Journal of Algebraic Combinatorics (2022) 55:173–184
https://doi.org/10.1007/s10801-020-01006-6

# Strongly regular graphs from reducible cyclic codes

**Minjia Shi**[1] · **Tor Helleseth**[2] · **Patrick Solé**[3]

Received: 21 December 2020 / Accepted: 28 December 2020 / Published online: 30 March 2021


**Abstract**
Let $p$ be a prime number. Reducible cyclic codes of rank 2 over $\mathbb{Z}_{p^m}$ are shown to have exactly two Hamming weights in some cases. Their weight distribution is computed explicitly. When these codes are projective, the coset graphs of their dual codes are strongly regular. The spectra of these graphs are determined.

**Keywords** 2-weight codes · Reducible cyclic codes · Strongly regular graphs

**Mathematics Subject Classification** Primary 94B15; Secondary 05E30

## 1 Introduction

Since the seminal paper of Delsarte [9] two-weight codes have been studied in symbiosis with combinatorial objects like strongly regular graphs (SRGs) [5,6,9] or geometrical structures like caps in projective spaces [8]. An important class of codes for construction of two-weight codes is that of irreducible cyclic codes [1,18]. In particular, it is conjectured that all two-weight projective irreducible cyclic codes are known [12,18]. More recently, *reducible* cyclic codes have been used as a source of construction of two-weight codes. The connection between SRG's and two-weight codes over finite fields was extended recently to two-weight codes over rings for the homogeneous weight [6,7].

This research is supported by the National Natural Science Foundation of China (12071001, 61672036), the Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20), the Academic Fund for Outstanding Talents in Universities (gxbjZD03).

✉ Minjia Shi
smjwcl.good@163.com

[1] Key Laboratory of Intelligent Computing and Signal Processing, Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei 230601, China

[2] The Selmer center, Department of Informatics, University of Bergen, Bergen, Norway

[3] I2M, CNRS, Centrale Marseille, University of Aix-Marseille, Marseille, France

In a companion paper [15], the authors have studied irreducible cyclic codes of rank 2 over $\mathbb{Z}_{p^m}$ that have two nonzero weights for the Hamming metric. In the present paper, we study *reducible* cyclic codes of rank 2 over $\mathbb{Z}_{p^m}$ that have two nonzero weights for the Hamming metric. Like in [13] the main enumeration technique is the connection with second-order recurrences. An extra difficulty in comparison with the finite field case is the size of the code which can be, in the case $m = 2$, either $p^4$ or $p^3$. This difficulty is overcome by using the notion of residue and torsion codes which are familiar in the domain of codes over rings [14]. Generalizing this approach to $m > 2$, is possible but very technical. In the section, on codes over $\mathbb{Z}_{p^m}$ we will not make any claims on the size of the code. Under a mild condition (see Proposition 3), our codes are projective, and thus SRGs can be constructed from them. Their size, degrees, their two restricted eigenvalues with their multiplicities are determined explicitly. They provide alternative coding constructions to some of the SRGs with parameters in Brouwer's table of SRGs [17].

The material is organized as follows. The next section collects notations, definitions and basic facts. Section 3 studies codes over $\mathbb{Z}_{p^2}$. Section 4 deals with their attached SRGs. Section 5 indicates how the material can be partially generalized to $\mathbb{Z}_{p^m}$. Section 5 recapitulates our results and presents some challenging open problems.

## 2 Definitions and notation

### 2.1 Linear codes over rings

Throughout the paper, let $p$ be an odd prime. Let $\mathbb{Z}_{p^m}$ denote the ring of integers modulo $p^m$, and let $\mathbb{Z}_{p^m}^{\times}$ denote its multiplicative group. The function $\phi()$ is Euler totient function. If $u$ and $v$ are two coprime integers, the notation $o_u(v)$ means the multiplicative order of $v$ modulo $u$, or in other words, its order as an element of the multiplicative group of the residue class ring $\mathbb{Z}_u$. A linear *code* $C$ of length $n$ over $\mathbb{Z}_{p^m}$ is a submodule of $\mathbb{Z}_{p^m}^n$. The residue and torsion codes of $C \leq \mathbb{Z}_{p^2}^n$, denoted $R(C)$ and $Tor(C)$ are two codes of length $n$ over $\mathbb{F}_p$ defined as

$$R(C) = \{r \in \mathbb{F}_p^n \mid \exists y \in C,\ y \equiv r \pmod{p}\},$$
$$Tor(C) = \{r \in \mathbb{F}_p^n \mid pr \in C\}.$$

Some elementary facts about these codes are as follows. For a proof of more general statements in the context of chain rings see [14, Chap. 5].

