-unit then

$$\begin{aligned} r^2 + v &= \kappa \\ \lambda + v + 2\kappa &= 0 \\ 2(\mu + \kappa + 1) + \mu + v &= 0. \end{aligned}$$

If s is a non-unit, and t a unit then

$$\begin{aligned} r^2 + \kappa + 1 &= 0 \\ 2r + \lambda &= 0 \\ \mu &= 0. \end{aligned}$$

If both s and t are units then $r = v = 0$.

We determine now when codes obtained from DRTs in the pure construction over \mathbb{Z}_4 are self-dual. If s and t are both non units then $r^3 = 3$, an equation without a solution. So we assume that at least one of s or t is a unit. If s is a non-unit, and t a unit then

$$\begin{aligned} r^3 + \kappa &= 3 \\ rt + sr + t^2(\kappa - 1 - \lambda) + st(\lambda + \mu) &= 0 \\ rt + sr + t^2(\kappa - \mu) + ts(\lambda + \mu) &= 0. \end{aligned}$$

If s is a unit, and t a non-unit then

$$\begin{aligned} r^3 + \kappa &= 3 \\ rt + sr + s^2(\kappa - 1 - \lambda) + st(\lambda + \mu) &= 0 \\ rt + sr + s^2(\kappa - \mu) + ts(\lambda + \mu) &= 0. \end{aligned}$$

If both s and t are units then

$$\begin{aligned} r^2 + 2\kappa &= 3 \\ rt + sr + 2(\kappa - 1 - \lambda) + st(\lambda + \mu) &= 0 \\ rt + sr + 2(\kappa - \mu) + ts(\lambda + \mu) &= 0. \end{aligned}$$

4.4.2. *Bordered Case.* We determine now when codes obtained from SRGs in the bordered construction over \mathbb{Z}_4 are self-dual.

If s, t are both non-units then $r^2 + \gamma^2 = 3$, an equation without a solution.

If s is a non-unit, and t a unit then

$$\begin{aligned} r^2 + v &= \kappa - \gamma^2 \\ \lambda + v + 2\kappa &= -\gamma^2 \\ 2(\mu + \kappa + 1) + \mu + v &= -\gamma^2. \end{aligned}$$

If s is a unit, and t a non-unit then

$$\begin{aligned} r^2 + \kappa &= 3 - \gamma^2 \\ 2r + \lambda &= -\gamma^2 \\ \mu &= -\gamma^2. \end{aligned}$$

If both s and t are units then

$$\begin{aligned} r^2 &= -\gamma^2 \\ v &= 0. \end{aligned}$$

We determine now when codes obtained from DRTs in the bordered construction over \mathbb{Z}_4 are self-dual.

If s, t are both non-units then $r^2 + \gamma^2 = 3$, an equation without a solution.

If s is a non-unit, and t a unit then

$$\begin{aligned} r^2 + \kappa &= 3 - \gamma^2 \\ rt + st + t^2(\kappa - 1 - \lambda) + st(\lambda + \mu) &= -\gamma^2 \\ rt + sr + t^2(\kappa - \mu) + ts(\lambda + \mu) &= -\gamma^2. \end{aligned}$$

If s is a unit, and t a non-unit then

$$\begin{aligned} r^2 + \kappa &= 3 - \gamma^2 \\ rt + sr + s^2(\kappa - 1 - \lambda) + st(\lambda + \mu) &= -\gamma^2 \\ rt + sr + s^2(\kappa - \mu) + ts(\lambda + \mu) &= 0. \end{aligned}$$

If both s and t are units then

$$\begin{aligned} r^2 + 2\kappa &= 3 - \gamma^2 \\ rt + sr + 2(\kappa - 1 - \lambda) + st(\lambda + \mu) &= -\gamma^2 \\ rt + sr + 2(\kappa - \mu) + ts(\lambda + \mu) &= 0. \end{aligned}$$

5. FAMILIES OF SRG

The following proposition follows by inspection of the generator matrix.

Proposition 1. *If $P(r, s, t)$ is a self-dual code then $B(r, s, t)$ with $\gamma = \beta = 0$, $\alpha = \sqrt{-1}$ is a self-dual code.*

We shall not record the bordered case if it is this case unless the code is Type II.

5.1. SPECIAL GRAPHS. The following graphs can be found in [6].

The **Petersen graph** with parameters $(10, 3, 0, 1)$ yields by bordered construction $(4, 3, 0)$ with $\alpha = 3, \beta = 4, \gamma = 1$ a $[22, 11, 6]$ self-dual code over \mathbb{F}_5 , with automorphism group S_5 .

The **Shrikhande graph** with parameters $(16, 6, 2, 2)$ yields by pure construction $(1, 1, 0)$ an extremal Type II $[32, 16, 8]$ code.

The **Clebsch graph** with parameters $(16, 10, 6, 6)$ yields by pure construction $(1, 0, 1)$ an extremal Type II $[32, 16, 8]$ code.

The three **Chang graphs** with parameters $(28, 12, 6, 4)$ yield by pure construction $(0, 0, 1)$ three Type II [56, 28, 8] code.

