Two-weight codes over chain rings *

Minjia Shi, Ruowen Liu, Patrick Solé

Two-weight codes over chain rings*

Minjia Shi, Ruowen Liu †, Patrick Solé ‡

Abstract

Irreducible cyclic codes of length p^2-1 are constructed as two-weight codes over a chain ring with a residue field of characteristic p. Their projective puncturings of length $p+1$ also yield two-weight codes. Under certain conditions, these latter codes qualify as Maximum Distance Rank codes (MDR). We construct strongly regular graphs from both types of codes and compute their parameters. Additionally, we construct an infinite common cover of these graphs for a given p by extending the alphabet to p-adic numbers.

Keywords: Finite chain ring, Irreducible cyclic codes, strongly regular graphs
MSC (2020): Primary 94B15 Secondary 05E30

1 Introduction

Since Delsarte's seminal paper [10], two-weight codes have been extensively studied in relation to combinatorial objects such as strongly regular graphs (SRGs) [4, 5, 10] and geometric structures like caps in projective spaces [8]. An important category within this field is irreducible cyclic codes [5, 12], which play a crucial role in constructing two-weight codes. It is conjectured that all two-weight projective irreducible cyclic codes have been identified [21, 23]. Specifically, for cyclic codes of dimension 2, it has been demonstrated that all such codes (whether irreducible or not) are classified as either one-weight or two-weight codes [17,22]. The association between SRGs and two-weight codes over finite fields has been further extended to two-weight codes over rings, specifically for the homogeneous weight [6, 7].

In this paper, we explore a novel approach by constructing two-weight codes over chain rings, focusing on the Hamming distance. Interestingly, the weight distributions vary based on the primitive status of the check polynomial. Through precise puncturing, we successfully construct projective two-weight codes of length $p+1$ in the primitive

*This research is supported by National Natural Science Foundation of China (12071001).

†Minjia Shi and Ruowen Liu are with the Key Laboratory of Intelligent Computing Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei 230601, China; State Key Laboratory of integrated Service Networks, Xidian University, Xi'an, 710071, China. smjwcl.good@163.com, liuruowen0116@163.com

‡ Patrick Solé is with I2M (Aix Marseille Univ, CNRS, Centrale Marseille), Marseilles, France. sole@enst.fr

case and shorter lengths in other cases. The codes of length $p+1$ achieve optimality as Maximum Distance Rank (MDR) codes [18]. We also detail the main parameters of the SRGs associated with these two classes of codes, which are derived using the coset graph construction on the dual code. Notably, in the primitive case, these SRGs are of the Latin square type [4, p.121]. Furthermore, the SRGs constructed for varying h share a common cover, which is a coset graph of a code defined on the p-adic integers, similar to those described in [9, 16].

The structure of this paper is as follows: Section 2 introduces the necessary definitions and notation. Section 3 provides preliminary information. Sections 4 and 5 deal with codes of length p^2-1 over chain rings of depth 2. Section 4 focuses on the weight distribution when the check polynomial is primitive, while Section 5 considers the more general situation of an irreducible check polynomial of degree 2. Section 6 constructs projective codes from those with a primitive check polynomial and details the associated SRGs. Section 7 extends the discussion to chain rings of arbitrary depths. The paper concludes with Section 8.

2 Definitions and Notation

2.1 Finite chain rings

We begin with some definitions and properties about finite chain rings. A commutative ring is called a *chain ring* if the lattice of all its ideals is a chain. Consider the two finite commutative chain rings with identity R and L. We say that the ring L is an extension of R of degree r, denoted by $L|R$, if R is a subring of L such that $1_R = 1_L$ and the rank of L over R is r. Let M be a maximal ideal of L, whose generator is γ. The chain of ideals is

$$L = \langle \gamma^0 \rangle \supset \langle \gamma^1 \rangle \supset \cdots \supset \langle \gamma^{h-1} \rangle \supset \langle \gamma^h \rangle = \{0\}.$$

