Constructions of Two-Weight Codes Over Finite Rings

Eimear Byrne, Alison Sneyd

I. Introduction

Delsarte ([6], [7]) showed that a projective code over $GF(q)$ with two non-zero Hamming weights yields a strongly regular graph. In [1] this result was extended to the case of a regular, projective code with two non-zero homogeneous weights over a finite Frobenius ring. Some constructions of two-weight codes over $GF(q)$ arise from taking unions of subspaces of $GF(q)^k$ (c.f. [4]). Here we describe some families of two-weight codes found using unions of submodules of R_R^k, where R is a finite Frobenius ring. Although the resulting codes are neither regular nor projective, they determine strongly regular graphs that are isomorphic to graphs from orthogonal arrays. We also show that the elements of certain rings give rise to strongly regular graphs.

II. Preliminaries

A. Strongly Regular Graphs

Definition 1: A simple graph $G = (V, E)$ with vertex set V and edge set E is a *strongly regular graph* with parameters (N, K, λ, μ) if:

1) G has N vertices and each vertex is connected to K edges.
2) Every adjacent pair of vertices have exactly λ common neighbours in V.
3) Every non-adjacent pair of vertices have exactly μ common neighbours in V.

There are several constructions of strongly regular graphs arising from codes and objects in finite geometry (c.f. [4], [5], [12]).

An *orthogonal array,* $OA(s, k)$ is an $s^2 \times k$ 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. An $OA(s, k)$ yields a strongly regular graph by taking the s^2 rows as vertices and two vertices are adjacent if they have a common entry in a column. The resulting strongly regular graph has parameters $(s^2, sk - s, k^2 - 3k + s, k^2 - k)$. The family of arrays with parameters $OA(s, 2)$ yield the family of strongly regular graphs called the lattice or s^2 graphs with parameters $(s^2, 2s-2, s-2, 2)$. For $s \neq 4$, these graphs are unique up to isomorphism.

B. Frobenius Rings and Homogeneous Weights

Let R be a finite Frobenius ring with (left) generating character χ. Then the (left, normalized) homogeneous weight (see [3], [13]) is given by

$$w(x) = 1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(ux).$$

Frobenius rings are important in coding theory: the MacWilliams' extension theorem holds for codes over finite Frobenius rings with respect to the homogeneous weight (c.f. [9], [15]) and restricted versions of the duality theorems hold (c.f. [2], [14]). In [1], it was shown that the known classical connections between two-weight codes over finite fields and strongly regular graphs also hold for certain two-weight codes over finite Frobenius rings.

Let $C \leq {}_R R^n$ denote a left linear code over R of length n. A *two-weight code* will mean a code whose codewords take one of exactly two non-zero homogeneous weights, w_1 and w_2, with $w_1 < w_2$. In what follows, we assume the only codeword of weight 0 in C is the zero-codeword (C is proper). For a two-weight code C, we let $G(C) = (V, E)$ denote the graph whose vertex set comprises the codewords of C and where two vertices are adjacent if and only if the weight of the difference of their corresponding codewords is w_1.

III. Linear Codes Over Finite Frobenius Rings

Given $M \leq R_R^k$, let $(M \backslash \mathbf{0})$ be a fixed $k \times |M| - 1$ matrix whose columns are the non-zero elements of M in some order. We make some easy observations.

Lemma 2: Let $C = \{x(M\backslash\mathbf{0}) : x \in R^k\}$. Then every non-zero codeword c satisfies $w(c) = |M|$.

Proof: For each $c \in C$ there is an $x \in R^k$ such that

$$\begin{aligned} w(c) &= \sum_{y \in M} w(xY) = \sum_{y \in M} (1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi^u(xY)) \\ &= |M| - \frac{1}{|R^\times|} \sum_{u \in R^\times} \sum_{y \in M} \chi^u(xY) \\ &= |M|, \end{aligned}$$

as $\chi^u(x\cdot)$ is a character on the additive group of M. ∎

For each $c \in R^n$, let $f_i(c) := c_i$ denote the projection of c onto its i^{th} coordinate.

Lemma 3: Let $C \leq {}_R R^n$. Then $\sum_{c \in C} w(c_i) = |C|$ for each $i \in \{1, \ldots, n\}$ such that $c_i \neq 0$.