The **Hoffman-Singleton graph** with parameters $(50, 7, 0, 1)$ yields by pure construction $(1, 0, \omega)$ a [100, 50, 14] hermitian self-dual code over \mathbb{F}_4 .

The **Gewirtz graph** with parameters $(56, 10, 0, 2)$ yields by pure construction $(1, 1, 0)$ a Type II [112, 56, 12] code.

5.2. LINE GRAPH OF COMPLETE GRAPH. The graph $L(K_n)$ is equivalent to the Johnson scheme $J(n, 2)$ [31, Chap.21], also called Triangular Graph. By [19, p. 218] the parameters are $\left(\binom{n}{2}, 2n - 4, n - 2, 4\right)$.

- If $n \equiv 0 \pmod{4}$ then $P_{\mathbb{F}_2}(0, 0, 1)$ is self-dual.
- If n is even then $P_{\mathbb{F}_2}(1, 1, 0)$ is a self-dual code.

Examples: For the graph $L(K_6)$ the code $P_{\mathbb{F}_2}(1, 1, 0)$ is an optimal Type I [30, 15, 6] code. For the graph $L(K_8)$ the code $P_{\mathbb{F}_2}(0, 0, 1)$ is a Type II [56, 28, 8] code.

- If $n \equiv 0 \pmod{4}$ then $P_{\mathbb{F}_4}(0, 0, a)$, $P_{\mathbb{F}_4}(0, a, 0)$ and $P_{\mathbb{F}_4}(0, a, a)$, where $a \neq 0$, are self-dual codes over \mathbb{F}_4 .
- If $n \equiv 1 \pmod{4}$ then $P_{\mathbb{F}_4}(0, a, a)$, where $a \neq 0$, is a self-dual code over \mathbb{F}_4 .
- If $n \equiv 2 \pmod{4}$ then $P_{\mathbb{F}_4}(a, a, a)$ and $P_{\mathbb{F}_4}(a, a, 0)$, where $a \neq 0$, is a self-dual code over \mathbb{F}_4 .
- If $n \equiv 3 \pmod{4}$ then $P_{\mathbb{F}_4}(\omega, 0, \omega^2)$, $P_{\mathbb{F}_4}(\omega^2, 0, \omega)$ and $P_{\mathbb{F}_4}(a, a, 0)$, where $a \neq 0$, are self-dual codes over \mathbb{F}_4 .

Examples: For the graph $L(K_3)$ the code $P_{\mathbb{F}_4}(\omega, 0, \omega^2)$ is a Type IV [6, 3, 2] code. For the graph $L(K_7)$ the code $P_{\mathbb{F}_4}(\omega, 0, \omega^2)$ is a Type IV [42, 21, 8] code.

5.3. LINE GRAPH OF BIPARTITE COMPLETE GRAPH. The graph $L(K_{n,n})$, also called square lattice graph, is equivalent to the Hamming scheme $H(2, n)$ [31, Chap.21]. By [19, p. 218] the parameters are $(n^2, 2n - 2, n - 2, 2)$.

If n is even then $P_{\mathbb{F}_2}(0, 0, 1)$ is a Type I code and $P_{\mathbb{F}_2}(1, 1, 0)$ is a Type II code.

Examples: For the graph $L(K_{4,4})$ the code $P_{\mathbb{F}_2}(0, 0, 1)$ is a [32, 16, 6] Type I code, and $P_{\mathbb{F}_2}(1, 1, 0)$ is an extremal Type II [32, 16, 8] code.

- If n is even then $P_{\mathbb{F}_4}(0, a, a)$, $P_{\mathbb{F}_4}(0, 0, a)$ and $P_{\mathbb{F}_4}(a, a, 0)$, where $a \neq 0$, are self-dual codes over \mathbb{F}_4 .
- If n is odd then $P_{\mathbb{F}_4}(\omega, 0, \omega^2)$, $P_{\mathbb{F}_4}(\omega^2, 0, \omega)$, $P_{\mathbb{F}_4}(\omega^2, \omega, 0)$ and $P_{\mathbb{F}_4}(\omega, \omega^2, 0)$ are self-dual codes over \mathbb{F}_4 .

Examples: For the graph $L(K_{3,3})$ the code $P_{\mathbb{F}_4}(\omega, 0, \omega^2)$ is a [18, 9, 6] Type IV code. For the graph $L(K_{5,5})$ the code $P_{\mathbb{F}_4}(\omega, 0, \omega^2)$ is a [50, 25, 8] Type IV code.

5.4. ORTHOGONAL ARRAYS. An orthogonal array $OA(h, n)$ as defined in [19, p. 224] is, in the notation of [31, Chap.21] a code of length h , dimension 2 over an alphabet of size n and dual distance ≥ 3 . Declare two codewords adjacent if they are at Hamming distance $h - 1$. By [19, Thm 10.4.2] the parameters are $(n^2, h(n - 1), n - 2 + (h - 1)(h - 2), h(h - 1))$. Equivalently an $OA(h, n)$ is a system of $h - 2$ mutually orthogonal Latin squares. The vertices of the SRG are the cells of the squares. Two cells are adjacent if they share a row or column or an entry in one of the squares.

- If both h and n are even then $P_{\mathbb{F}_2}(0, 0, 1)$ is a self-dual code and if $h \equiv 0 \pmod{4}$ the code is Type II.