The integer h is called the *nilpotency index* of $\langle \gamma \rangle$. It is well known that the residue field L/M is a finite field $\mathbb{F}_q$, where $q = p^r$ is a power of a prime p. The *Teichmüller set* $\mathcal{T} = \{x \in L \mid x^{p^r} = x\}$ is a set of representatives of $\mathbb{F}_{p^r}$ in that quotient. If $x \in L$, let $\tilde{x}$ denote its image in $\mathbb{F}_{p^r}$ by reduction modulo (γ). Let t^p denote the conjugate of t, where $t \in \mathcal{T}$. L can be expressed as $L = \mathcal{T} \oplus \gamma\mathcal{T} \oplus \gamma^2\mathcal{T} \oplus \cdots \oplus \gamma^{h-1}\mathcal{T}$ (the p-adic expansion of L). If $x \in L$, then $x = t_0 + \gamma t_1 + \cdots + \gamma^{h-1} t_{h-1}$, where $t_i \in \mathcal{T}$. The *Frobenius function* $F(x)$ is defined as $F(x) = \sum_{i=0}^{h-1} t_i^p \gamma^i$. The *trace* $Tr(x)$ from L down to R is defined as

$$Tr(x) = \sum_{i=0}^{r-1} F^i(x).$$

Let L be a quadratic extension of R, so $r = 2$, and thus $Tr(x) = x + F(x)$.

2.2 Codes over finite chain rings

A matrix $G \in R^{l \times n}$ is called a *generator matrix* of the linear code C if the rows of G generate C as an R-module. The *Hamming weight* $\omega_H(\boldsymbol{c})$ of $\boldsymbol{c} \in C$ counts the non-zero

components of $\boldsymbol{c}$. The *minimum distance* $d_H(C)$ of C is the minimum Hamming weight among all nonzero codewords in C. The *weight distribution* of C over R is defined as

$$[\langle 0, 1\rangle, \cdots, \langle \omega_i, A_i\rangle, \cdots, \langle \omega_n, A_n\rangle],$$

where A_i denotes the number of codewords $\boldsymbol{c}$ with $\omega_H(\boldsymbol{c}) = i$. The dual code $C^\perp$ of C is defined as $C^\perp = \{\mathbf{v} \in R^n \mid \mathbf{u} \cdot \mathbf{v} = 0, \forall \mathbf{u} \in C\}$, where $\cdot$ denotes the *standard inner product*.

A linear code C is *cyclic* if it is invariant under a cyclic shift, i.e., $(c_0, c_1, \ldots, c_{n-1}) \in C$ implies $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. A cyclic code C of length n over R can be identified with an ideal $\langle g(x)\rangle$ generated by a polynomial $g(x)$ dividing $x^n - 1$ in $R[x]/\langle x^n - 1\rangle$. The generator polynomial $g(x)$ and parity-check polynomial $h(x) = \frac{x^n-1}{g(x)}$ completely specify the cyclic code. The extension ring of the finite chain ring R of dimension 2, denoted by L, is defined as

$$L = \frac{R[x]}{\langle h(x)\rangle}$$

where $h(x)$ is a monic basic irreducible polynomial of degree 2 in $R[x]$. If $h(x)$ is basic irreducible and $h(\alpha) = 0$, then the code is a trace code of the form

$$C = \{c(A) = (\mathrm{Tr}(A\alpha^i))_{i=0}^{n-1} \mid A \in L\}.$$

Note that if α has order b, then $|\{\alpha^i \mid i = 0, \cdots, n-1\}| = b$. Let C have an $l \times n$ generator matrix $G = [g_1|\cdots|g_n]$. The code C is called *projective* if $Rg_i \neq Rg_j$ for any pair of distinct coordinates $i, j \in \{1, \cdots, n\}$. The parameters of a two-weight code C over an alphabet M of size q are listed as $[n, k, \{w_1, w_2\}]_q$ if M is a finite field, and C is of dimension k, and $(n, |C|, \{w_1, w_2\})_q$ if M is not a finite field.

