# Two-Weight Codes, Graphs and Orthogonal Arrays

Eimear Byrne · Alison Sneyd

Received: date / Accepted: date

Abstract We investigate properties of two-weight codes over finite Frobenius rings, giving constructions for the modular case. A  $\delta$ -modular code [15] is characterized as having a generator matrix where each column g appears with multiplicity  $\delta |gR^{\times}|$  for some  $\delta \in \mathbb{Q}$ . Generalizing [10] and [5], we show that the additive group of a two-weight code satisfying certain constraint equations (and in particular a modular code) has a strongly regular Cayley graph and derive existence conditions on its parameters. We provide a construction for an infinite family of modular two-weight codes arising from unions of submodules with pairwise trivial intersection. The corresponding strongly regular graphs are isomorphic to graphs from orthogonal arrays.

 $\label{eq:keywords} \begin{array}{l} \mbox{ring-linear code} \cdot \mbox{finite Frobenius ring} \cdot \mbox{orthogonal array} \cdot \mbox{strongly} \\ \mbox{regular graph} \cdot \mbox{homogeneous weight} \cdot \mbox{two-weight code} \cdot \mbox{modular code} \end{array}$ 

**Mathematics Subject Classification (2000)** 05E30 · 94B25 · 94B60 · 94B99 · 94B05

## **1** Introduction

Homogeneous weights have been widely studied in the context of linear codes over finite rings and modules [3,4,5,12,14,18,24]. They were first proposed for the integer residue rings in [18]. The concept was generalised in different ways in [12, 24]. We follow the definition given in [12], which requires such a weight on a ring R to be both invariant under the action of the unit group  $R^{\times}$  and to yield the same average value on every principal ideal. Finite Frobenius rings are central to ring-linear coding, allowing the generalisations of many classical results [12,27]. It was shown in [3] that regular, projective codes over finite Frobenius rings with two non-zero homogeneous weights yield strongly regular graphs. Honold asserted that

Research supported by Science Foundation Ireland Grant 08/RFP/MTH1181

Eimear Byrne · Alison Sneyd

School of Mathematical Sciences, University College Dublin, Ireland E-mail: alison.sneyd@ucd.ie

this result extended to the case of modular two-weight codes [15], which includes the class of regular, projective codes. In [5], generalising techniques of Delsarte [10], new relationships between the parameters of a projective, regular two-weight code and the eigenvalues of the corresponding strongly regular graph were established.

In this paper, we extend techniques used in [5,10] to describe the parameters of two-weight codes over finite Frobenius rings, whose corresponding Cayley graphs are strongly regular. As in [5], relationships between the eigenvalues of a two-weight code and its Cayley graph yield existence criteria for such objects.

We provide a construction of an infinite family of modular two-weight codes over a finite Frobenius ring R that arise from unions of submodules of  $R_R^k$  (see also [6]) and characterize all codes formed in this way. This establishes the existence of modular two-weight codes of any square order. This is the only known construction for an infinite family of two-weight codes over rings of non-prime-power order.

### 2 Preliminaries

#### 2.1 Orthogonal Arrays and Strongly Regular Graphs

We recall some elementary properties of orthogonal arrays and strongly regular graphs.

Let  $s, \kappa \geq 2$ . An orthogonal array with parameters s and  $\kappa$ , denoted  $OA(s, \kappa)$ , is an  $s^2 \times \kappa$  array with entries from an s-set S, such that in any two columns of the array, each ordered pair of symbols from  $S \times S$  occurs exactly once. Orthogonal arrays have a variety of applications such as in the design of experiments (where each row represents a test to be performed) and for constructions of authentication codes for cryptography. They also have strong connections to error correcting codes. The reader is referred to [9,13,25] for further details on orthogonal arrays, their generalisations and their relations to other structures.

An  $OA(s, \kappa)$  is equivalent to a set of  $\kappa - 2$  mutually orthogonal latin squares (MOLS) of side s. Other than obtaining new constructions of infinite families of orthogonal arrays, a classical problem of the theory is to know the maximum value of  $\kappa$  for which an  $OA(s, \kappa)$  exists (often denoted in MOLS terminology by N(s)). A well-known upper bound is given by  $N(s) \leq s + 1$ , which is tight if s is a prime power [9, Chapter III]. If s is not a power of a prime, little is known and there is no known value of s for which the maximum value of  $\kappa = s + 1$  is attained. In fact, an OA(s, s + 1) exists if and only if a finite projective plane of order s exists. MacNeish [23] showed there there exists an  $OA(s, p_1^{d_1} + 1)$  for  $s = p_1^{d_1} \dots p_r^{d_r}$ , where  $p_1, \dots, p_r$  are primes and  $p_1^{d_1} < \dots < p_r^{d_r}$  so in particular we have the lower bound  $p_1^{d_1} + 1 \leq N(s)$  for such s.

There is an extensive literature on strongly regular graphs. See for example, [8,9,11]. A K-regular graph  $\Gamma$  that is neither empty nor complete on N vertices is called *strongly regular* with parameters  $(N, K, \lambda, \mu)$  if every pair of adjacent vertices have  $\lambda$  common neighbours and every non-adjacent pair have  $\mu$  common neighbours. Equivalently, its adjacency matrix A satisfies the equation

$$AJ = JA = KJ$$
 and  $A^{2} - (\lambda - \mu)A - (K - \mu)I = \mu J.$  (1)

An eigenvalue of A is then called an eigenvalue of  $\Gamma$ . Strongly regular graphs have three eigenvalues, say  $\rho_1 \leq -1 < \rho_2 \leq K$ . If  $\Gamma$  is disconnected,  $\rho_1 = -1$  and  $\rho_2 = K$ . If  $\Gamma$  is connected, the three eigenvalues are distinct. In fact, any connected graph with three distinct eigenvalues is strongly regular. The eigenvalue  $\rho_2 = 0$  if and only if the complement of  $\Gamma$  is disconnected.  $\Gamma$  is called *imprimitive* (or *trivial*) if either  $\Gamma$  or is complement is disconnected. If  $\Gamma$  is not imprimitive,  $\Gamma$  is called *primitive*. Provided  $\Gamma$  is primitive, unless the  $\rho_i$  occur with the same multiplicity, they are integers of opposite sign satisfying  $K > \rho_2 > -1 > \rho_1$ .

The following construction of strongly regular graphs will be used later. Let B be an  $OA(s, \kappa)$ . Then B determines a strongly regular graph  $\Gamma(B)$  by taking its  $s^2$  rows as vertices and joining two vertices if they have a common entry in a column of B.  $\Gamma(B)$  has parameters

$$(s^2, \kappa(s-1), s-2 + (\kappa - 1)(\kappa - 2), \kappa(\kappa - 1)).$$

In the case that  $\kappa = 2$ , this graph is often called the  $s^2$  graph or lattice graph associated to B. Given a strongly regular graph  $\Gamma$ , if there exists some  $OA(s, \kappa)$  B such that  $\Gamma$  is isomorphic to  $\Gamma(B)$ , we will call  $\Gamma$  an  $OA(s, \kappa)$ -type graph.

#### 2.2 Homogeneous Weights and Frobenius Rings

We discuss some properties of finite Frobenius rings that will be used later. For a thorough discussion of ring theory, see [20]. A detailed treatment of (finite or infinite) Frobenius rings can be found in [19], while [14,27] discuss the finite case. Let R be a finite ring with identity. We denote the group of units of R by  $R^{\times}$ . Let  $\chi : R \to \mathbb{C}^{\times}$  be a character of (R, +). Let  $\hat{R} = Hom_{\mathbb{Z}}(R, \mathbb{C}^{\times})$  denote the group of characters of R.  $\hat{R}$  is an (R, R)-bimodule, given by  $\chi^{r}(x) = \chi(rx)$  and  ${}^{r}\chi(x) =$  $\chi(xr)$ , for all x, r in R, and for all  $\chi$  in  $\hat{R}$ .

A finite ring R is a *Frobenius ring* if it satisfies any of the following equivalent conditions (or their right counterparts) [14]:

- 1.  $_{R}R \cong _{R}\widehat{R},$
- 2.  $_R(R/\operatorname{Rad}(R)) \cong \operatorname{Soc}(_RR),$
- 3. The socle of  $_{R}R$ ,  $Soc(_{R}R)$ , is a principal left ideal.

Examples of finite Frobenius rings include finite fields and the integer residue rings. If R is Frobenius so is  $M_n(R)$ , the ring of  $n \times n$  matrices over R. The ring of  $2 \times 2$  upper triangular matrices over a finite field is not Frobenius. For more examples, see [19].

A character  $\chi$  of R is called a *left (resp. right) generating character* if the map  $\phi: R \to \hat{R}, \phi(r) = {}^{r}\chi$  is an isomorphism of left R modules. Every Frobenius ring possesses a left (which is also a right) generating character [27].

We now introduce the homogeneous weight on finite rings.