- If both h and n are even then $P_{\mathbb{F}_2}(1, 1, 0)$ is a self-dual code and if $h \equiv 2 \pmod{4}$ the code is Type II.
- If h is odd and n is even then $P_{\mathbb{F}_2}(0, 1, 0)$ is a self-dual code and if $h \equiv 3 \pmod{4}$ and $n \equiv 2 \pmod{4}$ or $h \equiv 1 \pmod{4}$ and $n \equiv 0 \pmod{4}$ then the code is Type II.
- If h is odd and n is even then $P_{\mathbb{F}_2}(1, 0, 1)$ is a self-dual code and if $h \equiv 3 \pmod{4}$ and $n \equiv 0 \pmod{4}$ or $h \equiv 1 \pmod{4}$ and $n \equiv 2 \pmod{4}$ then the code is Type II.

5.5. LINE GRAPHS OF STEINER SYSTEMS. A Steiner triple system on N points is a $2 - (N, M, 1)$ design. The vertices of the SRG are the blocks. Declare two block adjacent if they intersect in at least one point. For instance from $M = 3$, one gets an SRG with parameters $(N(N-1)/6, 3(N-3)/2, (N+3)/2, 9)$. If $n \equiv 7 \pmod{8}$ then $P_{\mathbb{F}_2}(1, 0, 1)$ is self-dual.

5.6. MAGMA DATABASE. The following parameters can be found in the Magma database of 43442 SRG's compiled by Brendan McKay [32].

Parameters: $[(36, 15, 6, 6)]$ By pure construction $(1, 0, 1)$ we obtain at least 4 non equivalent $[72, 36, 12]$ Type I codes. According to the data on Gaborit's HomePage [16] there were only two such codes known so far. Non equivalence results from different number of codewords of weight 12, that are, respectively, $\{490, 526, 634, 682\}$.

By pure construction $(0, 1, 0)$ we obtain at least 29 $[72, 36, 12]$ Type II codes, that are distinct from the thirty-two constructed in [13]. In the notation of [13] the α 's are

$$\{-3600, -3576, -3552, -3546, -3540, -3534, -3528, -3522, -3510, -3504, -3498, \\ -3492, -3480, -3468, -3462, -3456, -3444, -3432, -3420, -3408, -3396, \\ -3384, -3372, -3348, -3336, -3300, -3228, -3204, -2316\}$$

Non equivalence results from different number of codewords of weight 12. Note that these codes are different from the ones in [12] since the orders of their automorphism groups are in the set $\{2, 4, 6, 8, 12, 20, 48, 60, 3888\}$, none member of which is a multiple of 23. We have noticed that recently Bouyukliev et. al. [5] constructed numerous values of α including many of the above. But the values of α in the set

$$\{3600, -3576, -3528, -3408, -2316\}$$

are not included in the list given in [5].

Parameters: $[(40, 12, 2, 4)]$

By pure construction $(0, 0, 1)$ we obtain nine $[80, 40, 12]$ Type II codes.

5.7. RANK THREE GROUPS. Historically, the concept of SRGs was motivated by the action of sporadic simple groups on certain graphs [20]. Following table 10A1 in [20], we construct (from the pure construction) some self-dual codes invariant under sporadic groups. It is immediate that if a permutation matrix π acts on A by $\pi^T A \pi = A$, then it acts on $\mathcal{P} = \mathcal{P}_{\mathbb{F}_2}(r, s, t)$ by the rule

$$\pi^T \mathcal{P}(I_2 \otimes \pi) = \mathcal{P}.$$

The constructions are summarized in Table 7.

Examples: The **Higman Sims graph** produces two binary $[200, 100, 12]$ codes (Type I and Type II, respectively). The adjacency matrix was computed by the

Magma program of Paul Hafner [21]. The **Hall Janko Wales graph** produce two binary [200,100,16] codes (Type I and Type II, respectively). The adjacency matrix was computed by the Magma program of J.D. Key [28].

TABLE 7. Rank three groups: binary codes

Group	v	κ	λ	μ	(r, s, t)	Type
HJ	100	36	14	12	(0,0,1)	II
HJ	100	36	14	12	(1,1,0)	I
HS	100	22	0	6	(0,0,1)	I
HS	100	22	0	6	(1,1,0)	II
Suz	1782	416	100	96	(0,0,1)	I
Suz	1782	416	100	96	(1,1,0)	I
Co2	2300	891	378	324	(0,1,0)	II
Co2	2300	891	378	324	(1,0,1)	I
Ru	4060	2304	1328	1208	(0,0,1)	II
Ru	4060	2304	1328	1208	(1,1,0)	I
Fi22	3510	693	180	126	(0,1,0)	I
Fi22	3510	693	180	126	(1,0,1)	I
Fi23	31671	3510	693	351	(1,0,1)	I
Fi24	306936	31671	3510	3240	(0,1,0)	II
Fi24	306936	31671	3510	3240	(1,0,1)	I
Fi23	14080	10920	8408	8680	(0,0,1)	II
Fi23	14080	10920	8408	8680	(1,1,0)	I
Fi23	137632	109200	86600	86800	(0,1,0)	II
Fi23	137632	109200	86600	86800	(1,0,1)	I

6. CODES FROM DRTs

In this section we describe the codes constructed from DRTs. We begin with a proposition.

