KNESER-HECKE-OPERATORS FOR CODES OVER FINITE CHAIN RINGS

AMY FEAVER, ANNA HAENSCH, JINGBO LIU, AND GABI NEBE

Abstract. In this paper we extend results on Kneser-Hecke-operators for codes over finite fields, to the setting of codes over finite chain rings. In particular, we consider chain rings of the form $\mathbb{Z}/p^2\mathbb{Z}$ for p prime. On the set of self-dual codes of length N, we define a linear operator, T, and characterize its associated eigenspaces.

1. Introduction

Many of the concepts of lattice theory have analogues in coding theory and vice versa.

Lattices L are $\mathbb{Z}$-modules generated by a basis of Euclidean space $(\mathbb{R}^N, (,))$. So they come with a given inner product that is used to define the dual lattice

$$L^{\#} := \{x \in \mathbb{R}^N \mid (x, \ell) \in \mathbb{Z} \text{ for all } \ell \in L\}$$

which satisfies $\operatorname{vol}(\mathbb{R}^N/L)\operatorname{vol}(\mathbb{R}^N/L^{\#}) = 1$. The euclidean norm enables the counting of lattice points according to their length and therewith defines a holomorphic function

$$\theta_L(z) := \sum_{\ell \in L} \exp((\ell, \ell)\pi i z), z \in \mathbb{C}, \Im(z) > 0$$

on the upper half plane, the so called theta series of the lattice L. From the theta series, it is possible to read off important invariants of the lattice, such as the density of the associated sphere packing. Theta series have nice invariance properties, they are examples of modular forms. In particular for even unimodular lattices (i.e. $L = L^{\#}$ and $(\ell, \ell) \in 2\mathbb{Z}$ for all $\ell \in L$), this theta series is a modular form for the full modular group $\mathrm{SL}_2(\mathbb{Z})$ ([6, Theorem 2.1]). Good upper bounds on the sphere packing density of an even unimodular lattice can be found using the theory of modular forms.

For the purpose of this note, codes C are R-submodules of R^N, where R is a finite commutative ring. Also R^N has a standard inner product $(,)$ that is used to define the dual code

$$C^{\perp} = \{x \in R^N \mid (x, c) = 0 \text{ for all } c \in C\}$$

for which one has $|C||C^{\perp}| = |R|^N$. Important invariants of the code C are given in the complete weight enumerator of C (see Definition 10) which is a homogenous polynomial of degree N in $|R|$ variables. For self-dual codes (i.e. $C = C^{\perp}$) this

2010 *Mathematics Subject Classification.* Primary 11T71, 94B05.

Key words and phrases. Coding Theory, Hecke operators.

This work was started at the WIN3 workshop at the Banff International Research Station in Banff, Canada. The authors wish to thank the organizers for their tremendous efforts, and for providing the opportunity to begin this collaboration.

complete weight enumerator is invariant under the associated Clifford-Weil group (as defined in [10]) which is a finite complex matrix group. Again for certain families of self-dual codes invariant theory of these groups allow to find good upper bounds on the error correcting properties of the codes.

There is a direct connection relating lattices and codes given by the well known Construction A (cf. [4, Section 7.2]). This construction associates a lattice $L(C)$ to a code C over a finite prime field which inherits certain properties of the code: If C is self-dual then so is $L(C)$, more general $L(C)^{\#} = L(C^{\perp})$ and also the theta-series of $L(C)$ is obtained from the complete weight enumerator of C by inserting certain well defined theta functions (see [4, Theorem (7.3)]).

Also other concepts like Siegel theta series and Siegel's phi operator have their coding theory analogues: higher genus complete weight enumerators and Runge's phi operator [16]. Also theta-series with harmonic coefficients have a counterpart in coding theory (see [1], [2]). One of the major tools to study modular forms are Hecke-operators. Certain of these Hecke-operators may be expressed in terms of lattices (see for instance [9]). In [11], Nebe translates the notion of Hecke-operators for theta series to the setting of codes over finite fields, defining the Kneser-Hecke-operator for codes when $R = \mathbb{F}_q$ is a finite field and therewith answers a question raised in 1977 in [3]. The primary goal of this paper is to extend these results to codes over finite chain rings, beginning with those chain rings of the form $R = \mathbb{Z}/p^2\mathbb{Z}$.

As in [11], we consider the family $\mathcal{F}$ of codes of a certain Type. While [11] deals with self-dual codes over finite fields, the present note starts the investigation for self-dual codes over $R = \mathbb{Z}/p^2\mathbb{Z}$ (for a complete discussion of code Types, see [10]). The general strategy of these papers is the same, namely, we define some notion of equivalence for codes, define a neighboring relation, and then define a linear operator, T, on the set of equivalence classes of codes in $\mathcal{F}$. This operator maps a code C to the sum of equivalence classes containing neighboring codes to C. One new ingredient here is that self-dual codes of the same length need not be isomorphic as R-modules. This yields a natural partition of the set of equivalence classes of self-dual codes into module isomorphism classes. We describe the connected components of the restriction of the neighboring graph to each of these subsets. It turns out that odd and even primes behave quite differently very likely due to the fact that we only work with bilinear forms instead of quadratic forms. For the ring $R = \mathbb{Z}/4\mathbb{Z}$ we get a very nice description of these connected components in Theorem 38.

This note reports on research on a WIN project for which time was limited. As we are just at the starting point, this paper implicitly contains more questions than answers. Therefore, it should be considered as a motivation to continue and generalize the research on this topic.

2. Codes over $\mathbb{Z}/p^2\mathbb{Z}$.

In this note we will discuss codes over base rings R of the form $R = \mathbb{Z}/p^2\mathbb{Z}$ where $p \in \mathbb{Z}$ is prime. Our computations will be performed for $p = 2$ as there are programs available to test equivalence of quaternary codes.

Recall that a *code* C over a finite ring R is an R-submodule $C \leq R^N$ of the free R-module of rank $N \in \mathbb{N}$. The Krull-Schmidt theorem gives us valuable insight regarding structure of the R-module C. Before stating this result, it is helpful to recall some facts about the ring $R = \mathbb{Z}/p^2\mathbb{Z}$:

a) R is a local ring with maximal ideal pR and unit group $R^* = R \setminus pR$. The ideals in R are R, pR and $\{0\}$.
b) There are exactly two indecomposable R-modules,
   (1) the regular R-module R and
   (2) the simple R-module $S \cong R/pR \cong pR$.