Proof: Let $C_i = \{c_i : c \in C\}$. Then C_i is an ideal in ${}_R R$, and for each $\theta \in C$, there exist $|\ker f_i \cap C|$ codewords c in C such that $c_i = \theta$. Then, from Lemma 2, we have

$$\sum_{c \in C} w(c_i) = |\ker f_i \cap C||C_i| = |C|.$$

∎

For $M \leq R_R^k$, define

$$M^\perp := \{x \in R^k : x \cdot m = \mathbf{0} \ \forall \ m \in M\}.$$

ISBN 978-963-311-370-7

Given $Y = (y_1|\dots|y_n) \in M_{k\times n}(R)$, we denote by

$$Y^{\perp} := |\{x \in R^k : xY_i = 0 \ \forall\ i \in \{1,...,n\}\}|.$$

The next statement follows from a simple homomorphism argument.

Lemma 4: Let $Y = (y_1|\dots|y_n) \in M_{k\times n}(R)$ and let $C \leq {}_R R^n$ be the code generated by Y. Then

$$|C| = \frac{|R^k|}{|Y^{\perp}|}.$$

We now combine these observations.

Lemma 5: Let $M \leq R_R^k$ and let

$$C = \{x(M\backslash\mathbf{0}) : x \in R^k\}.$$

Then $|C| = |M|$.

Proof: We count the total weight of the codewords of C in two ways. Applying Lemmas 2 and 3 we have

$$(|C| - 1)|M| = (|M| - 1)|C|.$$

■

Let $M_1, M_2, \dots, M_r \leq R_R^k$ and let $n = \sum_{i=1}^r |M_i| - r$. By an extension of our previous notation, $(M_1\backslash\mathbf{0}|M_2\backslash\mathbf{0}|\dots|M_r\backslash\mathbf{0}) \in M_{k\times n}(R)$ denotes a fixed matrix whose columns consist of the non-zero elements of M_1 in some order, followed by the non-zero elements of M_2 and so on. Let

$$C^{|} = \{x(M_1\backslash\mathbf{0}|M_2\backslash\mathbf{0}|\dots|M_r\backslash\mathbf{0}) : x \in R^k\}$$

and let

$$C^{+} := \{x((M_1 + M_2 + \dots + M_r)\backslash\mathbf{0}) : x \in R^k\}.$$

Lemma 6: With the same notation as immediately above,

$$|C^{+}| = |C^{|}|.$$

Proof: By Lemma 4,

$$|C^{+}| = \frac{|R^k|}{|(\sum_{i=1}^r M_i)^{\perp}|} = \frac{|R^k|}{|\cap_{i=1}^r M_i^{\perp}|} = |C^{|}|.$$

■

In particular, by Lemma 5, $|C^{|}| = |\sum_{i=1}^r M_i|$.

IV. A Construction of Two-Weight Codes

We now give a construction for a family of two-weight codes from unions of submodules.

Theorem 7: Let $M_1, \dots, M_r, r \geq 2$ be submodules of R_R^k satisfying

1) $\cup_{i=1}^r M_i$ is not a submodule of R_R^k,
2) $|M_i| = v\ \forall\ i \in \{1,\dots,r\}$,
3) $M_i \cap M_j = \mathbf{0}\ \forall\ i,j \in \{1,\dots,r\}$ and
4) for every $x \in R^k$, $|\{i : x \in M_i^{\perp}\}| \in \{0,1,r\}$.

Let $Y = (M_1\backslash\mathbf{0}|M_2\backslash\mathbf{0}|\dots|M_r\backslash\mathbf{0})$ and let $C = \{xY : x \in R^k\}$. Then C is a two-weight code of order v^2 and length $rv - r$. The non-zero weights of C are given by rv and $rv - v$.

Proof: We first show that C is a two-weight code. For each $c \in C$, let $\pi_i(c)$ denote the projection of c onto the coordinates corresponding to the $v - 1$ columns of Y that are elements of M_i. Let $xY \in C$. Then

$$\begin{aligned} w(xY) &= \sum_{i=1}^{r} w(\pi_i(xY)) \\ &= rv - |\{i : x \in M_i^{\perp}\}|v, \text{ by Lemma 2} \\ &= \begin{cases} 0 & \text{if } |\{i : x \in M_i^{\perp}\}| = r, \\ (r-1)v & \text{if } |\{i : x \in M_i^{\perp}\}| = 1, \\ rv, & \text{if } |\{i : x \in M_i^{\perp}\}| = 0. \end{cases} \end{aligned}$$

We now prove that $|C| = v^2$. For any i,j let $Y_{ij} = (M_i\backslash\mathbf{0}|M_j\backslash\mathbf{0})$ and $C_{ij} = \{xY_{ij} : x \in R^k\}$. By Lemma 6, $|C_{ij}| = |M_i + M_j| = v^2$ as $M_i \cap M_j = \{\mathbf{0}\}$. Clearly if $r = 2$ then $|C| = v^2$, so suppose $r > 2$. If $|C| > v^2$ then there exist $x_1, x_2 \in R^k$ such that $x_1 \cdot Y_{ij} = x_2 \cdot Y_{ij}$ but $x_1 \cdot Y \neq x_2 \cdot Y$. Then $x_1 - x_2 \in M_i^{\perp} \cap M_j^{\perp}$, but there exists $k \neq i,j$ such that $x_1 - x_2 \notin M_k^{\perp}$, giving a contradiction. ■

Theorem 8: $G(C)$ is a strongly regular graph with parameters

$$(v^2, rv - r, r^2 + v - 3r, r^2 - r)$$

and is isomorphic to the graph of an orthogonal array $OA(v,r)$.