**Definition 1 ([12])** A map w:  $R \to \mathbb{R}$  is called a (left) homogeneous weight if w(0) = 0 and the following hold:

- (i) If Rx = Ry, then w(x) = w(y) for all x, y in R.
- (ii) There exists a real number  $\gamma \geq 0$  (independent of R) such that

$$\sum_{y \in Rx} w(y) = \gamma |Rx|, \text{ for all } x \in R \setminus \{0\}.$$

A left homogeneous weight exists on all finite rings and it is unique up to the choice of  $\gamma$ . Right homogeneous weights are defined similarly. If R is Frobenius, the right and left homogeneous weights coincide [24]. If  $\gamma = 1$ , we say the homogeneous weight is *normalized*.

Let q be a prime power. Over a finite field  $\mathbb{F}_q$ , the Hamming weight is homogeneous with  $\gamma = \frac{q-1}{q}$ . Over  $\mathbb{Z}_4$ , the Lee weight is given by w(0) = 0, w(1) = w(3) = 1, w(2) = 2. It is homogeneous with  $\gamma = 1$ . If  $R = \mathbb{F}_2 \oplus \mathbb{F}_2$ , the normalized homogeneous weight is given by w(0,0) = w(1,1) = 0, w(1,0) = w(0,1) = 2. Observe the non-zero ring element (1,1) has weight zero. We will call a ring R proper if the only ring element of weight 0 in R is the zero element.

We now discuss two well-known characterisations of the homogeneous weight.

Let  $\mu$  denote the Möbius function on the poset of principal left ideals of R partially ordered by set inclusion (cf. for example [21]). It is the integer-valued function implicitly defined by

$$\mu(Rx, Rx) = 1, \text{ for all } x \in R,$$
  

$$\mu(Ry, Rx) = 0, \text{ if } Ry \leq Rx, \text{ and}$$
  

$$\sum_{Ry \leq Rz \leq Rx} \mu(Rz, Rx) = 0, \text{ if } Ry < Rx.$$

**Theorem 2** ([12]) Let R be a finite ring,  $x \in R$  and  $\gamma \ge 0$  be a real number. Then the homogeneous weight of x is given by:

$$w(x) = \gamma \left(1 - \frac{\mu(0, Rx)}{\mid R^{\times}x \mid}\right)$$

**Theorem 3 ([14])** Let R be a finite Frobenius ring with generating character  $\chi$ . Then for a real constant  $\gamma > 0$  and  $x \in R$ , the homogeneous weight of x is given by:

$$w(x) = \gamma \left( 1 - \frac{1}{\mid R^{\times} \mid} \sum_{u \in R^{\times}} \chi(ux) \right).$$
(2)

From now on, we assume R is Frobenius with generating character  $\chi$  and we let w denote the homogeneous weight on R of average value  $\gamma$ .

#### 2.3 Codes over Rings

A (left) linear code  $C \leq {}_{R}R^{n}$  is a submodule of  ${}_{R}R^{n}$ . The elements of C are called codewords. For  $c = (c_{1}, \ldots, c_{n}) \in C$ , the homogeneous weight of c is given by  $w(c) := \sum_{i=1}^{n} w(c_{i})$ . A code C is called *proper* if the only codeword of weight 0 in C is the zero codeword.

A pair of vectors  $y, z \in \mathbb{R}^k$  are called *(right) projectively distinct* if  $y\mathbb{R} \neq z\mathbb{R}$  as right  $\mathbb{R}$ -modules, otherwise we say that y and z are in the same (right) projective class (which holds if and only if y = za for some  $a \in \mathbb{R}^{\times}$ ).

For the remainder we fix the following notation. For any  $x = (x_1, \ldots, x_n)$ ,  $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ , we have  $x \cdot y := \sum_{i=1}^n x_i y_i$ . We let  $C \leq {}_R \mathbb{R}^n$  denote a proper left linear code generated by the rows of a  $k \times n$  matrix  $G = [g_1, \ldots, g_n]$  over  $\mathbb{R}$  that has exactly r projectively distinct columns, indexed by a subset  $\mathcal{I} \subset \{1, \ldots, n\}$  of size r. Furthermore, we assume the following:

- 1.  $[i] := \{j \in \{1, ..., n\} : g_i R = g_j R\}, \text{ for each } i \in \mathcal{I};$
- 2.  $\eta_i$  columns of G are in the same projective class as  $g_i$ , for each  $i \in \mathcal{I}$ ; 3.  $\delta_i := \frac{\eta_i}{|g_i R^{\times}|}$ , for each  $i \in \mathcal{I}$ ;
- 4. for each  $j \in [i]$ , write  $g_j = g_i \tau_{ij}$  for some  $\tau_{ij} \in R^{\times}$ , for each  $i \in \mathcal{I}$ ; 5.  $G^{\perp} := \{ x \in R^k : x \cdot g_i = 0 \ \forall \ i \in \{1, ..., n\} \};$

6. 
$$M_G := \sum_{j=1} g_j R;$$

7. for each  $j \in \{1, ..., n\}$ , column  $g_j$  is non-zero.

For each  $y \in \mathbb{R}^k$  we write  $\operatorname{ann}_R(y) := \{s \in \mathbb{R} : ys = 0\} \leq \mathbb{R}_R$ .

A code over a finite Frobenius ring R is called *projective* if  $\eta_i = 1$  for all i and is called *regular* if  $\{x \cdot g_j : x \in \mathbb{R}^k\} = \mathbb{R}$  for all  $j \in \{1, \dots, n\}$ .

**Lemma 4** Let  $y \in R^k$  and  $\nu \in R^{\times}$ . Then  $R^{\times} \cap (1 + \operatorname{ann}_R(y))$  is a subgroup of  $R^{\times}$  and  $|R^{\times} \cap (\nu + \operatorname{ann}_{R}(y))||yR^{\times}| = |R^{\times}|.$ 

*Proof* The subgroup property is easy to check. Now  $R^{\times}$  acts on  $R^k$  by right multiplication. The orbit of any element  $y \in \mathbb{R}^k$  is given by  $y\mathbb{R}^{\times}$  and its stabilizer is  $R^{\times} \cap (1 + \operatorname{ann}_{R}(y))$ , which has order  $|R^{\times}|/|yR^{\times}|$ , by the Orbit-Stabilizer Theorem. The result now follows since for any  $\nu \in \mathbb{R}^{\times}$  the map :  $\nu + a \mapsto 1 + a\nu^{-1}$  is a bijection from  $R^{\times} \cap (\nu + \operatorname{ann}_R(y))$  onto  $R^{\times} \cap (1 + \operatorname{ann}_R(y))$ . П

**Definition 5 ([15])** We say that C is a  $\delta$ -modular code if  $\delta_i = \delta$  for each  $i \in \mathcal{I}$ .

*Example 1* A projective code over the finite field  $\mathbb{F}_q$  is  $\frac{1}{q-1}$ -modular. A projective, regular code over a finite Frobenius ring R is  $\frac{1}{|R^{\times}|}$ -modular. Over  $\mathbb{Z}_6$ , the code generated by  $\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 3 \end{bmatrix}$  is modular and the code generated by  $\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$  is not modular.

**Lemma 6** Let C be  $\delta$ -modular. If  $\gamma = \delta^{-1}$ , then  $w(c) \in \mathbb{Z}$  for all  $c \in C$ .

*Proof* Let  $c \in C$ . Then  $w(c) = \sum_{i \in \mathcal{I}} \eta_i w(c_i)$ . By hypothesis and Theorem 2 we have

$$\eta_i w(c_i) = \frac{\eta_i}{\delta} \left( 1 - \frac{\mu(0, c_i R)}{|c_i R^{\times}|} \right) = |g_i R^{\times}| \left( 1 - \frac{\mu(0, c_i R)}{|c_i R^{\times}|} \right)$$

Let  $x \in R^k$  such that c = xG. Then  $c_i = x \cdot g_i, \operatorname{ann}_R(g_i) \subset \operatorname{ann}_R(x \cdot g_i)$  and  $R^{\times} \cap (1 + \operatorname{ann}_R(g_i))$  is a subgroup of  $R^{\times} \cap (1 + \operatorname{ann}_R(x \cdot g_i))$ . The result now follows by Lemma 4. 

**Definition 7** The code C is called a two-weight code if for all  $c \in C$ ,  $w(c) \in$  $\{0, w_1, w_2\}$  for some  $0 < w_1 < w_2$ .

If C is a two-weight code, we define a graph  $\Gamma(C)$  as follows: The codewords of C are the vertices of  $\Gamma(C)$  and two codewords  $c, c' \in C$  are adjacent in  $\Gamma(C)$  if and only if  $w(c-c') = w_1$ .  $\Gamma(C)$  is the Cayley graph generated by set of codewords of C of weight  $w_1$ . Observe that changing the value  $\gamma$  of w does not affect  $\Gamma(C)$ . In certain cases,  $\Gamma(C)$  is a strongly regular graph, in which case we will call C primitive if  $\Gamma(C)$  is primitive.

