Three-Weight Codes over Rings and Strongly Walk Regular Graphs

Minjia Shi¹ · Michael Kiermaier² · Sascha Kurz² · Patrick Solé³

Received: 27 September 2020 / Revised: 27 September 2021 / Accepted: 29 September 2021 / Published online: 14 March 2022
© The Author(s), under exclusive licence to Springer Japan KK, part of Springer Nature 2022

Abstract
We construct strongly walk-regular graphs as coset graphs of the duals of codes with three non-zero homogeneous weights over \( \mathbb{Z}_{p^m} \), for \( p \) a prime, and more generally over chain rings of depth \( m \), and with a residue field of size \( q \), a prime power. In the case of \( p = m = 2 \), strong necessary conditions (diophantine equations) on the weight distribution are derived, leading to a partial classification in modest length. Infinite families of examples are built from Kerdock and generalized Teichmüller codes. As a byproduct, we give an alternative proof that the Kerdock code is nonlinear.

Keywords Strongly walk-regular graphs · Three-weight codes · Homogeneous weight · Kerdock codes · Teichmüller codes

Mathematics Subject Classification Primary 05 E 30 · Secondary 94 B 05

This research is supported by National Natural Science Foundation of China (12071001) and Excellent Youth Foundation of Natural Science Foundation of Anhui Province (1808085J20)

Minjia Shi
smjwcl.good@163.com

¹ Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, School of Mathematical Sciences, Anhui University, Hefei, Anhui, China
² Department of Mathematics, University of Bayreuth, Bayreuth, Germany
³ I2M, CNRS, Centrale Marseille, Aix-Marseille University, Marseille, France
1 Introduction

Since the seminal article of Delsarte [1], there is a well-known interplay between two-weight codes and strongly regular graphs (SRG) via the coset graph of the dual code [2, 3]. Strongly walk-regular graphs (SWRG) were introduced in ref. [4] as a generalization of strongly regular graphs. Instead of a regularity condition bearing on paths of length 2, the notion of SWRG demands a regularity on paths of length \( s > 1 \). Specifically, a graph is \( s \)-SWRG if there are three integers \((\lambda, \mu, \nu)\) such that the number of paths of length \( s \) between any two vertices \( x \) and \( y \) is

- \( \lambda \) if \( x \) and \( y \) are connected;
- \( \mu \) if \( x \) and \( y \) are disconnected;
- \( \nu \) if \( x = y \).

This is reminiscent of strongly regular graph (SRG) a regular graph on \( v \) vertices such that the number of paths of length 2 between any two vertices \( x \) and \( y \) is

- \( \lambda \) if \( x \) and \( y \) are connected;
- \( \mu \) if \( x \) and \( y \) are disconnected;
- \( \kappa \) if \( x = y \).

Note that an immediate counting argument shows that strongly regular graphs are \( s \)-SWRG for all \( s > 1 \). In a previous paper [5], the authors connected together the two notions of triple sum sets (TSS) and SWRG over finite fields. In the present paper we extend this correspondence to a correspondence between TSS’s over certain finite rings and SWRG’s via the notions of syndrome graphs and homogeneous weights. This leads us to study the sum of the weights of three-weight codes. The first class of rings we consider is that of \( \mathbb{Z}_{pm} \), for \( p \) a prime, when the homogeneous weight can be described explicitly. Building on the study in ref. [6], we give a sufficient condition to construct SWRGs from the dual code of a three-weight code. This condition bears on the sum of the three weights in question. In concrete examples, we focus on \( \mathbb{Z}_4 \)-codes which have been studied extensively since [7]. The Gray map, which preserves MacWilliams duality, allows us to write the four Pless power moments for the binary image code, and to classify the relevant three-weight codes in short length. Further, a class of irreducible cyclic codes [8] related to the Kerdock code [7] gives an alternative proof of the nonlinearity of the binary Kerdock code. The second class of rings considered is that of chain rings of given depth and residue field. The \( p \)-ary three-weight codes introduced in ref. [9], and the generalized Teichmüller codes of [10] provide infinite families of three-weight codes leading to SWRG’s.

The material is organized as follows. The next section collects some prerequisite on, successively, homogeneous weights, triple sum sets, and coset graphs of codes over rings. Section 3 derives the preliminary results coming from spectral graph theory. Section 4 focuses on \( \mathbb{Z}_4 \) codes, derives strong necessary conditions, gives examples in short lengths, as well as an infinite family related to the Kerdock codes. Section 5 describes how the main results extend when the alphabet is a finite chain ring, and gives an infinite family related to generalized Teichmüller codes.
2 Background

2.1 Homogeneous Weight

For simplicity, let $R$ be a finite commutative ring. A linear code $C$ over $R$ of length $n$ is an $R$-submodule of the standard $R$-module $R^n$. The dual code of $C$ is defined as $C^\perp = \{x \in R^n \mid x \cdot C = 0\}$, where $x \cdot y = x_1y_1 + \ldots + x_ny_n$ denotes the standard inner product on $R^n$.

**Definition 1** Let $R$ be a finite ring. A function $w : R \to \mathbb{R}$ is called a homogeneous weight, 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 $\gamma \neq 0$ such that $\sum_{y \in Rx} w(y) = \gamma |Rx|$ for all $x \in R \setminus \{0\}$.

It is known from the work in ref. [11–13] that a homogeneous weight exists for all finite commutative rings $R$, and is uniquely determined up to the normalization factor $\gamma$. In the sequel we will denote the homogeneous weight by $w_{\text{hom}}$, assuming that $\gamma$ has been fixed. As usual we extend $w_{\text{hom}}$ to a weight function on $R^n$ by

$$w_{\text{hom}}(x_1, \ldots, x_n) = \sum_{i=1}^n w_{\text{hom}}(x_i).$$

The set $R^n$ then forms a distance space under the homogeneous distance $d_{\text{hom}}$ defined by $d_{\text{hom}}(x, y) = w_{\text{hom}}(x - y)$. A code $C \subseteq R^n$ is called a (homogeneous) three-weight code with weights $w_1 < w_2 < w_3$ if every non-zero codeword has homogeneous weight $w_1, w_2,$ or $w_3$, and the three weights actually occur. If the code $C$ is linear then on $C \times C$ the homogeneous distance takes only these three values and zero.

A matrix $G \in R^{\ell \times n}$ is called a generator matrix of the linear code $C$ if the rows of $G$ generate $C$ as an $R$-module.

**Definition 2** Let $C$ have $\ell \times n$ generator matrix $G = [g_1|\ldots|g_n]$. The code $C$ is called:

1. regular if $\{x \cdot g_i \mid x \in R^{\ell}\} = R$ for $i = 1, \ldots, n$;
2. projective if $Rg_i \neq Rg_j$ for any pair of distinct coordinates $i, j \in \{1, \ldots, n\}$.

In particular, a code is regular if every column contains at least one unit element. We extend this notion also to a single column vector.

In the sequel we shall be interested mostly in the case $R = \mathbb{Z}_p^m$, the ring of integers modulo a prime power $p^m$. In this case the homogeneous weight is given by
The chosen normalization constant is $\gamma = (p - 1)p^{m-2}$, which is the most convenient for our purposes. For $m \geq 2$ the homogeneous weight is always an integer. For general $p$ and $m$, regular and projective is characterized by a metric property of the dual [14]. For $p = m = 2$, the homogeneous distance coincide with the classical Lee distance of [7]. For a $\mathbb{Z}_4$-code to be both regular and projective is equivalent to $d^\perp \geq 3$, where $d^\perp$ denotes the dual Lee distance.

### 2.2 Triple Sum and s-Sum Sets

We extend the definition of triple sum sets given in ref. [15] from finite fields to finite commutative rings $R$ with a unit group $R^\times$. The set $\Omega \subseteq R^k$ is a *triple sum set* (TSS) if it is stable by scalar multiplication by units $\in R^\times$ and if there are integer constants $\sigma_0$ and $\sigma_1$ such that a non-zero $h \in R^k$ can be written as

$$h = x + y + z, \quad \text{with } x, y, z \in \Omega,$$

- $\sigma_0$ times if $h \in \Omega$,
- $\sigma_1$ times if $h \in R^k \setminus \Omega$.

This can generalized immediately to the notion of an *s-sum set* by replacing the equation $h = x + y + z$ by $h = \sum_{i=1}^s x_i$ where each $x_i \in \Omega$.

### 2.3 Syndrome Graph

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 $\eta$.

**Definition 3** Let $T$ be a finite abelian group and $S \subseteq T$ a subset satisfying $S = -S$ and $0_T \not\in S$. The corresponding *Cayley graph* $C(T, S)$ has vertex set equal to $T$; two vertices $g, h \in T$ are adjacent in $C(T, S)$ iff $g - h \in S$.

The conditions imposed on $S$ ensure that $C(T, S)$ is a simple graph. The graph $C(T, S)$ is regular of degree $|S|$, and it is connected iff $S$ generates the group $T$. We use the same idea as in ref. [16] to associate with any linear code $C$ over $\mathbb{Z}_{p^m}$ a certain Cayley graph, called the *syndrome graph* of $C$ and denoted by $\Gamma(C)$.