Applying the *Krull-Schmidt theorem*, we have that every finitely generated R-module M decomposes as $M \cong R^a \oplus S^b$ for unique $a, b \in \mathbb{N}_0 = \{0, 1, 2, \dots\}$.

2.1. **Self-dual codes.** One class of codes of particular interest is self-dual codes. Here we present the definition:

Definition 1. *The standard inner product is given by $b : R^N \times R^N \to R$ where $b(x, y) := \sum_{i=1}^N x_i y_i$. For a code $C \leq R^N$, the* dual code *is defined as*

$$C^\perp := \{x \in R^N \mid b(x, c) = 0 \text{ for all } c \in C\}.$$

C is called self-orthogonal *if $C \subseteq C^\perp$ and C is called* self-dual *if $C = C^\perp$.*

Let $C \leq R^N$ be a code of length N over the ring R. We write the elements of C as rows. Let $d \in \mathbb{N}$ be the smallest integer such that there exist $r_1, ..., r_d \in R^N$ which generate the R-module C. Then a generator matrix of C is a matrix $G \in R^{d \times N}$ where the rows of G are d elements $r_1, ..., r_d$ generating C. The isomorphism type of C as an R-module may be read off from a canonical generator matrix which we will define below. There is also a more structural way to obtain this information.

Remark 2. *As $|C||C^\perp| = |R|^N = p^{2N}$ (see for instance* [10, Lemma 3.3.4]*) any self-dual code $C = C^\perp \leq R^N$ is isomorphic, as an R-module, to $R^a \oplus S^b$ with $2a + b = N$.*

We first define families $\mathcal{F}$ of self-dual codes. Let $\mathcal{F} := \left\{C = C^\perp \leq R^N\right\}$. For $N = 2a + b$ with $a, b \in \mathbb{N}_0$ we define the set

$$\mathcal{F}_{a,b} := \left\{C \leq R^N \mid C = C^\perp, C \cong R^a \oplus S^b\right\} \subseteq \mathcal{F}.$$

Then $\mathcal{F}$ is the disjoint union of the sets $\mathcal{F}_{a,b}$. Let $[C]$ denote the permutation equivalence class of the code $C \in \mathcal{F}$. Then any of the sets $\mathcal{F}_{a,b}$ is the disjoint union of finitely many equivalence classes

$$\mathcal{F}_{a,b} = [C_1] \,\dot\cup \dots \dot\cup \left[C_{h(a,b)}\right].$$

We call $h(a, b)$ the *class number* of $\mathcal{F}_{a,b}$. Note that, when $a = 0$ and $b = N$ we always have $h(0, N) = 1$, as $\mathcal{F}_{0,N}$ consists of a single code:

$$\mathcal{F}_{0,N} = \left\{pR^N\right\} = \left[pR^N\right].$$

Let $C \in \mathcal{F}_{a,b}$. Then after replacing C by some equivalent code, if necessary, the code C has a generator matrix

$$G = \begin{bmatrix} I_a & X & Y \\ 0 & pI_b & pZ \end{bmatrix}$$

where I_a and I_b denote the unit matrices of size a and b respectively, $X \in \{0, \dots, p-1\}^{a \times b}$, $Y \in R^{a \times a}$ and $Z \in \{0, \dots, p-1\}^{b \times a}$. The self-duality of C is equivalent to $GG^{tr} = 0$. Thus $XX^{tr} + YY^{tr} = -I_a$ and $YZ^{tr} = -X \pmod p$.

2.2. **Torsion and residue codes.** To any code C over R we can associate a chain of codes over $\mathbb{F}_p$ using the general constructions for codes over finite chain rings (see [5] or [13]) as follows.

Definition 3. *For a vector $v \in R^N$, let $\overline{v}$ denote the canonical projection of v to the vector space $(R/pR)^N \cong \mathbb{F}_p^N$. Then the* torsion code *is given by*

$$Tor(C) = \{\overline{v} : pv \in C\} \leq (R/pR)^N \cong \mathbb{F}_p^N$$

and $Tor(C)$ has the generator matrix

$$\begin{bmatrix} I_a & X & Y \\ 0 & I_b & Z \end{bmatrix}$$

where X, Y and Z are given by the generator matrix G of C. The residue code *is given by*

$$Res(C) = \{\overline{v} : v \in C\} \leq (R/pR)^N \cong \mathbb{F}_p^N,$$

and $Res(C)$ has the generator matrix

$$\begin{bmatrix} I_a & X & Y \end{bmatrix}.$$

From this definition, it is clear that $\mathrm{Res}(C) \subseteq \mathrm{Tor}(C)$. It will be helpful for us to consider the following equivalent definitions for $\mathrm{Tor}(C)$ and $\mathrm{Res}(C)$. Identifying pR with $\mathbb{F}_p$ by $p \mapsto 1$, we have

$$\mathrm{Tor}(C) = C \cap pR^N \leq \mathbb{F}_p^N$$

and

$$\mathrm{Res}(C) = (C + pR^N)/pR^N \leq \mathbb{F}_p^N.$$

We also note that C is of module isomorphism type $R^a \oplus S^b$ if and only if $\dim(\mathrm{Tor}(C)) = a + b$ and $\dim(\mathrm{Res}(C)) = a$.

The lemma which follows is just [5, Lemma 5.4], but we present a proof here for the sake of exposition.

Lemma 4. *If the code $C \leq R^N$ is self-dual then $Res(C)^\perp = Tor(C)$ with respect to the standard inner product on $\mathbb{F}_p^N$.*

Proof. Let $C = C^\perp \cong R^a \oplus S^b \leq R^N$. Then by Remark 2 we have that $2a + b = N$ and hence $\dim(\mathrm{Tor}(C)) + \dim(\mathrm{Res}(C)) = N$. Thus it is enough to show that $C \subseteq C^\perp$ implies that $\mathrm{Tor}(C) \subseteq \mathrm{Res}(C)^\perp$.