# **3** Two-Weight Rings

We call a finite Frobenius ring R a two-weight ring if for all  $r \in R$ ,  $w(r) \in \{0, w_1, w_2\}$  for some  $0 < w_1 < w_2$  and there exist some  $u, v \in R$  such that  $w(u) = w_1$  and  $w(v) = w_2$  (that is to say that R has exactly two non-zero homogeneous weights). For the remainder of this section, we assume all two-weight rings are proper and that the homogeneous weight is normalised. If R is a two-weight ring, then  $\Gamma(R)$ , the Cayley graph of the set of ring elements of weight  $w_1$  in R is a strongly regular graph (cf. [3,5]). We now show that any two-weight ring is isomorphic to one of the following:

1. Let R be a local ring with residue field of order q. Then for all non-zero  $x \in R$ ,

$$w(x) = \begin{cases} w_1 = 1, & \text{if } x \notin \text{Soc}(R), \\ w_2 = \frac{q}{q-1}, & \text{otherwise.} \end{cases}$$

The local R has a non-trivial socle if and only if R is not a finite field, in which case it is a two-weight ring. If R is a finite field it is not a two-weight ring and every non-zero element has weight  $\frac{q}{q-1}$ .

2. Let q > 2. Then  $R = \mathbb{F}_q \oplus \mathbb{F}_q$  is a two-weight ring: for all non-zero  $x \in R$ ,

$$w(x) = \begin{cases} w_1 = \frac{q(q-2)}{(q-1)^2}, & \text{if } x \in R^{\times}, \\ w_2 = \frac{q}{q-1}, & \text{otherwise.} \end{cases}$$

3.  $M_2(\mathbb{F}_q)$  is a two-weight ring: for all non-zero  $x \in \mathbb{R}^{1}$ 

$$w(x) = \begin{cases} w_1 = \frac{q(q^2 - q - 1)}{(q^2 - 1)(q - 1)}, & \text{if } x \in R^{\times}, \\ w_2 = \frac{q^2}{q^2 - 1}, & \text{otherwise.} \end{cases}$$

Let R be a two-weight ring with non-zero weights  $w_1 < w_2$ . It can easily be deduced from [3,5] that  $w_1 \leq 1 < w_2$ , with equality if and only if  $\Gamma(R)$  is imprimitive. It follows that for any non-zero  $x \in R$ ,  $w(x) = w_2$  if and only if  $\mu(0, Rx) < 0$  and  $w(x) = w_1$  if and only if  $\mu(0, Rx) \geq 0$ .

**Lemma 1** Let R be a two-weight ring. Then  $\Gamma(R)$  is imprimitive if and only if R is a local ring.

Proof For a non-zero  $x \in R$ ,  $w(x) = w_1 = 1$  if and only if  $\mu(0, Rx) = 0$ . Since  $\operatorname{Soc}(_RR)$  is principal, this holds if and only if  $\operatorname{Soc}(_RR)$  is simple. Since R is Frobenius, we have  $_R(R/\operatorname{Rad}(R)) \cong \operatorname{Soc}(_RR)$ .

Recall that a semi-simple ring is one satisfying  $\operatorname{Rad}(R) = \{0\}$  (cf. [20]).

**Lemma 2** Let R be a two-weight ring. Then if  $\Gamma(R)$  is primitive, R is semisimple.

Proof Since  $\operatorname{Soc}(_RR)$  is principal, if  $\operatorname{Soc}(R) \neq R$ , there exists  $a \notin \operatorname{Soc}(R)$  such that w(a) = 1. This contradicts the assumption  $\Gamma(R)$  is primitive. Applying the identity  $_R(R/\operatorname{Rad}(R)) \cong \operatorname{Soc}(_RR)$  gives  $\operatorname{Rad}(R) = \{0\}$ .

<sup>&</sup>lt;sup>1</sup> It is well-known that  $M_2(\mathbb{F}_q)$  determines a strongly regular graph by taking the ring elements as vertices and joining two vertices if their difference has rank 2 (cf. [9]); this is the same relation as induced by the homogeneous weight.

**Observation 8** In [5, Corollary 15], it was shown that for a proper regular, projective, two-weight code C, with homogeneous weights  $0 < w_1 < w_2$  that  $(w_2 - w_1)|R^{\times}|$  is an integral divisor of |C|. Then in particular if R is a two-weight ring we see that  $(w_2 - w_1)|R^{\times}|$  is an integral divisor of |R|.

**Observation 9** It is well-known that all finite semi-simple rings are isomorphic to direct sums of matrix rings over finite fields.

We will use these observations in the proof of the following classification result.

**Theorem 10** Let R be a two-weight ring with  $\Gamma(R)$  primitive. Then R is isomorphic to either  $\mathbb{F}_q \oplus \mathbb{F}_q$ , q > 2, or to  $M_2(\mathbb{F}_q)$ .

Proof Since R is semi-simple, we may write  $R \cong \bigoplus_{i=1}^{t} M_{n_i}(\mathbb{F}_{q_i})$  for some prime powers  $q_i$  and positive integers  $n_i$ . Observe all minimal (left) ideals Rx in R have the same order  $m = \frac{w_2}{w_2-1}$ , since any generator x of such an ideal satisfies  $\mu(x) = -1$  and  $w(x) = w_2 = \frac{|Rx|}{|Rx|-1}$ . Now let  $R_j = M_{n_j}(\mathbb{F}_{q_j})$ . For  $x_j \in R_j$ , we let  $\bar{x}_j \in R$  have  $x_j$  in the  $j^{th}$  coordinate and zeroes elsewhere. If  $R_j x_j$  is minimal of order  $m_j$ , it follows that  $R\bar{x}_j$  is also minimal of order  $m_j = m$  (thus  $m_j$  is independent of j).

Suppose for the sake of contradiction that t > 2. Then for  $j \in \{1, 2, 3\}$ , let  $x_j \in R_j$  such that  $R_j x_j$  is minimal of order m. Then  $x = \bar{x}_1 + \bar{x}_2 + \bar{x}_3 \in R$  satisfies  $\mu(x) = -1$ . Therefore  $w(x) = 1 + \frac{1}{(m-1)^3} \neq w_2$ , unless m = 2. If m = 2, R is not proper.

Let t = 2 and without loss of generality, suppose  $n_1 > 1$ . Then  $m = q_1^{n_1}$ . Let  $A \in M_{n_1}(\mathbb{F}_{q_1})$  have  $a_{11} = a_{22} = 1$  and all other coordinates equal to zero. Then  $\bar{A} \in R$  satisfies  $\mu(\bar{A}) = q_1, |R^{\times}\bar{A}| = q_1(q_1^{n_1} - 1)(q_1^{n_1-1} - 1)$  and  $w(\bar{A}) = w_1 = 1 - \frac{1}{(q_1^{n_1} - 1)(q_1^{n_1-1} - 1)}$ . Now for  $j = \{1, 2\}$ , let  $x_j \in R_j$  such that  $R_j x_j$  is minimal. Then  $\mu(\bar{x}_1 + \bar{x}_2) = 1$  and  $w(\bar{x}_1 + \bar{x}_2) = 1 - \frac{1}{m_1} \neq w_1$  as required

Then  $\mu(\bar{x}_1 + \bar{x}_2) = 1$  and  $w(\bar{x}_1 + \bar{x}_2) = 1 - \frac{1}{(q_1^{n_1} - 1)^2} \neq w_1$  as required. Finally, suppose t = 1 and  $R = M_n(\mathbb{F}_q)$ . Suppose for the sake of contradiction that  $n \geq 3$ . Since  $m = q^n$ ,  $w_2 = \frac{q^n}{q^n - 1}$ , and using the same notation as above,

that  $n \geq 3$ . Since  $m = q^n$ ,  $w_2 = \frac{q^n}{q^{n-1}}$ , and using the same notation as above,  $w(A) = w_1 = 1 - \frac{1}{(q^n - 1)(q^{n-1} - 1)}$ . As  $|M_n(\mathbb{F}_q)^{\times}| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1)$ , it follows by [5, Corollary 15] that

$$|R^{\times}|(w_2 - w_1) = q^{n(n-1)/2 + n-1} \prod_{i=1}^{n-2} (q^i - 1)$$

is an integral divisor of  $|R| = q^{n^2}$ . This only happens if n = 3 and q = 2, in which case,  $R = M_3(\mathbb{F}_2)$  and  $w_2 = \frac{8}{7}$ . It can be checked that  $\mu(0, RI) = -8$  and  $w(I) = \frac{22}{21} \neq w_2$ . The result follows.

