On the Parameters of Codes with Two Homogeneous Weights

Eimear Byrne, Alison Sneyd

On the Parameters of Codes with Two Homogeneous Weights

Eimear Byrne and Alison Sneyd*

School of Mathematical Sciences, University College Dublin, Ireland
ebyrne@ucd.ie, alison.sneyd@ucdconnect.ie

Abstract. Delsarte showed that for any projective linear code over a finite field $GF(p^r)$ with two nonzero Hamming weights $w_1 < w_2$ there exist positive integers u and s such that $w_1 = p^s u$ and $w_2 = p^s(u + 1)$. Moreover, he showed that the additive group of such a code has a strongly regular Cayley graph. Here we show that for any proper, regular, projective linear code C over a finite Frobenius ring with two integral nonzero homogeneous weights $w_1 < w_2$ there is a positive integer d, a divisor of $|C|$, and positive integer u such that $w_1 = du$ and $w_2 = d(u+1)$. In doing so, we present a new proof that any such code yields a strongly regular graph.

1 Introduction

The homogeneous weight, introduced for integer residue rings in [7] and extended for arbitrary finite rings in [10], has been studied extensively in the context of ring-linear coding. It can be viewed as a generalization of the Hamming weight; in fact it coincides with the Hamming weight when the underlying ring is a finite field and is the Lee weight when defined over $\mathbb{Z}_4$.

Many of the classical results for codes over finite fields for the Hamming weight have corresponding homogeneous weight versions for codes over finite rings. In particular, in [2] it was shown that strongly regular graphs can be constructed from codes over finite Frobenius rings with exactly two nonzero homogeneous weights.

In this paper, we examine properties of the parameters of a regular projective two-weight code over a finite Frobenius ring. We obtain the analogue of a result of Delsarte [8, Corollary 2], namely that such a code C must have nonzero homogenous weights of the form $w_1 = du$ and $w_2 = d(u + 1)$ (after scaling by $|R^\times|$), where d is a divisor of $|C|$ and u is a positive integer. This emerges by an analysis of the eigenvalues of the Cayley graph Γ of C, which turns out to have exactly 3 distinct eigenvalues and is therefore strongly regular. The integer u mentioned above has the value $-\rho - 1$, where ρ is the least eigenvalue of Γ.

* Work supported by Science Foundation of Ireland grant 08/RFP/MTH1181

2 Preliminaries

2.1 Finite Rings and Homogeneous Weights

We recall some properties of finite rings that meet our purposes, many of which are discussed in [16]. For a finite ring R, we denote by $\hat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^{\times})$, the group of additive characters of R. $\hat{R}$ is an R-R bimodule according to the relations

$$ {}^{r}\chi(x) = \chi(rx), \quad \chi^{r}(x) = \chi(xr) $$

for all $x, r \in R, \chi \in \hat{R}$. A character χ is called left (resp. right) generating if given any $\phi \in \hat{R}$ there is some $r \in R$ satisfying $\phi = {}^{r}\chi$ (resp. $\phi = \chi^{r}$). The next result gives a characterization of finite Frobenius rings.

Theorem 1. *Let R be a finite ring. The following are equivalent.*

1. *R is a Frobenius ring*
2. *$\mathrm{Soc}\,{}_{R}R$ is left principal,*
3. *${}_{R}(R/Rad\ R) \simeq \mathrm{Soc}\,{}_{R}R$,*
4. *${}_{R}R \simeq {}_{R}\hat{R}$*

Then ${}_{R}\hat{R} = {}_{R}\langle\chi\rangle$ for some (left) generating character χ. It can be shown that any left generating character is also a right generating character (c.f. [22]).

For an arbitrary finite ring, the homogeneous weight is defined as follows [7, 10].