The *original Singleton bound* posits that $d \leq n - \log_q(|C|) + 1$, where C is a code over an alphabet of cardinality q, n is the code's length, and d is the minimum Hamming distance of code C. Codes meeting this bound are called maximum distance separable (MDS). Codes meeting the bound are termed maximum distance with respect to rank (MDR), where the bound is $d \leq n - k + 1$ and k is the rank of the code.

The *Griesmer bound* on a linear $[n, k, d]_q$ code is given by

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil,$$

where $\lceil a \rceil$ is the least integer greater than or equal to a real number a.

2.3 Strongly regular graph

A graph $\Gamma = (V, E)$ is called a *strongly regular graph* with parameters (v, k, λ, μ) if

- Each vertex has k neighbors.
- Adjacent vertices have λ common neighbors.

- Non-adjacent vertices have μ common neighbors.

An *eigenvalue* of a graph Γ (i.e., an eigenvalue of its adjacency matrix) is called a *restricted eigenvalue* if there is a corresponding eigenvector which is not a multiple of the all-one vector $\mathbf{1}$. Note that for an η-regular connected graph, the restricted eigenvalues are simply the eigenvalues different from η. The coset graph of a projective code $C \subseteq L^n$ has vertices representing the cosets of C, with two vertices being connected if and only if they differ by a coset of minimum Hamming weight one.

2.4 Frobenius rings

For a finite ring R, let $\widehat{R} := \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{C}^{\times})$, referred to as the character module of R. We denote a left (resp. right) R-module M by ${}_RM$ (resp. M_R). A finite ring R is termed a Frobenius ring if it satisfies any one of the following two equivalent conditions:

$$1.\ {}_RR \cong_R \widehat{R}.$$
$$2.\ R_R \cong \widehat{R}_R.$$

In particular, it is well-known that chain rings are Frobenius rings.

3 Preliminaries

Let R be a finite commutative ring, L be a quadratic extension of R with maximal ideal M, and $Z = \mathcal{T} \setminus \{0\}$. Then $|Z| = p^2 - 1$. We consider trace codes defined by

$$C_d = \{c(A) = (\mathrm{Tr}(Ax))_{x \in Z^d} \mid A \in L\},$$

where d is an arbitrary divisor of p^2-1, and Z^d is the multiset $\{\{x^d \mid x \in Z\}\}$, repetitions being allowed. In fact, Z^d is the repetition of d sets of size $\frac{p^2-1}{d}$. By the preceding section, we see that C_1 is permutation equivalent to a cyclic code with a primitive check polynomial, while C_d, in general, is permutation equivalent to a cyclic code with a basic irreducible check polynomial the roots of which have order $\frac{p^2-1}{d}$.

We will use the following lemma:

Lemma 3.1.

$$\omega_H(c(A)) = p^2 - 1 - |\{x \in Z \mid Ax^d + F(A)x^{dp} = 0\}|.$$

Proof. Because L is a quadratic extension of R, the weight of $c(A)$ can be calculated by length minus the number of times the Trace $\mathrm{Tr}(Ax^d) = Ax^d + F(A)x^{dp} = 0$, for $x \in Z^d$. □

4 Primitive check polynomial

In this section, we calculate the weight distribution of C_1.

Theorem 4.1. *The code C_1 is a two-weight code with $w_1 = p^2 - p$, and $w_2 = p^2 - 1$. Letting A_1, A_2 denote their respective frequencies, we have*

$$A_1 = (p+1)(p^3-1), \tag{1}$$

$$A_2 = p(p^2-1)(p^3-1). \tag{2}$$

Proof. In view of Lemma 3.1, we need to count the solutions in $x \in Z$ of $\mathrm{Tr}(Ax) = 0$. Write $A = a + \gamma b + \gamma^2 c$, with a, b, c in $Z \cup \{0\}$. The equation $\mathrm{Tr}(Ax) = 0$ can be rewritten as

$$ax + \gamma bx + \gamma^2 cx = -\left(a^p x^p + \gamma b^p x^p + \gamma^2 c^p x^p\right). \tag{3}$$

We remark that, if p is odd, we have $(-1) \in Z$, since $(-1)^{p^2-1} = 1$. Thus the terms $-a^p x^p$, $-b^p x^p$, $-c^p x^p$ are in Z, just like ax, bx, cx.