Let $H = [h_1 \mid \ldots \mid h_\eta] \in (\mathbb{Z}_{p^m})^{\ell \times n}$ be a parity-check matrix of $C$. The vertex set of $\Gamma(C)$ is $V = \{Hx; x \in (\mathbb{Z}_{p^m})^n\}$, the column space of $H$, which is isomorphic to the
The elements of $V$ are called syndromes of $C$. Two syndromes $Hx, Hy$ are adjacent in $\Gamma(C)$ if they differ by a unit-multiple of a column of $H$:

$$Hx \sim Hy : \iff H(x - y) = uh_i \quad \text{for some } 1 \leq i \leq n \text{ and } u \in \mathbb{Z}_p^m. \quad (1)$$

It is obvious that $\Gamma(C)$ is the Cayley graph of $V$ corresponding to the generating set $S = \{uh_i: u \in \mathbb{Z}_p^m, 1 \leq i \leq n\}$. If $C$ is regular then $0 \not\in S$ and $-S \subseteq S$, implying that $\Gamma(C)$ is simple. Moreover, if $C$ is projective, $\Gamma(C)$ is regular of degree $|S| = p^{m-1}(p - 1)n$ and has $\frac{p^m}{|S|}$ vertices. The latter follows from $|C||C^\perp| = |\mathbb{Z}_p^n|^n = p^{mn}$.

As defined, $\Gamma(C)$ depends on the particular choice of $H$. The terminology “syndrome graph of $C$” is justified, however, since $\Gamma(C)$ has another representation as a “coset graph” of $C$, which shows that its isomorphism type is determined by $C$. It is well-known that there is a one-to-one correspondence between syndromes of a code and its cosets [17], given by $x + C \rightarrow Hx$. The condition in (1) can be restated as $H(x - y - ue_i) = 0$, where $e_i$ denotes the $i$th standard unit vector in $(\mathbb{Z}_p^n)^n$. Thus $\Gamma(C)$ is isomorphic to the graph whose vertices are the cosets of $C$ and in which two vertices $x + C, y + C$ are adjacent if their difference is a coset of the form $ue_i + C$.

This is the Cayley graph of the quotient group $(\mathbb{Z}_p^n)^n / C$ with generating set

$$S^* = \cup_{i=1}^n \cup_{u \in \mathbb{Z}_p^m} (ue_i + C).$$

Now, we recall the relation between the weight distribution of a linear code over $\mathbb{Z}_p^n$ and the eigenvalues of the syndrome graph of its dual code. This extension of Lemma 3.4 in ref. [16] was derived in ref. [6] Theorem 4.1 and its proof is omitted here.

**Theorem 1** Suppose that $C$ is a regular, projective linear code over $\mathbb{Z}_p^n$ with homogeneous weights $w_i$ and corresponding weight distribution $A_i = |\{x \in C; w_{\text{hom}}(x) = w_i\}|$. Then the eigenvalues of $\Gamma(C^\perp)$ are $n(p - 1)p^{m-1} - pw_i$ with multiplicity $A_i$.

The coset graph with $b$ loops $\Gamma(C)^b$ of a code $C$ is obtained from $\Gamma(C)$ by adding $b$ loops around every vertex. The following result is immediate from the previous theorem. The proof is omitted. (In general, we call dual weight distribution of a code the weight distribution of the dual code).

**Corollary 1** If $C$ is a $\mathbb{Z}_p^n$-code, with dual weight distribution $[(w_i, A_i)]$, such that $C^\perp$ is regular and projective, then the spectrum of $\Gamma(C)^b$ is $\{b + n(p - 1)p^{m-1} - pw_i)^{A_i}\}$. Thus $A_i$ is the frequency of the homogeneous weight $w_i$ in $C^\perp$ and the multiplicity of the eigenvalue $b + n(p - 1)p^{m-1} - pw_i$.

### 3 Spectral Graph Theory

Let $\overline{R^k}$ denote the set of all regular vectors in $R^k$, i.e.,

\[\overline{R^k} = \{v \in R^k; \sum_{i=1}^k v_i = 0\}\]
\( R^k = \{ \omega \in \mathbb{R}^k : \{ \omega \cdot x : x \in \mathbb{R}^k \} = \mathbb{R} \} \).

If \( \Omega \subseteq R^k \), we denote by \( C(\Omega) \) the regular and projective code of length \( n = \frac{||\Omega||}{||R^k||} \) obtained as the kernel of the \( k \times n \) matrix \( H \) with columns the projectively non-equivalent elements of \( \Omega \). Thus \( H \) is the check matrix of \( C(\Omega) \). To simplify notation, let \( \Gamma_{C(\Omega)} = \Gamma(\Omega) \) and \( \Gamma_{C(\Omega)}^b = \Gamma(\Omega)^b \), where we also write \( \Gamma(\Omega)^0 \) for \( \Gamma(\Omega) \).

The following result is immediate from the definitions in the introduction, and will be used repeatedly and implicitly in the rest of the paper.

**Theorem 2** Keep the above notation. Assume that \( C(\Omega) \) is regular and projective. The following are equivalent

- \( \Omega \) (resp. \( \Omega \cup 0 \)) is an \( s \)-sum set,
- \( \Gamma(\Omega) \) (resp. \( \Gamma(\Omega)^1 \)) is an \( s \)-SWRG.

**Proof** Observe that \( \Gamma(\Omega) \) is a Cayley graph on the group \( (R^k, +) \) with generators the columns of \( H \). Thus the definition of an \( s \)-sum set can be regarded as a statement on the number of paths of length \( s \) between 0 and a linear combination of \( s \) columns of \( H \). (By translation, we can assume that 0 is the first endpoint of the path).

The following result comes from the well-known connection between SRGs and two-weight codes. It is described for codes over fields in ref. [2, 3], and for codes over rings in ref. [18].

**Theorem 3** If \( C(\Omega)^1 \) is a two-weight code, then both \( \Omega \cup 0 \) and \( \Omega \) are \( s \)-sum sets for all \( s > 1 \).

**Proof** If \( C(\Omega)^1 \) is a two-weight code, it is well-known that \( \Gamma(\Omega) \) is an SRG [18]. The result follows by Theorem 2, and the observation, made in the introduction, that SRGs are \( s \)-SWRG for all \( s > 1 \).

The following result was observed in ref. [19] Theorem III.6 for the Hamming weight.

**Theorem 4** If \( \Omega \) or \( \Omega \cup 0 \) is an \( s \)-sum set, then \( C(\Omega)^1 \) has at most three nonzero weights. Furthermore, if \( s \) is even, then \( C(\Omega)^1 \) is a 2-weight code.

**Proof** This is a consequence of [4, Theorem 3.4] applied to the graph \( \Gamma(\Omega) \), and based on Theorem 2.

We come to the coding-theoretic characterization of 3-sum sets which is contained for finite fields in ref. [15, Th. 2.1]. The consideration of syndrome graphs with loops might seem artificial but is justified by the existence of several non-trivial examples, as evidenced by Sect. 4.

The relation with the 3-SWRG property and the eigenvalues of a connected regular graph was obtained in ref. [4] Proposition 4.1:

**Theorem 5** Let \( \Gamma \) be a connected regular graph with four distinct eigenvalues \( k > \theta_1 > \theta_2 > \theta_3 \). Then \( \Gamma \) is a 3-SWRG iff \( \theta_1 + \theta_2 + \theta_3 = 0 \).
In our setting the formulas for the eigenvalues in Theorem 1 and Corollary 1 give:

**Theorem 6** Assume that $C(\Omega)\perp$ is of length $n$ and has three nonzero weights $w_1 < w_2 < w_3$. Let $b$ be any non-negative integer.

- $\Omega$ is a TSS iff $w_1 + w_2 + w_3 = 3n(p-1)p^{m-2}$;
- $\Omega \cup 0$ is a TSS iff $w_1 + w_2 + w_3 = 3\frac{1+n(p-1)p^{m-1}}{p}$;
- $\Gamma^b_{C(\Omega)}$ is a 3-SWRG iff $w_1 + w_2 + w_3 = 3\frac{b+n(p-1)p^{m-1}}{p}$.

**Proof** For the first two cases we apply Theorem 2 to conclude the equivalence to $\Gamma^b_{C(\Omega)}$ being a 3-SWRG for $b = 0$ and $b = 1$, respectively. Combining Corollary 1 with Theorem 5 gives the third case, which contains the first two cases for $b = 0$ and $b = 1$, respectively.

Note that if $m \geq 2$ and $p \neq 3$, then the second case of Theorem 6 is impossible. More generally, for the third case of Theorem 6 the assumptions $m \geq 2$ and $p \neq 3$ imply that $b$ has to be divisible by $p$. Then, the condition may be rewritten as $w_1 + w_2 + w_3 \geq 3n(p-1)p^{m-2}$ and $w_1 + w_2 + w_3 \equiv 0 (\mod 3)$.

**Example 1** If $p = m = 2$ and $n = 4$, then the possible triples of weights in the first case of Theorem 6 are, with simplified notation, and by increasing value of $w_2$ equal to

$$129, 138, 237, 147, 246, 345, 156, 255.$$ We will see in Subsect. 4.2 that none of these possibilities can be attained by a $\mathbb{Z}_4$-code and the smallest possible length for $p = m = 2$ and $b = 0$ is indeed $n = 6$.