**Proposition 1** *If $C$ is a linear code over $\mathbb{Z}_{p^2}$, the following properties hold.*

1. *$R(C)$ are linear codes;*
2. *$R(C) \subseteq Tor(C)$;*
3. *$|C| = |R(C)||Tor(C)|$;*
4. *$\dim(Tor(C))$ is at most the rank of $C$ as a $\mathbb{Z}_{p^2}$-module.*

***Proof*** If $r \in R(C)$, then there is $s \in \mathbb{F}_p^n$ such that $r + ps \in C$. Hence $p(r + ps) = pr \in C$, and $r \in Tor(C)$. That proves 2. To prove point 3, we apply the first

isomorphism theorem to the map $\alpha : C \to \mathbb{F}_p^n$, defined by $x \mapsto x \pmod p$. Note that $\alpha(C) = R(C)$ and that $Ker(\alpha) = pTor(C)$. This remark also shows point 1. Point 4 is immediate from $pTor(C) \subseteq C$. □

### 2.2 Weights

The *Hamming weight* of $\mathbf{x} \in \mathbb{Z}_{p^2}^n$ is denoted by $w_H(\mathbf{x})$. The *weight distribution* of a code $C$ of length $n$ over $\mathbb{Z}_{p^2}$ is defined as the list

$$[\langle 0, 1\rangle, \ldots, \langle w_i, A_i\rangle, \ldots, \langle w_n, A_n\rangle],$$

where $A_i$ is the numbers of $c \in C$ with $w_H(c) = w_i$. The number $A_i$ is called the *frequency* of the weight $w_i$. The *dual* $C^\perp$ of $C$ is understood with respect to the standard inner product. The *minimum distance* of a linear code is its minimum nonzero Hamming weight. A linear code is *projective* if any pair of columns of its generator matrix are linearly independent.

### 2.3 Cyclic codes

A code is *cyclic* if it is linear and invariant under the cyclic shift. We consider cyclic codes of the form $\langle g(x)\rangle$ with $g(x)$ a divisor of $x^n - 1$. All the cyclic codes in this paper are *reducible*, in the sense that their *check polynomial* $h(x) = \frac{x^n-1}{g(x)}$ is *not* irreducible. The parameters of a two-weight code $C$ over an alphabet $A$ of size $q$ are listed as $[n, k, \{w_1, w_2\}]_q$ if $A$ is a finite field, and $C$ is of dimension $k$, and $(n, |C|, \{w_1, w_2\})_q$ if $A$ is a finite ring, but not a finite field.

### 2.4 Graphs

A simple graph on $v$ vertices is called a *strongly regular graph* with parameters $(v, \eta, \lambda, \mu)$ if

1. each vertex is adjacent to $\eta$ vertices;
2. for each pair of adjacent vertices, there are $\lambda$ vertices adjacent to both;
3. for each pair of non-adjacent vertices, there are $\mu$ vertices adjacent to both.

An *eigenvalue* of a graph $\Gamma$ (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 $\eta$-regular connected graph, the restricted eigenvalues are simply the eigenvalues different from $\eta$. The two restricted eigenvalues of an SRG are usually denoted by $r$, $s$, with respective multiplicities $f$, $g$. The *spectrum* of an SRG is then compactly denoted by $\{\eta^1, r^f, s^g\}$. Given the spectrum, the parameters $\lambda$, $\mu$ are uniquely determined by the formulas of [2, §1.1.1], or [5, Th. 1.3.1]. The *coset graph* of a projective code $C \subseteq \mathbb{Z}_{p^m}^n$ has for vertices the cosets of $C$, two vertices being connected iff they differ by a coset of minimum Hamming weight one.

## 3 Codes

Let $p$ an odd prime, and let $N > 1$ be a divisor of $\phi(p^m) = p^{m-1}(p-1)$. Let $a, b$ be two *distinct* elements of $\mathbb{Z}_{p^m}^{\times}$, both of order a divisor of $N$. Let $C(a,b)$ denote the cyclic code of length $N$ over $\mathbb{Z}_{p^m}$ of check polynomial $h(x) = \frac{(1-ax)(1-bx)}{ab}$. Its generator matrix $G$ can then be described as

$$G = \begin{pmatrix} a & a^2 & \dots & a^N \\ b & b^2 & \dots & b^N \end{pmatrix}.$$

Different pairs $(a,b)$ can construct equivalent codes $C(a,b)$ as the next result shows.