Definition 1. *Let R be a finite ring. A weight $w : R \longrightarrow \mathbb{Q}$ is* (left) homogeneous*, if $w(0) = 0$ and*

1. *If $Rx = Ry$ then $w(x) = w(y)$ for all $x, y \in R$.*
2. *There exists a real number γ such that*

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

Example 1. On every finite field $\mathrm{GF}(q)$ the Hamming weight is a homogeneous weight of average value $\gamma = \frac{q-1}{q}$.

Example 2. On the ring $\mathbb{Z}_{pq}, p, q$ prime, a homogeneous weight with average value $\gamma = 1$ is given by

$$ w : R \longrightarrow \mathbb{R}, \quad x \mapsto \begin{cases} 0 & \text{if } x = 0, \\ \dfrac{p}{p-1} & \text{if } x \in p\mathbb{Z}_{pq}, \\ \dfrac{q}{q-1} & \text{if } x \in q\mathbb{Z}_{pq}, \\ \dfrac{pq-p-q}{(p-1)(q-1)} & \text{otherwise.} \end{cases} $$

In fact the homogeneous weight is unique up to choice of γ on any finite ring. The definition used in [7, 10] uses the notion of a Möbius function μ on the set of left principal ideals of R, given the partial order induced by set inclusion.

Definition 2. *Let μ denote the Möbius function on the partially ordered set of left principal ideals of R. For any $r \in R$ the homogeneous weight of r is given by*

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

where γ is a real constant. We say that w is the normalized *homogeneous weight for the case $\gamma = 1$.*

Clearly, $w(r) \in \mathbb{Q}$ whenever $\gamma \in \mathbb{Q}$. In particular, if $\gamma = |R^{\times}|$ then w is an integer-valued function, since $|R^{\times}| = |R^{\times}x||\mathrm{Stab}_{R^{\times}}(x)|$ for all $x \in R$.

Example 3. On a local Frobenius ring R with q-element residue field, we have $\mu(0, Rx) = -1$ for $Rx = \mathrm{Soc}\, R$ and $\mu(0, Rx) = 0$ for $x \in R \backslash \mathrm{Soc}\, R$. The homogeneous weight is given by

$$w : R \longrightarrow \mathbb{R}, \quad x \mapsto \begin{cases} 0 & \text{if } x = 0, \\ q & \text{if } x \in \mathrm{Soc}(R),\ x \neq 0, \\ q-1 & \text{if otherwise,} \end{cases}$$

where we choose $\gamma = q - 1$.

A description of the homogeneous weight in terms of sums of generating characters is given by the following [16].

Theorem 2. *Let R be a finite Frobenius ring with generating character χ. Then the homogeneous weights on R are precisely the functions*

$$w : R \longrightarrow \mathbb{R}, \quad x \mapsto \gamma\left(1 - \frac{1}{|R^{\times}|}\sum_{u \in R^{\times}} \chi(xu)\right)$$

where γ is a real number.

2.2 Codes Over Rings

For the remainder, we let R denote a finite Frobenius ring endowed with a homogeneous weight w. We extend w to a weight function on R^n in the obvious way:

$$w : R^n \longrightarrow \mathbb{R} : w(c_1, ..., c_n) \mapsto \sum_{i=1}^{n} w(c_i).$$

We also let $C \leq {}_R R^n$ denote a left linear code. As usual, I and J will denote the real identity matrix and the real all-ones matrix, respectively.

Definition 3. *Let C have $k \times n$ generator matrix $Y = (y_1|y_2|\ldots|y_n)$ over R. C is called*

1. *proper if $w(c) > 0$ for any non-zero $c \in C$,*[1]
2. *regular if $\{x \cdot y_i : x \in {}_R R^k\} = R$ for each $i \in \{1, \ldots, n\}$,*
3. *projective if $y_i R \neq y_j R$ for any pair of distinct coordinates $i, j \in \{1, \ldots, n\}$.*

[1] Note that on some finite Frobenius rings w is not positive definite, for example in the ring $\mathbb{F}_2 \times \mathbb{F}_2$ we have $w(00) = w(11) = 0$.