Proposition 4.3 in ref. [4] gives an explicit diophantine equation bearing on the eigenvalues of $\Gamma$ to be an $s$-SWRG:

**Theorem 7** Let $\Gamma$ be a connected regular graph with four distinct eigenvalues $k > \theta_1 > \theta_2 > \theta_3$ and $s \geq 3$. Then $\Gamma$ is an $s$-SWRG iff

$$((\theta_2 - \theta_3)\theta_1^s + (\theta_3 - \theta_1)\theta_2^s + (\theta_1 - \theta_2)\theta_3^s = 0. \tag{2}$$

We remark that for $s = 3$ eq. (2) is equivalent to $(\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3)(\theta_1 + \theta_2 + \theta_3) = 0$, i.e., Theorem 5 is contained as a special case. Similar as in the proof of Theorem 6, we can use the formulas for the eigenvalues in Theorem 1 and Corollary 1 to transfer [4, Proposition 4.3] to $s$-sum sets:

**Theorem 8** Assume that $C(\Omega)\perp$ is of length $n$ and has three nonzero weights $w_1 < w_2 < w_3$. Let $b \geq 0$ and $s \geq 3$ be integers.

- $\Omega$ is an $s$-sum set iff $(w_3 - w_2)(n(p-1)p^{m-2} - pw_1)^s + (w_1 - w_3)(n(p-1)p^{m-2} - pw_2)^s + (w_2 - w_1)(n(p-1)p^{m-2} - pw_3)^s = 0.$
• $\Omega \cup 0$ is an s-sum set iff $(w_3 - w_2)(1 + n(p - 1)p^{m-2} - pw_1)^s + (w_1 - w_3)(1 + n(p - 1)p^{m-2} - pw_2)^s = 0$.

• $\Gamma_{C(\Omega)}^b$ is an s-SWRG iff $(w_3 - w_2)(b + n(p - 1)p^{m-2} - pw_1)^s + (w_1 - w_3)(b + n(p - 1)p^{m-2} - pw_2)^s = 0$.

**Example 4** If $n = 12, p = m = 2$ the only triples $(w_1, w_2, w_3)$ satisfying the first condition of Theorem 8 for $s = 5$ are $\{11 - i, 12, 13 + i\}$, for $i = 0, 1, \ldots, 10$.

Note that $w_2 = 12 = n$ in all cases. This can be partially explained by the fact that eq. (2) admits the solution $\theta_2 = 0, \theta_1 = -\theta_3$ for all odd $s$. In other words, a graph $\Gamma$ with these eigenvalues is an $s$-SWRG for all odd $s > 1$, cf. [4, Proposition 4.2]. Using Theorem 2 and Theorem 1, this observation translates into a result that is new in the context of $s$-sum sets:

**Theorem 9** Assume that $C(\Omega)^\perp$ is of length $n$ and has three nonzero weights $w_1 < w_2 = n(p - 1)p^{m-2} < w_3$, with $w_1 + w_3 = 2n(p - 1)p^{m-2}$. Then $\Omega$ is an s-sum set for all odd $s > 1$.

In ref. [4, Theorem 4.4] it is essentially proven that if eq. (2) admits a solution $(\theta_1, \theta_2, \theta_3)$ with $\theta_1 > \theta_2 > \theta_3$ for two different values of $s > 1$, then $\theta_2 = 0$ and $\theta_1 = -\theta_3$. This directly leads to:

**Theorem 10** Assume that $C(\Omega)^\perp$ is of length $n$ and has three nonzero weights $w_1 < w_2 < w_3$. If $w_2 \neq n(p - 1)p^{m-2}$, or $w_1 + w_3 \neq 2n(p - 1)p^{m-2}$, then there is at most one $s > 1$ such that $\Omega$ is an s-sum set.

If we are not in the situation of Theorem 9, then any given code can yield an s-sum set for at most one value of $s$. There are other solutions of eq. (2), e.g. $(5, \frac{1}{2}(-3 + \sqrt{281}), \frac{1}{2}(-3 - \sqrt{281}))$ for $s = 5$. However, the found solutions are non-integral and no graph that is an s-SWRG and attains these eigenvalues is known, see [4, p. 808]. Since the eigenvalues corresponding to an s-sum set are integral, we state:

**Conjecture 1** $\Omega$ is an s-sum set for some $s > 3$ iff

$$(w_1, w_2, w_3) = (w_1, n(p - 1)p^{m-2}, 2n(p - 1)p^{m-2} - w_1),$$

for some $0 < w_1 < n(p - 1)p^{m-2}$.

At least for the special case $p = m = 2$, i.e., $\mathbb{Z}_4$-codes, Conjecture 1 seems to be true also for $s = 3$, see Conjecture 2 in Sect. 4. In ref. [20] it has been shown that all s-sum sets of a special type also have to be 3-sum sets.
4 $\mathbb{Z}_4$-Codes

Here we consider $\mathbb{Z}_4$ linear codes and assume that the reader is familiar with [7]. When we say that $C$ is an $[n, k]$ code, where $k = (k_1, k_2)$ is the shape, this means that $C$ is a linear code over $\mathbb{Z}_4$ of length $n$, which admits a generator matrix of the form

$$G = \begin{pmatrix} I_{k_1} & A & B \\ 0 & 2I_{k_2} & 2D \end{pmatrix},$$

where $I_{k_1}$ and $I_{k_2}$ denote the $k_1 \times k_1$ and $k_2 \times k_2$ identity matrices, respectively, $A$ and $D$ are 0, 1 valued matrices, and $B$ is a $\mathbb{Z}_4$ matrix. We assume that the stated generator matrix consists of $n$ columns (and $k_1 + k_2$ rows). We will say that the length $n$ is effective to mean that the generator matrix does not contain an all-zero vector $0$ as a column. The code size, i.e., the number of codewords, is given by

$$\#C = 4^{k_1} \cdot 2^{k_2} = 2^{k_1+k_2}.$$ For $\mathbb{Z}_4$-codes we note that the homogeneous weight coincides with the Lee weight.

We note the following compatibility between a $\mathbb{Z}_4$-code and its Gray image.

**Proposition 1** If $C$ is a $\mathbb{Z}_4$-code with three Lee weights satisfying the hypotheses of Theorem 6, then its binary image $C^G$ satisfies the hypotheses of Theorem 6.

**Proof** As is well-known, the Hamming weights of $C^G$ are the Lee weights of $C$. If $n$ is the length of $C$ then $C^G$ is of length $2n$. The third condition of Theorem 6 becomes with $p = m = 2$,

$$w_1 + w_2 + w_3 = 3 \frac{b + n(p - 1)p^{m-1}}{p} = 3 \frac{b + 2n}{2},$$

which is the same with $p = 2, m = 1$ and length $2n$. \qed

By $A_i$ we denote the number of codewords of $C$ of homogeneous weight $i$ and by $B_i$ we denote the number of codewords of homogeneous weight $i$ of its dual code $C^\perp$. The cardinality of the dual code is $\#C^\perp = 2^{2n-2k_1-k_2}$. Since we assume that a corresponding generator matrix does not have a zero column, we have $B_1 = 0$ in our context. As mentioned at the end of Subsect. 2.1, every $\mathbb{Z}_4$ code has minimum dual distance $d^\perp \geq 3$ iff it is regular and projective. The numbers $A_i$ can be encoded in a weight enumerator of $C$:

$$\text{Hom}_C(X, Y) = \sum_{c \in C} X^{2n-w_{\text{hom}}(c)} Y^{w_{\text{hom}}(c)} = \sum_{i=0}^{2n} A_i X^{2n-w_i} Y^{w_i}. \quad (4)$$

The corresponding MacWilliams identity is given by $\text{Hom}_C(X, Y) = \frac{1}{|C|} \cdot \text{Hom}_{C^\perp} (X + Y, X - Y)$, see e.g. [7]. Note that this formula equals the Hamming weight enumerator for a linear code over $\mathbb{F}_2$ with cardinality $\#C = 2^k$ if we replace $n$ by $2n$ and $k$ by $2k_1 + k_2$. As mentioned in the introduction and used in the proof of Lemma 1, the same conclusion can be obtained via the Gray map. Thus, we can easily rewrite the classical MacWilliams identities [21] or
the Pless power moments [22] for the Hamming weight over \( \mathbb{F}_2 \). Using \( A_0 = B_0 = 1 \) and \( B_1 = 0 \) the first four (Pless) power moments for the \( w_{\text{hom}} \) are given by:

\[
\sum_{i > 0} A_i = 2^{2k_1+k_2} - 1, \tag{5}
\]

\[
\sum_{i \geq 0} i A_i = 2^{2k_1+k_2} n, \tag{6}
\]

\[
\sum_{i \geq 0} i^2 A_i = 2^{2k_1+k_2-1}(B_2 + n(2n + 1)), \tag{7}
\]

\[
\sum_{i \geq 0} i^3 A_i = 2^{2k_1+k_2-2}(3(B_2n - B_3) + 2n^2(2n + 3)). \tag{8}
\]

We remark, that the first three equations (including \( B_1 \)) can also be found in ref. [23, Theorem 3.1].