**Proposition 2** *If $(a,b) = \lambda(a',b')$ for some $\lambda \in \mathbb{Z}_{p^m}^{\times}$, then $C(a,b)$ and $C(a',b')$ are monomially equivalent. If $(a,b) = (a'^{\theta}, b'^{\theta})$ for some $\theta \in \mathbb{Z}_{p^m}^{\times}$, coprime with $N$, then $C(a,b)$ and $C(a',b')$ are permutation equivalent.*

***Proof*** If $(a,b) = \lambda(a',b')$ then the column $i$ of $G$ is scaled by $\lambda^i$. Hence, coordinate $i$ of each codeword is scaled by $\lambda^i$. This is monomial equivalence with an identity permutation part [11, §1.7]. The second assertion is a special case of multiplier equivalence of cyclic codes [11, §4.3]. □

For the next section, we need the following result.

**Proposition 3** *Assume $m = 2$. If $a \equiv b \pmod p$, the code $C(a,b)$ is not projective. If $a \neq b \pmod p$, the code $C(a,b)$ is a projective code iff $ord_{p^2}(\frac{b}{a}) \geq N$.*

***Proof*** Suppose there is a nontrivial linear combination between the columns of indices $i$ and $j$ of $G$ of the form

$$\lambda \begin{pmatrix} a^i \\ b^i \end{pmatrix} + \mu \begin{pmatrix} a^j \\ b^j \end{pmatrix} = 0.$$

Four cases can occur depending on the invertibility of $\lambda$ and $\mu$.

1. Since both $a$ and $b$ are invertible, the two cases $\lambda \notin \mathbb{Z}_{p^2}^{\times}$, $\mu \in \mathbb{Z}_{p^2}^{\times}$, or $\lambda \in \mathbb{Z}_{p^2}^{\times}$, $\mu \notin \mathbb{Z}_{p^2}^{\times}$, cannot happen.
2. If both $\lambda, \mu \in p\mathbb{Z}_{p^2}^{\times}$, then letting $\lambda = p\lambda'$, and $\mu = p\mu'$ yields

$$\lambda' \begin{pmatrix} a^i \\ b^i \end{pmatrix} + \mu' \begin{pmatrix} a^j \\ b^j \end{pmatrix} \equiv 0 \pmod p.$$

   (a) If $a \equiv b \pmod p$, the system reduces to

$$\lambda' a^i + \mu' a^j \equiv 0 \pmod p.$$

   Given $i < j$, it is easy to find $\lambda'$, $\mu'$ that satisfy that equation. So the code is not projective in that case.

(b) If, on the other hand, $a \not\equiv b \pmod p$, the system above forces $\lambda' = \mu' = 0$, entailing in turn $\lambda = \mu = 0$.

3. If both $\lambda, \mu \in \mathbb{Z}_{p^2}^{\times}$, then getting rid of $\lambda,\ \mu$ yields $(\frac{b}{a})^{j-i} = 1$, which is impossible if $ord_{p^2}(\frac{b}{a}) \geq N$ and $j - i < N$.

Case 2(a) proves the first assertion. From cases 2(b) and 3, the second assertion follows. □

### 3.1 $a \not\equiv b \pmod p$

In this subsection, assume $m = 2$. We give next a case where $C(a, b)$ is a two-weight code, and, in that case, compute its weight distribution.

**Theorem 1** *Let $e' = ord_p(\frac{b}{a})$, and $e = ord_{p^2}(\frac{b}{a})$. Suppose that $e' = e$, and that $a \not\equiv b \pmod p$. Then the code $C(a, b)$ has nonzero weights $\{N - \frac{N}{e}, N\}$. Their respective frequencies are*

$$A_1 = e(p^2 - 1),\ A_2 = (p^2 - 1)(p^2 - e + 1).$$

***Proof*** Write $c = (c_n)$ for a codeword of $C = C(a, b)$. By linearity $c_n = \lambda a^n + \mu b^n$, for some $\lambda, \mu \in \mathbb{Z}_{p^2}$..