By the uniqueness of the p-adic expansion in L while $h = 3$, equation (3) yields the system

$$ax = -a^p x^p, \tag{4}$$

$$bx = -b^p x^p, \tag{5}$$

$$cx = -c^p x^p. \tag{6}$$

Up to permutations of a, b, c, we claim that three cases can occur where this system has at least one solution. In each case, the number of solutions turns out to be $p - 1$.

(1). $a \neq 0$, $b = c = 0$
There are $p-1$ solutions of $x^{p-1} = -a^{1-p}$, if $-1 = \varepsilon^{p-1}$, for some ε in Z. This is possible if $(-1)^{p+1} = 1$, which holds true for p odd.

(2). $ab \neq 0$, $c = 0$
There are $p-1$ solutions of $x^{p-1} = -a^{1-p} = -b^{1-p}$, provided $a^{p-1} = b^{p-1}$.

(3). $abc \neq 0$
There are $p-1$ solutions of $x^{p-1} = -a^{1-p} = -b^{1-p} = -c^{1-p}$, provided $a^{p-1} = b^{p-1} = c^{p-1}$.

The number of values of A for each case is

(1). $a \neq 0$, $b = c = 0$
$p^2 - 1$ since a is arbitrary in Z.

(2). $ab \neq 0$, $c = 0$
$(p^2-1)(p-1)$ since $\left(\frac{b}{a}\right)^{p-1} = 1$.

(3). $abc \neq 0$
$(p^2-1)(p-1)^2$ since $\left(\frac{b}{a}\right)^{p-1} = \left(\frac{c}{a}\right)^{p-1} = 1$.

Thus, accounting for permutations of a, b, c we obtain

$$A_1 = 3(p^2-1) + 3(p^2-1)(p-1) + (p^2-1)(p-1)^2 = \frac{(p^2-1)}{p-1}(p^3-1) = (p+1)(p^3-1).$$

Since $1 + A_1 + A_2 = |C| = p^6$, the result follows. □

Example 4.2. When $p = 5, 7$, and 11, we obtain codes of different lengths with the following weight distributions:

- For $p = 5$, the codes have length 24 with weight distribution:

$$[\langle 0, 1\rangle, \langle 20, 744\rangle, \langle 24, 14880\rangle].$$

- For $p = 7$, the codes have length 48 with weight distribution:

$$[\langle 0, 1\rangle, \langle 42, 2736\rangle, \langle 48, 114912\rangle].$$

- For $p = 11$, the codes have length 120 with weight distribution:

$$[\langle 0, 1\rangle, \langle 110, 15960\rangle, \langle 120, 1755600\rangle].$$

5 Irreducible check polynomial

Theorem 5.1. *The code C_d is a two-weight code with $w_1 = p^2 - 1 - m$, where $m = (d, p+1)(p-1)$, and $w_2 = p^2 - 1$. Letting A_1, A_2 denote their respective frequencies, we have*

$$A_1 = \frac{(p^2-1)}{m}((m+1)^3 - 1), \tag{7}$$

$$A_2 = p^6 - 1 - A_1. \tag{8}$$

Proof. (sketch) The proof is similar to that of Theorem 4.1. The system of equations (4), (5), (6) is replaced by

$$ax^d = -a^p x^{dp}, \tag{9}$$

$$bx^d = -b^p x^{dp}, \tag{10}$$

$$cx^d = -c^p x^{dp}. \tag{11}$$

Because $x \in Z$, we have $x^{d(p-1)} = x^m$, where

$$m = (d(p-1), p^2-1) = (d, p+1)(p-1).$$

The same discussion as in the proof of Theorem 4.1 yields

$$A_1 = 3(p^2-1) + 3(p^2-1)m + (p^2-1)m^2 = \frac{(p^2-1)}{m}((m+1)^3 - 1).$$

This completes the proof. □

If $m = p-1$, the weight distribution is the same as in the primitive case. In the case $m > p-1$, the following values were computed in Magma.