Let $v, w \in R^N$ such that $\overline{v} \in \mathrm{Tor}(C)$ and $\overline{w} \in \mathrm{Res}(C)$. Then $b(pv, w) = pb(v, w) = 0$, since $pv, w \in C$ and C is self-dual. But then $b(v, w) \in pR$, and consequently $\overline{v}$ and $\overline{w}$ have inner product 0 in $\mathbb{F}_p^N$. □

Corollary 5. *Let $C = C^\perp \leq R^N$. Then C is uniquely determined by any of its maximal free submodules.*

Proof. Assume that $C \cong R^a \oplus S^b$ and let $C_1 \leq C$ be such a maximal free submodule, so $C_1 \cong R^a$. Then $\mathrm{Res}(C) = \mathrm{Res}(C_1)$, so given such a C_1 it is possible to find $\mathrm{Res}(C)$. Combining this with Lemma 4, we have

$$\mathrm{Tor}(C) = \mathrm{Res}(C)^\perp = \mathrm{Res}(C_1)^\perp$$

and therefore we can determine $C \cap pR^N$. But since $C = C_1 + (C \cap pR^N)$, we see that C_1 uniquely determines C. □

Suppose that we have a self-orthogonal code $C_1 \subseteq C_1^\perp \leq R^N$ with $C_1 \cong R^a$. Then we also have that $R^N/C_1 \cong \mathrm{Hom}_R(C_1, R) \cong R^a$ and hence $C_1^\perp \cong R^{N-a}$. Consequently, we have $C_1 + pC_1^\perp \cong R^a \oplus S^{N-2a}$. Moreover $C_1 + pC_1^\perp$ is self-orthogonal and hence self-dual, because $|C_1 + pC_1^\perp| = p^N$. Therefore we make the following remark:

Remark 6. *Given any self-orthogonal code $C_1 \subseteq C_1^\perp \leq R^N$ with $C_1 \cong R^a$ for some a, there is always a unique self-dual code $C \cong R^a \oplus S^{N-2a}$ containing C_1 as a maximal free submodule, namely $C = C_1 + pC_1^\perp$.*

A code C over $\mathbb{F}_2$ is called *doubly-even* if the number of nonzero entries in every codeword in C is divisible by 4. This definition will be illuminated further in the next section, but a preliminary notion is necessary for the following result.

Corollary 7. *If $C \subseteq C^\perp \leq R^N$ is a self-orthogonal code then Res(C) is a self-orthogonal code of length N over $\mathbb{F}_p$. Moreover if $p = 2$ then Res(C) is doubly-even.*

A special case is $b = 0$: here C is a free R-module so $\mathrm{Res}(C) = \mathrm{Tor}(C)$. If we additionally have that $C = C^\perp$, then $\mathrm{Res}(C) \leq \mathbb{F}_p^N$ is a self-dual code, which is doubly even if $p = 2$.

Doubly-even self-dual binary codes exist if and only if the length N is a multiple of 8. For odd primes p self-dual codes over $\mathbb{F}_p$ exist if and only if either the length N is a multiple of 4, or N is even and $p \equiv 1 \pmod 4$.

Corollary 8. *Let $C = C^\perp \leq R^N$ be a self-dual code that is also a free R-module. Then $C \cong R^{N/2}$ so N is even. If $p = 2$ then the length N is a multiple of 8 and if $p \equiv 3 \pmod 4$, the length N is a multiple of 4.*

We usually get a smoother theory of orthogonal groups (such as Witt's extension theorem) if we work with quadratic forms. This is straightforward if $p \neq 2$: The function $q : R^N \to R$ given by $q(x) := \frac{1}{2}b(x, x)$ is a quadratic form with associated bilinear form b, as

$$b(x, y) = q(x + y) - q(x) - q(y).$$

Thus the orthogonal groups of b and q coincide and any self-orthogonal code C satisfies $q(C) = \{0\}$, i.e. C is isotropic.

If $p = 2$ and $R = \mathbb{Z}/4\mathbb{Z}$ the situation is more complicated: There is a well defined quadratic form

$$q : R^N \to \mathbb{Z}/8\mathbb{Z}, q(x) := \sum_{i=1}^{N} x_i^2$$

where $x_i^2 = 1 \in \mathbb{Z}/8\mathbb{Z}$ if $x_i = 1$ or $3 \in R$, $x_i^2 = 0$ if $x_i = 0$, and $x_i^2 = 4$ if $x_i = 2 \in R$. Then $b(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$ for all $x, y \in R^N$. We call C *isotropic* if $q(C) = \{0\}$. Clearly isotropic codes are always self-orthogonal. Isotropic self-dual codes are also called *doubly-even self-dual codes.*

Essentially the same form q may also be obtained as an R-valued quadratic form. If $C \leq R^N$ is a self-orthogonal code, then $b(c, c) = 0$ for all $c \in C$, so the number of odd entries in c is 0 mod 4. Let

$$\mathcal{X} := \{x \in R^N \mid b(x, \mathbf{1}) \equiv 0 \pmod 2\}$$

(where $\mathbf{1}$ is the all-ones vector) denote the submodule of all vectors having an even number of odd entries. Then $b(x, x)$ is always even for $x \in \mathcal{X}$, so

$$\overline{q} : \mathcal{X} \to R, x \mapsto \frac{1}{2}|\{i \mid x_i \text{ is odd }\}| + 2|\{i \mid x_i = 2\}|$$

is a well defined R-valued quadratic form with associated bilinear form b. In fact this quadratic form is obtained from the restriction of the $\mathbb{Z}/8\mathbb{Z}$ valued form to $\mathcal{X}$ and then dividing by 2. The radical of $\mathcal{X}$ is $\mathcal{X}^{\perp} = \langle 2 \cdot \mathbf{1} \rangle$ and self-dual isotropic codes correspond to the maximal isotropic subspaces of the non-degenerate quadratic module $(\mathcal{X}/\mathcal{X}^{\perp}, \overline{q})$.

Note that any self-dual code C contains $\mathcal{X}^{\perp} = \langle 2 \cdot \mathbf{1} \rangle$ as $b(x, 2 \cdot \mathbf{1}) = 2$ times the number of odd entries in x. So the doubly-even self-dual codes are in natural bijection to the maximal isotropic subspaces of $\mathcal{X}/\mathcal{X}^{\perp}$.

Note that the module structure of $\mathcal{X}/\mathcal{X}^{\perp}$ is $R^{N-2} \oplus S^2$ if N is even and it is R^{N-1} if N is odd. A similar situation has been investigated by J.A.Wood [18] for the case that $R = \mathbb{F}_2$ and the quadratic form is $\mathbb{Z}/4\mathbb{Z}$-valued. The second approach to the quadratic form clarifies his "obstruction" to the extendability of isometries.

2.3. **Weight enumerators.** In this section we will build to the definitions of two different types of weight enumerators of codes.