In this section we are interested in structural results for \( l \)-weight codes where \( l \) is small. Mostly we will restrict our attention to projective codes only. In some cases we will require additional constraints on the sum \( \sum_{i=1}^t w_i \) of weights (which are motivated by strongly walk regular graphs, see e.g. [4] and see also [5], which studies the field case).

### 4.1 Theoretical Results for \( \mathbb{Z}_4 \)-Codes with Few Weights

In this section we give only very few results that are of interest for the remaining part of this paper. For more information we refer the interested reader to e.g. [23, 24], where one-Lee weight codes and projective two-Lee weight codes are studied. For every pair \( (k_1, k_2) \) of non-negative integers there exists exactly one non-isomorphic 1-weight \( [n, (k_1, k_2)] \) code (for a unique length \( n \) depending on \( k_1 \) and \( k_2 \)), see [25].

**Lemma 1** Let \( C \) be a \( [n, (k_1, k_2)] \) code. By \( C_2 \) we denote the subcode of \( C \) spanned by the codewords of even weight. The cardinality of \( C_2 \) is either \( 2^{2k_1+k_2-1} \) or \( 2^{2k_1+k_2} \) and all codewords of \( C_2 \) have an even weight.

**Proof** Let \( E \) be the code consisting of codewords of \( C \) of even Lee weight. This code is linear as the dual of the code spanned by the all-2 vector, so that \( C_2 = E \cap C \). Thus \( C_2 \) is linear and its size depends on whether \( 2 \cdot 1 \in C^\perp \) or not.

We also call \( C_2 \) the even-weight subcode of \( C \).

**Lemma 2** Let \( C \) be an \( [n, (k_1, k_2)] \) code with \( t \geq 2 \) different nonzero weights. Then, at most \( t - 1 \) weights can be odd.

**Proof** Let \( c \in C \) be a codeword of odd weight, then \( 2c \in C \) is a codeword of even weight.
Lemma 3 Let $C$ be an $[n, (k_1, k_2)]$ three-weight code with $d^3 \geq 3$ and weights $w_1$, $w_2$, and $w_3$ that occur $A_1$, $A_2$, and $A_3$ times, respectively. Using the abbreviation $y = 2^{k_1+k_2-1}$ we have

\[ A_1 = \frac{y \cdot (2n^2 - 2nw_2 - 2nw_3 + 2w_2w_3 + n) - w_2w_3}{(w_2 - w_1)(w_3 - w_1)} \]  

(9)

\[ A_2 = \frac{y \cdot (2n^2 - 2nw_1 - 2nw_3 + 2w_1w_3 + n) - w_1w_3}{(w_2 - w_3)(w_2 - w_1)} \]  

(10)

\[ A_3 = \frac{y \cdot (2n^2 - 2nw_1 - 2nw_2 + 2w_1w_2 + n) - w_1w_2}{(w_3 - w_1)(w_3 - w_2)} \]  

(11)

and

\[ 3B_3 = 2n^2(2n + 3) - (w_1 + w_2 + w_3)2n(2n + 1) - 4w_1w_2w_3 + 2(w_1w_2 + w_1w_3 + w_2w_3)2n + \frac{2w_1w_2w_3}{y} \]

for the number of dual codewords of weight 3.

Proof Solving the first three power moment equations (5)–(7) for $A_1$, $A_2$, and $A_3$ gives the first statement. Plugging into the fourth power moment equation (8) and solving for $3B_3$ gives the last equation of the statement. \qed

We remark that the integrality of $B_3$ implies that the product of the three weights $w_1w_2w_3$ is divisible by $y/2 = 2^{k_1-k_2-2}$. Now let us look at the first case of Theorem 6, which is $w_1 + w_2 + w_3 = 3n$ in our situation. Our first observation is that the length $n$ has to be even.

Lemma 4 Let $C$ be an $[n, (k_1, k_2)]$ 3-weight code with $d^3 \geq 3$ and weights $w_1$, $w_2$, and $w_3$ satisfying $w_1 + w_2 + w_3 = 3n$. Then $n \equiv 0 \pmod{2}$.

Proof Assume that $n$ is odd. Then, also $w_1 + w_2 + w_3 = 3n$ is odd. Using Lemma 2 we conclude that exactly one weight—say $w_2$—is odd. We consider the even weight subcode $C_2$ of $C$. Due to Lemma 1 $C_2$ only contains codewords of even weight and has cardinality $\#C_2 = 2^{k_1+k_2-1}$, i.e., $A_2 = 2^{k_1+k_2-1}$. Since $C$ is projective $C_2$ has effective length $n' \in \{n - 1, n\}$. Equation (6) gives

\[ w_1A_1 + w_2A_2 + w_3A_3 = 2^{k_1+k_2}n \]

for $C$ and

\[ w_1A_1 + w_3A_3 = 2^{k_1+k_2-1}n' \]

for $C_2$. Taking the difference and dividing by $A_2 = 2^{k_1+k_2-1}$ yields $w_2 = n + (n - n')$. Since $w_2, n$ are odd and $n - n' \in \{0, 1\}$, we have $n' = n$ and $w_2 = n$. So, let us write $w_1 = n - t$ and $w_3 = n + t$ for some odd integer $t$ (observe that $w_1$ and $w_3$ have to be even). With this, eq. (10) and $A_2 = 2^{k_1+k_2-1} = y$ gives...
\[(y - 1)t^2 = (y - n)n.\] Note that \(t = 1\) gives \(y = n + 1\) or \(n = 1\). In the first case we have \(A_1 = 0\) and \(w_1 = 0\) in the second, so that we can assume \(t \geq 3\). Solving the above equations for \(n\) gives

\[
n = \frac{y}{2} \pm \frac{\sqrt{-4t^2y + 4t^2 + y^2}}{2}.
\]

So, we consider the diophantine equation

\[
x^2 = -4t^2y + 4t^2 + y^2, \tag{12}
\]

where \(y\) is a power of 2 and all integers are positive.\(^1\) In our situation we have \(t \geq 3\), so that \(y \geq 64 = 2^6\), since \(x^2\) would be negative for \(t \geq 3\) and \(y \leq 32\). Now let us set \(x = 2z\) and \(y = 2^{r+1}\), i.e., \(r \geq 5\). With this we can rewrite eq. (12) to

\[
(z - t)(z + t) = 2^{2r} - 2^{r+1}t^2. \tag{13}
\]

Since \(t\) is odd, \(z\) has to be odd too. We conclude that either \(z - t\) or \(z + t\) has to be divisible by \(2^r\) from the fact that the greatest common divisor of \(z - t\) and \(z + t\) divides \(2t\) and \(r \geq 5\).

Assume that \(z = s2^r - t\) for some nonzero integer \(s\) (this is the case that \(2^r\) divides \(z + t\)). Plugging in into eq. (13), dividing by \(2^{r+1}\), and simplifying gives \((2^{r-1}s - t) \cdot s = 2^{r-1} - t^2\), so that

\[
2^{r-1} \cdot (s^2 - 1) = t \cdot (s - t).
\]

Note that \(s^2 \geq 1\). If \(s^2 = 1\), then \(s = t\) or \(s = 0\), which contradicts \(t \geq 3\). Thus, the left hand side is positive and \(s > t \geq 3\). This implies \(t(s - t) \leq s(s - t) < 2^{r-1}(s^2 - 1)\) – contradiction.

Assume that \(z = s2^r + t\) for some nonzero integer \(s\) (this is the case that \(2^r\) divides \(z - t\)). Plugging in into eq. (13), dividing by \(2^{r+1}\), and simplifying gives \((2^{r-1}s + t) \cdot s = 2^{r-1} - t^2\), so that

\[
2^{r-1} \cdot (s^2 - 1) = t \cdot (s - t).
\]

Note that \(s^2 \geq 1\). If \(s^2 = 1\), then \(s = -t\) or \(t = 0\), which contradicts \(t \geq 3\). Thus, the left hand side is positive and \(-s > t \geq 3\). This implies \(t(s - t) \leq s(s - t) < 2^{r-1}(s^2 - 1)\) – contradiction. \(\square\)

We remark that in the case where also \(C_2\) is projective the proof can be shortened significantly since [26, Corollary 16] implies that \(2t\) is a power of two. An example where Lemma 4 excludes parameters of a code is given by \(n = 29\), \(2k_1 + k_2 = 8\), \(w = (24, 31, 32)\), and weight distribution \(0^124^{76}31^{128}32^{51}\). Applying the MacWilliams transform gives \(B_0 = 1, B_1 = B_2 = 0, B_3 = 164\), and indeed all \(B_i\) are non-negative integers. Moreover, the number of even-weight codewords is 128, i.e., half the size of the code.

\(^1\) Note that eq. (12) has infinitely many solutions for \(t \in \{-1, 0, 1\}\). Also if \(y\) is not a power of 2 there are lots of solutions, e.g. \((x, t, y) \in \{(1, 2, 15), (11, 2, 21), (14, 3, 40), (17, 6, 145)\}\).
Next we show that under the assumption of Theorem 10 the length and the three weights all are divisible by large powers of 2 if the length is suitably large.