1. $\mu \not\equiv 0 \pmod p$. Hence $\mu \in \mathbb{Z}_{p^2}^{\times}$, and we can rewrite the equation for $c_n$ as

$$c_n = \mu a^n \left( \frac{\lambda}{\mu} + (\frac{b}{a})^n \right).$$

   If $\frac{\lambda}{\mu} \in \langle \frac{b}{a} \rangle$, this equation in $n$ admits $\frac{N}{e}$ solutions, and $w_H(c) = N - \frac{N}{e}$.

   If, on the other hand, $\frac{\lambda}{\mu} \notin \langle \frac{b}{a} \rangle$, it has no solution and $w_H(c) = N$.
2. $\mu \equiv 0 \pmod p$, $\lambda \not\equiv 0 \pmod p$. By reduction $\pmod p$ we see that $c_n \neq 0$, and $w_H(c) = N$.
3. $\mu \equiv 0 \pmod p$, $\lambda \equiv 0 \pmod p$. That means that $c = pc'$ for some $c' \in Tor(C)$. But $Tor(C)$ is a replication of a reducible cyclic code of dimension 2 over $\mathbb{F}_p$. Thus, its possible nonzero weights are, by [15], $\{N',\ N' - \frac{N'}{e'}\}$, for some divisor $N'$ of $N$. Since $e' = e$, we see that

$$\frac{N}{N'}\{N',\ N' - \frac{N'}{e'}\} = \{N,\ N - \frac{N}{e}\}.$$

   We claim that $|C| = p^4$. This will be proved upon using Proposition 1 as follows. Since $R(C) \subseteq Tor(C)$ and $\dim R(C) = 2$, we see that $Tor(C) = R(C)$ (note that the dimension of $Tor(C)$ is at most 2 by point 4). Then $|C| = |R(C)||Tor(C)| = p^2 \times p^2 = p^4$, by the above considerations.

We can now compute the weight distribution of $C$ as a function of $N$ and $p$. Since $a, b \in \mathbb{Z}_{p^2}^{\times}$, we see that the dual distance of $C(a, b)$ is at least two. The frequencies of the weights can then be computed by the first two Pless power moments [10, §7.3]. They are thus solutions of the system

$$A_1 + A_2 = p^4 - 1, (N - \frac{N}{e})A_1 + NA_2 = p^2(p^2 - 1)N. \quad \square$$

*Example* For $p = 3$, $N = 6$ and $a = 1$, $b = 8$, we have $e = e' = 2$ and we obtain the weight distribution

$$[\langle 0, 1\rangle, \langle 3, 16\rangle, \langle 6, 64\rangle].$$

The case $e = N$ of Theorem 1 gives the best parameters.

**Corollary 1** *Let $e' = ord_p(\frac{a}{b})$, and $e = ord_{p^2}(\frac{a}{b})$. Suppose that $e' = e = N$, and that $a \neq b \pmod p$. Then the code $C(a, b)$ is optimal.*

***Proof*** In that case, the minimum distance is $N - 1$. The code is MDR in the sense of [14, Chap. 12]. $\square$

*Example* For $p = 5$, $N = 4$ and $a = 24$, $b = 7$, we have $e = e' = 4$ and we obtain the weight distribution

$$[\langle 0, 1\rangle, \langle 3, 96\rangle, \langle 4, 528\rangle].$$

### 3.2 $a \equiv b \pmod p$

In this subsection, assume $m = 2$. We give a construction with hypotheses exclusive from that of Theorem 1.

**Theorem 2** *Let $e = ord_{p^2}(\frac{a}{b})$. Suppose that $a \equiv b \pmod p$. Then the code $C(a, b)$ has nonzero weights $\{N - \frac{N}{e}, N\}$. Their respective frequencies are*

$$A_1 = e(p - 1), A_2 = (p - 1)(p^2 + p + 1 - e).$$

***Proof*** Write $c = (c_n)$ for a codeword of $C = C(a, b)$. By linearity $c_n = \lambda a^n + \mu b^n$, for some $\lambda, \mu \in \mathbb{Z}_{p^2}$. We have the same three cases as in the proof of Theorem 1, that is

1. $\mu \neq 0 \pmod p$;
2. $\mu \equiv 0 \pmod p$, $\lambda \neq 0 \pmod p$;
3. $\mu \equiv 0 \pmod p$, $\lambda \equiv 0 \pmod p$.