Definition 9. *Let R be any ring and $N \in \mathbb{N}$.*

(1) *For any $c := (c_1, ..., c_N) \in R^N$ the* Hamming weight *of c is*
$$\mathrm{wt}(c) := |\{i, 1 \leq i \leq N : c_i \neq 0\}|.$$
(2) *For any subset $C \subseteq R^N$ the* minimal Hamming weight *of C is*
$$\mathrm{wt}(C) = \min\{\mathrm{wt}(c) | 0 \neq c \in C\}.$$

More generally, for each $c \in R^N$ we can use the notion of the *composition* of c to refine its Hamming weight. For each $r \in R$ define $a_r(c) := |\{i : c_i = r\}|$. The set $\{a_r(c) | r \in R\}$ is the *composition* of c and tells us the number of components of c which are equal to each $r \in R$. This is connected to the Hamming weight in that $\mathrm{wt}(c) = N - a_0(c)$.

For a code $C \leq R^N$ the weight enumerator of C is a polynomial attached to the code and the associated weight. These may give, for example, the number of codewords with a given weight or with a given composition. Here are two weight enumerators associated to the Hamming weight:

Definition 10. *Let R be a ring and $C \leq R^N$ be a code of length $N \in \mathbb{N}$.*

(1) *The* Hamming weight enumerator *of C is*
$$\mathrm{hwe}(C)(x, y) := \sum_{c \in C} x^{N - \mathrm{wt}(c)} y^{\mathrm{wt}(c)} \in \mathbb{C}[x, y]$$
(2) *The* complete weight enumerator *of C is*
$$\mathrm{cwe}(C) := \sum_{c \in C} \prod_{i=1}^{N} x_{c_i} = \sum_{c \in C} \prod_{v \in V} x_v^{a_v(c)} \in \mathbb{C}[x_v : v \in V].$$

Note that in the above definition, both weight enumerators are homogeneous polynomials of degree N.

Another weight, the Lee weight, is defined on elements of rings of the form $R = \mathbb{Z}/m\mathbb{Z}$ for $m \in \mathbb{N}$ which we identify with the set $\{0, \ldots, m-1\} \subset \mathbb{Z}$. The Lee weight can be thought of as the minimum "distance" of an element of $r \in R$ to $0 \in R$. More precisely:

Definition 11. *Let $R = \mathbb{Z}/m\mathbb{Z}$ for some $m \in N$.*

(1) *The* Lee weight *of an element* $r \in R$ *is* $\mathrm{Lee}(r) := \min\{r, m-r\}$.
(2) *For any* $N \in \mathbb{N}$ *and any vector* $c = (c_1, ..., c_N) \in R^N$ *we define the* Lee weight *of* c *as*

$$\mathrm{Lee}(c) = \sum_{i=1}^{N} \mathrm{Lee}(c_i).$$

Note that in the case where $m = 2$ we find that for any $c \in R^N$ $\mathrm{wt}(c) = \mathrm{Lee}(c)$. In the case of quartenary codes we have $R = \{0, 1, 2, 3\}$ and the Lee weights of these elements are, respectively, $0, 1, 2, 1$.

2.4. **The associated Clifford-Weil groups.** One main goal of the book [10] is to develop a general theory of a "Type" $\mathcal{T}$ of a self-dual code over a finite alphabet V. To such a Type one may associate in a very natural way a finite subgroup $\mathcal{C}(\mathcal{T}) \leq \mathrm{GL}_{|V|}(\mathbb{C})$, *the associated Clifford-Weil group* such that the complete weight enumerators of self-dual codes of Type $\mathcal{T}$ are invariant under $\mathcal{C}(\mathcal{T})$. In fact one of the main results of [10] is that for codes over finite chain rings (or more general matrix rings over finite chain rings) the complete weight enumerators of self-dual codes of Type $\mathcal{T}$ and length N span the space of degree N homogeneous invariants of $\mathcal{C}(\mathcal{T})$. This section intends to explain the recipe to compute $\mathcal{C}(\mathcal{T})$ for our situation without introducing the general, but quite heavy, machinery from [10].

In our situation the alphabet $V = R = \mathbb{Z}/p^2\mathbb{Z}$ is the ring itself. As any code $C \leq R^N$ is an R-module we have $C = rC$ for any $r \in R^*$ and hence also

$$cwe(C)(x_0, x_1, \ldots, x_{p^2-1}) = cwe(C)(x_{r\cdot 0}, x_{r\cdot 1}, \ldots, x_{r\cdot(p^2-1)})$$

so complete weight enumerators of codes are invariant under all variable substitutions

$$m_r : x_v \mapsto x_{rv},$$

where r is a unit in R.

There is a famous theorem, proven in the PhD thesis of Jessie MacWilliams, that relates the weight enumerator of a code over a finite field to the weight enumerator of its dual code. This result is proved in greater generality in [10, Section 2.2]). In our situation this reads as follows: Let $\zeta := \exp(\frac{2\pi i}{p^2}) \in \mathbb{C}$ be a primitive p^2-th root of unity. For $v \in \mathbb{Z}/p^2\mathbb{Z}$ we define $h(x_v) := \sum_{w \in \mathbb{Z}/p^2\mathbb{Z}} \zeta^{vw} x_w$. Then for any code $C \leq (\mathbb{Z}/p^2\mathbb{Z})^N$ the complete weight enumerator of the dual code is

$$cwe(C^{\perp})(x_0, x_1, \ldots, x_{p^2-1}) = \frac{1}{|C|} cwe(C)(h(x_0), h(x_1), \ldots, h(x_{p^2-1})).$$

In particular if $C = C^{\perp}$ then $|C| = p^N$ and $cwe(C)$ is invariant under

$$H := \frac{1}{p} h : x_v \mapsto \frac{1}{p} \sum_{w \in \mathbb{Z}/p^2\mathbb{Z}} \zeta^{vw} x_w.$$

One additional ingredient of a Type are certain quadratic conditions. One of these conditions comes from the inner product of codewords with themselves: If $C \leq R^N$ is self-orthogonal, then $b(c,c) = \sum_{i=1}^{N} c_i^2 = 0$ for all $c \in C$ and hence $cwe(C)$ is invariant under the variable substitution d with

$$d(x_v) := \zeta^{v^2} x_v$$

Definition 12. *The associated Clifford Weil group of the Type of all self-dual codes over $\mathbb{Z}/p^2\mathbb{Z}$ is*

$$\mathcal{C}(p^2) := \langle m_r, H, d \mid r \in \mathbb{Z}/p^2\mathbb{Z}^* \rangle \leq \mathrm{GL}_{p^2}(\mathbb{Q}[\zeta]).$$