**Proposition 2** Let $C$ be an $[n, (k_1, k_2)]$ 3-weight code with $d^1 \geq 3$ and weights satisfying $w_1 + w_2 + w_3 = 3n$ and $w_2 = n$. For each positive integer $r$ there exists an integer $N(r)$ such that $n \geq N(r)$ implies that $2^r$ divides $n$ and $2^{r-1}$ divides all three weights $w_1, w_2, w_3$.

**Proof** Let $t$ be a positive integer with $w_1 = n - t$ and $w_3 = n + t$. With this (and $y = 2^{2k_1 + k_2 - 1}$) the equations of Lemma 3 are equivalent to

$$A_1 = \frac{n(y - n - t)}{2t^2}$$

(14)

$$A_2 = \frac{t^2(2y - 1) - n(y - n)}{t^2}$$

(15)

$$A_3 = \frac{n(y - n + t)}{2t^2}$$

(16)

and

$$3B_3 = \frac{2n(n - t)(n + t)}{y}.$$ (17)

Since $A_3 - A_1 = \frac{n}{t}$ the effective length $n$ has to be divisible by $t$. From $A_2 \in \mathbb{N}$ we conclude that $t^2$ divides $n(y - n)$. So, if $p^l$ divides $t$ for some odd prime $p$, then $p^{2l}$ has to divide $n$ since $y$ is a power of 2. As an abbreviation we set $k = 2k_1 + k_2$. Now let us try to parameterize $t = 2^u \cdot v$ and $n = 2^x \cdot v^2 \cdot z$ for odd positive integers $v, z$ and non-negative integers $u, x$. Plugging in and simplifying gives

$$A_1 = \frac{z \cdot (2^{k-u-1} - 2^{-u}v^2z - v)}{2u+1-x}$$

(18)

$$A_2 = 2^{2(2-u)}v^2z^2 + 2^k - 2^{x+k-2u-1}z - 1$$

(19)

$$A_3 = \frac{z \cdot (2^{k-u-1} - 2^{-u}v^2z + v)}{2u+1-x}$$

(20)

$$3B_3 = \frac{v^4z \cdot (2^{k-u}vz - 1) \cdot (2^{k-u}vz + 1)}{2^{k-x+2u-2}},$$

(21)

where $u \leq x$ ($t$ divides $n$) and $x \leq k - 1$ ($n \leq 2^k - 1$ since $C$ is projective).

If $k - x - 2u - 2 \geq 1$ then $B_3 \in \mathbb{N}$ and $v, z \equiv 1 \pmod{2}$ imply $u = x$. Since $\gcd(vz - 1, vz + 1) = 2$, we have that $2^{2k-3u-3}$ either divides $vz - 1$ or $vz + 1$. So, we use the parameterization $vz = s \cdot (2^{2k-3u-3}) + x$ for some positive integer $s$ and $x \in \{-1, 1\}$. With this $A_1 > 0$ gives
have the following exceptional tuples
\[ v(s \cdot (2^{k-3u-3}) + \alpha + 1) > 0, \]
so that \( v_s < 2^{2u+2} \), i.e., \( sv \leq 2^{2u+2} - 1 \). Now \( A_2 > 0 \) gives \( v^2 z^2 + 2^k > 2^{k-u-1} z \), which is equivalent to
\[ sv(v_s)^2 + 2^k sv > s^2 2^{k-u-1} v_s = s^2 2^{2k-4u-4} + 2^k s 2^{k-u-1} > s^2 2^{2k-4u-4} - s^2 2^{k+2u+2}. \] (22)

Since \( sv \leq 2^{2u+2} - 1 \) the left hand side is at most
\[
\begin{align*}
& s^2 2^{2k-4u-4} - s^2 2^{2k-6u-6} + s x 2^{k-u} - s x 2^{k-3u-2} \\
& + 2^{2u+2} - 2^k + 2^{k+2u+2} - 2^k \\
& \leq s^2 2^{2k-4u-4} - s^2 2^{2k-6u-6} + 2 x 2^{k-6u} + 2^{2u+2} + 2^{k+2u+2} \\
& \leq s^2 2^{2k-4u-4} - s^2 2^{2k-6u-6} + 3 s 2^{k+2u+2}.
\end{align*}
\]
Thus
\[ 4 s \cdot 2^{k+2u+2} > s^2 2^{2k-6u-6} \] (23)
has to be satisfied, so that \( k \leq 8u + 9 \) and
\[ x = u \geq \frac{k - 9}{8}. \] (24)

Otherwise we have \( k \leq x + 2u + 2 \). From \( A_1 > 0 \) we conclude \( y - n > 0 \). Since \( y - n \) is an integer and both \( y \) and \( n \) are divisible by \( 2^k \) we have \( y - n \geq 2^x \). Now \( A_2 > 0 \), eq (15), and \( 2y - 1 \leq 2^k \) imply
\[ v^2 z^2 \cdot 2^k - 2^x v^2 z^2 \cdot 2^x > 0, \]
so that \( k + 2u > 2x \), i.e.,
\[ k \geq 2x - 2u + 1. \] (25)
Combined with \( k \leq x + 2u + 2 \) we obtain \( x \leq 4u + 1 \) and \( k \leq 6u + 3 \), i.e.,
\[ x \geq u \geq \frac{k - 3}{6}. \] (26)

In both cases we can conclude \( x \geq u \geq \frac{k}{2} \), so that the result follows from \( n < 2^k \). \( \Box \)

**Conjecture 2** Let \( C \) be an \([n, (k_1, k_2)]\) 3-weight code with \( d^\perp \geq 3 \) and weights satisfying \( w_1 + w_2 + w_3 = 3n \) and \( w_1 < w_2 < w_3 \). Then, \( w_2 = n \).

We remark that in order to prove Conjecture 2 the Diophantine conditions of Lemma 3, i.e., \( A_1, A_2, A_3 \in \mathbb{N}_0 \) and \( B_3 \in \mathbb{N}_0 \geq 0 \) are not sufficient. Up to \( n = 50 \) we have the following exceptional tuples \((n, w_1, w_2, w_3, y, A_1, A_2, A_3, B_3)\):

- (29, 24, 31, 32, 64, 76, 128, 51, 164)
- (33, 29, 32, 38, 64, 64, 111, 80, 157)

\( \copyright \) Springer
So, from Lemma 4 we can conclude that Conjecture 2 is true for all \( n < 34 \). We remark that the examples for \( n \in \{29, 34, 50\} \) satisfy \( B_i \in \mathbb{N}_{\geq 0} \) for all \( 1 \leq i \leq n \), i.e., the MacWilliams identities are not sufficient in order to conclude the non-existence of the corresponding code.

### 4.2 Classification of 3-Weights \( \mathbb{Z}_4 \)-Codes with \( d^\perp \geq 3 \) and Short Length

Having Theorem 6 in mind we aim to classify 3-weights \( \mathbb{Z}_4 \)-codes with \( d^\perp \geq 3 \) and short length. Optimal linear codes over \( \mathbb{Z}_4 \) with length \( n \leq 7 \) were classified in ref. [27]. Without the restriction to optimal codes, all linear codes over \( \mathbb{Z}_4 \) with length \( n \leq 10 \) and \( 2k_1 + k_2 \leq 8 \) were classified in ref. [28] for the homogeneous weight. The corresponding tables at [http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/CanonicalForm/Classification/index.html](http://www.algorithm.uni-bayreuth.de/en/research/Coding_Theory/CanonicalForm/Classification/index.html) contain the complete counts for \( n \leq 10 \). E.g. for \( n = 10 \) and \( (k_1, k_2) = (5, 0) \) there are exactly 8 848 026 non-isomorphic codes. For each given \( n \) our approach is to loop over all \( 1 \leq w_1 < w_2 < w_3 \leq 2n \) such that \( A_1, A_2, A_3, B_3 \), as specified in Lemma 3, are integers with \( A_1, A_2, A_3 \geq 1 \) and \( B_3 \geq 0 \). Since \( 2^{2k_1+k_2-2} \) has to divide \( w_1w_2w_3 \), which is due to \( B_3 \in \mathbb{N} \), we obtain a finite list of possibilities for each length \( n \). Note that \( d^\perp \geq 3 \) implies \( k_1 \geq 1 \). With respect to Theorem 6 we consider all remaining tuples where \( w_1 + w_2 + w_3 \geq 3n \) and \( w_1 + w_2 + w_3 \equiv 0(\text{mod } 3) \). In Table 1 we list the parameters that can be attained by a \( \mathbb{Z}_4 \) codes and refer to a corresponding generator matrix. As abbreviations we use \( w = (w_1, w_2, w_3), \ S = w_1 + w_2 + w_3, \) and \( A = (A_1, A_2, A_3) \). The parameters of computationally excluded codes are listed in Tables 2 and 3. For the latter we perform an exhaustive search using the given restrictions on the weights \( w_i \), the length \( n \), and the shape \( (k_1, k_2) \).