2.3 Strongly Regular Graphs

We recall some elementary facts about strongly regular graphs. There are many texts on the subject. The reader is referred to [9] for further details.

Definition 4. *A graph G on N vertices is called strongly regular with parameters (N, k, λ, μ) if*

1. *G is regular of degree k,*
2. *every pair of adjacent vertices has exactly λ common neighbours,*
3. *every pair of non-adjacent vertices has exactly μ common neighbours.*

It is well-known that a regular connected graph of degree k is strongly regular if it has exactly three distinct eigenvalues. Conversely, if G is strongly regular then it has exactly three eigenvalues k, ρ_1, ρ_2 from which λ and μ are completely determined:

Lemma 1. *Let G be a strongly regular graph with parameters (N, k, λ, μ). Let G have adjacency matrix with eigenvalues ρ_1, ρ_2, k. Then*

$$\mu = k + \rho_1\rho_2 \text{ and } \lambda = k + \rho_1 + \rho_2 + \rho_1\rho_2 \tag{1}$$

It can be deduced from the fact that A has zero trace that if G is non-trivial, unless the ρ_i occur with the same multiplicity, they are integers of opposite sign, say, $k > \rho_2 > 0 > \rho_1$ and further, that $\rho_1 < -1$.

In [8] it was shown that every projective code over a finite field with exactly two non-zero Hamming weights (also called a two-weight code) has a strongly regular Cayley graph. This was extended for regular, projective codes over finite Frobenius rings with two homogenous weights [2].

Given a two-weight code C, with non-zero weights $w_1 < w_2$, we denote by $\Gamma(C)$ the graph whose vertices are the codewords of C and whose edges are pairs of vertices (c, c') such that $w(c - c') = w_1$. $\Gamma(C)$ is the Cayley graph of the set of codewords of weight w_1 in C. If C is a two-weight code, we say that C is imprimitive if $\Gamma(C)$ is trivial. Otherwise we say that C is primitive.

3 Main Results

We now determine relations between the eigenvalues of $\Gamma(C)$ and the weights of a two-weight code C.

Definition 5. *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 $D_{uv} = w(u - v)$.*

The following is an extension of [8, Th 1]. Due to space constraints we omit a proof here, but mentions that our approach relies on the character description of the homogeneous weight given in Theorem 2 in the distance matrix D.

Theorem 3. *Let C be a regular, projective code. Then*

(1) $DJ = \gamma n|C|J$ *and*
(2) $D^2 + \dfrac{|C|\gamma}{|R^\times|}D = n\gamma^2|C|\left(\dfrac{1}{|R^\times|} + n\right)J.$

Corollary 1. *Let C be a proper regular projective two-weight code with nonzero weights $w_1 < w_2$. Then $\Gamma := \Gamma(C)$ is strongly regular and the eigenvalues k, ρ_1, ρ_2 of the adjacency matrix of Γ satisfy*

(1) $(w_2 - w_1)k = w_2(|C| - 1) - \gamma n|C|$
(2) $(w_2 - w_1)\rho_1 = -w_2$
(3) $(w_2 - w_1)\rho_2 = -w_2 + \dfrac{\gamma|C|}{|R^\times|}$

Proof: Since C is proper, the adjacency matrix A of Γ satisfies

$$(w_2 - w_1)A = w_2(J - I) - D. \tag{2}$$

A, D, J are real symmetric commuting matrices and can thus be simultaneously diagonalized by an orthogonal matrix. Applying Theorem 3, (1) we observe that $\mathbf{1}$ is an eigenvector of A with eigenvalue k satisfying (1), above. Any eigenvector e of A orthogonal to $\mathbf{1}$ satisfies

$$(w_2 - w_1)Ae = (w_2 - w_1)\rho e = w_2(J - I)e - De = -(w_2 + \theta)e$$

where ρ, θ are the associated eigenvalues of A and D, respectively. From Theorem 3, (2), we have $(D - n\gamma|C|I)(D)(D + \frac{\gamma|C|}{|R^\times|}I) = 0$, and hence D has exactly two eigenvalues $\theta_1 = 0$ and $\theta_2 = -\frac{\gamma|C|}{|R^\times|}$ corresponding to eigenvectors orthogonal to $\mathbf{1}$. The result follows. □