Proof: We now construct an orthogonal array with parameters $OA(v,r)$ from C. With π_i as before, by Lemma 5, $|\{\pi_i(c) : c \in C\}| = v$ for each i. Let V be a v-set. For each M_i, let $f_i : \{\pi_i(c) : c \in C\} \to V$ be a bijection. Then define

$$\begin{aligned} F : C &\to V^r \\ : c &\mapsto c_F := (f_1(\pi_1(c)), f_2(\pi_2(c)), \dots, f_r(\pi_r(c))) \end{aligned}$$

Arrange $\{c_F : c \in C\}$ as the rows of an array, OA_C. As $|C_{ij}| = v^2$ for each pair M_i, M_j, OA_C is a $v^2 \times r$ orthogonal array. Let $G(OA_C)$ denote the strongly regular graph resulting from this array. We will now show $G(C)$ is isomorphic to $G(OA_C)$. Let $c, c' \in C$. Then

$$\begin{aligned} (c,c') \in E(G(C)) &\Leftrightarrow \exists!\ i \text{ such that } \pi_i(c - c') = \mathbf{0} \\ &\Leftrightarrow \pi_i(c) = \pi_i(c') \\ &\Leftrightarrow f_i(\pi_i(c)) = f_i(\pi_i(c')) \\ &\Leftrightarrow (c_F, c'_F) \in E(G(OA_C)). \end{aligned}$$

As $G(C)$ is isomorphic to $G(OA_C)$, $G(C)$ is strongly regular and has parameters $(v^2, rv - r, r^2 + v - 3r, r^2 - r)$. ■

We give an explicit construction.

Theorem 9: Let $a \in R\backslash\{0\}$, $k = 2l$ and $e_i \in R^k$ denote the vector with a 1 in the i^{th} coordinate and zeros elsewhere. Let $M_1, M_2, M_3 \leq R_R^k$ where

$$\begin{aligned} M_1 &= \langle e_1 a, e_2 a, \dots, e_l a\rangle_R, \\ M_2 &= \langle e_{l+1} a, e_{l+2} a, \dots, e_{2l} a\rangle_R, \\ M_3 &= \langle (e_1 a + e_{j_1} a u_1), (e_2 a + e_{j_2} a u_2), \dots (e_l a + e_{j_l} a u_l)\rangle_R, \end{aligned}$$

with $u_1, u_2, \dots u_l \in R^{\times}$ and $\{e_{l+1}, e_{l+2}, \dots, e_{2l}\} = \{e_{j_1}, e_{j_2}, \dots e_{j_l}\}$. Then by Theorems 7 and 8,

1)

$$C = \{x \cdot (M_1\backslash\mathbf{0}|M_2\backslash\mathbf{0}) : x \in R^k\}$$

is a two-weight code of length $2|aR|^l - 2$ and order $|aR|^k$ with $w_1 = |aR|^l$ and $w_2 = 2|aR|^l$. $G(C)$ is a strongly regular graph with parameters

$$(|aR|^k, 2|aR|^l - 2, |aR|^l, 2)$$

and is isomorphic to the $(|aR|^l)^2$-graph.

2) If $|aR| > 2$, then the code

$$C = \{x(M_1\backslash\mathbf{0}|M_2\backslash\mathbf{0}|M_3\backslash\mathbf{0}) : x \in R^k\}$$

is a two-weight code of length $3|aR|^l - 3$ and order $|aR|^k$ with $w_1 = 2|aR|^l$ and $w_2 = 3|aR|^l$. $G(C)$ is a strongly regular graph with parameters

$$(|aR|^k, 3|aR|^l - 3, |aR|^l, 6)$$

and is isomorphic to a graph from an orthogonal array $OA(|aR|^l, 3)$ constructed from C.