Proposition 2 ([29]). *Let (X, R_1) be a DRT with parameters $(v, \kappa, \lambda, \mu)$. In the case of the pure construction, $v \equiv 3 \pmod{8}$ if and only if $P_{\mathbb{F}_2}(0, 1, 0)$ and $P_{\mathbb{F}_2}(0, 0, 1)$ are singly-even self-dual. Further in the case of a bordered construction, suppose that $\alpha = 0, \gamma = \beta = 1$. Then $v \equiv 3 \pmod{8}$ if and only if $B_{\mathbb{F}_2}(1, 1, 0)$ and $B_{\mathbb{F}_2}(1, 0, 1)$ are doubly-even self-dual codes.*

Proof. From Lemma 2, we have $AA^T = \kappa I + \lambda A + \lambda \bar{A}$, and $v \equiv 3 \pmod{8}$ if and only if $\lambda \equiv 0 \pmod{2}$. First consider the pure construction. Suppose that $v \equiv 3 \pmod{8}$. Then

$$Q_{\mathbb{F}_2}(0, 1, 0)Q_{\mathbb{F}_2}(0, 1, 0)^T = AA^T = \kappa I + \lambda A + \lambda \bar{A} \equiv I \pmod{2}.$$

Therefore $P_{\mathbb{F}_2}(0, 1, 0)$ is self-dual. As each row of $\mathcal{P}_{\mathbb{F}_2}(0, 1, 0)$ has weight $1 + \kappa \equiv 2 \pmod{4}$, $P_{\mathbb{F}_2}(0, 1, 0)$ is singly-even. Similarly we can show that $P_{\mathbb{F}_2}(0, 0, 1)$ is singly-even self-dual. Conversely if $P_{\mathbb{F}_2}(0, 1, 0)$ is self-dual, then the inner product of any two distinct rows of $Q_{\mathbb{F}_2}(0, 1, 0)$ is λ . This needs to be even since $P_{\mathbb{F}_2}(0, 1, 0)$ is self-dual. Thus $v \equiv 3 \pmod{8}$.

Next let us consider the bordered construction. We only consider $B_{\mathbb{F}_2}(1, 1, 0)$ since $B_{\mathbb{F}_2}(1, 0, 1)$ can be proved similarly. We have

$$\begin{aligned} Q_{\mathbb{F}_2}(1, 1, 0)Q_{\mathbb{F}_2}(1, 1, 0)^T &= (I + A)(I + A^T) = I + A + A^T + AA^T \\ &= J + AA^T = J + \kappa I + \lambda A + \lambda \bar{A} \\ &\equiv I + J \pmod{2} \\ &\text{as } \lambda \equiv 0 \pmod{2}. \end{aligned}$$

Further the top row of $\mathcal{B}_{\mathbb{F}_2}(1, 1, 0)$ is orthogonal to the remaining rows of $\mathcal{B}_{\mathbb{F}_2}(1, 1, 0)$. Hence $B_{\mathbb{F}_2}(1, 1, 0)$ is self-dual. Note that all the rows of $\mathcal{B}_{\mathbb{F}_2}(1, 1, 0)$ have weight a multiple of 4 using the condition that λ is even. Therefore $B_{\mathbb{F}_2}(1, 1, 0)$ is a doubly-even self-dual code.

Conversely suppose that $B_{\mathbb{F}_2}(1, 1, 0)$ is doubly-even self-dual. Then from the above calculation, $Q_{\mathbb{F}_2}(1, 1, 0)Q_{\mathbb{F}_2}(1, 1, 0)^T = J + \kappa I + \lambda A + \lambda \bar{A}$. So the inner product of any two distinct rows of $Q_{\mathbb{F}_2}(1, 1, 0)$ is $1 + \lambda$. This needs to be odd since $B_{\mathbb{F}_2}(1, 1, 0)$ is self-dual. Therefore λ must be even. Hence $v \equiv 3 \pmod{8}$. \square