| \( n \) | \( w \) | \( A \) | \( (k_1, k_2) \rightarrow G \) |
|---|---|---|---|
| 6 | (4,6,8) | (6,16,9) | \( 2, 1 \rightarrow G_{6,1}^1 \) |
| 6 | (4,6,8) | (18,24,21) | \( 3, 0 \rightarrow G_{6,2}^1, \ (2, 2) \rightarrow G_{6,3}^1 \) |
| 8 | (4,8,12) | (1,27,3) | \( 2, 1 \rightarrow G_{8,1}^2 \) |
| 8 | (4,8,12) | (5,51,7) | \( 3, 0 \rightarrow G_{8,2}^1, \ (2, 2) \rightarrow G_{8,3}^1 \) |
| 3 | (2,4,6) | (15,15,1) | \( 2, 1 \rightarrow G_{3,1}^3 \) |
| 5 | (4,6,8) | (16,12,3) | \( 2, 1 \rightarrow G_{5,1}^2 \) |
| 7 | (6,8,10) | (42,7,14) | \( 3, 0 \rightarrow G_{7,1}^2 \) |
| 9 | (8,10,12) | (15,12,4) | \( 2, 1 \rightarrow G_{9,1}^3 \) |
| 10 | (8,12,16) | (62,64,1) | \( 3, 1 \rightarrow G_{10,1}^2 \) |
| 10 | (8,12,16) | (130,120,5) | \( 4, 0 \rightarrow G_{10,2}^2 \) |
\[ G_{6,1}^1 = \begin{pmatrix} 101112 \\ 010331 \\ 002200 \end{pmatrix}, G_{6,2}^1 = \begin{pmatrix} 100122 \\ 010212 \\ 001331 \end{pmatrix}, G_{6,3}^1 = \begin{pmatrix} 101112 \\ 011121 \\ 002002 \end{pmatrix} \]

\[ G_{8,1}^1 = \begin{pmatrix} 10101122 \\ 01112311 \\ 00220202 \end{pmatrix}, G_{8,2}^1 = \begin{pmatrix} 10001222 \\ 01022111 \\ 00110013 \end{pmatrix}, G_{8,3}^1 = \begin{pmatrix} 10111112 \\ 01112331 \\ 00200020 \end{pmatrix} \]

\[ G_{3,1}^2 = \begin{pmatrix} 101 \\ 011 \\ 002 \end{pmatrix}, G_{5,1}^2 = \begin{pmatrix} 10122 \\ 01111 \end{pmatrix}, G_{7,1}^2 = \begin{pmatrix} 1001112 \end{pmatrix} \]

\[ G_{9,1}^2 = \begin{pmatrix} 101111122 \\ 011223311 \\ 002020202 \end{pmatrix}, G_{10,1}^2 = \begin{pmatrix} 1000211111 \\ 0101223010 \\ 0010111233 \end{pmatrix}, G_{10,2}^2 = \begin{pmatrix} 1000212110 \\ 0100031232 \\ 0010132012 \end{pmatrix} \]

We remark that more examples can be found for the parameters:

- \( n = 15, k = 9, w = (12, 16, 20), A = (190, 255, 66); \)
- \( n = 18, k = 8, w = (16, 20, 24), A = (153, 72, 30); \)
- \( n = 22, k = 7, w = (20, 24, 28), A = (71, 43, 13). \)

### 4.3 Cyclic Kerdock Codes

The Kerdock code \( K \) of length \( 2^s \) with \( s \geq 3 \) odd over \( \mathbb{Z}_4 \) can be expressed as

\[ K = \mathbb{Z}_4 j \oplus Q, \]

where \( j \) denotes the all-one vector. The code \( Q \) is a free code of size \( 4^s \) with weight spectrum

\[ 2^i, 2^s \pm 2^{i-1}. \]

By puncturing on the first coordinate we obtain a cyclic code of length \( n = 2^s - 1 \) that was used in ref. [8] to generate low correlation quadriphase sequences. This code is called \( K^- \) in ref. [7] and has the same weights as \( Q \). It can be shown to be projective by the same type of arguments as in ref. [7, §3.3]. The sum of these weights being \( 3 \cdot 2^s = 3(n + 1) \), we see that, by Theorem 6 with \( b = 2 \), the syndrome graph of \( K^- \) with a double loop at each vertex is a 3-SWRG. It can be easily checked that the parameters of \( K^- \) go in line with our results the previous subsection.

We observe that the binary images have a length congruent to \( 2 \bmod 4 \), which is enough to show they are not linear, since by [29, Corollary 1], we should have a length multiple of 4. This is an alternative proof that Kerdock codes cannot be
linear. The classical proof builds on the fact that the Preparata code, or any code with the same weight distribution is nonlinear [30].

5 Extension to Chain Rings

In this section, we briefly indicate how the preceding work extends when replacing $\mathbb{Z}_p^m$ by a finite chain ring $R$ of depth $r \geq 2$, say, and residue field $\mathbb{F}_q$, for some prime power $q$. Recall that such a ring is a local ring whose lattice of ideals form a chain of length $r$. In particular, the maximal ideal is principal, generated by an element $c$, a nilpotent element of nilpotency index $r$ [31, Chap. 3]. An example is $\mathbb{Z}_p^m$ when $r = m$, and $q = p$. The definition of the homogeneous weight becomes

| $n$ | $2k_1 + k_2$ | $w$  | $A$      | $(k_1, k_2)$ |
|-----|--------------|------|----------|--------------|
| 2   | 3            | (1,2,3) | (1,3,3)  | (1,1)        |
| 4   | 4            | (2,4,6) | (1,11,3) | (2,0), (1,2) |
| 4   | 5            | (2,4,6) | (5,19,7) | (2,1), (1,3) |
| 4   | 6            | (2,4,6) | (13,35,15) | (3,0), (2,2), (1,4) |
| 6   | 5            | (4,6,8) | (6,16,9)  | (1,3)        |
| 6   | 6            | (4,6,8) | (18,24,21) | (1,4)      |
| 8   | 5            | (6,8,10)| (6,15,10) | (2,1), (1,3) |
| 8   | 6            | (6,8,10)| (22,15,26) | (3,0), (2,2), (1,4) |
| 8   | 7            | (6,8,10)| (54,15,58) | (3,1), (2,3), (1,5) |
| 8   | 6            | (4,8,12)| (12,27,3) | (1,3)        |
| 8   | 7            | (4,8,12)| (5,51,7)  | (1,4)        |
| 8   | 7            | (4,8,12)| (13,99,15) | (3,1), (2,3), (1,5) |
| 10  | 5            | (8,10,12)| (5,16,10) | (2,1), (1,3) |
| 10  | 6            | (8,10,12)| (25,8,30) | (3,0), (2,2), (1,4) |

| $n$ | $2k_1 + k_2$ | $w$       | $A$  | $(k_1, k_2)$ |
|-----|--------------|-----------|------|--------------|
| 3   | 5            | (2,4,6)   | (15,15,1) | (1,3)        |
| 5   | 5            | (4,6,8)   | (16,12,3) | (1,3)        |
| 7   | 5            | (6,8,10)  | (16,11,4) | (2,1), (1,3) |
| 7   | 6            | (6,8,10)  | (42,7,14) | (2,2), (1,4) |
| 7   | 7            | (4,8,12)  | (31,95,1) | (3,1), (2,3), (1,5) |
| 7   | 8            | (4,8,12)  | (65,187,3) | (4,0), (3,2), (2,4), (1,6) |
| 9   | 5            | (8,10,12) | (15,12,4) | (1,3)        |
| 9   | 6            | (8,11,14) | (43,16,4) | (3,0), (2,2), (1,4) |
| 10  | 7            | (8,12,16) | (62,64,1) | (2,3), (1,5) |
| 10  | 8            | (8,12,16) | (130,120,5) | (3,2), (2,4), (1,6) |
\[
\text{w}_{\text{hom}}(x) = \begin{cases} 
0 & \text{if } x = 0, \\
q^{r-1} & \text{if } 0 \neq x \in (q^{r-1}), \\
(q - 1)q^{r-2} & \text{otherwise}. 
\end{cases}
\]

The definition of the syndrome graph in Subsect. 2.3 to this generalized situation only needs the obvious modifications. Also the proof of [6, Theorem 4.1] can be generalized to conclude the connection between coset graph eigenvalues and weights:

**Theorem 11** Suppose that \( C \) is a regular, projective linear code over \( R \) with homogeneous weights \( w_i \) and corresponding weight distribution \( A_i = |\{ x \in C; \text{w}_{\text{hom}}(x) = w_i \}|. \) Then the eigenvalues of \( \Gamma(C^\perp) \) are \( n(q - 1)q^{r-1} - qw_i \) with multiplicity \( A_i. \)

In particular, for the coset graph with loops, we have the following result.

**Corollary 2** If \( C \) is an \( R \)-code, of minimum distance at least three, with dual weight distribution \( [\{ w_i, A_i \}] \), then the spectrum of \( \Gamma(C)^b \) is \( \{ (b + n(q - 1)q^{r-1} - qw_i)^A_i \} \). Thus \( A_i \) is the frequency of the homogeneous weight \( w_i \) in \( C^\perp \) and the multiplicity of the eigenvalue \( b + n(q - 1)q^{r-1} - qw_i. \)

From there, upon observing that Theorem 2 is valid for any finite commutative ring, the main condition for the existence of a TSS becomes

**Theorem 12** Assume that \( C(\Omega)^\perp \) is of length \( n \) and has three nonzero weights \( w_1 < w_2 < w_3. \) Let \( b \) be any integer.