Example 10: Let $a \in R\backslash\{0\}$. Let $M_1, M_2 \leq R_R^2$, where $M_1 = \langle(a,0)\rangle_R$ and $M_2 = \langle(0,a)\rangle_R$. Then the code

$$C = \{x \cdot (M_1\backslash\mathbf{0}|M_2\backslash\mathbf{0}) : x \in R^2\}$$

is a two-weight code of length $2|aR| - 2$ and order $|aR|^2$ with $w_1 = |aR|$ and $w_2 = 2|aR|$. $G(C)$ is a strongly regular graph with parameters

$$(|aR|^2, 2|aR| - 2, |aR|, 2)$$

and is isomorphic to the $|aR|^2$-graph.

Example 11: Let $a \in R$ satisfy $|aR| > 2$. Let $M_1, M_2, M_3 \leq R_R^2$, where $M_1 = \langle(a,0)\rangle_R$, $M_2 = \langle(0,a)\rangle_R$ and $M_3 = \langle(a,a)\rangle_R$. Then the code

$$C = \{x(M_1\backslash\mathbf{0}|M_2\backslash\mathbf{0}|M_3\backslash\mathbf{0}) : x \in R^2\}$$

is a two-weight code of length $3|aR| - 3$ and order $|aR|^2$ with $w_1 = 2|aR|$ and $w_2 = 3|aR|$. $G(C)$ is a strongly regular graph with parameters

$$(|aR|^2, 3|aR| - 3, |aR|, 6)$$

and is isomorphic to a graph from an orthogonal array $OA(|aR|, 3)$ constructed from C.

Remark 12: For a code C constructed by Example 10 or Example 11, let C_p denote the shortened code from C given by

$$C_p = \{x \cdot \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : x \in R^2\}$$

in the case of Example 10 and

$$C_p = \{x \cdot \begin{pmatrix} a & 0 & a \\ 0 & a & a \end{pmatrix} : x \in R^2\}$$

in the case of Example 11. C_p is projective, but for R not a finite field, C_p is not in general a two-weight code. An exception is the code C given by Example 11 with $R = \mathbb{Z}_4$ and $a = 1$. In this case, C_p is a two-weight code with $w_1 = 2$ and $w_2 = 4$ and $G(C_p)$ is strongly regular. But $G(C_p)$ and $G(C)$ are not isomorphic as $G(C_p)$ has parameters $(16, 6, 2, 2)$ and is isomorphic to the Shrikhande graph.

V. Two-Weight Rings

We show certain rings can be viewed as two-weight codes that determine strongly regular graphs.

Definition 13: A *two-weight ring* is a ring whose elements take exactly two non-zero homogeneous weights, w_1 and w_2, with $w_1 < w_2$.

Proposition 14: Let R be a two-weight ring. Then by [1, Theorem 5.5], the elements of R yield a strongly regular graph.

Theorem 15: $M_2(\mathbb{F}_q)$ is a two-weight ring with $w_1 = \frac{q^3-q^2-q}{q^3-q^2-q+1}$ and $w_2 = \frac{q^2}{q^2-1}$. The corresponding strongly regular graph has parameters

$$(q^4, q^4 - q^3 - q^2 + q, q^4 - 2q^3 - q^2 + 3q, q^4 - 2q^3 + q).$$

In fact the construction given in Theorem 15 is not new, since the relation on elements of $M_2(\mathbb{F}_q)$ induced by the homogeneous weight is exactly the same as that induced by the rank of a matrix in this ring. But the connection to two-weight codes is a new perspective.

VI. Cayley Graphs

We mention another construction of a graph from a linear code. This is a straightforward extension of the finite field case (c.f. [7], [4]). Let $\Omega \subset R^k\backslash\{0\}$ satisfy $\Omega R^\times = \Omega$. Let $M < {}_R R^k$. For each $v \in M$, define a function $c^v : \Omega \longrightarrow R : x \mapsto \langle v, x\rangle$. We define the left R-linear code $C := C(\Omega) = \{c^v : v \in M\}$. The Cayley graph of Ω is the graph $G := G(\Omega)$ with vertex set M, where $u, v \in M$ are adjacent in $G(\Omega)$ if $u - v \in \Omega$. Let $A := A(\Omega)$ denote the $|M| \times |M|$ adjacency matrix of $G(\Omega)$. For each $v \in M$, define the vector $e^v = (\chi_v(x))_{x\in M}$ in $\mathbb{C}^{|M|}$.

Lemma 16: For each $v \in M$, the vector e^v is an eigenvector of A with eigenvalue $\lambda^v := \sum_{x\in\Omega} \chi_v(x)$. Moreover, the vectors e^v are orthogonal.