### 4 The Order of Linear Codes

We establish results on the order of linear codes over finite Frobenius rings that will be needed later. First, we again fix some notation. **Definition 11** Let S be a non-empty subset of  $\mathbb{R}^k$ .

$$S^{\perp} := \{ x \in R^{k} : x \cdot s = 0 \text{ for all } s \in S \} < {}_{R}R^{k}, \\ C(S) := \{ (x \cdot s)_{s \in S \setminus \{0\}} : x \in R^{k} \} < {}_{R}R^{|S \setminus \{0\}|}, \\ M_{S} := \sum_{s \in S} sR < R^{k}_{R}.$$

Let  $S_1, ..., S_t$  be non-empty subsets of  $\mathbb{R}^k$ . We denote by  $C(S_1, ..., S_t)$  the left *R*-linear code of length  $\sum_{i=1}^t |S_i \setminus \{0\}|$  defined by

$$C(S_1, ..., S_t) := \{ ((x \cdot s_1)_{s_1 \in S_1 \setminus \{0\}}, ..., (x \cdot s_t)_{s_t \in S_t \setminus \{0\}}) : x \in \mathbb{R}^k \}$$

Given a  $k \times n$  matrix  $Y = [y_1, ..., y_n]$  over R with each  $y_i$  non-zero, we write C(Y) in place of  $C(\{y_1\}, ..., \{y_n\})$ . Then with respect to this notation, we have C = C(G).

**Lemma 12** Let  $S_1, ..., S_t$  be non-empty subsets of  $\mathbb{R}^k$ . Then the codes  $C(S_1, ..., S_t)$ and  $C(\sum_{i=1}^t M_{S_i})$  are isomorphic as left  $\mathbb{R}$ -modules. In particular,  $|C(S_1, ..., S_t)| = |C(\sum_{i=1}^t M_{S_i})|$ .

*Proof* Clearly, we have the left R-module isomorphisms

$$C(S_1, ..., S_t) \cong R^k / \bigcap_{i=1}^t S_i^{\perp} \text{ and } C\left(\sum_{i=1}^t M_{S_i}\right) \cong R^k / \left(\sum_{i=1}^t M_{S_i}\right)^{\perp}.$$

The result now follows from the fact that  $\left(\sum_{i=1}^{t} M_{S_i}\right)^{\perp} = \bigcap_{i=1}^{t} M_{S_i}^{\perp}$  and that for each  $i, S_i^{\perp} = M_{S_i}^{\perp}$ .

Since R is Frobenius, for any left or right ideal I of R, the average value of the homogeneous weight of its elements is also constant, that is,  $\sum_{x \in I} w(x) = \gamma |I|$  [12,14]. This gives the following two results.

**Lemma 13** (See also [26, Lemma 15]) Let  $M < R_R^k$ . Then every non-zero codeword  $c \in C(M)$  satisfies  $w(c) = \gamma |M|$ .

**Lemma 14 ([12])** For each  $i \in \{1, ..., n\}$ ,  $\sum_{c \in C} w(c_i) = \gamma |C|$ .

**Lemma 15** Let  $M \le R_R^k$ . Then |C(M)| = |M|.

*Proof* We count the total weight of the codewords of C(M) in two ways. Applying Lemmas 13 and 14 gives  $(|C(M)| - 1)\gamma|M| = (|M| - 1)\gamma|C(M)|$ .

**Corollary 16**  $|C| = |M_G|$ .

Proof  $C = C(G) \cong C(M_G)$  by Lemma 12. From Lemma 15 we then get  $|C| = |C(M_G)| = |M_G|$ .

# 5 Two-Weight Codes and Graphs

We determine relations between the parameters of a two-weight code and its corresponding Cayley graph. We will use the concept of the distance matrix of a code [5,10].

**Definition 17** The distance matrix of C is the  $|C| \times |C|$  matrix D with rows and columns indexed by the elements of C and whose (u, v)-th entry is  $D_{uv} = w(u-v)$  for  $u, v \in C$ . For each  $i \in \mathcal{I}$ , the  $i^{th}$  coordinate distance matrix of C is the  $|C| \times |C|$  matrix  $D_i$  defined by  $(D_i)_{uv} = w(u_i - v_i)$ .

**Definition 18 ([5,10])** We denote by  $\mathcal{X}$  the complex  $|C| \times |R^{\times}|n$  matrix whose components satisfy  $(\mathcal{X})_{c,(\lambda,i)} := \chi(c_i\lambda)$  for each  $c \in C$ ,  $i \in \{1,...,n\}$  and  $\lambda \in \mathbb{R}^{\times}$ . For each  $i \in \mathcal{I}$  we let  $\mathcal{X}_i$  be the  $|C| \times |R^{\times}|\eta_i$  submatrix of  $\mathcal{X}$  whose columns are those indexed by  $(j, \lambda)$  for  $j \in [i]$  and  $\lambda \in \mathbb{R}^{\times}$ .

Given a complex matrix X, we write  $X^*$  to denote the conjugate transpose matrix of X. We let J denote the  $|C| \times |C|$  all-ones matrix.

#### Theorem 19

(i) 
$$DJ = \gamma n |C| J$$
 and  
(ii)  $D^2 = \gamma |C| \left( \gamma \left( n^2 + \gamma \sum_{i \in \mathcal{I}} \delta_i \eta_i \right) J - \sum_{i \in \mathcal{I}} \delta_i \eta_i D_i \right).$ 

*Proof* The proof of (i) follows immediately from Lemma 14 since

$$(DJ)_{uv} = \sum_{x \in C} w(u - x) = \sum_{x \in C} w(x) = \sum_{i=1}^{n} \sum_{x \in C} w(x_i) = \gamma n |C|,$$

for any  $u, v \in C$ .

For fixed  $i, j \in \{1, ..., n\}$  and  $\lambda, \tau \in \mathbb{R}^{\times}$ , define

$$\Lambda: \mathbb{R}^n \longrightarrow \mathbb{R}: c = (c_1, ..., c_n) \mapsto c_j \tau - c_i \lambda.$$

Then  $\Lambda$  is the zero map on C if and only if  $g_j \tau - g_i \lambda = 0$ , in which case  $j \in [i]$ and  $g_j = g_i \tau_{ij}$ , which holds if and only if  $\tau_{ij} \tau - \lambda \in \operatorname{ann}_R(g_i)$ . It follows that

$$\begin{aligned} (\mathcal{X}^*\mathcal{X})_{(i,\lambda),(j,\tau)} &= \sum_{c \in C} \chi \left( c_j \tau - c_i \lambda \right) \\ &= \begin{cases} |\ker \Lambda \cap C| \text{ if } \Lambda(C) = \{0\}, \\ 0 & \text{otherwise.} \end{cases} \\ &= \begin{cases} |C| \text{ if } j \in [i] \text{ and } \lambda \in \tau_{ij} \tau + \operatorname{ann}_R(g_i), \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Then from Lemma 4,

$$((\mathcal{X}^*\mathcal{X})\mathcal{X}^*)_{(i,\lambda),c} = |C| \sum_{\substack{j \in [i] \\ +\operatorname{ann}_R(y_i)}} \overline{\chi}(x \cdot g_i \lambda) = |C| |R^{\times}| \frac{\eta_i}{|g_i R^{\times}|} \overline{\chi}(x \cdot g_i \lambda).$$

It is straightforward to show that  $\mathcal{X}^*J = 0$ ,  $\mathcal{X}_i\mathcal{X}_i^* = |R^{\times}|\eta_i(J - \gamma^{-1}D_i)$  and  $\mathcal{X}\mathcal{X}^* = |R^{\times}|(nJ - \gamma^{-1}D)$ . It follows that

$$\mathcal{X}^*(\mathcal{X}\mathcal{X}^*) = |R^{\times}|\mathcal{X}^*\left(J - \gamma^{-1}D\right) = -|R^{\times}|\gamma^{-1}\mathcal{X}^*D$$

and so for each  $i \in \mathcal{I}$ ,  $|C||R^{\times}|\frac{\eta_i}{|g_iR^{\times}|}\mathcal{X}_i^* + |R^{\times}|\gamma^{-1}\mathcal{X}_i^*D = 0$ . Then

$$0 = |C||R^{\times}|\sum_{i\in\mathcal{I}}\delta_i\mathcal{X}_i\mathcal{X}_i^* + |R^{\times}|\gamma^{-1}\mathcal{X}\mathcal{X}^*D,$$
  
=  $|C||R^{\times}|\sum_{i\in\mathcal{I}}\delta_i\eta_i(J-\gamma^{-1}D_i) + |R^{\times}|\gamma^{-1}(nJ-\gamma^{-1}D)D.$ 

The result now follows from (i).

The proof of the following corollary uses arguments similar to those in [5, 10].

**Corollary 20** Let C be a proper two-weight code with non-zero weights  $w_1 < w_2$ . Then  $\Gamma(C)$  is strongly regular if and only if there exist some  $\alpha, \beta \in \mathbb{R}$  such that  $\sum_{i \in \mathcal{I}} \delta_i \eta_i D_i = \alpha D + \beta (J - I)$ , in which case the eigenvalues  $K, \rho_1, \rho_2$  of  $\Gamma(C)$ satisfy

- (i)  $(w_2 w_1)K = w_2(|C| 1) \gamma n|C|,$ (ii)  $(w_2 w_1)\rho_1 = -w_2 + \frac{1}{2}\left(\gamma|C|\alpha \sqrt{\gamma^2|C|^2\alpha^2 + 4\gamma|C|\beta}\right),$ (iii)  $(w_2 w_1)\rho_2 = -w_2 + \frac{1}{2}\left(\gamma|C|\alpha + \sqrt{\gamma^2|C|^2\alpha^2 + 4\gamma|C|\beta}\right),$
- (iv)  $|R^{\times}|^2 |C|^2 \alpha^2$  and  $|R^{\times}| |C|^{\beta}$  are integers and  $\sqrt{|R^{\times}|^2 |C|^2 \alpha^2 + 4|R^{\times}||C|^{\beta}}$  is an integer divisible by  $\rho_2 - \rho_1$ .