Corollary 2. *Let C be a proper, regular, projective two-weight code with nonzero weights $w_1 < w_2$. Let the adjacency matrix of $\Gamma(C)$ have eigenvalues $\rho_1 < \rho_2$, orthogonal to $\mathbf{1}$. Then*

$$w_1 = \frac{\gamma|C|(\rho_1 + 1)}{(\rho_1 - \rho_2)|R^\times|} \text{ and } w_2 = \frac{\gamma|C|\rho_1}{(\rho_1 - \rho_2)|R^\times|}.$$

Proof: From Corollary 1, $(w_2 - w_1)(\rho_2 - \rho_1) = \frac{\gamma|C|}{|R^\times|}$. Let $d = w_2 - w_1$. Now solve for w_1 and w_2 using the equations $d\rho_1 = -w_2$ and $d = w_2 - w_1$. □

The following holds, with $t = -(\rho_1 + 1)$.

Corollary 3. *Let C be a proper, regular, projective two-weight code with nonzero weights $w_1 < w_2$ where the weight function is computed for $\gamma = |R^\times|$. Then there exists a positive integer d, a divisor of $|C|$, and positive integer t such that $w_1 = dt$ and $w_2 = d(t + 1)$.*

Corollary 4. *Let C be a regular, projective two-weight code with nonzero weights $w_1 < w_2$ where the weight function is computed for $\gamma = |R^\times|$. Let the adjacency matrix of $\Gamma(C)$ have simple eigenvalue k and restricted eigenvalues $\rho_1 < \rho_2$. Then the corresponding multiplicities of m_1 and m_2 of ρ_1 and ρ_2 are given by*

$$m_1 = |C| - 1 - n|R^\times| \text{ and } m_2 = n|R^\times|.$$

4 Feasible Parameter Sets

Corollaries 2 and 4 can be used to analyse tables of feasible parameters of strongly regular graphs to see which might arise from two-weight codes over rings (cf. [1]). Given a strongly regular graph G on N vertices with eigenvalues k, ρ_1, ρ_2, for $\gamma = |R^\times|$, the numbers $w_1 = \frac{N(\rho_1+1)}{(\rho_1-\rho_2)}$ and $w_2 = \frac{N\rho_1}{(\rho_1-\rho_2)}$ must be positive integers if $G = \Gamma(C)$ for a proper, regular projective code C of order N and nonzero weights w_1 and w_2. Furthermore, the unit group of the alphabet must have order dividing the multiplicity of ρ_2. For the remainder of this section, a 'two-weight code' will mean a primitive, proper, regular, projective two-weight code.

4.1 Existence of Graphs From Codes Over Rings

There are currently 91 feasible parameter sets for strongly regular graphs on at most 225 vertices for which the actual existence of the corresponding graph is not yet known [1] (we have not counted graphs complements in this number). Using the integrality conditions on w_1 and w_2, we calculate that at most 27 of these could arise as Cayley graphs of two-weight codes over finite rings. The regularity condition on a two-weight code C over R means that $|R| \leq |C|$, so we need only consider codes over rings of order at most $|C|$. Checking for the existence of rings R for which there exists a code $C <_R R^n$ of order N with $|R^\times|$ dividing m_1 or m_2 allows us to eliminate a further 11 cases (the classification results of [21] were useful here). We tabulate the remaining 16 possible parameters sets below.