Proof: Let $v \in M$,

$$\begin{aligned}(Ae^v)_y &= \sum_{x\in M} A_{xy}\chi_v(x) = \sum_{x\in\Omega+y} \chi_v(x) \\ &= \sum_{x\in\Omega} \chi_v(x+y) = \chi_v(y)\sum_{x\in\Omega} \chi_v(x) = \lambda^v(e^v)_y.\end{aligned}$$

Let $u, v \in M$. Then

$$\begin{aligned}\langle e^v, e^u\rangle &= \sum_{x\in M} \chi_v(x)\chi_u(x) \\ &= \sum_{x\in M} \chi_{u+v}(x) = \begin{cases} 0 & \text{if} u \neq v \\ |M| & \text{otherwise} \end{cases}\end{aligned}$$

■

Theorem 17: Then G is strongly regular if and only if C has exactly two non-zero homogeneous weights.

Proof: We compute $w(c^v)$ for each $v \in M$.

$$\begin{aligned}w(c^v) &= \sum_{x\in\Omega} w(c^v(x)) = \sum_{x\in\Omega}(1 - \frac{1}{|R^\times|}\sum_{\delta\in R^\times} \chi(\langle v, x\rangle\delta)) \\ &= |\Omega| - \frac{1}{|R^\times|}\sum_{\delta\in R^\times}\sum_{x\in\Omega} \chi_v(x\delta) = |\Omega| - \sum_{x\in\Omega} \chi_v(x),\end{aligned}$$

since $\Omega = \Omega R^\times$. It follows that $\lambda^v = |\Omega| - w(c^v)$ for each $v \in M$, and these comprise all the eigenvalues of A. Then C has exactly two non-zero homogeneous weights if and only if A has exactly 3 distinct eigenvalues. The graph G is regular of degree $\lambda^0 = |\Omega| = \sum_{x\in\Omega} \chi(0)$, which is a simple eigenvalue of G since C is assumed throughout to be regular. The usual argument (c.f. [8, Ch. 10]), gives that G is strongly regular if and only if C is a two-weight code. ■

Remark 18: The general construction described in Theorem 7 is an instance of a *modular code* as defined in [10]. Such a code is generated by the rows of a $k \times n$ matrix $Y = (y_1, ..., y_n)$ such that for each column y, the number $|\{i : y_i R^\times = yR^\times\}| = r|R^\times|$ for some constant r. In fact we did not use Honold's results here, but applied a direct argument to describe the graphs induced by these two-weight codes.

REFERENCES

[1] E. Byrne, M. Greferath, and T. Honold, "Ring geometries, two-weight codes, and strongly regular graphs", *Designs, Codes and Cryptography* 48 (2008).

[2] E. Byrne, M. Greferath, M.O'Sullivan, "'The Linear Programming Bound for Codes Over Finite Frobenius Rings", *Designs, Codes and Cryptography*, 42 (3): (2007) 289-301.

[3] I. Constantinescu and W. Heise, "A metric for codes over residue class rings of integers", *Problemy Peredachi Informatsii* **33**, No. 3, (1997) 22–28.

[4] R. Calderbank, W. M. Kantor, "The geometry of two-weight codes", Bulletin of the London Mathematical Society, 18, (1986) 97–122.

[5] P. J. Cameron, J. H. van Lint, *Designs, Graphs, Codes and their Links*, Cambridge University Press, 1991.

[6] P. Delsarte, "Two-weight linear codes and strongly regular graphs", Report R160, MBLE Res. Labs., Brussels, 1971.

[7] P. Delsarte, "Weights of linear codes and strongly regular normed spaces", *Discrete Math.*, **3** (1972) 47–64.

[8] C. D. Godsil, *Algebraic Combinatorics*, Chapman-Hall, 1993.

[9] M. Greferath and S. E. Schmidt. Finite-ring combinatorics and MacWilliams' equivalence theorem. *Journal of Combinatorial Theory, Series A*, 92 (2000) 17–28.

[10] T. Honold, "Further Results on Homogeneous Two-Weight Codes, *Proceedings of Optimal Codes and Related Topics*, Bulgaria (2007).

[11] T. Y. Lam, *Lectures on Modules and Rings*, Graduate Texts in Mathematics, Vol. 189, Springer-Verlag, 1999.

[12] J. H. van Lint, R. M. Wilson, *A Course in Combinatorics*, Cambridge Univ. Press, 1998

[13] T. Honold, Characterization of finite Frobenius rings. *Arch. Math.* (Basel) 76 no. 6, (2001) 406–415.

[14] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575.

[15] J. A. Wood, *Weight functions and the extension theorem for linear codes over finite rings*, in Finite Fields: Theory, Applications and Algorithms, Contemp. Math. 225, Providence: Amer. Math. Soc., 1999, 231–243.