Proof The adjacency matrix A of  $\Gamma(C)$  satisfies  $(w_2 - w_1)A = w_2(J - I) - D$ . Then from Equation (1),  $\Gamma(G)$  is strongly regular if and only if  $D^2$  is an  $\mathbb{R}$ -linear combination of D, J and I. Suppose there exist  $\alpha, \beta \in \mathbb{R}$  such that  $\sum_{i \in \mathcal{I}} \delta_i \eta_i D_i =$  $\alpha D + \beta (J-I)$ . Then any restricted eigenvalue  $\rho$  of A satisfies  $(w_2 - w_1)\rho = -w_2 - \theta$ , where  $\theta$  is a restricted eigenvalue of D. From Theorem 19, such  $\theta$  are roots of the polynomial  $x^2 + \gamma |C| \alpha + \gamma |C| \beta \in \mathbb{R}[x]$  which gives (ii) and (iii). Part (iv) follows since the homogeneous weight is integer-valued for  $\gamma = |R^{\times}|$  and so, using (ii) and (iii), we get  $(w_2 - w_1)(\rho_2 - \rho_1) = \sqrt{|R^{\times}|^2 |C|^2 \alpha^2 + 4|R^{\times}||C|\beta} \in \mathbb{Z}$ . The rest can be deduced from (ii). П

*Example 2* Let  $R = \mathbb{Z}_6$  and let C be the code generated by [2 3 2 2 2 3 3]. C is a two-weight code of order 6 with normalized weights  $w_1 = 6, w_2 = 12$ . Then  $\mathcal{I} = \{1, 2\}, \ \delta_1 = 2, \delta_2 = 3, \ \eta_1 = 4 \ \text{and} \ \eta_2 = 3.$  Then  $\Gamma(C)$  is strongly regular if and only if there exist  $\alpha, \beta \in \mathbb{Q}$  such that  $8w(c_1) + 9w(c_2) = \alpha w(c) + \beta$  for all non-zero  $c \in C$ . It is easy to check that no such  $\alpha$  and  $\beta$  exist.

*Example 3* Let  $R = \mathbb{Z}_4$  and  $M_1 = \mathbb{Z}_4(0,1), M_2 = \mathbb{Z}_4(1,0) \leq \mathbb{Z}_4^2$ . Then C = $C(M_1, M_2, \mathbb{Z}_4^2)$  is a non-modular two-weight code with normalized weights  $w_1 =$ 20,  $w_2 = 24$ . As  $\alpha = 3$ ,  $\beta = -24$  satisfy  $\sum_{i \in I} \delta_i \eta_i w(c_i) = \alpha w(c) + \beta$  for all non-zero  $c \in C$ ,  $\Gamma(C)$  is strongly regular (in fact  $\Gamma(C)$  is an OA(4, 2)-type strongly regular graph).

These existence criteria are greatly simplified for the case  $\beta = 0$ , in which case the eigenvalues of D are 0 and  $\gamma |C| \alpha$ .

**Corollary 21** Let C be a proper two-weight code with non-zero weights  $w_1 < w_2$ and suppose that  $\sum_{i \in \mathcal{I}} \delta_i \eta_i D_i = \alpha D$  for some  $\alpha \in \mathbb{R}$ . Let  $\Gamma(C)$  have restricted eigenvalues  $\rho_1 < \rho_2$ . Then

(i)  $\rho_2 - \rho_1$  is an integral divisor of  $|R^{\times}||C|\alpha$ ;

(ii) 
$$w_1 = \frac{\gamma |C|(\rho_1 + 1)\alpha}{(\rho_1 - \rho_2)}$$
 and  $w_2 = \frac{\gamma |C|(\rho_1 \alpha)}{(\rho_1 - \rho_2)};$   
(iii) the multiplicities  $m_1$  and  $m_2$  of  $\rho_1$  and  $\rho_2$ , respectively, satisfy

$$m_1 = |C| - 1 - \frac{n}{\alpha}$$
 and  $m_2 = \frac{n}{\alpha}$ .

In particular, if C satisfies the hypothesis of Corollary 21, then  $\alpha \in \mathbb{Q}$ .

**Corollary 22** Let C satisfy the hypothesis of Corollary 21. Then  $\Gamma(C)$  is imprimitive if and only if  $w_2 = \gamma \alpha |C|$ .

Proof Using Part (ii) of Corollary 21 we see that  $w_2 = \gamma \alpha |C|$  if and only if  $\rho_2 = 0$ , in which case the complement of  $\Gamma(C)$  is disconnected. If  $\Gamma(C)$  itself is disconnected then we have  $\rho_1 = -1$ , which, again from Part (ii), yields  $w_1 = 0$ , giving a contradiction. П

## 6 Modular Two-Weight Codes

The code C is modular if for each  $i \in \mathcal{I}$ ,  $\delta_i = \delta = \alpha$  and  $\beta = 0$ . We have the following result.

**Corollary 23** Let C be a  $\delta$ -modular code. Then 1

$$D^{2} + \gamma |C|\delta D = n\gamma^{2} |C| (\gamma \delta + n) J.$$

In particular, if C is a proper two-weight code, then  $\Gamma(C)$  is strongly regular.

*Proof* This follows immediately from Theorem 19, since  $\delta_i = \delta$  for each i and  $\sum_{i\in\mathcal{I}}\eta_i=n.$ П

We remark that it was already known that a proper modular two-weight code has a strongly regular Cayley graph: Honold asserted this in [15]. A proof may be read in [16, Theorem 12], which appeared on arXiv.org during the review of this paper. An important component of our approach is that Corollaries 21 and 23 yield explicit relations between the weights of a proper modular two-weight code C and the eigenvalues of  $\Gamma(C)$  in the form of Corollary 26. This provides useful existence criteria for modular two-weight codes and their corresponding strongly regular Cayley graphs.

We now consider existence questions for modular two-weight codes. We first show that we may assume  $\delta = 1$  without loss of generality.

**Lemma 24** Let C be a  $\delta$ -modular two-weight code with non-zero weights  $0 < w_1 < \delta$  $w_2$ . Then there exists a 1-modular two-weight code  $C' \leq {}_R R^{n'}$  of order |C'| = |C|and length  $n' = n\delta^{-1}$  with non-zero weights  $w'_1 = w_1\delta^{-1}$  and  $w'_2 = w_2\delta^{-1}$  such that  $\Gamma(C)$  is isomorphic to  $\Gamma(C')$ .

*Proof* Let G' be the  $k \times \sum_{i \in \mathcal{I}} |g_i R^{\times}|$  matrix formed by replacing, for each  $i \in \mathcal{I}$  the  $\eta_i$  columns that are unit multiples of  $g_i$  with some (not necessarily distinct)  $|g_i R^{\times}|$ unit multiples of  $g_i$ . Then C' = C(G') has length  $n' = \sum_{i \in \mathcal{I}} |g_i R^{\times}| = \sum_{i \in \mathcal{I}} \frac{\eta_i}{\delta} =$  $\frac{n}{\delta}$  and is 1-modular. The order of C' is  $|C'| = |M_{G'}| = |M_G|$  by Lemma 16 and so there is a one-to-one correspondence between the words of C and C'. Explicitly, given any  $c = xG \in C$ , let c' = xG' be the corresponding codeword in C'. Clearly for any  $i \in \mathcal{I}$ ,  $w(c'_i) = w(c_i)$ , so that

$$w(c') = \sum_{i \in \mathcal{I}} |g_i R^{\times}| w(c'_i) = \sum_{i \in \mathcal{I}} |g_i R^{\times}| w(c_i) = \sum_{i \in \mathcal{I}} \frac{\eta_i}{\delta} w(c_i) = \delta^{-1} w(c).$$

Then C' is a 1-modular two-weight code with  $\Gamma(C')$  isomorphic to  $\Gamma(C)$ .

We now show that if C is a 1-modular two-weight code, there exists a 1-modular two-weight code C' such that  $\Gamma(C')$  is isomorphic to  $\Gamma(C)^c$ , the complement of  $\Gamma(C).$ 

**Lemma 25** Suppose C is a primitive, proper 1-modular two-weight code with nonzero normalized weights  $0 < w_1 < w_2$ . Then  $C' = C(M_G \setminus \bigcup_{i=1}^n g_i R^{\times})$  is a proper, 1-modular two-weight code of order |C| with non-zero normalized weights  $w'_1 < w'_2$ where  $w'_1 = |C| - w_2$  and  $w'_2 = |C| - w_1$ . Moreover,  $\Gamma(C)^c$  is isomorphic to  $\Gamma(C')$ .