$\|C\|$	w_1	w_2	ρ_1	ρ_2	m_1	m_2	k	λ	μ
96	16	24	-3	9	75	20	45	24	18
144	84	96	-8	4	52	91	52	16	20
162	90	108	-6	3	56	105	21	0	3
162	54	72	-4	5	92	69	23	4	3
162	18	27	-3	15	138	23	69	36	24
196	140	154	-11	3	45	150	45	4	12
196	112	126	-9	5	75	120	75	26	30
196	70	84	-6	8	117	78	78	32	30
216	126	144	-8	4	75	140	40	4	8
216	72	90	-5	7	129	86	43	10	8
216	168	180	-15	3	40	175	75	18	30
216	36	48	-4	14	172	43	86	40	30
225	165	180	-12	3	48	176	48	3	12
225	150	165	-11	4	64	160	64	13	12
225	135	150	-10	5	80	144	80	25	30
225	120	135	-9	6	96	128	96	39	42

Note that if a strongly regular graph G has restricted eigenvalues ρ_1, ρ_2 with respective multiplicities m_1 and m_2, then its complement $\overline{G}$ has restricted eigenvalues $\overline{\rho}_1, \overline{\rho}_2$ occurring with multiplicities m_2 and m_1, respectively. Thus in the

above table, for $G = \Gamma(C)$ to exist we require that C be an R-linear code of length n such that $|R^\times|n$ is equal to either m_1 or m_2, as complements have been excluded.

4.2 The Existence of Two-Weight Codes of Order 100

We claim that there do not exist any two-weight codes of order 100. We first note that no two-weight code of order 100 whose Cayley graph is strongly regular with parameters $(100, 33, 14, 9)$ or $(100, 66, 41, 48)$ exists over any finite Frobenius ring, as the weights required for such a code to exist are not integral. We now consider the existence of two-weight codes of order 100. Let R be a ring of order at most 100. Let M be the set of all multiplicities of positive eigenvalues of feasible strongly regular graphs on 100 vertices. We remove 24 and 75 from this set as by the above note, the corresponding graphs are not the Cayley graphs of two-weight codes. Then $M = \{18, 22, 27, 33, 36, 44, 45, 54, 55, 63, 66, 72, 77, 81\}$. If $\frac{m}{|R^\times|}$ is not an integer for any m in M, then no two-weight code of order 100 over R exists. We classify such rings as *Type I*. If $|R^\times|$ does divide an m in M, we call R *Type II*. For many *Type II* rings, the existence of two-weight codes of order 100 may be eliminated simply by considering the weight composition of codewords of a given length.

Example 4. We consider the existence of two-weight codes over $\mathbb{F}_{25} \oplus \mathbb{Z}_2$, whose group of units has order 24 and divides only $m = 72$. Then the only two-weight code of order 100 that can exist over $\mathbb{F}_{25} \oplus \mathbb{Z}_2$ is one whose Cayley graph is a $(100, 72, 50, 56)$ strongly regular graph, or its complement. If such a code existed, it would have length 3 and non-zero weights $w_1 = 70$ and $w_2 = 80$, which is impossible since the non-zero weights of $\mathbb{F}_{25} \oplus \mathbb{Z}_2$ are $23, 25$ and 48.