With this notation the main result of [10] implies that

Theorem 13. *The invariant ring of $\mathcal{C}(p^2)$ is spanned by the complete weight enumerators of all self-dual codes over $\mathbb{Z}/p^2\mathbb{Z}$.*

As an example we give explicit generators for $p = 2$ and $p = 3$:

$$\mathcal{C}(4) = \langle m_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, H = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \zeta & -1 & -\zeta \\ 1 & -1 & 1 & -1 \\ 1 & -\zeta & -1 & \zeta \end{pmatrix}, d = \mathrm{diag}(1, \zeta, 1, \zeta)\rangle$$

of order $2^6 = 64$ where $\zeta = i$ is a primitive fourth root of unity and

$$\mathcal{C}(9) = \langle m_2, H, d\rangle$$

where $d = \mathrm{diag}(1, \zeta, \zeta^4, 1, \zeta^7, \zeta^7, 1, \zeta^4, \zeta)$, and ζ is a primitive ninth root of unity,

$$m_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \text{ and } H = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \zeta & \zeta^2 & \zeta^3 & \zeta^4 & \zeta^5 & \zeta^6 & \zeta^7 & \zeta^8 \\ 1 & \zeta^2 & \zeta^4 & \zeta^6 & \zeta^8 & \zeta & \zeta^3 & \zeta^5 & \zeta^7 \\ 1 & \zeta^3 & \zeta^6 & 1 & \zeta^3 & \zeta^6 & 1 & \zeta^3 & \zeta^6 \\ 1 & \zeta^4 & \zeta^8 & \zeta^3 & \zeta^7 & \zeta^2 & \zeta^6 & \zeta & \zeta^5 \\ 1 & \zeta^5 & \zeta & \zeta^6 & \zeta^2 & \zeta^7 & \zeta^3 & \zeta^8 & \zeta^4 \\ 1 & \zeta^6 & \zeta^3 & 1 & \zeta^6 & \zeta^3 & 1 & \zeta^6 & \zeta^3 \\ 1 & \zeta^7 & \zeta^5 & \zeta^3 & \zeta & \zeta^8 & \zeta^6 & \zeta^4 & \zeta^2 \\ 1 & \zeta^8 & \zeta^7 & \zeta^6 & \zeta^5 & \zeta^4 & \zeta^3 & \zeta^2 & \zeta \end{pmatrix}.$$

We computed that $|\mathcal{C}(9)| = 2^3 3^4 = 648$.

Adding certain "quadratic" conditions we obtain overgroups of these associated Clifford Weil groups: For instance we may consider only those self-dual codes that contain the all ones vector $\mathbf{1} = (1, \dots, 1)$. We have that $\mathbf{1} \in C^{\perp}$ if and only if $b(c, \mathbf{1}) = \sum_{i=1}^{N} c_i = 0$ for all $c \in C$. Then the weight enumerator of C is invariant under $d_{\mathbf{1}} : x_v \mapsto \zeta^v x_v$ and we obtain the associated Clifford Weil groups

$$\mathcal{C}_{\mathbf{1}}(p^2) := \langle \mathcal{C}(p^2), d_{\mathbf{1}} \rangle.$$

For $p = 2$ we could also restrict to doubly-even self-dual codes which yields an additional invariance condition of the weight enumerator under the transformation $d_q : x_v \mapsto \zeta_8^{v^2} x_v$, where ζ_8 is a primitive 8th root of unity. We hence obtain

$$\mathcal{C}_q(4) := \langle \mathcal{C}(4), d_q \rangle \text{ and } \mathcal{C}_{\mathbf{1},q}(4) := \langle \mathcal{C}(4), d_q, d_{\mathbf{1}} \rangle.$$

The isomorphism type of these Clifford Weil groups may be read off from the description of the hyperbolic co-unitary groups in [10, Definition 5.2.4]. From this we obtain the following:

Remark 14. *For odd primes p the group $\mathcal{C}(p^2)$ is isomorphic to $\mathrm{SL}_2(\mathbb{Z}/p^2\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^3 : \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. The group $\mathcal{C}(4)$ is isomorphic to an extension of $(\mathbb{Z}/2\mathbb{Z})^2$ by a certain Sylow 2-subgroup $\mathcal{S}$ of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$, namely*

$$\mathcal{S} = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z}) \mid ac \in 2\mathbb{Z}, bd \in 2\mathbb{Z}\}.$$

2.5. **Equivalence of codes.**

Definition 15. *Let $\pi \in S_N$ be a permutation of $\{1, ..., N\}$ and let $a_1, \ldots, a_N \in R^*$. A* monomial map *is a map $((a_1, \ldots, a_N), \pi) : R^N \to R^N$ given by*

$$((a_1, \ldots, a_N), \pi)(r_1, ..., r_N) := \left(a_1 r_{\pi(1)}, \ldots, a_N r_{\pi(N)}\right).$$

For the ring R, the set of all monomial maps is a group. We call this the *monomial group* and denote it by $\mathrm{Mon}_N(R)$.

Monomial maps are interesting in this context because of their connection to the Hamming weight. What follows is the MacWilliams extension theorem which was originally proved for codes over finite fields, but later extend to the more general setting of codes over finite rings by Wood in [17].

Theorem 16 (*MacWilliams extension theorem*)**.** *Let $C \leq R^N$ and $\varphi : C \to R^N$ be a homomorphism which preserves the Hamming weight, i.e.* $\mathrm{wt}(c) = \mathrm{wt}(\varphi(c))$ *for all $c \in C$. then there exists a monomial map $((a_1, \ldots, a_N), \pi)$ such that*

$$((a_1, \ldots, a_N), \pi)(c) = \varphi(c)$$

for all $c \in C$.

So if one only considers the Hamming weight, the natural notion of equivalence for codes is monomial equivalence, where two codes are called monomially equivalent if they are in the same orbit under the monomial group.

Monomial maps do not preserve the bilinear form b and hence they do not preserve self-duality. This leads to the notion of strong monomial equivalence: this is where we restrict the values $a_1, ..., a_N$ to the set $\{\pm 1\}$. In this case, $a_i^2 = 1$ and thus the bilinear form b is preserved.