*Proof* As C is 1-modular, C' is 1-modular. Now if xG = 0 then  $x \in M_G^{\perp}$  and xG' = 0. By Lemma 13, for any  $x \in \mathbb{R}^k$  such that  $xG \neq 0$ , w(xG') + w(xG) = w(xG') + w(xG) $|M_G| = |C|$ . As  $\Gamma$  is primitive, Corollary 22 implies  $w_2 < |C|$  and  $|C| - w_2 > 0$ . Then C' is a two-weight code with the weights claimed. Further, if w(xG') = 0, xG = 0 (else we would have w(xG) = |C|) and so xG' = 0. It follows that C' is proper and |C| = |C'|. Finally, as  $w(xG) = w_1$  if and only if  $w(xG') = w'_2$ ,  $\Gamma(C)^c$ is isomorphic to  $\Gamma(C')$ .

**Corollary 26** Let  $\Gamma$  be a strongly regular graph with parameters  $(N, K, \lambda, \mu)$  and restricted eigenvalues  $\rho_1 < \rho_2$  of multiplicities  $m_1, m_2$  respectively. Then  $\Gamma$  is the Cayley graph of a  $\delta$ -modular two-weight code over R if and only if  $\Gamma$  is isomorphic to  $\Gamma(C)$ , where C is a 1-modular two-weight code with non-zero weights  $w_1, w_2$ such that the following hold.

(i) |C| = N and  $\rho_1 - \rho_2$  is an integer dividing N. (ii)

$$w_1 = \frac{(\rho_1 + 1)N}{\rho_1 - \rho_2}$$
 and  $w_2 = \frac{\rho_1 N}{\rho_1 - \rho_2}$ .

- (iii) The length of C is given by  $n = m_2$ .
- (iv)  $C' = C(M_G \setminus \bigcup_{i=1}^n g_i R^{\times})$  has length  $n' = m_1$ , two non-zero weights  $w'_1 =$  $N - w_2, w'_2 = N - w_1$  and  $\Gamma(C')$  is a strongly regular graph with parameters  $(N, N - K - 1, N - 2K + \mu - 2, N - 2K + \lambda).$

This result can be used to analyse a feasible parameter set  $(N, K, \lambda, \mu)$  [2] of a strongly regular graph that might arise from a modular two-weight code C, or conversely to check the existence of a modular two-weight code. Moreover, if a strongly regular graph is the Cayley graph of a modular two-weight code, so is its complement, thus it suffices to check parameters up to complements only. For

example, the first constraint " $\rho_1 - \rho_2$  divides N" shows that at most 732 of the 2140 feasible parameters sets (counted up to complements) for graphs on at most 1300 vertices listed in [2] could be the parameters of a strongly regular graph  $\Gamma(C)$  for a modular two-weight code C. Among these there are 1514 putative parameter sets, for which graph existence is not known, and only 433 of these could come from a modular two-weight code.

A search was carried out in [5] for the sub-class of regular projective twoweight codes. There are significant differences between this and the more general case of modular codes. In the first instance, the complement of a strongly regular graph  $\Gamma(C)$  coming from a two-weight code C does not necessarily arise from a regular-projective two-weight code, so any search cannot exclude complementary parameters. Secondly, in the projective, regular case, N = |C| is an upper bound on |R|. It is therefore often possible to produce an exhaustive list of candidate coefficient rings over which search can be conducted. A further complication in both cases is that canonical descriptions of generator matrices for rings that are not direct products of chain rings are not known in general, making a complete search a very difficult task. We remark that in the regular projective case, out of the 2956 (up to complements 1514) putative parameter sets for which the existence of a graph is not yet known, there remain only 82 open cases. All regular projective two-weight codes found by the search had order the square of a prime power.

Example 4 The parameter set (64, 36, 20, 20) corresponds to a graph with eigenvalues -4,4 and respective multiplicities 27, 36. Any 1-modular two-weight code determining a graph with these parameters has order 64, length 27 and normalized weights  $w_1 = 24, w_2 = 32$ . Over  $R = M_2(\mathbb{F}_2) \oplus \mathbb{F}_4$ , we suppose C is generated by a single codeword c and the identity element (I, 1) of R is a coordinate of c. Then 18 entries of c are units in R and they contribute weight 20 to c. By examining the weights of the ring elements, we see the remaining nine coordinates of c must have total weight 12 and therefore be ring elements of the form (A, 0), where A has rank 1 in  $M_2(\mathbb{F}_2)$ . It can be checked that the following vector generates a  $\frac{1}{3}$ -modular version of the required code:

$$\left[ (I,1), (I,1), (I,1), (I,1), (I,1), (I,1), \left( \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, 0 \right), \left( \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, 0 \right), \left( \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, 0 \right) \right]$$

Example 5 Consider the feasible parameter set (96, 45, 24, 18). Suppose that a strongly regular graph  $\Gamma$  for such parameters exists, in which case it has eigenvalues -3, 9, with multiplicities 75 and 20, respectively. Suppose that C is a two-weight code over  $R = \mathbb{F}_{32} \oplus \mathbb{F}_3$  satisfying  $\Gamma = \Gamma(C)$ . Let  $k \in \mathbb{Z}$ , and let  $g \in R^k$  have  $(u, a) \in R$  in some coordinate, with  $u \neq 0$ . Then as  $|gR^{\times}| \geq 31$ , if the vectors in the projective class of g are columns in  $G, n \geq 31$ . This contradicts  $n = m_2 = 20$ . It follows that every coordinate of every vector of  $R_R^k$  that is a column of G must be of the form (0, a) and thus  $|C| = 3^b$ , for some  $b \in \mathbb{N}$ , giving a contradiction.

### 7 Codes, Arrays and Graphs

In the following section we show that modular two-weight codes can be constructed by taking unions of submodules of  $R_R^k$  with pairwise trivial intersection. We thus illustrate connections between two-weight codes, orthogonal arrays and partial congruence partitions.

These examples establish the existence of primitive (those codes C such that  $\Gamma(C)$  is primitive) modular two-weight codes over any finite Frobenius ring R and of any square order N > 4. No regular, projective two-weight codes of non-prime-power order are known to exist and their existence has been excluded for numerous non-prime-power square orders [5]. In fact, this construction is the only known infinite family of primitive two-weight codes over rings whose orders are not all prime powers.

We first show certain (not necessarily two-weight) codes can be used to construct orthogonal arrays and strongly regular graphs. We will use the following result.

**Lemma 27** Let  $S_1, \ldots, S_t \subseteq R^k, t \geq 2$ . Then for every  $x \in R^k, |\{i : x \in S_i^{\perp}\}| \in \{0, 1, t\}$  if and only if for all distinct  $i, j \in \{1, \ldots, t\}, M_{S_i} + M_{S_j} \supseteq M_{S_l}$  for all  $l \in \{1, \ldots, t\}$ .

Proof We have  $M_{S_i} + M_{S_j} \supseteq M_{S_l}$  if and only if  $(M_{S_i} + M_{S_j})^{\perp} \subseteq M_{S_l}^{\perp}$  which holds if and only if  $M_{S_i}^{\perp} \cap M_{S_j}^{\perp} \subseteq M_{S_l}^{\perp}$ . Since  $S_i^{\perp} = M_{S_i}^{\perp}$ , any  $x \in \mathbb{R}^k$  is contained in exactly one, none or all  $S_i^{\perp}$ .

Let  $S_1, \ldots, S_t \subseteq \mathbb{R}^k$ . For each  $i \in \{1, \ldots, t\}$  and  $c \in C(S_1, \ldots, S_t)$ , let  $\Pi_i(c) \in C(S_i)$  be the projection of c onto the coordinates indexed by the elements of  $S_i$ . Define a graph  $H(S_1, \ldots, S_t)$  whose vertices are the codewords of  $C(S_1, \ldots, S_t)$  and where two vertices c, c' are adjacent if and only if  $\Pi_i(c) = \Pi_i(c')$  for some  $i \in \{1, \ldots, t\}$ .

**Theorem 28** Let  $t \ge 2$  and let  $S_1, \ldots, S_t \subset \mathbb{R}^k$  be a family of sets satisfying

- (i)  $|M_{S_i}| = v$  for all *i*. (ii)  $M_G \cap M_G = \{0\}$  for
- (ii)  $M_{S_i} \cap M_{S_j} = \{0\}$  for all i, j. (iii)  $M_{S_i} + M_{S_j} \supseteq M_{S_\ell}$  for all  $i, j, \ell \in \{1, ..., t\}$  with  $i \neq j$ .

Then  $H(S_1, ..., S_t)$  is an OA(v, t)-type graph.