Example 5.2. When $p = 5, 7$, and 11, we obtain codes of different lengths with distinct weight distributions as $d > 1$ varies:

- For $p = 5$, the codes have length 24 with two distinct weight distributions:

$$[\langle 0,1\rangle, \langle 12, 248\rangle, \langle 24, 15376\rangle], \quad [\langle 0,1\rangle, \langle 16, 372\rangle, \langle 24, 15252\rangle].$$

- For $p = 7$, the codes have length 48 with two distinct weight distributions:

$$[\langle 0,1\rangle, \langle 24, 684\rangle, \langle 48, 116964\rangle], \quad [\langle 0,1\rangle, \langle 36, 1368\rangle, \langle 48, 116280\rangle].$$

- For $p = 11$, the codes have length 120 with four distinct weight distributions:

$$[\langle 0,1\rangle, \langle 60, 2660\rangle, \langle 120, 1768900\rangle], \quad [\langle 0,1\rangle, \langle 80, 3990\rangle, \langle 120, 1767570\rangle],$$

$$[\langle 0,1\rangle, \langle 90, 5320\rangle, \langle 120, 1766240\rangle], \quad [\langle 0,1\rangle, \langle 100, 7980\rangle, \langle 120, 1763580\rangle].$$

6 Projective codes and SRG's

6.1 Projective codes

If C is a linear code over finite chain ring L with depth of 3, the projective code $\widehat{C}$ is given by

$$\widehat{C} = \{c(A) = (\mathrm{Tr}(A(\alpha^{p-1})^i))_{i=0}^{n-1} \mid A \in L\}.$$

More generally, we consider trace codes defined by

$$\widehat{C_d} = \{c(A) = (\mathrm{Tr}(Ax^{p-1}))_{x \in Z^d} \mid A \in L\},$$

where d is an arbitrary divisor of $p^2 - 1$.

Theorem 6.1. *The code $\widehat{C_1}$ is a two-weight code with parameters $(p+1, p^6, \{p, p+1\})_{p^3}$. It is optimal with these parameters.*

Proof. Note that two columns $x, y \in Z$ of the generator matrix of $C_1^{\perp}$ are linearly dependent if and only if $x/y \in Z \cap L$, if and only if $(x/y)^{p-1} = 1$. Thus, the parameters of $\widehat{C_1}$ are obtained from those of C_1 by dividing the length and the weights by $p-1$. This code meets the Singleton bound mentioned earlier. Indeed, it is a free code of rank 2, length $p+1$, and distance p. According to the previous definition, it can be concluded that code $\widehat{C_1}$ is MDR. □

The analogous theorem for $d > 1$ is as follows.

Theorem 6.2. *The code $\widehat{C_d}$ is a two-weight code with parameters*

$$\left(\tfrac{p^2-1}{m}, p^6, \left\{\tfrac{p^2-1}{m}-1, \tfrac{p^2-1}{m}\right\}\right)_{p^3},$$

where $m = (d, p+1)(p-1)$.

Proof. Note that two columns labelled by $x, y \in Z$ of the generator matrix of $C_d^{\perp}$ are linearly dependent if and only if $(x/y)^d \in Z \cap L$, if and only if $(x/y)^{d(p-1)} = 1$. Let $m = (d(p-1), p^2-1) = (d, p+1)(p-1)$. Now, $(x/y)^m = 1$ if and only if $(x/y)^{d(p-1)} = 1$, and given x there are exactly m elements $y \in Z$ such that $(x/y)^{d(p-1)} = 1$. Thus, the parameters of $\widehat{C_d}$ are obtained from those of C_d by dividing the length and the weights by m. □