Example 5. We consider the existence of two-weight codes over $\mathbb{Z}_{10}$. Now $|\mathbb{Z}_{10}^\times| = 4$, which divides $m_2 = 36, 44$ and 72. We consider the case $m_2 = 36$ and we will show that no $(100, 36, 14, 12)$ strongly regular graph is the Cayley graph of a two-weight code over $\mathbb{Z}_{10}$. Now any $(100, 36, 14, 12)$ strongly regular graph has restricted eigenvalues $\rho_1 = 4, \rho_2 = 6$ with corresponding multiplicities $m_1 = 63, m_2 = 36$. If such a graph could be constructed from a two-weight code C over $\mathbb{Z}_{10}$, C would necessarily have length $n = 9$ and non-zero weights $w_1 = 30$ and $w_2 = 40$. We now prove that no such C exists. Suppose otherwise, and let G be its generator matrix. We may assume G has two rows, r_1 and r_2, with $|\mathbb{Z}_{10}r_i| = 10$. Over $\mathbb{Z}_{10}^2$, there are 18 projective, regular points, namely $\{(0,1), (1,r), (2,u), (2,5), (5,1), (5,2) : r \in \mathbb{Z}_{10}, u \in \mathbb{Z}_{10}^\times\}$. We determine the possible weight compositions of r_1 and r_2. In $\mathbb{Z}_{10}$ with $\gamma = 4$, $u \in \mathbb{Z}_{10}^\times$, $w(u) = 3, w(2u) = 5$ and $w(5) = 8$. For a given word, let a be the number of coordinates of weight 3, b the number of weight 5 and c the number of weight 8. We solve $3a + 5b + 8c \in \{30, 40\}$, where $0 \leq a \leq 10, 0 \leq b \leq 5, 0 \leq c \leq 2$ and $a + b + c = 8$ and arrive at two possible solutions: $a = 3, b = 3, c = 2$ and $a = 5, b = 3, c = 0$. There are three possible forms for G. It can be seen by immediate inspection that both rows of G cannot have weight composition $a = 3, b = 3, c = 2$. Next,

we suppose both rows of G have weight composition $a = 5, b = 3, c = 0$. Then up to monomial equivalence,

$$G = \begin{pmatrix} 0\,1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1\,0 & u_1 & 2u_2 & 2u_3 & 2u_4 & u_5 & u_6 & u_7 \end{pmatrix},$$

$u_i \in \mathbb{Z}_{10}^{\times}$. Now adding the rows of G gives a codeword of weight $24, 29, 34$ or 39. The third possibility is that the first row of G has weight composition $a = 3, b = 3, c = 2$ and the second row $a = 5, b = 3, c = 0$. Then up to monomial equivalence,

$$G = \begin{pmatrix} 0\,1 & 1 & 1 & 2 & 2 & 2 & 5 & 5 \\ 1\,0 & 2u_1 & 2u_2 & u_3 & u_4 & u_5 & 2u_6 & u_7 \end{pmatrix},$$

$u_i \in \mathbb{Z}_{10}^{\times}$. Adding the rows of G gives a codeword of weight $29, 34$ or 39.

Using similar arguments, it can be shown that no primitive two-weight code of order 100 exists. Our results are summarized in the following table.

$\lvert R\rvert$	R	*Type*
100	$\mathbb{Z}_{100}$	*I*
100	$\mathbb{Z}_{25} \oplus \mathbb{F}_4$	*I*
100	$\mathbb{Z}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	*I*
100	$\mathbb{Z}_{25} \oplus \mathbb{Z}_2[x]/\langle x^2 \rangle$	*I*
100	$\mathbb{F}_{25} \oplus \mathbb{Z}_4$	*I*
100	$\mathbb{F}_{25} \oplus \mathbb{F}_4$	*II*
100	$\mathbb{F}_{25} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	*II*
100	$\mathbb{F}_{25} \oplus \mathbb{Z}_2[x]/\langle x^2 \rangle$	*I*
100	$\mathbb{Z}_5[x]/\langle x^2 \rangle \oplus \mathbb{F}_4$	*I*
100	$\mathbb{Z}_5[x]/\langle x^2 \rangle \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	*I*
100	$\mathbb{Z}_5[x]/\langle x^2 \rangle \oplus \mathbb{Z}_2[x]/\langle x^2 \rangle$	*I*
100	$\mathbb{Z}_5[x]/\langle x^2 \rangle \oplus \mathbb{Z}_4$	*I*
100	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_4$	*I*
100	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{F}_4$	*I*
100	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	*I*
100	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2[x]/\langle x^2 \rangle$	*I*
50	$\mathbb{Z}_{50}$	*I*
50	$\mathbb{F}_{25} \oplus \mathbb{Z}_2$	*II*
50	$\mathbb{Z}_5[x]/\langle x^2 \rangle \oplus \mathbb{Z}_2$	*I*
50	$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_2$	*I*
20	$\mathbb{Z}_{20}$	*II*
20	$\mathbb{Z}_5 \oplus \mathbb{F}_4$	*II*
20	$\mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$	*II*
20	$\mathbb{Z}_5 \oplus \mathbb{Z}_2[x]/\langle x^2 \rangle$	*II*
10	$\mathbb{Z}_{10}$	*II*

5 Gray Isometries

An immediate consequence of Corollary 3 is given by the following.