Points 1 and 2 can be treated as in the proof of Theorem 1. To deal with case three, we write $c = pc'$ with $c'_n = \lambda' a^n + \mu' b^n$. Now $c_n = 0$ iff $c'_n \equiv 0 \pmod p$, which happens iff $\lambda' + \mu' \equiv 0 \pmod p$, since $a^n \equiv b^n \pmod p$, and $a^n \not\equiv 0 \pmod p$. Thus either $c = 0$ or $c'_n \not\equiv 0$, for all $n = 1, 2, \ldots, N$. In that case $w_H(c) = N$.

We claim that $|C| = p^3$. Indeed $|R(C)| = p$, by the condition $a \equiv b \pmod p$. That $Tor(C) = R(C)$ is impossible since then the code would be generated by

$$\begin{pmatrix} a & a^2 & \dots & a^N \\ pa & pa^2 & \dots & pa^N \end{pmatrix},$$

which generates a one-weight code, contradicting the previous paragraph. Thus, $Tor(C)$ has dimension 2, by 4. of Proposition 1, and by 3. of Proposition 1 we obtain

$$|C| = |R(C)||Tor(C)| = p \times p^2 = p^3.$$

We can now compute the weight distribution of $C$. Since $a, b \in \mathbb{Z}_{p^2}^{\times}$, we see that the dual distance of $C(a, b)$ is at least two. The frequencies of the weights can then be computed by the first two Pless power moments [11, §7.3]. They are thus solutions of the system

$$A_1 + A_2 = |C| - 1, (N - \frac{N}{e})A_1 + NA_2 = N|C|\frac{(p^2-1)}{p^2}. \qquad \square$$

*Example* For $p = 3$, $N = 6$ and $a = 1$, $b = 4$, or $a = 1$, $b = 7$, we have $e = 3$ and we obtain the weight distribution

$$[\langle 0, 1\rangle, \langle 4, 6\rangle, \langle 6, 20\rangle].$$

## 4 Strongly regular graphs

Define the graph $\Gamma(a, b)$ as the coset graph of $C(a, b)^{\perp}$. The codes of Theorem 1 give the following graphs.

**Theorem 3** *Keep the notation and hypotheses of Theorem 1. Assume, furthermore, that* $ord_{p^2}(\frac{b}{a}) \geq N$. *Then the graph* $\Gamma(a, b)$ *is a SRG on* $p^4$ *vertices of degree* $N(p^2 - 1)$. *Its restricted eigenvalues are* $\frac{N}{e}(q - e), -N$ *of respective multiplicities* $A_1$, $A_2$ *of Theorem 1.*

***Proof*** By Proposition 3 the code $C(a, b)$ is projective, which shows that $\Gamma(a, b)$ has no multiple edges. By Theorem 11.1.11 of [2], the restricted eigenvalues are computed as $\lambda_i = n(p^2 - 1) - p^2 w_i'$ for $i = 1, 2$ with the weights $w_1' = N - \frac{N}{e}$ and $w_2' = N$ from Theorem 1, and their multiplicities equal the frequencies of the corresponding weights. $\square$

*Examples*

- For $p = 3$, $N = 2$ and $a = 1, b = 8$, we have $e = e' = N = 2$ and we obtain a SRG of parameters $(81, 16, 7, 2)$, and spectrum $\{16^1, 7^{16}, -2^{64}\}$. This SRG is unique with these parameters from [17]. Alternative constructions include

a $[8, 4, \{6, 9\}]_3$. The fact that $C(1, 8)^{\perp} = \{0\}$, shows that it is a Hamming graph $H(2, 9)$, also called grid graph in [2, p.262].

- For $p = 5$, $N = 4$ and $a = 24, b = 7$, we have $e = e' = N = 4$ and we obtain a SRG of parameters $(625, 96, 29, 12)$, and spectrum $\{96^1, 21^{96}, -4^{528}\}$. Alternative constructions from [17] are from a $[24, 4, \{15, 20\}]_5$, and [3]. It would be interesting to find a direct link between the $[24, 4, \{15, 20\}]_5$, and our $(4, 25^2, \{3, 4\})_{25}$.