6.2 Their graphs

Theorem 6.3. *The coset graph of* $\widehat{C_1}^{\perp}$ *is a strongly regular graph (SRG) of degree* $(p+1)(p^3-1)$*, on* p^6 *vertices with restricted eigenvalues* p^3-p-1 *and* $-(p+1)$ *of respective multiplicities* A_1 *and* A_2 *of Theorem 4.1.*

Proof. By Theorem 11.1.11 of [2], the restricted eigenvalues are computed as $\lambda_i = n(p^3-1) - pw_i'$ for $i = 1, 2$ with the weights $w_1' = p$ and $w_2' = p+1$ from Theorem 6.1, and their multiplicities equal the frequency of the corresponding weights. This completes the proof. □

Example 6.4. We use a special finite chain ring $\mathbb{Z}_{p^3}$ as an example, take $p = 3$ to obtain an SRG on 729 vertices of degree 104, and eigenvalues 23 and -4 with respective multiplicities 104 and 624. As per [3], alternate constructions include a $[52, 6, \{27, 36\}]_3$, and a $[13, 3, \{9, 12\}]_9$.

Theorem 6.5. *The coset graph of* $\widehat{C_d}^{\perp}$ *is a SRG of degree* $\frac{(p^2-1)}{m}(p^3-1)$*, on* p^6 *vertices with restricted eigenvalues* $p^3 - \frac{(p^2-1)}{m}$ *and* $-\frac{(p^2-1)}{m}$ *of respective multiplicities* A_1 *and* A_2 *of Theorem 6.2.*

Proof. By Theorem 11.1.11 of [2], the restricted eigenvalues are computed as $\lambda_i = n(p^3-1) - pw_i'$ for $i = 1, 2$ with the weights $w_1' = \frac{p^2-1}{m} - 1$ and $w_2' = \frac{p^2-1}{m}$ from Theorem 6.2, and their multiplicities equal the frequency of the corresponding weights. This completes the proof. □

7 Generalization

7.1 Codes

We give without proof the generalization of Theorem 6.1.

Theorem 7.1. *The code* C_1 *is a two-weight code with* $w_1 = p^2 - p$*, and* $w_2 = p^2 - 1$*. Letting* A_1 *and* A_2 *denote their respective frequencies, we have*

$$A_1 = (p+1)(p^h-1), \tag{12}$$
$$A_2 = p(p^{h-1}-1)(p^h-1). \tag{13}$$

This code is optimal as the next result shows.

Theorem 7.2. *The code C_1 meets the Griesmer bound for finite Frobenius rings with equality.*

Proof. Note that the residue field of L is $\mathbb{F}_p$. The rank of the free code C_1 is 2 and its minimum Hamming distance is $p^2 - p$. By theorem 3.11 of [18, p.27], or [20], we know that its length

$$n \geq (p^2 - p) + \left\lceil \frac{p^2 - p}{p} \right\rceil = p^2 - 1.$$

But, by construction $n = p^2 - 1$. The result follows. □

Theorem 7.3. *Assume $d > 1$ and $h > 1$. The code C_d is a two-weight code with $w_1 = p^2 - 1 - m$, where $m = (d, p+1)(p-1)$, and $w_2 = p^2 - 1$. Letting A_1 and A_2 denote their respective frequencies, we have*

$$A_1 = \frac{(p^2-1)}{m}((m+1)^h - 1), \tag{14}$$

$$A_2 = p^{2h} - 1 - A_1. \tag{15}$$

Remark 7.4. If $h = 1$ and $m = p - 1$, we have $A_1 = p^2 - 1$ and C_d is a one-weight code. This is the case $u = 1$ of [22].

Theorem 7.5. *The code $\widehat{C_1}$ is a two-weight code with parameters $(p+1, p^{2h}, \{p, p+1\})_{p^h}$. It is optimal with these parameters.*

Proof. The parameters of $\widehat{C_1}$ are obtained from those of C_1 by dividing length and weights by $p-1$. This code meets the Singleton bound of [18, Chap. 12]. Indeed, it is a free code of rank 2, length $p+1$ and distance p. It is thus MDR in the sense of [18, Chap. 12]. □

The analogous result for $d > 1$ is as follows.