6.1. DRTS OF ORDER 3. It is known that there is a unique DRT of order 3 which is of a Paley type.

- For the binary case since $n \equiv 3 \pmod{8}$, we have that $P_{\mathbb{F}_2}(0, 1, 0)$ and $P_{\mathbb{F}_2}(0, 0, 1)$ are self-dual $[6, 3, 2]$ codes. It is interesting to note that $B_{\mathbb{F}_2}(1, 1, 0)$ and $B_{\mathbb{F}_2}(1, 0, 1)$ with $\alpha = 0, \beta = \gamma = 1$, are equivalent to the unique extended Hamming code of length 8.
- For the ternary case, since $\lambda = 0, \kappa = 1$, and $\mu = 1$, there is no ternary code from the pure/bordered construction by Table 5 and Table 6.
- For the field of order 4 we have that $P_{\mathbb{F}_4}(1, \omega, \omega)$ is the hexacode h_6 [34] which is the unique Hermitian self-dual $[6, 3, 4]$ code over \mathbb{F}_4 . The code $B_{\mathbb{F}_4}(1, 1, 0)$ with $\alpha = 0, \beta = \gamma = 1$ is the unique Hermitian self-dual $[8, 4, 4]$ code over \mathbb{F}_4 whose generator matrix is that of the binary Hamming $[8, 4, 4]$ code.
- For the ring \mathbb{Z}_4 , the code $B_{\mathbb{Z}_4}(2, 1, 3)$ with $\alpha = 2, \beta = 1, \gamma = 3$ is the octacode o_8 [34, p. 193]. This is the unique Type II \mathbb{Z}_4 -code of length 8. More precisely, there are exactly 24 codes from the bordered construction which are all equivalent to o_8 . The code $B_{\mathbb{Z}_4}(0, 1, 3)$, with $\alpha = 0, \beta = 1, \gamma = 3$ is a lift of the binary extended Hamming code of length 8. It is denoted by \mathcal{E}_8 [34, p. 193]. Since o_8 and \mathcal{E}_8 are the only codes with minimum Hamming weight 4 for this length, our bordered construction over \mathbb{Z}_4 using the DRT of order 3 finds both codes.

6.2. DRTS OF ORDER 7. There is a unique DRT of order 7 (No.2 of [22]).

- For the binary case the pure construction $P_{\mathbb{F}_2}(1, 0, 0)$ is a Type I $[14, 7, 2]$ code. The code $B_{\mathbb{F}_2}(0, 1, 1)$, with $\alpha = 0, \gamma = \beta = 1$, is a Type II $[16, 8, 4]$ code.
- For the ternary case, there are 32 extremal self-dual $[16, 8, 6]$ codes over \mathbb{F}_3 from bordered construction with various values of $\alpha, \beta, \gamma, r, s$, and t . We get only one such code up to equivalence. For example, $B_{\mathbb{F}_3}(1, 1, 0)$ with $\alpha = 1, \beta = 1, \gamma = 2$ is equivalent to the unique extremal ternary self-dual code f_8^{2+} in the notation of [34].
- For the field of order 4 we have that the code $P_{\mathbb{F}_4}(1, \omega, \omega)$ is a Type IV $[14, 7, 4]$ code, and other pure constructions give self-dual codes over \mathbb{F}_4 with $d = 2$ or $d = 4$. Similarly, $B_{\mathbb{F}_4}(0, 1, 1)$ with $\alpha = 0, \beta = 1, \gamma = \omega^2$ is a Type IV $[16, 8, 4]$ code.

- Over \mathbb{Z}_4 we find two inequivalent self-dual codes of length 16 and the highest Hamming weight 4. The first code is $B_{\mathbb{Z}_4}(0, 1, 3)$ with $\alpha = 0, \beta = 1, \gamma = 1$. This code has 678 codewords of Hamming weight 8. It has the highest Lee weight 6 and the highest Euclidean weight 8. This is a Type II code over \mathbb{Z}_4 (i.e., all Euclidean weights are divisible by 8). The other code is $B_{\mathbb{Z}_4}(2, 1, 1)$ with $\alpha = 2, \beta = 1, \gamma = 2$. It also has the highest Lee weight 6 and the highest Euclidean weight 8, but it is not Type II. It has 422 codewords of Hamming weight 8. For the current status of classification of \mathbb{Z}_4 -codes, see Table 9 of [25].

6.3. DRTs OF ORDER 11. It is known that there is a unique DRT of order 11, which is of a Paley type.

- In the binary case it follows from Proposition 2 that $P_{\mathbb{F}_2}(0, 1, 0)$ and $B_{\mathbb{F}_2}(1, 1, 0)$ with $\alpha = 0, \gamma = \beta = 1$ are self-dual codes of length 22 and length 24, respectively. Their minimum distances are computed as 6 and 8, respectively. Hence $B_{\mathbb{F}_2}(1, 1, 0)$ is equivalent to the extended Golay code of length 24.
- For the ternary case the code $B_{\mathbb{F}_3}(0, 1, 2)$ with $\alpha = 0, \beta = 1, \gamma = 2$ is the Pless Symmetry code $S(24)$.
- For the field of order 4 we have that the code $P_{\mathbb{F}_4}(1, 1, \omega)$ is an extremal Type IV [22, 11, 8] code over \mathbb{F}_4 with automorphism group order $2^7 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11$. $B_{\mathbb{F}_4}(\omega, \omega, 0)$ with $\alpha = 0, \beta = 1, \gamma = 1$ is an optimal Type IV [24, 12, 8] code over \mathbb{F}_4 with automorphism group order $2^{10} \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 \cdot 23$.
- For the ring \mathbb{Z}_4 we have that there are no self-dual \mathbb{Z}_4 -codes from the pure construction. On the other hand, there are exactly 48 self-dual \mathbb{Z}_4 -codes from the bordered constructions. For example, $B_{\mathbb{Z}_4}(0, 1, 3)$ with $\alpha = 0, \beta = 1, \gamma = 1$ has minimum Hamming weight 4 and minimum Lee weight 8 while $B_{\mathbb{Z}_4}(1, 1, 2)$ with $\alpha = 0, \beta = 1, \gamma = 1$ has minimum Hamming weight 8 and minimum Lee weight 8. These are not Type II \mathbb{Z}_4 -codes. The code $B_{\mathbb{Z}_4}(1, 1, 0)$ with $\alpha = 2, \beta = 1, \gamma = 1$ is a Type II \mathbb{Z}_4 -code with minimum Hamming weight 8, minimum Lee weight 8, and minimum Euclidean weight 8. We check that there are exactly $528 = 24 \cdot 22$ codewords of minimum Euclidean weight 8. So the corresponding 24-dimensional even unimodular lattice by Construction A is the Niemeier lattice with root system D_{12}^2 (see Table 16.1 of Conway and Sloane [10]).