## 5 Generalization

In this section, we indicate briefly how the previous constructions generalize from $p^2$ to $p^m$. The length of the codes considered is $N \mid \phi(p^m) = p^{m-1}(p-1)$. The generalization of Theorem 1 is as follows. Note that, since no claim is made on $|C(a, b)|$ we can do without the hypothesis $a \neq b \pmod{p^{m-1}}$.

**Theorem 4** *Let $m \geq 2$ be an integer, and put $e_i = ord_{p^{m-i}}(\frac{a}{b})$. Suppose that for all $i = 0, 1, \ldots, m-1$ we have $e_i = e$. Then the code $C(a, b)$ has nonzero weights $\{N - \frac{N}{e}, N\}$. Their respective frequencies are*

$$A_1 = e\left(\frac{M}{p^m} - 1\right), A_2 = M - 1 - e\left(\frac{M}{p^m} - 1\right),$$

*where we have let $M = |C(a, b)|$.*

***Proof*** The proof goes by induction on $m$. The base point $m = 2$ of the induction is Theorem 3 of [15]. Write $c = (c_n)$ for a codeword of $C = C(a, b)$. By linearity $c_n = \lambda a^n + \mu b^n$, for some $\lambda, \mu \in \mathbb{Z}_{p^m}$. We have the same three cases as in the proof of Theorem 1, that is

1. $\mu \not\equiv 0 \pmod{p}$;
2. $\mu \equiv 0 \pmod{p}$, $\lambda \not\equiv 0 \pmod{p}$;
3. $\mu \equiv 0 \pmod{p}$, $\lambda \equiv 0 \pmod{p}$.

Points 1 and 2 are exactly like before. To deal with case three, we write $c = pc'$ with $c'_n = \lambda' a^n + \mu' b^n$. In fact $c'_n \pmod{p^m}$ is a replication of a codeword in a code $C(a', b')$, of length $N' \mid N$ with $a', b'$ the remainders of $a$ and $b$, respectively, under division by $p^{m-1}$. Thus, its possible nonzero weights are, by induction hypothesis, $\{N', N' - \frac{N'}{e_1}\}$, for some divisor $N'$ of $N$. Since $e_1 = e_0 = e$, we see that

$$\frac{N}{N'}\left\{N',\ N'-\frac{N'}{e_1}\right\}=\left\{N,\ N-\frac{N}{e}\right\}.$$

Since $a, b \in \mathbb{Z}_{p^m}^{\times}$, we see that the dual distance of $C(a,b)$ is at least two. The frequencies of the weights can then be computed by the first two Pless power moments [11, §7.3]. They are thus solutions of the system

$$A_1+A_2=M-1,\left(N-\frac{N}{e}\right)A_1+NA_2=NM\frac{(p^m-1)}{p^m}.$$

□

The generalization of Theorem 2 is as follows.

**Theorem 5** *Let $e = ord_{p^m}(\frac{a}{b})$. Suppose that $a \equiv b \pmod{p^{m-1}}$. Then the code $C(a,b)$ has nonzero weights $\{N-\frac{N}{e}, N\}$. Their respective frequencies are*

$$A_1=e\left(\frac{M}{p^m}-1\right),A_2=M-1-e\left(\frac{M}{p^m}-1\right),$$

*where we have let $M = |C(a,b)|$.*

***Proof*** Write $c = (c_n)$ for a codeword of $C = C(a,b)$. By linearity $c_n = \lambda a^n + \mu b^n$, for some $\lambda, \mu \in \mathbb{Z}_{p^m}$. We have the same three cases as in the proof of Theorem 1, that is

1. $\mu \not\equiv 0 \pmod{p}$;
2. $\mu \equiv 0 \pmod{p}$, $\lambda \not\equiv 0 \pmod{p}$;
3. $\mu \equiv 0 \pmod{p}$, $\lambda \equiv 0 \pmod{p}$.

Points 1 and 2 are exactly like before. To deal with case three, we write $c = pc'$ with $c'_n = \lambda' a^n + \mu' b^n$. Now $c_n = 0$ iff $c'_n \equiv 0 \pmod{p^{m-1}}$, which happens iff $\lambda' + \mu' \equiv 0 \pmod{p^{m-1}}$, since $a^n \equiv b^n \pmod{p^{m-1}}$, and $a^n \not\equiv 0 \pmod{p^m}$. Thus either $c = 0$, or $c'_n \not\equiv 0$, for all $n = 1, 2, \ldots, N$. In that case $w_H(c) = N$.