Theorem 7.6. *The code $\widehat{C_d}$ is a two-weight code with parameters*

$$\left(\tfrac{(p^2-1)}{m}, p^{2h}, \left\{\tfrac{(p^2-1)}{m} - 1, \tfrac{(p^2-1)}{m}\right\}\right)_{p^h}.$$

Example 7.7. With $p = 7$, $h = 2$, $d = 2$, $m = 12$, the code $\widehat{C_2}$ has length 4 and weight distribution $[\langle 0, 1\rangle, \langle 2, 96\rangle, \langle 4, 2304\rangle]$.

7.2 Finite Graphs

The proof of the following theorem is analogous to that of Theorem 6.3 and is omitted.

Theorem 7.8. *The coset graph of $\widehat{C_1}^{\perp}$ is a SRG of degree $(p+1)(p^h-1)$, on p^{2h} vertices with restricted eigenvalues $p^h - p - 1$ and $-(p+1)$ with respective multiplicities A_1 and A_2 of Theorem 7.3.*

Example 7.9. With $p = 2$, $h = 4$, we obtain a SRG on 256 vertices, degree 45, unrestricted eigenvalues 13 and -3. Alternate constructions include as per [3] a $[15, 4, \{8, 12\}]_4$, a binary $[45, 8, \{16, 24\}]$.

Remark 7.10. In [4, p.121], an SRG is said to be of Latin square type if its parameters are

$$(v, \eta, \lambda, \mu) = (N^2, M(N-1), (M-1)(N-2) + N - 2, M(M-1)),$$

for some integers M, N with restricted eigenvalues $N - M, -M$, and respective multiplicities $M(N-1)$ and $(N - M + 1)(N - 1)$. It can be checked that the parameters above are of this form with $N = p^h, M = p + 1$.

The proof of the following is analogous to that of Theorem 6.5 and is omitted.

Theorem 7.11. *The coset graph of* $\widehat{C_d}^{\perp}$ *is a SRG of degree* $\frac{(p^2-1)}{m}(p^h - 1)$*, on* p^{2h} *vertices with restricted eigenvalues* $p^h - \frac{(p^2-1)}{m}$ *and* $-\frac{(p^2-1)}{m}$ *with respective multiplicities* A_1 *and* A_2 *of Theorem 7.3.*

Example 7.12. With $p = 7$, $h = 2$, $d = 2$, the code $\widehat{C_2}$ has length 4 and we obtain a SRG on $7^4 = 2401$ vertices of degree 192 with restricted eigenvalues $94, -4$. These parameters are beyond the table of [3]. They are not of Latin square type (see the preceding Remark).

7.3 Infinite Graphs

Denote by Γ_h the coset graph of $\widehat{C_1}^{\perp}$ over $\mathbb{Z}_{p^h}$. Following [9], we denote by $\mathbb{Z}_{p^\infty}$, the ring of p-adic integers, that is to say the topological closure of $\mathbb{Z}$ for the p-adic topology [15]. Denote by Γ_∞ the coset graph of $\widehat{C_1}^{\perp}$ over $\mathbb{Z}_{p^\infty}$. Both $\widehat{C_1}$ and $\widehat{C_1}^{\perp}$ can be seen as obtained by extension of scalars from their counterparts over $\mathbb{F}_p$, or as Hensel lifts from them [9]. Thus Γ_∞ is a graph with a denumerably many vertices. Recall that a *cover* of a graph H by a graph G is an adjacency preserving surjection from G to H. The next result shows that, roughly speaking, Γ_∞ is a kind of limit of the Γ_h's.

Theorem 7.13. *For all* $h > 0$*, we have*

- Γ_{h+1} *is a cover of* Γ_h*,*
- Γ_∞ *is a cover of* Γ_h*.*

Proof. Follows immediately by reduction modulo p^h, that preserves the coset graph definition. □

A similar result holds for any fixed $d > 1$ that divides $p^2 - 1$.