- \( \Omega \) is a TSS iff \( w_1 + w_2 + w_3 = 3n(q - 1)q^{r-2}; \)
- \( \Omega \cup 0 \) is a TSS iff \( w_1 + w_2 + w_3 = 3\frac{1+n(q-1)q^{r-1}}{q}; \)
- \( \Gamma_{C(\Omega)}^b \) is a 3-SWRG iff \( w_1 + w_2 + w_3 = 3\frac{b+n(q-1)q^{r-1}}{q}. \)

We remark that \( r \geq 2 \) and \( q \) not being divisible by \( 3 \) the second case is impossible and \( b \) has to be divisible by \( q \) in the third case.

### 5.1 Trace Codes over Chain Rings

Consider the chain ring \( \mathbb{F}_p + u\mathbb{F}_p \), with \( u^2 = 0 \). This is a chain ring with \( r = 2 \) and \( q = p \). The codes \( C(m, p) \) of length \( \frac{p^{2m} - p^m}{2} \) with \( m \) singly even in ref. [9, §5.1] are defined as

\[ \{(\text{Tr}(ax))_{x \in L} | a \in \mathcal{R}\}, \]

where \( L = Q + u\mathbb{F}_p^m, \ Q \) is the set of squares of \( \mathbb{F}_p^m \), and \( \mathcal{R} = \mathbb{F}_p^m + u\mathbb{F}_p^m. \) Note that, since \( m \) is even, we have \( \mathbb{F}_p^x \subseteq Q. \) This implies that these codes are replications by a factor \( p - 1 \) of projective codes \( P(m, p) \) say of length \( n = \frac{p^{2m} - p^m}{2(p-1)}. \) These latter codes have weights
\[ p^{2m-1} - p^{m-1}, p^{2m-1} - p^{m-1} - p^{m/2} + 1, p^{2m-1} - p^{m-1} + p^{m/2} - 1, \]
and so satisfy the relation
\[ w_1 + w_2 + w_3 = 3(1 - 1/p)n, \]
for the weight of the Gray map in ref. [9], normalized by a factor 2. This shows, by the first condition of Theorem 12, that the coset graph \( \Gamma(C) \) is a 3-SWRG, or, equivalently, that the \( \Omega \) such that \( C(\Omega) = C \) is a TSS.

### 5.2 Generalized Teichmüller Codes

Let \( q = 2^r \) and \( R = \text{GR}(4, r) \) the Galois ring of characteristic 4 and residue field \( \mathbb{F}_{2^r} \). The order of \( R \) is \( q^2 \). For integers \( k \geq 2 \) and
\[
s \in \begin{cases} 
0, 2, 4, \ldots, (k-1)r & \text{if } k \text{ odd;} \\
0, 2, 4, \ldots, (k-1)r & \text{if } k \text{ even,}
\end{cases}
\]
the generalized Teichmüller codes \( T_{q,k,s} \) are constructed in ref. [10, Sec. 3.1], [32], generalizing the Teichmüller codes in ref. [33]. They are regular projective \( R \)-linear codes of length \( n = 2^s \cdot \frac{q^k - 1}{q-1} \) and with three non-zero homogeneous weights, scaled by the factor \( 1/qr^2 \),
\[ w = \left( 2^s q^k - 2^{s/2} q^{(k-1)/2}, 2^s q^k, 2^s q^k + 2^{s/2} q^{(k-1)/2} \right) \]
of frequencies
\[ A = \left( \frac{1}{2} (q^k - 1)(q^k + 2^{s/2} q^{(k+1)/2}), q^k - 1, \frac{1}{2} (q^k - 1)(q^k - 2^{s/2} q^{(k+1)/2}) \right). \]
From the length we get \( 2^s q^k = n(q-1) \). Thus, the sum of the weights is
\[ S = 3 \cdot 2^s q^k q^{r-2} = 3(n(q-1) + 2^s) q^{r-2} = \frac{3}{q^r} (b + n(q-1) q^{r-1}) \]
for \( b = 2^s q^{r-1} \). By Theorem 12 we see that the coset graph with \( b \) loops on each vertices is a 3-SWRG.

We remark that in ref. [33] and [10], more projective three-weight-codes over Galois rings are found, among them the dualized extended Kerdock codes \( \hat{K}_{k+1}^* \) and the dualized generalized Teichmüller codes \( T_{q,k,s}^* \). However, they are either not regular or the sum of the weights does not satisfy the divisibility conditions needed in the context of this paper.

### 5.3 Classification of 3-Weights Codes over \( \mathbb{F}_2 + u \mathbb{F}_2 \) with \( d^1 \geq 3 \) and Short Length

In a similar manner as what we did over \( \mathbb{Z}_4 \), we classify 3-weight codes with dual weight \( d^1 \geq 3 \) over the other proper chain ring of order 4, which is the ring \( R = \mathbb{F}_2 + u \mathbb{F}_2 \)

\[ \text{The scaling of the homogeneous weight in ref. [10] and [33] differs by ours by the factor } q^{-2}. \]
$\mathbb{F}_2 + u\mathbb{F}_2$ of dual numbers over $\mathbb{F}_2$. The Gray image of such a code is always a linear binary code, and a linear binary code is the Gray image of an $R$-linear code if and only if it has a fixed-point free automorphism of order 2 [34]. We classify the codes in the same range of parameters as in the $\mathbb{Z}_4$-case, that is $n \leq 10$, $S \geq 3n$ and $S \equiv 0 \pmod{3}$. Since the MacWilliams identities for $R$-linear codes are the same as for $\mathbb{Z}_4$-linear codes (and up to doubling the length, the same as the MacWilliams identities for the linear Gray image), we can start with the same list of feasible parameters we computed for $\mathbb{Z}_4$-linear codes.

The feasible parameters, together with the weight distribution and the value $S - 3n \geq 0$, are listed in Table 4. The column $(k_1, k_2)$ lists the shapes of the realizable codes. An entry “—” indicates that no $R$-linear code with the given parameters does exist.

A list of suitable generator matrices for the realizable parameters is given in Table 5.

We remark that we found further examples of $R$-linear three-weight codes with $d \geq 3$, $S - 3n \geq 0$ and $3 \mid S$. Their parameters are displayed in Table 6.
In this work we have generalized from fields to rings the constructions of SWRGs from [5]. The rings considered here are $\mathbb{Z}_{p^n}$, and more generally finite chain rings. The weight playing the role of the Hamming in this generalization is the homogeneous weight. This weight can be defined in general over finite Frobenius rings. It would be of theoretical interest to consider three-weight codes over those rings.

### Table 5
Generator matrices for $R = \mathbb{F}_2[X]/(X^2)$, $S \geq 3n$, $n \leq 10$

| $n$ | $k$ | weights | $S - 3n$ | $(k_1, k_2)$ | $G$ |
|-----|-----|---------|----------|--------------|-----|
| 3   | 5   | $2^315\cdot 4\cdot 5^6$ | 3        | (2,1)        | \[
\begin{pmatrix}
1 & 0 & 1 \\
0 & 1 & 0 \\
0 & 0 & 1 \\
\end{pmatrix}
\] |
| 5   | 5   | $4^6\cdot 6^{12}8^3$ | 3        | (2,1)        | \[
\begin{pmatrix}
1 & 0 & 1 & 0 & X \\
0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & X \\
\end{pmatrix}
\] |
| 6   | 5   | $4^6\cdot 6^{16}8^9$ | 0        | (2,1)        | \[
\begin{pmatrix}
1 & 0 & X & X + 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 1 & X \\
0 & 0 & 0 & 0 & X & X \\
\end{pmatrix}
\] |
| 6   | 6   | $4^6\cdot 6^{24}8^{21}$ | 0        | (3,0)        | \[
\begin{pmatrix}
1 & 0 & 0 & 1 & 1 & X + 1 \\
0 & 1 & 0 & 1 & X & 0 \\
0 & 0 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\] |
| 6   | 6   | $4^6\cdot 6^{24}8^{21}$ | 0        | (2,2)        | \[
\begin{pmatrix}
1 & 0 & 1 & 1 & 0 & 1 \\
0 & 1 & 1 & X & 1 & X + 1 \\
0 & 0 & 0 & 0 & X & X \\
\end{pmatrix}
\] |
| 8   | 5   | $4^82^{7}12^3$ | 0        | (2,1)        | \[
\begin{pmatrix}
1 & 0 & X & 1 & 0 & 1 & X & 1 \\
0 & 1 & 1 & X & 1 & 1 & 1 & X + 1 \\
0 & 0 & 0 & 0 & X & X & X & X \\
\end{pmatrix}
\] |
| 8   | 6   | $4^85^112^7$ | 0        | (3,0)        | \[
\begin{pmatrix}
1 & 0 & 0 & X & X & 0 & 1 & X \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & X & X & X + 1 \\
\end{pmatrix}
\] |
| 8   | 6   | $4^85^112^7$ | 0        | (2,2)        | \[
\begin{pmatrix}
1 & 0 & X & 1 & 1 & 1 & 1 & X + 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & X & X & 0 & X & X \\
0 & 0 & 0 & 0 & 0 & X & X & 0 \\
\end{pmatrix}
\] |
| 9   | 5   | $8^51^012^4$ | 3        | (2,1)        | \[
\begin{pmatrix}
1 & 0 & 1 & X & 0 & 1 & 1 & 1 & X + 1 \\
0 & 1 & 1 & 1 & X & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & X & X & X & X & 0 \\
\end{pmatrix}
\] |
| 10  | 7   | $8^21^26^416^1$ | 6        | (3,1)        | \[
\begin{pmatrix}
1 & 0 & 0 & 1 & X & X & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & X & 0 & 1 & 1 & X + 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & X & 1 \\
0 & 0 & 0 & 0 & X & X & X & X & 0 \\
0 & 0 & 0 & 0 & X & X & X & X & 0 \\
\end{pmatrix}
\] |
| 10  | 8   | $8^31^012^4016^5$ | 6        | (4,0)        | \[
\begin{pmatrix}
1 & 0 & 0 & 0 & 1 & 0 & X & X & X + 1 & 1 \\
0 & 1 & 0 & 0 & X & X & 0 & 1 & X + 1 & 1 \\
0 & 0 & 1 & 0 & 0 & X & 1 & X & 1 & 1 \\
0 & 0 & 0 & 1 & X & 1 & X & 0 & 1 & 1 \\
\end{pmatrix}
\] |