Corollary 5. *Let R have prime power order p^s for some prime p and positive integer s. Let C be a proper, regular, projective two-weight code over R with nonzero weights $w_1 < w_2$, where the weight function is computed for $\gamma = |R^\times|$. Then there exist integers r and t satisfying $w_1 = p^r t$ and $w_2 = p^r(t+1)$.*

One question that arises from Corollary 5 is whether or not a two-weight code of prime power order yields a graph isomorphic to one arising from a finite field.

Let C_1, C_2 be a pair of two-weight codes over finite rings R_1, R_2 respectively, with respect to a pair of (possibly distinct) weight functions w^1, w^2. Let $\Gamma_i := \Gamma(C_i)$ for $i = 1, 2$. Then clearly Γ_1 and Γ_2 are isomorphic graphs if and only if there is an isometry $\iota : (C_1, w^1) \longrightarrow (C_2, w^2)$.

We now consider the possibility that some of the known constructions of linear two-weight codes over a finite field are images of linear codes over a finite chain ring under the Gray isometry. A number of authors have looked into extending the standard Gray isometry between $(\mathbb{Z}_4, w_{\mathrm{Lee}})$ and $(\mathbb{Z}_2^2, w_{\mathrm{Ham}})$ for the case of a finite chain ring (c.f. [13, 15, 18, 20]). If R is a finite chain ring of length n and residue field $\mathrm{GF}(q)$ there is an isometric embedding of R for the homogeneous weight into $\mathrm{GF}(q)^{q^{n-1}}$ for the Hamming weight, in which case the image of R is the generalized Reed-Muller code $\mathrm{GRM}(1, n-1)$.

For example, in [2, Prop 6.2] a construction is given for a two-weight code C over a finite chain ring R of length 2 and having residue field $\mathrm{GF}(q)$. C has a $2 \times s(q+1)$ generator matrix whose $s(q+1)$ columns comprise s distinct elements from each equivalence class of q points in the projective Hjelmslev plane over R, $1 \leq s \leq q-1$. Then C has q^4 codewords and non-zero homogeneous weights

$$w_1 = q^2(qs-1) \text{ and } w_2 = q^3 s = q^2(qs),$$

for $\gamma = |R^\times| = q^2 - q$. We easily solve for k, ρ_1, ρ_2 to find $k = s(q^3 - q)$, $\rho_1 = -qs$ and $\rho_2 = q^2 - qs$, from which we may conclude, using Lemma 1, that $\Gamma(C)$ is a strongly regular graph with parameters

$$(q^4, s(q^3-q), \lambda = q^2(s^2+1) - 3qs, \mu = qs(qs-1)).$$

For the case $s = 1$, $R = \mathbb{Z}_4, \mathbb{Z}_9$ and $\mathrm{GR}(4, 2)$ the corresponding two-weight codes have lengths 3, 4 and 5, sizes 16, 81 and 256 and yield strongly regular graphs with parameters $(16, 4, 2, 2)$, $(81, 24, 9, 6)$ and $(256, 60, 20, 12)$, respectively. While each such graph has the same parameters as the Cayley graph of a binary $[6, 4, 2, 4]$ two-weight code, a ternary $[12, 4, 6, 9]$ two-weight code, and a $\mathrm{GF}(4)$-$[20, 4, 12, 16]$ two-weight code, respectively, we have verified by computer search that no Gray image of any of the $4, 77$ or 1023 distinct $\mathbb{Z}_4, \mathbb{Z}_9$ or $\mathrm{GR}(4, 2)$ codes constructed as above is $\mathbb{Z}_2, \mathbb{Z}_9$ or $GF(4)$-linear.