Other interesting codes are obtained from $B_{\mathbb{Z}_4}(r, s, t)$ with

$$(\alpha, \beta, \gamma, r, s, t) = (2, 1, 1, 2, 1, 3), (2, 1, 1, 2, 3, 1), (2, 1, 3, 2, 1, 3), (2, 1, 3, 2, 3, 1), \\ (2, 3, 1, 2, 1, 3), (2, 3, 1, 2, 3, 1), (2, 3, 3, 2, 1, 3), (2, 3, 3, 2, 3, 1).$$

By inspection, we see that these are equivalent. Further they are Type II \mathbb{Z}_4 -codes with minimum Hamming weight 4 and minimum Lee weight 8. We check that there are 66 codewords of Hamming weight 4 and 66 codewords of Lee weight of 8. This implies that there is no codeword of Euclidean weight 8. Hence these codes have minimum Euclidean weight 16. We remark that the third case of the above list is the code by Chapman [7] as mentioned in 4.4.

6.4. DRTs OF ORDER 15. There is only one DRT of order 15 [22].

- For the binary case the code $B_{\mathbb{F}_2}(0, 1, 1)$ with $\alpha = 0, \beta = \gamma = 1$ is a Type II [32, 16, 4] code.
- For the ternary case there are no self-dual codes over $GF(3)$ from the pure construction nor the bordered construction.

- For the field of order 4, the code $P_{\mathbb{F}_4}(1, \omega, \omega)$ is a Type IV [30, 15, 4] code and $P_{\mathbb{F}_4}(0, \omega, \omega)$ with $\alpha = 0, \beta = 1, \gamma = 1$ is a Type IV [32, 16, 4] code.
- 6.5. DRTS OF ORDER 19. There are two DRTs of order 19 [22].
- For the binary case, from No. 2 of [22] we get $P_{\mathbb{F}_2}(0, 1, 0)$ which is a Type I [38, 19, 6] code. Similarly we get a Type I [38, 19, 8] code from $P_{\mathbb{F}_2}(0, 1, 0)$ using No. 3 of [22]. The code $B_{\mathbb{F}_2}(1, 1, 0)$ with $\alpha = 0, \beta = \gamma = 1$, from each DRT respectively, are two inequivalent extremal Type II [40, 20, 8] codes.
 - For the ternary case, the code $B_{\mathbb{F}_3}(1, 1, 0)$ with $\alpha = 1, \beta = 2, \gamma = 1$ from each DRT respectively give two inequivalent extremal Type III [40, 20, 12] codes.
 - For the field of order 4 we get Type IV [38, 19, 8] codes and [40, 20, 8] codes from the pure and bordered constructions.
- 6.6. DRTS OF ORDER 23. There are 19 DRTs of order 23 [22].
- For the binary case, we get Type II [48, 24, 4] codes from $B_{\mathbb{F}_2}(0, 1, 1)$ with $\alpha = 0, \beta = \gamma = 1$.
 - For the ternary case, there are no self-dual codes over $GF(3)$ from the pure construction. There are exactly 8 extremal Type III [48, 24, 15] codes from the bordered construction using only No. 20 [22]. The code $B_{\mathbb{F}_3}(0, 1, 2)$ with $\alpha = 0, \beta = \gamma = 1$ is an example. These codes are all equivalent to the Pless symmetry code $S(48)$, which is, in fact, $B_{\mathbb{F}_3}(0, 1, 2)$ with $\alpha = 0, \beta = 1, \gamma = 2$. Bordered constructions from other DRTs give self-dual [48, 24] codes over $GF(3)$ with minimum distance at most 12.
- 6.7. DRTS OF ORDER 27. There are 374 DRT of order 27 [22].
- For the binary case, only No. 378 from the website [22] produces an extremal Type I [54, 27, 10] code from $P_{\mathbb{F}_2}(0, 1, 0)$ and an extremal Type II [56, 28, 12] code from $B_{\mathbb{F}_2}(1, 1, 0)$ with $\alpha = 0, \beta = \gamma = 1$. The remainder of the DRTs give Type I codes with $d = 6$ or 8 from the pure construction and Type II codes with $d = 8$ from the bordered construction with $\alpha = 0, \beta = \gamma = 1$.
- 6.8. DRTS OF ORDER 31. There are at least 6 skew Hadamard matrices of order 32 [30]. So there exists DRTs of order 31 [35]. We only consider the Paley type matrix below.
- For the ternary case, we can check there is no self-dual code over $GF(3)$ from the pure construction. The code $B_{\mathbb{F}_3}(2, 0, 2)$ with $\alpha = \beta = \gamma = 1$ gives an extremal Type III [64, 32, 18] code over \mathbb{F}_3 . We further note that $B_{\mathbb{F}_3}(1, 2, 3)$ with $\alpha = 1, \beta = 2, \gamma = 1$ is Beenker's code [3], which is the only known code for this length [25]. It appears that all extremal Type III codes from the bordered construction using the Paley type matrix of order 32 are equivalent.
- 6.9. DRTS OF ORDER 35. It is known that there exist at least 18 skew Hadamard matrices of order 36 [30]. So there exist(s) DRT of order 35 [35].
- For the binary case, we obtain two inequivalent Type I [70, 35, 10] codes from $P_{\mathbb{F}_2}(0, 1, 0)$ and one Type II [72, 36, 12] code from $B_{\mathbb{F}_2}(1, 1, 0)$ with $\alpha = 0, \beta = \gamma = 1$ using the 15th and 16th skew Hadamard matrices in [30], after normalizing them according to [35].
 - For the ternary case, we obtain self-dual [72, 36, 15] codes from $B_{\mathbb{F}_3}(0, 1, 2)$ with $\alpha = 0, \beta = 1, \gamma = 2$, using these matrices. This minimum distance is 3 less than the ternary quadratic residue code which is an extremal Type III