In this paper we consider an even finer equivalence relation, the permutation equivalence:

Definition 17. *Two codes $C, D \leq R^N$ are called (permutation)* equivalent*, $C \equiv D$, if there is a coordinate permutation $\pi \in S_N$ such that $\pi(C) = D$. Let*

$$[C] := \{D \mid D \equiv C\}$$

denote the (permutation) equivalence class of the code C and

$$\mathrm{Aut}(C) := \{\pi \in S_N \mid \pi(C) = C\}$$

the automorphism group *of C.*

Note that permutation equivalent codes have the same complete weight enumerator.

No matter which type of equivalence we take, equivalent codes are always isomorphic as modules. However, two codes of the same module type need not be equivalent as codes. Thus

$$C \equiv D \Rightarrow C \cong D.$$

3. The action of the orthogonal group

Definition 18. *The orthogonal group $\mathcal{O}_N(R)$ is the group of all R-linear maps preserving the bilinear form b,*

$$\mathcal{O}_N(R) := \{\varphi \in \mathrm{GL}_N(R) \mid b(\varphi(x), \varphi(y)) = b(x, y) \text{ for all } x, y \in R^N\}.$$

For $R = \mathbb{Z}/4\mathbb{Z}$ the theory becomes much smoother if we work with quadratic forms. Recall that $\mathcal{X} = \{x \in (\mathbb{Z}/4\mathbb{Z})^N \mid b(x,x) \in 2\mathbb{Z}\}$ with radical $\mathcal{X}^\perp = \langle 2 \cdot \mathbf{1} \rangle$. Then

$$\overline{q} : \mathcal{X} \to R, x \mapsto \frac{1}{2}|\{i \mid x_i \text{ is odd }\}| + 2|\{i \mid x_i = 2\}|$$

is a well defined R-valued quadratic form, and $\mathcal{X}/\mathcal{X}^\perp$ is a nondegenerate quadratic space with respect to $\overline{q}$. Note that the module structure of $\mathcal{X}/\mathcal{X}^\perp \cong R^{N-2} \oplus S^2$ if N is even and it is R^{N-1} if N is odd.

For orthogonal groups of quadratic forms over fields, there is a famous theorem attributed to Ernst Witt, that orthogonal mappings from subspaces extend to orthogonal mappings of the full space.

Theorem 19. *(Witt's extension theorem) (See for instance* [7] *or* [18]*)*
Let (V,q) be a regular quadratic space over a field K and $U \leq V$. For any K-linear injective map $\varphi : U \to V$ with $q(\varphi(u)) = q(u)$ for all $u \in U$, there is $g \in \mathcal{O}(V,q)$ such that $\varphi = g_{|U}$.

Martin Kneser [7] generalized this theorem to local rings, if U is a free module.

It is easy to see that Witt's extension theorem is wrong without this assumption that U be free: In our situation $R = \mathbb{Z}/p^2\mathbb{Z}$ we could choose $u := (p, 0, \ldots, 0)$ and $w := (\underbrace{p, \ldots, p}_{p}, 0, \ldots, 0)$. Then $b(u,u) = b(w,w) = 0$ but there is no $g \in \mathcal{O}_N(R)$ with $g(u) = w$, because any such g would map $\tilde{u} := \{x \in R^N \mid px = u\} = (1, 0, \ldots, 0) + pR^N$ to $\tilde{w} = (1, \ldots, 1, 0, \ldots, 0) + pR^N$ but the elements $x \in \tilde{u}$ satisfy $b(x,x) \in 1 + pR$ and the elements $y \in \tilde{w}$ satisfy $b(y,y) \in pR$.

Note that this is also true for odd primes p, so this is not caused by the problem of working with a bilinear form instead of a quadratic form.

Nevertheless, the following theorem is true:

Theorem 20. *Let $\mathcal{F}_{a,b} := \{C = C^\perp \leq R^N \mid C \cong_R R^a \oplus S^b\}$ so $a, b \in \mathbf{N}_0$, $2a + b = N$. If $p \neq 2$, then $\mathcal{O}_N(R)$ acts transitively on $\mathcal{F}_{a,b}$.*

Proof: Let $C, D \in \mathcal{F}_{a,b}$ and choose subcodes $C' \leq C, D' \leq D$ so that $C' \cong R^a$, $D' \cong R^a$. Then C' is a free module, any R-isomorphism $\varphi : C' \to D'$ preserves the bilinear form (as this is 0 on C' and also on D'), and

$$\mathrm{Hom}_R(C', R) = \{c \mapsto b(c,x) \mid x \in R^N\}.$$

So by [7, Folgerung (4.4)] there is $g \in \mathcal{O}_N(R)$ such that $g_{|C'} = \varphi$. Then Corollary 5 implies that $g(C) = D$. q.e.d.

For $p = 2$ we want to proceed similarly as for odd primes but $(C' + \mathcal{X}^\perp)/\mathcal{X}^\perp \leq \mathcal{X}/\mathcal{X}^\perp$ does not satisfy the conditions from [7, Folgerung (4.4)], because $(C' + \mathcal{X}^\perp)/\mathcal{X}^\perp$ is usually not free.

Remark 21. *If $p = 2$, then define*

$$\mathcal{F}_{a,b}^{(q)} := \{C = C^\perp \leq R^N \mid q(C) = \{0\}, C \cong R^a \oplus S^b\}$$

$2a + b = N$ for $a, b \in N_0$. For $C \in \mathcal{F}_{a,b}^{(q)}$ there are two possibilities,
(1) $2 \cdot \mathbf{1} \in 2C$ and then $C/\mathcal{X}^\perp \cong R^{a-1} \oplus S^{b+1}$; or,
(2) $2 \cdot \mathbf{1} \notin 2C$ then $C/\mathcal{X}^\perp \cong R^a \oplus S^b$.
According to these two possibilities the orthogonal group $\mathcal{O}(\mathcal{X}/\mathcal{X}^\perp, \overline{q})$ has at least two orbits $\mathcal{F}_{a,b}^{(q)}(1)$ and $\mathcal{F}_{a,b}^{(q)}(2)$ on $\mathcal{F}_{a,b}^{(q)}$.