The computation of the weight distribution is the same as in the proof of Theorem 4.

□

Denote by $\Gamma(a,b)$ the coset graph for $C(a,b)^{\perp}$.

**Theorem 6** *Keep the notation and hypotheses of Theorem 4. Assume, furthermore, that $C(a,b)$ is projective. Then the graph $\Gamma(a,b)$ is a SRG on $|C(a,b)|$ vertices of degree $N(p^m-1)$. Its restricted eigenvalues are $\frac{N}{e}(q-e), -N$ of respective multiplicities $A_1$, $A_2$ of Theorem 4.*

The proof is similar to that of Theorem 3 and is omitted.

*Example* For $p = m = 3$, $N = 2$ and $a = 1\, b = 8$, we have $e = 2$ and we obtain the weight distribution

$$[\langle 0,1\rangle, \langle 1,52\rangle, \langle 2,676\rangle],$$

yielding a SRG of parameters $(729, 52, 25, 2)$, with the spectrum $\{52^1, 25^{52}, -2^{676}\}$. As per [17], the SRG is unique with these parameters and can be also constructed from a $[26, 6, \{9, 18\}]_3$. The fact that $C(1, 8) = \mathbb{Z}_{27}^2$ shows that it is the Hamming graph $H(2, 27)$ in the notation of [5].

## 6 Double-root cyclic codes

Let $p$ an odd prime, and let $N > 1$ be a divisor of $p\phi(p^m) = p^m(p-1)$. Let $a$ be an element of $\mathbb{Z}_{p^m}^{\times}$. Let $C((a))$ denote the cyclic code of length $p^m(p-1)$ over $\mathbb{Z}_{p^m}$ of check polynomial $h(x) = (\frac{(1-ax)}{a})^2$. Note that, since $\frac{(1-ax)}{a} \mid x^{\phi(p^m)} - 1$ its square $h(x)$ divides $x^{p\phi(p^m)} - 1 = (x^{\phi(p^m)} - 1)^p$. Consider the punctured code $C_a$ of length $p$ of $C((a))$ defined by its generator matrix $G_a$ as

$$G_a = \begin{pmatrix} a & a^2 & \dots & a^p \\ a & 2a^2 & \dots & pa^p \end{pmatrix}.$$

**Theorem 7** *The code $C_a$ is a projective two-weight code of parameters $(p, p^{2m}, \{p-1, p\}$, with weight distribution*

$$[\langle 1, 0\rangle, \langle p-1, p(p^m-1)\rangle, \langle p, (p^m-1)(p^m-p+1)\rangle].$$

***Proof*** The code is projective as can be seen by adapting the proof of Proposition 3. Computing the determinant of $\begin{pmatrix} a^i & a^j \\ ia^i & ja^j \end{pmatrix}$, which equals $(j-i)a^{i+j}$, modulo $p^{m-1}$ concludes the last case of the proof.

The determination of the weights goes by induction on $m$. The base point $m = 1$ of the induction is Theorem 3 of [13]. Write $c = (c_n)$ for a codeword of $C = C_a$. By linearity $c_n = (\lambda + \mu n)a^n$, for some $\lambda, \mu \in \mathbb{Z}_{p^m}$. We have the same three cases as in the proof of Theorem 1, that is

1. $\mu \not\equiv 0 \pmod{p}$;
2. $\mu \equiv 0 \pmod{p}$, $\lambda \not\equiv 0 \pmod{p}$;
3. $\mu \equiv 0 \pmod{p}$, $\lambda \equiv 0 \pmod{p}$.

In case 1, the equation $c_n = 0$ has at most one solution in $n$. In that case, $w_H(c) = p-1$ or $w_H(c) = p$. Case 2 by reduction modulo $p$ implies that $c_n \neq 0$. In case 3, we write $c_n = pc'_n$, where $c'_n$ belongs to the code $C_a$ over $\mathbb{Z}_{p^{m-1}}$ and conclude by induction hypothesis.

The weight distribution is determined by solving the system

$$A_1 + A_2 = p^{2m} - 1, (p-1)A_1 + pA_2 = p^m(p^m-1)p. \qquad \square$$

*Examples*

1. For $p = 3$, $m = 2$ with $a = 1$, we obtain a code of weight distribution

$$[\langle 0, 1\rangle, \langle 2, 16\rangle, \langle 3, 64\rangle],$$

and a SRG of parameters $(81, 24, 9, 6)$ with spectrum $\{24^1, 6^{16}, -3^{64}\}$. An alternate construction from [4] is by considering a $[12, 4, \{6, 9)]_3$.