[72, 36, 18] code. This gives a further motivation of the construction of skew Hadamard matrices of order 36.

We consider one additional length.

6.10. DRTS OF ORDER 51. It is known [30] that there exist at least 561 skew Hadamard matrices of order 52. So there exists DRTs of order 51.

- For the binary case, many $P_{\mathbb{F}_2}(0, 1, 0)$, using these matrices, give Type I [102, 51, 12] codes, and many $B_{\mathbb{F}_2}(1, 1, 0)$, with $\alpha = 0, \beta = \gamma = 1$, give Type II [104, 52, 12] codes. It is well known that there is an extremal Type II QR [104, 52, 20] code.

7. QUADRATIC DOUBLE CIRCULANT CODES

Quadratic Double Circulant Codes (QDC) are defined as follows. Let q be an odd prime power. Let χ denote the indicator function of the quadratic residues of \mathbb{F}_q . Let Q and N denote q by q matrices with zeroes on the main diagonal and for $j \neq i$, $Q_{i,j} = \frac{1+\chi(j-i)}{2}$ and $N_{i,j} = \frac{1-\chi(j-i)}{2}$. For scalars r, s, t of R define the matrix $Q_q(r, s, t) := rI + sQ + tN$.

The matrix Q in this construction is the matrix A of our construction and the matrix N is \overline{A} .

If $q = 4\ell + 1$ then A is the adjacency matrix of an SRG, with the following parameters:

$$v = q, \kappa = 2\ell, \lambda = \ell - 1, \mu = \ell.$$

If $q = 4\ell + 3$ then A is the adjacency matrix of a DRT, with the following parameters:

$$v = q, \kappa = 2\ell + 1, \lambda = \ell, \mu = \ell + 1.$$

The pure and the bordered constructions given in [15] correspond to our pure and bordered constructions. He constructs $P_{\mathbb{F}_2}(0, 1, 0)$ when $q = 8\ell + 3$, $P_{\mathbb{F}_4}(1, \omega, \omega^2)$ when $q = 8\ell + 1$, $B_{\mathbb{F}_4}(0, \omega, \omega^2)$, $\alpha = 0, \beta = 1$ when $q = 8\ell + 1$, $P_{\mathbb{F}_4}(0, \omega, \omega^2)$ when $q = 8\ell - 1$, $B_{\mathbb{F}_4}(1, \omega, \omega^2)$, $\alpha = 0, \beta = 1$ when $q = 8\ell - 1$, as well as numerous self-dual codes over \mathbb{F}_9 , \mathbb{F}_5 and \mathbb{F}_7 .

8. CONCLUSION AND OPEN PROBLEMS

In this article we have described two very general constructions (pure and bordered) of self-dual codes from either SRGs or DRTs. One interest of this construction is to unify earlier known constructions of double circulant codes, thus generalizing further [15].

A second interest is to construct self-dual codes with interesting automorphism groups, in keeping with the relations between sporadic simple groups and SRGs.

A third interest is to construct new self-dual codes with high minimum distance. In that respect these constructions perform better when there are many SRG with the same parameters. For instance the 32548 SRGs with parameters (36, 15, 6, 6) yield the best known (and conjecturally the best possible) distances for binary self-dual codes of length 72. (The success rate is about of one per thousand). This suggests that new additions in the Magma database of SRG in the range 40–100 might result into new records for binary self-dual codes of lengths 80–200. In particular the present work is a further motivation for “pseudo-random” constructions of SRGs [1].