Remark 22. *Keeping the notation of the previous remark, let $C' \leq C$ be a subcode of C that is free of rank a. Then $2C' = 2C$ and in the first case $\mathcal{X}^{\perp} \subseteq C'$ and $C'/\mathcal{X}^{\perp} = C_1 \oplus \langle v \rangle$ with $C_1 \cong R^{a-1}$ and $2v = 2 \cdot \mathbf{1}$. In the second case $\mathcal{X}^{\perp} \not\subseteq C'$ and $C' + \mathcal{X}^{\perp}/\mathcal{X}^{\perp} \cong C' \cong R^a$ is free. So here we may directly apply Witt's theorem for local rings* [7, Folgerung (4.4)] *to show that $\mathcal{O}(\mathcal{X}/\mathcal{X}^{\perp}, \overline{q})$ acts transitively on $\mathcal{F}_{a,b}^{(q)}(2)$.*

For $\mathcal{F}_{a,b}^{(q)}(1)$ we can apply [7, Folgerung (4.4)] twice to obtain transitivity:

Lemma 23. *Let $C, D \in \mathcal{F}_{a,b}^{(q)}(1)$, C', D' free submodules of rank a as before and $C' = C_1 \oplus \langle v \rangle$, $D' = D_1 \oplus \langle w \rangle$ as in Remark 22. Then there is $u \in \mathcal{O}(\mathcal{X}/\mathcal{X}^{\perp}, \overline{q})$ mapping $C'/\mathcal{X}^{\perp}$ onto $D'/\mathcal{X}^{\perp}$.*

Proof: We first want to find reflections in $\mathcal{O}(\mathcal{X}/\mathcal{X}^{\perp}, \overline{q})$ that map v to w. As both vectors v, w satisfy $2v = 2 \cdot \mathbf{1} = 2w$, we have $v, w \in \{1, -1\}^N$. The element $z_i := 2e_i = (0, \ldots, 0, 2, 0, \ldots, 0)$, with 2 at the i-th place lives in $\mathcal{X}$. We have $q(z_i) = 2$, $b_q(z_i, x) \in 2R$ for all $x \in \mathcal{X}$, so the map

$$s_{z_i} : \mathcal{X} \to \mathcal{X}, x \mapsto x - b_q(z_i, x)e_i$$

is a well defined orthogonal mapping $s_{z_i} \in \mathcal{O}(\mathcal{X}/\mathcal{X}^{\perp}, q)$. If $x = (x_1, \ldots, x_N)$, then $b_q(z_i, x) = 2x_i$ and hence

$$q(s_{z_i}(x)) = q(x - x_i z_i) = q(x) + x_i^2 q(z_i) - x_i b_q(x, z_i) = q(x) + 2x_i^2 - 2x_i^2 = q(x).$$

Moreover s_{z_i} multiplies the i-th coordinate of v by -1, so a certain product of these reflections s_{z_i} will map v to w. So we may assume without loss of generality that $v = w$. We now replace $\mathcal{X}/\mathcal{X}^{\perp}$ by the subspace

$$E := \langle v \rangle^{\perp} = \{x + \mathcal{X}^{\perp} \mid x \in \mathcal{X}, b_q(x, v) = 0\} \leq \mathcal{X}/\mathcal{X}^{\perp}.$$

As $E^{\perp} = \langle v \rangle/\mathcal{X}^{\perp}$ any $g \in \mathcal{O}(E, \overline{q})$ perserves v. Moreover $C_1 \cong C_1 + \mathcal{X}^{\perp}/\mathcal{X}^{\perp} \leq E$ and $D_1 \cong D_1 + \mathcal{X}^{\perp}/\mathcal{X}^{\perp} \leq E$ are both free submodules of E. By Witt's theorem for free modules over local rings, there is such a mapping $g \in \mathcal{O}(E, \overline{q})$ with $g(C_1) = D_1$. q.e.d.

Corollary 24. *The orthogonal group $\mathcal{O}(\mathcal{X}/\mathcal{X}^{\perp}, \overline{q})$ has two orbits on the set $\mathcal{F}_{a,b}^{(q)}$:*

$$\begin{array}{lcl} \mathcal{F}_{a,b}^{(q)}(1) & := & \{C \in \mathcal{F}_{a,b}^{(q)} \mid 2 \cdot \mathbf{1} \in 2C\} \\ \textit{and} & & \\ \mathcal{F}_{a,b}^{(q)}(2) & := & \{C \in \mathcal{F}_{a,b}^{(q)} \mid 2 \cdot \mathbf{1} \not\in 2C\} \end{array}$$

One might replace $\mathcal{O}(\mathcal{X}/\mathcal{X}^{\perp}, \overline{q})$ by the group $\mathcal{O}_N(R, q)$ in this corollary, however we have not yet closed a necessary gap in the proof. It would also be interesting to have a similar result for $p = 2$ and $\mathcal{O}_N(\mathbb{Z}/4\mathbb{Z})$ for the set $\mathcal{F}_{a,b}$. This might be obtained along the lines of [15].

4. Hecke operators

4.1. **Survey of the results over fields.** The paper [11] defines and analyses certain linear operators that are shown to be Hecke operators for the associated Clifford Weil groups in [12]. Let $\mathbb{F}$ be a finite field, $N \in 2\mathbb{N}$ and $\mathcal{F}$ be the set of all self-dual codes in $\mathbb{F}^N$. Assume that $C_1, \ldots, C_h$ represent the permutation equivalence classes of codes in $\mathcal{F}$. Let $\mathcal{V}$ denote the h-dimensional complex vector space

$$\mathcal{V} := \left\{ \sum_{i=1}^{h} a_i[C_i] \mid a_i \in \mathbb{C} \right\},$$

and define a Hermitian positive definite scalar product by

$$([C],[D]) := |\mathrm{Aut}(C)|\, \delta_{[C],[D]}$$

for all $C, D \in \mathcal{F}$.

Definition 25. *(1) For $0 \le k \le N/2$, two codes $C, D \in \mathcal{F}$ are called* k-neighbors*, written as $C \sim_k D$, if $\dim(C \cap D) = \dim(C) - k$.*

(2) Define a linear operator T_k on $\mathcal{V}$ by

$$T_k([C]) := \sum_{D \sim_k C} [D],$$

where the sum is over all k-neighbors $D \in \mathcal{F}$ of the code C. The operator T_k is called the k-th Kneser-Hecke-operator *for $\mathcal{F}$.*

(3) Let $T := T_1$ be the Kneser-Hecke-operator *and call 1-neighbors simply* neighbors*.*

The following result and it's proof can be found as [11, Theorem 3], but we state it here in order to illustrate the approach for codes over fields as compared to codes over finite chain rings.