References

1. A. E. Brouwer, Tables of Parameters of Strongly Regular Graphs http://www.win.tue.nl/∼aeb/graphs/srg/srgtab.html
2. E. Byrne, M. Greferath and T. Honold, *Ring Geometries, Two-Weight Codes and Strongly Regular Graphs*, Designs, Codes and Cryptography, 48 (1) (2008) 1–16.
3. E. Byrne, M. Greferath and M. E. O'Sullivan, *The Linear Programming Bound for Codes over Finite Frobenius Rings,* Designs, Codes and Cryptography, 42 , **3** (2007), 289–301.
4. E. Byrne, M. Greferath, A. Kohnert, V. Skachek, *New Bounds for Codes Over Finite Frobenius Rings* Designs, Codes and Cryptography, 42 **3** (2010), Online First.
5. E. Byrne, A. Sneyd, *Constructions of Two-Weight Codes Over Finite Rings*, Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2010), Budapest, July, 2010.
6. C. Carlet, $\mathbb{Z}_{2^k}$*-Linear Codes*, IEEE Trans. Inform. Th., Vol. 44, , (1998) 1543–1547.
7. I. Constantinescu and W. Heise, *A Metric for Codes over Residue Class Rings of Integers*, Problemy Peredachi Informatsii, 33 (3) (1997).
8. P. Delsarte, "Weights of linear codes and strongly regular normed spaces", *Discrete Math.*, **3** (1972) 47–64.
9. C. D. Godsil, *Algebraic Combinatorics*, Chapman-Hall, 1993.
10. M. Greferath and S. E. Schmidt, *Finite-Ring Combinatorics and MacWilliams Equivalence Theorem*, J. of Combinatorial Theory (A) **92** (2000), 17–28.
11. M. Greferath, A. Nechaev, R. Wisbauer, *Finite Quasi-Frobenius Modules and Linear Codes*, Journal of Algebra and its Application, **3** (3) (2004) 247–272.
12. M. Greferath and M. E. O'Sullivan, *On Bounds for Codes over Frobenius Rings under Homogeneous Weights*, Discrete Mathematics **289** (2004), 11–24.
13. M. Greferath, *Gray Isometries for Finite Chain Rings and a Nonlinear Ternary* $(36, 3^{12}, 15)$ *Code*, IEEE Transactions on Information Theory, **45** (7) (1999), 2522–2523.
14. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbb{Z}_4$*-linearity of Kerdock, Preparata, Goethals and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.
15. W. Heise, T. Honold, A. A. Nechaev, *Weighted Modules and Representations of Codes*, Probl. Peredachi Inf. Vol. 35, **3** (1999) 18-39.
16. T. Honold, *A Characterization of Finite Frobenius Rings*, Arch. Math. (Basel), **76** (2001).
17. T. Honold, *Further Results on Homogeneous Two-Weight Codes*, Proceedings of Optimal Codes and Related Topics, Bulgaria (2007).
18. T. Honold and I. Landjev, *Linearly Representable Codes Over Chain Rings*, Abhandlungen aus dem Mathematischen Seminar der Universitt Hamburg, Vol. 69, **1**, (1999) 187–203.
19. T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Vol. 189, Springer-Verlag, 1999.
20. A. A. Nechaev and A. S. Kuzmin, *Linearly presentable codes*, in Proc. IEEE Int. Symp. Information Theory and Its Applications (1996) 31-34.
21. R. Raghavendran, *Finite Associative Rings*, Compositio Math., 21 (1969) 195-229.
22. J. A. Wood, *Duality for Modules over Finite Rings and Applications to Coding Theory*, Amer. J. Math. **121** (1999), 555–575.