*Proof* By Lemmas 12 and 15,  $|C(S_i)| = |M_{S_i}| = v$  for each *i* and

$$|C(S_1, ..., S_t)| = |C(M_{S_1}, ..., M_{S_t})| = |\sum_{i=1}^t M_{S_i}| = |M_{S_i} + M_{S_j}| = v^2,$$

for any distinct i and j. We now construct an OA(v, t) from  $C(S_1, ..., S_t)$ . Let V be an arbitrary v-set. For each i, let  $f_i : C(S_i) \to V$  be a bijection. Then define maps

$$F: C(S_1, ..., S_t) \to V^t: c \mapsto (f_1(\Pi_1(c)), f_2(\Pi_2(c)), ..., f_t(\Pi_t(c))),$$
  
$$F_{ij}: C(S_i, S_j) \to V^2: c \mapsto (f_i(\Pi_i(c)), f_j(\Pi_j(c))).$$

Arrange  $\{F(c) : c \in C\}$  as the rows of an array, A. As  $|C(S_i, S_j)| = |M_{S_i} + M_{S_j}| = v^2$  for any distinct *i* and *j*, the map  $F_{ij}$  is a bijection. Then every element of  $V \times V$  occurs exactly once in the  $i^{th}$  and  $j^{th}$  columns of A, which we then conclude is an OA(v, t).

Finally, we show  $H(S_1, ..., S_t)$  is isomorphic to  $\Gamma(A)$ . Let  $c, c' \in C(S_1, ..., S_t)$ . Now (c, c') is an edge of  $H(S_1, ..., S_t)$  if and only if there exists a unique *i* such that  $\Pi_i(c - c') = 0$ , or equivalently,  $\Pi_i(c) = \Pi_i(c')$ . This holds if and only if  $f_i(\Pi_i(c)) = f_i(\Pi_i(c'))$  which is precisely the condition needed for F(c) and F(c') to be adjacent in  $\Gamma(A)$ .

We now show that a modular two-weight code can be constructed from any family of subsets of  $R_R^k$  satisfying Theorem 28. This generalises a well-known construction for two-weight codes over  $\mathbb{F}_q$  that takes unions of subspaces of  $\mathbb{F}_q^k$  (cf. [7]).

**Corollary 29** Let  $S_1, \ldots, S_t, t \ge 2$  be subsets of  $R_R^k$  satisfying the hypothesis of Theorem 28 with t < v + 1. For each  $i \in \{1, ..., t\}$  write  $\overline{M}_i = M_{S_i} \setminus \{0\}$ . Let  $Y = [(y_1)_{y_1 \in \overline{M}_1}, ..., (y_t)_{y_t \in \overline{M}_t}]$ . Then

- (i)  $C(Y) = C_Y$  is a 1-modular two-weight code of order  $v^2$  with non-zero weights  $w_1 = (t-1)v$  and  $w_2 = tv$ ,
- (ii)  $\Gamma(C_Y)$  is an OA(v, t)-type graph.

Proof We first show  $C_Y$  is a two-weight code. For each  $c \in C_Y$ , let  $\pi_i(c)$  denote the projection of c onto the coordinates corresponding to the v-1 non-zero elements of  $M_{S_i}$ . Let  $c = xY \in C_Y$  for some  $x \in \mathbb{R}^k$ . Then  $\pi_i(c) = 0$  if and only if  $x \in M_{S_i}^{\perp}$  and so we compute

$$w(xY) = \sum_{i=1}^{t} w(\pi_i(xY)) = tv - |\{i : x \in S_i^{\perp}\}|v$$

If follows by Lemma 27 that  $C_Y$  has non-zero weights  $w_1 = (t-1)v$  and  $w_2 = tv$ (since t < v + 1, C is not a constant weight code). Then  $C_Y$  is a 1-modular two-weight code and by Corollary 20,  $\Gamma(C_Y)$  is a strongly regular graph with parameters

$$(v^{2}, t(v-1), v-2 + (t-1)(t-2), t(t-1)).$$

It is easy to see that  $\Gamma(C_Y)$  is isomorphic to  $H(C(S_1, ..., S_t))$  since  $w(c-c') = w_1$ if and only if there exists a unique *i* such that  $\pi_i(c) = \pi_i(c')$ .

Remark 1 Not every modular two-weight code produced by Theorem 28 has Cayley graph  $\Gamma(C)$  isomorphic to H(C). Let p be a prime and C the code over  $R = \mathbb{Z}_{p^2}$  generated by

$$\begin{bmatrix} 1 & 0 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & (p-1) \end{bmatrix} \in R^{2 \times (p+1)}.$$

Then C satisfies the conditions of Theorem 28 and H(C) is an  $OA(p^2, p+1)$ -type graph. On the other hand, as observed in [3, Proposition 6.2], C is a regular, projective two-weight code and  $\Gamma(C)$  has the parameters of the strongly regular graph from an  $OA(p^2, p)$ .

Remark 2 Corollary 29 Part (i) can also be arrived at by combining [22, Proposition 3.4] and Theorem 17 of the preprint [16] as follows. Let Y and  $C_Y$  be as in Corollary 29. Then  $\bigcup_{i=1}^{t} \overline{M}_i$  is a partial difference set by [22, Proposition 3.4], and so  $C_Y$  is a two-weight code by [16, Theorem 17].

Given  $S_1, ..., S_t \subset \mathbb{R}^k$  satisfying the hypothesis of Theorem 28, the set of modules  $\mathcal{M} = \{M_{S_1}, ..., M_{S_t}\}$  is an example of a *partial congruence partition* [1, Definition 9.3], for the group  $(G, +) = (M_{S_i} + M_{S_j}, +)$ , or equivalently a *translation net*. If R is a finite field then  $\mathcal{M}$  is a *partial-spread*.

Jungnickel characterized all partial congruence partitions in  $(\mathbb{Z}_q^k, +)$  [17, Theorem 2.1]. The argument given therein and outlined briefly below extends immediately for submodules of  $R_R^k$  and allows us to describe all such sets  $\mathcal{M}$ .

Let  $\mathcal{M} = \{M_1, ..., M_t\}$  for some  $M_i < R_R^k$  such that for some  $M < R_R^k$ ,  $M = M_i \oplus M_j$  for each pair of distinct  $i, j \in \{1, ..., t\}$ . Then the  $M_i$  are all isomorphic as right *R*-modules. Let  $a \in M_i$  for some  $i \geq 3$ . Then a = x + y for uniquely determined  $x \in M_1, y \in M_2$ . In particular, there is a bijection  $\sigma : M_1 \longrightarrow M_2$  such that  $M_i = \{x + \sigma(x) : x \in M_1\}$  and in fact  $\sigma$  must be a right *R*-module isomorphism.

We hence give an explicit construction of two-weight codes arising from Corollary 29, which is essentially unique.

**Construction 30** Let  $M_1, M_2 < R_R^k$  be isomorphic as right R-modules and have order v. Let  $\operatorname{Hom}_R(M_1, M_2)$  denote the additive group of right R-module homomorphisms from  $M_1$  onto  $M_2$ . Let  $\Sigma$  be an m-subset of the isomorphisms of  $\operatorname{Hom}_R(M_1, M_2)$  such that  $\sigma - \tau$  is an isomorphism for any distinct  $\sigma, \tau \in \Sigma$ . Then

$$\mathcal{M} = \{M_1, M_2, \{x + \sigma(x) : x \in M_1\} : \sigma \in \Sigma\}$$

forms a set of submodules of  $R_R^k$  satisfying the conditions of Corollary 29. Let Y be the  $k \times n$  matrix whose columns comprise the non-zero elements in the union of the submodules of  $\mathcal{M}$  and let C = C(Y). Then

- C has order  $v^2$ , length n = (m+2)(v-1) and exactly two non-zero normalized homogeneous weights  $w_1 = (m+1)v$ ,  $w_2 = (m+2)v$ ;
- $\Gamma(C)$  is an OA(v, m+2)-type graph.

Construction 30 gives all possible matrices Y and two-weight codes C(Y), formed as in the statement of Corollary 29. Note that orthogonal arrays with the above parameters were known to exist (see for example [23]), independently of these constructions.

Example 6 Let  $k = 2\ell$ , let R be commutative and let  $A \cong R^{\ell}$ . Let  $\Sigma$  be an *m*-subset of the invertible matrices of  $M_{\ell}(R)$  such that the difference between any pair of elements of  $\Sigma$  represents an element of  $\operatorname{Aut}_{R}(A)$ . Then the  $k \times n$  matrix Y whose columns comprise the elements of

$$\{(x,0),(0,x),(x,Lx):x\in A\backslash\{0\},L\in\Sigma\}\subset R^{k}$$

generates a code C(Y) of order  $|A|^2$ , length n = (m+2)(|A|-1) having two non-zero normalized weights  $w_1 = (m+1)|A|$ ,  $w_2 = (m+2)|A|$ . It is easy to see that m is less than the size of any minimal left ideal of  $M_{\ell}(R)$ .