2. For $p = 3$, $m = 3$ with $a = 1$, we obtain a code of weight distribution

$$[\langle 0, 1\rangle, \langle 2, 78\rangle, \langle 3, 650\rangle],$$

and a SRG of parameters $(729, 78, 27, 6)$ with spectrum $\{78^1, 24^{78}, -3^{650}\}$. Alternate construction from [17]: a $[39, 6, \{18, 27\}]_3$.

3. For $p = 5$, $m = 2$ with $a = 1$, we obtain a code of weight distribution

$$[\langle 0, 1\rangle, \langle 4, 120\rangle, \langle 5, 504\rangle],$$

a SRG on parameters $(625, 120, 35, 20)$ with spectrum $\{120^1, 20^{120}, -5^{504}\}$. An alternate construction from [17] is by considering a $[30, 4, \{20, 25)\}]_5$.

## 7 Conclusion

In this paper, we have constructed projective two-weight codes from reducible cyclic codes of rank 2 over the ring $\mathbb{Z}_{p^m}$. The weight distribution, and, in some cases, the size of the code, have been determined explicitly. In particular, when the check polynomial is a square, we have used a punctured code to construct projective two-weight codes.

In all these constructions, the same weight distributions are reached several times for different values of $a$ and $b$, or of $a$ in the double-root case. It would be interesting to know how many of the codes with the same weight distribution are permutation inequivalent. Proposition 2 is a first step in that direction. From the projective two-weight codes constructed SRGs have been built, giving rise to alternative realizations of the parameters in [17], using shorter codes over larger alphabets. In such a case, finding a direct link between the two codes involved in the spirit of [16] might be illuminating.

At a more fundamental level, generalizing this work to other rings is a promising direction of research.

**Acknowledgements** All authors thank Denis Krotov for helpful discussions.

## References

1. Baumert, L.D., McEliece, R.J.: Weights of irreducible cyclic codes. Information and Control **20**, 158–175 (1972)
2. Brouwer, A.E., Van Maldeghem, H.: Fragments of a text on strongly regular graphs. https://www.win.tue.nl/~aeb/
3. Brouwer, A.E.: Some new two-weight codes and strongly regular graphs. Discrete Appl. Math. **10**, 111–114 (1985)
4. Brouwer, A.E., Haemers, W.H.: Spectra of Graphs. Universitext. Springer, New York (2012)
5. Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-Regular Graphs. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 18. Springer-Verlag, Berlin (1989)

6. Byrne, E., Greferath, M., Honold, T.: Ring geometries, two-weight codes and strongly regular graphs. Des. Codes Cryptogr. **48**, 1–16 (2008)
7. Byrne, E., Kiermaier, M., Sneyd, A.: Properties of codes with two homogeneous weights. Finite Fields Appl. **18**, 711–727 (2012)
8. Calderbank, R., Kantor, W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. **18**, 97–122 (1986)
9. Delsarte, P.: Weights of linear codes and strongly regular normed spaces. Discrete Math. **3**, 47–64 (1972)
10. http://magma.maths.usyd.edu.au/calc/
11. Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)
12. Schmidt, B., White, C.: All two-weight irreducible cyclic codes? Finite Fields Appl. **8**, 1–17 (2002)
13. Shi, M., Helleseth, T., Solé, P.: Two-Weight Codes Over the Integers Modulo a Prime Power, Submitted. arXiv:1911.07657
14. Shi, M., Alahmadi, A., Solé, P.: Codes and Rings: Theory and Practice. Academic Press, London (2017)
15. Shi, M., Zhang, Z., Solé, P.: Two-weight codes and second order recurrences. Chinese Journal of Electronics **28**(6), 1127–1130 (2019)
16. Shi, M., Krotov, D., Solé, P.: A new approach to the Kasami codes of type 2. IEEE Trans. Inform. Theory **66**(4), 2456–2465 (2019)
17. Table of Strongly Regular Graphs. https://www.win.tue.nl/~aeb/graphs/srg/
18. Vega, G.: A critical review and some remarks about one- and two-weight irreducible cyclic codes. Finite Fields Appl. **33**, 1–13 (2015)