REFERENCES

- [1] P. J. Cameron, *Random strongly regular graphs?*, “Electronic Notes in Discrete Math,” ed. Jaroslav Nešetřil, Marc Noy and Oriol Serra, Vol. 10, Elsevier, Amsterdam, 2001, <http://www.maths.qmul.ac.uk/~pjc/papers.html>
- [2] Bannai E., Dougherty S. T., Harada M. and Oura M., *Type II codes, even unimodular lattices and invariant rings*, IEEE-IT, **45** (1999), 1194–1205.
- [3] G. F. Beenker, *A note on extended quadratic residue codes over GF(9) and their ternary images*, IEEE-IT, **30** (1984), 403–405.
- [4] A. Bonnetcaze, P. Solé, C. Bachoc and B. Mourrain, *Type II codes over \mathbb{Z}_4* , IEEE Trans. Inform. Theory, **43** (1997), 969–976.
- [5] I. Bouyukliev, V. Fack and J. Winne, *Hadamard matrices of order 36 and double-even self-dual [72, 36, 12] codes*. DMTCS proc, AE (2005), 93–98.
- [6] A. E. Brouwer, A. M. Cohen and A. Neumaier, “Distance-regular graphs,” Springer, New York (1985), EMG 18.
- [7] R. J. Chapman, *Double circulant constructions of the Leech lattice*, J. Austral. Math. Soc. Ser. A, **69** (2000), 287–297.
- [8] A. R. Calderbank, N. J. A. Sloane, *Double circulant codes over \mathbb{Z}_4 and even unimodular lattices*, J. of Algebraic Combinatorics, **6** (1997), 119–131.
- [9] J. H. Conway, N. J. A. Sloane, *Self-dual codes over the integers modulo 4*, J. Combinatorial Th. A, **62** (1993), 30–45.
- [10] Conway J. H., Sloane N. J. A., “Sphere Packings, Lattices and Groups,” Springer, New York, 1993.
- [11] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Reports Suppl., **10** (1973).
- [12] R. Dontcheva, *New binary self dual [70, 35, 12] and binary [72, 36, 12] self dual doubly even codes*, Serdica Math. J., **27** (2001), 287–302.
- [13] S. T. Dougherty, T. A. Gulliver and M. Harada, *Extremal Binary Self-dual codes*, IEEE Trans. Inform. Theory, **43** (1997), 2036–2046.
- [14] Dougherty S. T., Gulliver T. A. and Harada M., *Type II codes over finite rings and even unimodular lattices*, J. Alg. Combin., **9** (1999), 233–250.
- [15] P. Gaborit, *Quadratic double circulant codes over fields*, Journal of Combinatorial Theory Series A, **97** (2002), 85–107.
- [16] P. Gaborit, http://www.unilim.fr/pages_perso/philippe.gaborit/SD/
- [17] C. D. Godsil, “Algebraic Combinatorics,” Chapman and Hall, 1993.
- [18] P. Gaborit, A. Natividad and P. Solé, *Eisenstein lattices, Galois rings and quaternary codes*, I. J. of Number Theory, to appear.
- [19] C. D. Godsil, G. Royle, “Algebraic Graph Theory,” Springer, New York, 2001.
- [20] R. L. Griess, jr “Twelve Sporadic Simple Groups,” Springer SMM (1998).
- [21] P. R. Hafner, <http://www.math.auckland.ac.nz/~hafner/his/his.m>
- [22] A. Hanaki, I. Miyamoto, <http://kissme.shinshu-u.ac.jp/as/>
- [23] Masaaki Harada, *New extremal Type II codes over \mathbb{Z}_4* , Designs, Codes and Cryptography, **13** (1998), 271–284.
- [24] D. G. Higman, *Coherent configuration*, Geom. Dedicata, **4** (1975), 1–32.
- [25] W. C. Huffman, *On the classification and enumeration of self-dual codes*, Finite Fields and Their Applications, **11** (2005), 451–490.
- [26] W. C. Huffman, V. S. Pless, “Fundamentals of Error-correcting Codes,” Cambridge University Press, Cambridge, 2003.
- [27] Yury J. Ionin, Hadi Kharaghani, *Doubly regular digraphs and symmetric designs*, J. Combinatorial Th. A, **101** (2003), 35–48.
- [28] J. D. Key, http://www.ces.clemson.edu/~keyj/Key/Janko/J2_July00
- [29] J. -L. Kim, *Codes constructed from Non-Symmetric Association Schemes*, preprint, 1997, www.math.louisville.edu/~jlkim/preprints.html
- [30] C. Koukouvinos, <http://www.math.ntua.gr/people/ckoukou/hadamard.htm>
- [31] F. J. MacWilliams, N. J. A. Sloane, “The theory of error correcting codes,” North Holland, 1981.
- [32] <http://magma.maths.usyd.edu.au/magma/htmlhelp/text1394.htm#14180>
- [33] V. Pless, *On a new family of symmetry codes and related new 5-designs*, Bull. AMS, **75** (1969), 1339–1342.

- [34] E. Rains, N. J. A. Sloane, *Self-dual codes*, in “Handbook of Coding Theory,” V. S. Pless and W. C. Huffman, eds., Elsevier, Amsterdam (1998), pp. 177-294.
- [35] K. B. Reid, E. Brown, *Doubly regular tournaments are equivalent to skew Hadamard matrices*, J. Combinatorial Th. A, 1972, 332–338.

Received April 2006; revised August 2006.

E-mail address: doughertys1@scranton.edu

E-mail address: jl.kim@louisville.edu

E-mail address: sole@essi.fr