Example 7 Let  $\ell = 2$ , let  $R = \mathbb{Z}_{pq}$  for primes p < q, and let  $M = R^2$ . For  $i \in \{1, ..., p-1\}$ , define  $\sigma_i : R^2 \to R^2, \sigma_i(x) = ix$ . Then  $\Sigma = \{\sigma_1, \ldots, \sigma_{p-1}\} \subset \operatorname{Aut}(R^2), m = |\Sigma| = p-1$  and  $\sigma_i - \sigma_j \in \operatorname{Aut}(R^2)$  for distinct i and j.  $\Sigma$  determines

a two-weight code C of order  $p^4q^4$  and length  $(p+1)(p^2q^2-1)$  with  $w_1 = p^3q^2$ and  $w_2 = (p+1)p^2q^2$ .  $\Gamma(C)$  is an  $OA(p^2q^2, p+1)$ -type graph. C is generated by

$$\left[ \begin{pmatrix} 0 \\ x \end{pmatrix}_{x \in M \setminus \{0\}} \middle| \begin{pmatrix} x \\ 0 \end{pmatrix}_{x \in M \setminus \{0\}} \middle| \begin{pmatrix} x \\ x \end{pmatrix}_{x \in M \setminus \{0\}} \middle| \cdots \middle| \begin{pmatrix} x \\ (p-1)x \end{pmatrix}_{x \in M \setminus \{0\}} \right]$$

**Construction 31** Let  $a \in R \setminus \{0\}$ . Choose  $U \subseteq R^{\times}$  of order m such that for every distinct  $u_i, u_j \in U, u_i - u_j$  is a unit. Let

$$\mathcal{M} = \{(1,0)aR, (0,1)aR, (1,u_1)aR, \dots, (1,u_m)aR\}.$$

 $\mathcal{M}$  forms a set of submodules of  $R_R^2$  as special case of Construction 30 with  $\ell = 1$ and  $A_1 = A_2 = aR$ . Let Y be the  $2 \times n$  matrix whose columns comprise the non-zero elements in the union of these submodules and let C = C(Y). Then

- C has order  $|aR|^2$ , length n = (m+2)(|aR|-1) and non-zero normalized weights  $w_1 = (m+1)|aR|$ ,  $w_2 = (m+2)|aR|$ ;
- $\Gamma(C)$  is an OA(|aR|, m+2)-type graph;
- $-m < \min\{|I| : I \triangleleft R_R\}.$

*Example 8* Let a = 1 and  $U = \{1\}$ . The corresponding two-weight code C has length 3|R| - 3, order  $|R|^2$  and non-zero weights  $w_1 = 2|R|$ ,  $w_2 = 3|R|$ .  $\Gamma(C)$  is an OA(|R|, 3)-type graph. G has the structure

$$\left[ \begin{pmatrix} 0 \\ r \end{pmatrix}_{r \in R \setminus \{0\}} \middle| \begin{pmatrix} r \\ 0 \end{pmatrix}_{r \in R \setminus \{0\}} \middle| \begin{pmatrix} r \\ r \end{pmatrix}_{r \in R \setminus \{0\}} \right]$$

*Example 9* Let  $R = \mathbb{Z}_{pq}$  for primes p < q. Then R has the non-trivial proper ideals pR and qR. Let  $U = \{1, ..., p-1\}$ . Then  $U \subset R^{\times}, m = |U| = p - 1$  and the difference between any pair of elements of U is a unit in R. Then U yields 3 two-weight codes and orthogonal arrays with parameters as indicated in the following table.

|    | n           | $w_1$  | $w_2$   | OA( aR , p+1) |
|----|-------------|--------|---------|---------------|
| pR | (p+1)(q-1)  | pq     | (p+1)q  | OA(q, p+1)    |
| qR | (p+1)(p-1)  | $p^2$  | (p+1)p  | OA(p, p+1)    |
| R  | (p+1)(pq-1) | $p^2q$ | (p+1)pq | OA(pq, p+1)   |

Example 10 Let S be a finite Frobenius ring,  $R = M_2(S), U_1 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, U_2 = \begin{bmatrix} 0 & 1 \end{bmatrix}$ 

 $\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ . Let  $U = \{I, U_1, U_2\}$  and let a = I. Then a and U determine a two-weight code C of order  $|S|^8$  and length  $5(|S|^4 - 1)$  with  $w_1 = 4|S|^4, w_2 = 5|S|^4$ .  $\Gamma(C)$  is an  $OA(|S|^4, 5)$ -type graph. The structure of a generator matrix for C is given by

$$\left[ \begin{pmatrix} 0 \\ A \end{pmatrix}_{A \in R \setminus \{0\}} \middle| \begin{pmatrix} A \\ 0 \end{pmatrix}_{A \in R \setminus \{0\}} \middle| \begin{pmatrix} A \\ A \end{pmatrix}_{A \in R \setminus \{0\}} \middle| \begin{pmatrix} A \\ U_1 A \end{pmatrix}_{A \in R \setminus \{0\}} \middle| \begin{pmatrix} A \\ U_2 A \end{pmatrix}_{A \in R \setminus \{0\}} \right].$$

Acknowledgement: The authors would like to thank the anonymous reviewers for their comments and suggestions, which has led to a great improvement in the presentation of this paper.

## References

- 1. Beth, T., Jungnickel, D., Lenz, H. (eds.): Design Theory, second edn. Discrete Mathematics and its Applications (Boca Raton). Cambridge University Press (1999)
- 2. Brouwer, A.E.: Tables of parameters of strongly regular graphs. http://www.win.tue.nl/~aeb/graphs/srg/srgtab.html
- Byrne, E., Greferath, M., Honold, T.: Ring geometries, two-weight codes, and strongly regular graphs. Des. Codes Cryptogr. 48(1), 1–16 (2008)
   Byrne, E., Greferath, M., Kohnert, A., Skachek, V.: New bounds for codes over finite
- Byrne, E., Greferath, M., Kohnert, A., Skachek, V.: New bounds for codes over finite Frobenius rings. Des. Codes Cryptogr. 57(2), 169–179 (2010)
- 5. Byrne, E., Kiermaier, M., Sneyd, A.: Properties of codes with two homogeneous weights. Finite Fields Appl. 18(4), 711–727 (2012)
- Byrne, E., Sneyd, A.: Constructions of two-weight codes over finite rings. Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010) (2010)
- 7. Calderbank, R., Kantor, W.M.: The geometry of two-weight codes. Bull. London Math. Soc. 18(2), 97–122 (1986)
- Cameron, P.J., van Lint, J.H.: Graphs, codes and designs, London Mathematical Society Lecture Note Series, vol. 43. Cambridge University Press, Cambridge (1980)
- Colbourn, C.J., Dinitz, J.H. (eds.): Handbook of combinatorial designs, second edn. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL (2007)
- Delsarte, P.: Weights of linear codes and strongly regular normed spaces. Discrete Math. 3, 47–64 (1972)
- 11. Godsil, C., Royle, G.: Algebraic graph theory, *Graduate Texts in Mathematics*, vol. 207. Springer-Verlag, New York (2001)
- Greferath, M., Schmidt, S.E.: Finite-ring combinatorics and MacWilliams' equivalence theorem. J. Combin. Theory Ser. A 92(1), 17–28 (2000)
- Hedayat, A.S., Sloane, N.J.A., Stufken, J.: Orthogonal arrays. Springer Series in Statistics. Springer-Verlag, New York (1999)
- Honold, T.: Characterization of finite Frobenius rings. Arch. Math. (Basel) 76(6), 406–415 (2001)
- 15. Honold, T.: Further results on homogeneous two-weight codes. Proceedings of Optimal Codes and Related Topics, Bulgaria (2007)
- 16. Honold, T.: The geometry of homogeneous two-weight codes. arXiv:1401.7414 (2014)
- 17. Jungnickel, D.: Partial spreads over  $Z_q$ . Linear Algebra Appl. 114/115, 95–102 (1989)
- 18. Konstantinesku, I., Khaĭze, V.: A metric for codes over residue class rings of integers. Problemy Peredachi Informatsii 33(3), 22–28 (1997)
- Lam, T.Y.: Lectures on modules and rings, Graduate Texts in Mathematics, vol. 189. Springer-Verlag, New York (1999)
- Lam, T.Y.: A first course in noncommutative rings, Graduate Texts in Mathematics, vol. 131, second edn. Springer-Verlag, New York (2001)
- van Lint, J.H., Wilson, R.M.: A course in combinatorics, second edn. Cambridge University Press, Cambridge (2001)
- 22. Ma, S.: Partial difference sets. Discrete Mathematics 52(1), 75–89 (1984)
- MacNeish, H.F.: Euler squares. Ann. of Math. (2) 23(3), 221–227 (1922)
   Nechaev, A.A., Honold, T.: Fully weighted modules and representations of codes. Problemy Peredachi Informatsii 35(3), 18–39 (1999)
- Stinson, D.R.: Cryptography. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL (1995)
- 26. Wood, J.: Relative one-weight codes. Designs, Codes and Cryptography 76 (2012)
- Wood, J.A.: Duality for modules over finite rings and applications to coding theory. Amer. J. Math. 121(3), 555–575 (1999)