8 Conclusion

In this paper, we have constructed two-weight codes over chain rings by focusing on irreducible cyclic codes of dimension 2. This opens the way to considering other families of cyclic codes over these rings, or cyclic codes over other families of rings. Irreducible cyclic codes of dimension three or more over rings might have many weights.

Utilizing these specific codes, we have successfully constructed strongly regular graphs (SRGs). Based on the computations in this paper and in [17], it appears that the coset graphs of the dual of a maximum distance rank code of dimension 2 consistently yield SRGs of the Latin square type. A direct combinatorial explanation for this phenomenon might exist, especially considering the established equivalence between Mutually Orthogonal Latin Squares and MDS codes [11].

It is a worthwhile project to compute the spectrum of the graph Γ_∞ defined as the spectrum of its adjacency operator. An engineering application can be found in [16].

References

[1] L. D. Baumert, R. J. McEliece, Weights of irreducible cyclic codes, Inf. and Control, 1972, **20**(2): 158-175.

[2] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs*, Springer New York, 2012.

[3] Table of Strongly regular graphs, `https://www.win.tue.nl/~aeb/graphs/srg/`.

[4] A. E. Brouwer, W. H. Haemers, *Spectra of graphs*, Springer Science, 2011.

[5] A. E. Brouwer, H. Van Maldeghem, *Fragments of a text on strongly regular graphs*, `https://www.win.tue.nl/~aeb/`.

[6] E. Byrne, M. Greferath, T. Honold, Ring geometries, two-weight codes and strongly regular graphs, Des. Codes Cryptogr., 2008, **48**(1): 1-16.

[7] E. Byrne, M. Kiermaier, A. Sneyd, Properties of codes with two homogeneous weights, Finite Fields and their App., 2012, **18**(4): 711-727.

[8] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, Bull. of the London Math. Soc., 1986, **18**(2): 97-122.

[9] A. R. Calderbank, N. J. A. Sloane, Modular and p-adic cyclic codes, Des. Codes Cryptogr., 1995, **6**(1): 21-35.

[10] P. Delsarte, Weights of linear codes and strongly regular normed spaces, Discrete Math, 1972, **3**(1-3): 47-64.

[11] S. Golomb, E. Posner, Rook domains, Latin squares, affine planes, and error-distributing codes, IEEE Trans. Inf. Theory, 1964, **10**(3): 196-208.

[12] R. J. MacEliece, H. Rumsey Jr., Euler products, Cyclotomy and Coding, J. of Number Theory, 1972, **4**(3): 302-311.

[13] `http://magma.maths.usyd.edu.au/calc/`.

[14] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Pub. Co., 1977.

[15] J. P. Serre, *A course in arithmetic*, Springer Science, 2012.

[16] P. Solé, J. P. Tillich, Block codes for dyadic phase shift keying, in Springer LNCS, 1995: 244-262.

[17] M. Shi, Z. Zhang, P. Solé, Two-weight codes and second order recurrences, Chinese Journal of Electronics, 2019, **28**(6): 1127-1130.

[18] M. Shi, A. Alahmadi, P. Solé, *Codes and Rings: Theory and Practice*, Academic Press, 2017.

[19] K. Shiromoto, A Singleton-like bound for codes over finite rings, J. of Algebraic Combinatorics, 2000, **12**(1): 95-99.

[20] K. Shiromoto, L. Storme, A Griesmer bound for linear codes over quasi Frobenius rings, Discrete Appl. Math., 2003, **128**(1): 263-274.

[21] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, Finite Fields and their App., 2002, **8**(1): 1-17.

[22] G. Vega, Determining the full weight distribution of any irreducible cyclic code over any finite field of dimension two, available from `https://arxiv.org/pdf/1606.08510.pdf`.

[23] G. Vega, A critical review and some remarks about one- and two-weight irreducible cyclic codes, Finite Fields and their App., 2015, **33**(2): 1-13.

[24] Z. X. Wan, *Finite Fields and Galois Rings*, World Scientific, 2003.