### 6 Conclusion and Open Problems

In this work we have generalized from fields to rings the constructions of SWRGs from [5]. The rings considered here are $\mathbb{Z}_{p^n}$, and more generally finite chain rings. The weight playing the role of the Hamming in this generalization is the homogeneous weight. This weight can be defined in general over finite Frobenius rings. It would be of theoretical interest to consider three-weight codes over those rings.
We have classified short length three-weight \( \mathbb{Z}_4 \)-codes leading to SWRGs. To undertake such a classification for higher lengths and other rings is a challenging open problem, both theoretically and computationally. The polynomial analogues of \( \mathbb{Z}_m \), namely the rings \( \mathbb{F}_p[x]/(x^m) \) [35], are worth considering.

| \( n \) | \( k \) | \( \text{weights} \) | \( S - 3n \) |
|------|------|----------------|----------|
| 11   | 9    | 8^{162} \cdot 12^{312} \cdot 16^{37} | 3        |
| 11   | 10   | 8^{380} \cdot 12^{610} \cdot 16^{57} | 3        |
| 13   | 6    | 12^{45} \cdot 16^{17} \cdot 20^{1}  | 9        |
| 15   | 9    | 12^{190} \cdot 16^{255} \cdot 20^{56} | 3        |
| 18   | 8    | 16^{153} \cdot 20^{72} \cdot 24^{30} | 6        |
| 26   | 8    | 24^{172} \cdot 28^{32} \cdot 32^{51} | 6        |
| 42   | 8    | 40^{189} \cdot 48^{33} \cdot 56^{3}  | 18       |
| 49   | 7    | 48^{91} \cdot 52^{28} \cdot 56^{8}   | 9        |
| 54   | 11   | 48^{724} \cdot 56^{104} \cdot 64^{219} | 6  |
| 61   | 11   | 56^{980} \cdot 64^{147} \cdot 72^{220} | 9  |
| 63   | 13   | 56^{255} \cdot 64^{409} \cdot 72^{1540} | 3  |

References

1. Delsarte, P.: Weights of linear codes and strongly regular normed spaces. Discret. Math. 3(1), 47–64 (1972)
2. Brouwer, A.E., Cohen, A.M., Neumaier, A.: Distance-Regular Graphs. Springer, Berlin (1989)
3. Brouwer, A.E., Haemers, W.H.: Spectra of Graphs. Springer, Berlin (2012)
4. van Dam, E.R., Omid, G.R.: Strongly walk-regular graphs. J. Comb. Theory A 120(4), 803–810 (2013)
5. Shi, M., Solé, P.: Three weight codes, triple sum sets and strongly walk regular graphs. Des. Codes Cryptogr. 87(10), 2395–2404 (2019)
6. Shi, M., Honold, T., Qiu, Y., Sepasdar, Z., Wu, R.S., Solé, P.: The geometry of two-weight codes over \( \mathbb{Z}_p \). IEEE Trans. Inf. Theory (2021). https://doi.org/10.1109/TIT.2021.3114636
7. Hammons, A.R., Kumar, P.V., Calderbank, A.R., Sloane, N.J.A., Solé, P.: The \( \mathbb{Z}_4 \)-linearity of ker-

dock, preparata, goethals and related codes. IEEE Trans. Inf. Theory 40(2), 301–319 (1994)
8. Solé, P.: A quaternary cyclic code, and a family of quadruphas sequences with low correlation properties. In: Cohen, G., Wolfmann, J. (eds.) Coding theory and applications, Lecture Notes in Computer Science, Springer, p. 388 (1988)
9. Shi, M., Wu, R., Liu, Y., Solé, P.: Two and three weight codes over \( \mathbb{F}_p + u \mathbb{F}_p \). Cryptogr. Commun. 9(5), 637–646 (2017)
10. Kiermaier, M.: Geometrische konstruktionen linearer codes über galois-ringen der charakteristik 4 von hoher homogener minimaldistanz, dissertation, Universität Bayreuth (2012). https://epub.uni-bayreuth.de/id/eprint/195
11. Constantinescu, I., Heise, W.: A metric for codes over residue class rings. Probl. Inf. Transm. 33(3), 208–213 (1997)
12. Greferath, M., Schmidt, S.E.: Finite-ring combinatorics and MacWilliams equivalence theorem. J. Comb. Theory Ser. A 92, 17–28 (2000)
13. Honold, T., Nechaev, A.A.: Weighted modules and representations of codes. Probl. Inf. Transm. 35(3), 205–223 (1999)
14. Krotov, D.S.: \( \mathbb{Z}_2^n \) dual binary codes. IEEE Trans. Inf. Theory 53(4), 1532–1537 (2007)
15. Courteau, B., Wolfmann, J.: On triple sum sets and two or three-weight codes. Discret. Math. 50(2–3), 179–191 (1984)
16. Calderbank, R., Kantor, W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. 18(2), 97–122 (1986)
17. Ling, S., Xing, C.-P.: Coding Theory A First Course. Cambridge University Press, Cambridge (2004)
18. Byrne, E., Greferath, M., Honold, T.: Ring geometries, two-weight codes and strongly regular graphs. Des. Codes Cryptogr. 48(1), 1–16 (2008)
19. Gria, M., RifÁ, J., Huguet, L.: On s-sum-sets and projective codes. In: International conference on applied algebra, algebraic algorithms, and error-correcting codes, pp. 135-142. Springer, Berlin (1985)
20. Coma, J.R.: All s-sum sets of type 2 or 3 are triple-sum sets. Comput. Math. Appl. 23(1), 35–43 (1992)
21. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. Amsterdam, North-Holland (1977)
22. Pless, V.: Power moment identities on weight distributions in error correcting codes. Inf. Control 6(2), 147–152 (1963)
23. Shi, M., Wang, Y.: A note on one weight and two weight projective Z4-codes. J. Syst. Sci. Complex. 27(4), 795–810 (2014)
24. Shi, M., Xu, L., Yang, G.: Optimal binary codes from one-Lee weight codes and two-Lee weight projective codes over Z4. IEEE Trans. Inf. Theory 63(1), 177–182 (2017)
25. Carlet, C.: One-weight Z4-linear codes, coding theory, cryptography and related areas, Springer, 2000. Proceedings of an international conference on coding theory, cryptography and related areas, held in Guanajuato, Mexico, pp. 57–72 (1998)
26. Byrne, E., Kiermaier, M., Sneyd, A.: Properties of codes with two homogeneous weights. Finite Fields Their Appl. 18(4), 711–727 (2012)
27. Wong, J.N.C.: Classification of small optimal linear codes over Z4, Master thesis, University of Victoria (2002)
28. Feulner, T.: Canonization of linear codes over Z4. Adv. Math. Commun. 5(2), 245–266 (2011)
29. Kiermaier, M., Kurz, S., Solé, P., Stoll, M., Wassermann, A.: On strongly walk regular graphs, triple sum sets and their codes (2020) https://arxiv.org/pdf/2012.06160.pdf
30. Goethals, J.-M.: Nonlinear codes defined by quadratic forms over GF(2). Inf. Control 31, 43–74 (1976)
31. Shi, M., Alahmadi, A., Solé, P.: Codes and Rings: Theory and Practice. Academic Press, Cambridge (2017)
32. Kiermaier, M.: Generalized Teichmüller codes, in preparation (2021)
33. Kiermaier, M., Zwanzger, J.: New ring-linear codes from dualization in projective Hjelmslev geometries. Des. Codes Cryptogr. 66(1–3), 39–55 (2013)
34. Honold, T., Landjev, I.: All Reed-Muller codes are linearly representable over the ring of dual numbers over Z2. IEEE Trans. Inf. Theory 45(2), 700–701 (1999)
35. Shi, M., Zhu, S., Yang, S.: A class of optimal p-ary codes from one-weight codes over Fpn / <u^m >. J. Franklin Inst. 350(5), 929–937 (2013)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.