Theorem 26. *For $0 \le k \le N/2$, the operator T_k is a self-adjoint linear operator on the Hermitian vector space $\mathcal{V}$.*

The main result of [11] is an explicit computation of the T-eigenspace decomposition of $\mathcal{V}$ and the corresponding eigenvalues for all classical types of self-dual codes over finite fields.

In [12] the action of T on the space of genus m-weight enumerators of the codes in $\mathcal{F}$ coincides with the action of a certain linear combination of double cosets of the associated Clifford Weil groups.

There is also a nice representation theoretic interpretation of T (see [14, Chapter 5]): Let A denote the adjacency matrix of the neighboring graph whose vertices are the elements of $\mathcal{F}$ and two vertices C and D are connected by an edge, if and only if C and D are neighbors. The associated orthogonal group $\mathcal{O}(\mathbb{F}^N)$ acts on the set $\mathcal{F}$ and respects the neighboring relation. In particular, A is an element in the endomorphism ring of the corresponding permutation representation of $\mathcal{O}(\mathbb{F}^N)$. This endomorphism ring is well-known and can be described in the framework of Bruhat Tits theory using the Weil group of $\mathcal{O}(\mathbb{F}^N)$. In particular, it is shown in [14, Section 5.3.13] that the action of A coincides with the one of a certain (very natural) double coset of $\mathcal{O}(\mathbb{F}^N)$. This implies that A generates the endomorphism ring of this permutation representation as a $\mathbb{C}$-algebra, and in particular, this endomorphism ring is commutative and hence the permutation representation is multiplicity free.

The aim of the next section is to generalize some of these aspects to codes over finite chain rings, where we start with $R = \mathbb{Z}/p^2\mathbb{Z}$.

4.2. **Kneser-Hecke-operators for R.** We now return to the situation where $R = \mathbb{Z}/p^2\mathbb{Z}$. As before, let $\mathcal{F} = \dot\bigcup_{2a+b=N} \mathcal{F}_{a,b}$ denote the set of all self-dual codes in R^N. Assume that $C_1, \ldots, C_h$ represent the permutation equivalence classes of codes in $\mathcal{F}$. Let $\mathcal{V}$ denote the h-dimensional complex vector space

$$\mathcal{V} := \left\{ \sum_{i=1}^{h} a_i [C_i] \mid a_i \in \mathbb{C} \right\},$$

and define a Hermitian positive definite scalar product by

$$([C], [D]) := |\mathrm{Aut}(C)| \, \delta_{[C],[D]}$$

for all $C, D \in \mathcal{F}$. Then, $\mathcal{V}$ is the orthogonal sum of all $\mathcal{V}_{a,b}$ with $2a + b = N$, where $\mathcal{V}_{a,b}$ is the subspace of $\mathcal{V}$ generated by all $[C]$ with $C \in \mathcal{F}_{a,b}$.

Definition 27. *(1) Two codes $C, D \in \mathcal{F}$ are called* neighbors*, denoted $C \sim D$, if $C/(C \cap D) \cong D/(C \cap D) \cong pR$. We call them* free neighbors*, denoted $C \sim_R D$, if $C/(C \cap D) \cong D/(C \cap D) \cong R$.*

(2) We define a graph Γ with vertex set $\mathcal{F}$. Two vertices C and D are joined by an edge in Γ, if $C \sim D$. Similarly we define the graph Γ_a as the restriction of Γ to $\mathcal{F}_{a,b}$.

In the following we will mainly be concerned with the neighboring relation $\sim$ and the graphs Γ_a. However $\sim_R$ might be the more suitable generalization of neighbors over fields, as this relation preserves the module isomorphism type.

Lemma 28. *If $C \sim_R D$, then $C \cong D$ as R-modules.*

Proof. By definition, we have the exact sequences

$$0 \to C \cap D \to C \to R \to 0, \quad 0 \to C \cap D \to D \to R \to 0.$$

As R is a free module, both sequences split and hence $C \cong C \cap D \oplus R \cong D$. □

Note that this lemma is not true if one replaces free neighbors by neighbors. Now we define a linear operator T on $\mathcal{V}$ by $T([C]) = \sum_{D \sim C} [D]$. By arranging the basis elements according to module isomorphism type, we have

$$T = \begin{bmatrix} T_0 & \cdots & & \\ \vdots & T_1 & & \\ & & \ddots & \vdots \\ & & \cdots & T_n \end{bmatrix},$$

where $n = \lfloor \frac{N}{2} \rfloor$ and

$$T_a : \mathcal{V}_{a,b} \to \mathcal{V}_{a,b}, T_a([C]) := \sum_{D \sim C, D \in \mathcal{F}_{a,b}} [D]$$

can be computed from the adjacency matrix of the neighboring graph Γ_a. We immediately observe that for any choice of $\mathcal{F}$, $T_0 = [0]$, since there is only one code in $\mathcal{F}$ of isomorphism type S^N. Note that our notation does not imply that T is a block diagonal matrix. On the contrary, as we will see below, for odd primes p the matrices T_a are all 0. So the T_a are only interesting for $p = 2$ and for odd primes one should probably consider free neighbors or the matrix T^2 to obtain interesting operators on $\mathcal{V}_{a,b}$.

Theorem 29. *The Kneser-Hecke-operators T (and hence all the T_a) and T_R are self-adjoint linear operators on the Hermitian space $\mathcal{V}$.*

Proof. Let us prove the self-adjointness of T, this implies that the T_a as the summands of $\mathcal{V}_{a,b}$ are orthogonal. By definition, T is linear. For basis vectors $[C], [D]$ with $C, D \in \mathcal{F}$, one has

$$\begin{aligned} &\tfrac{N!}{|\operatorname{Aut}(D)|} |\{C' \in \mathcal{F} \mid C' \sim D \text{ and } C' \equiv C\}| \\ &= \textstyle\sum_{\tilde{D} \equiv D} |\{C' \in \mathcal{F} \mid C' \sim \tilde{D} \text{ and } C' \equiv C\}| \\ &= \textstyle\sum_{\tilde{C} \equiv C} |\{D' \in \mathcal{F} \mid D' \sim \tilde{C} \text{ and } D' \equiv D\}| \\ &= \tfrac{N!}{|\operatorname{Aut}(C)|} |\{D' \in \mathcal{F} \mid D' \sim C \text{ and } D' \equiv D\}|. \end{aligned}$$

The middle equality follows since the neighboring relation is symmetric and invariant under equivalences. Therefore

$$\begin{aligned} &(T([C]), [D]) = |\operatorname{Aut}(D)| \, |\{D' \in \mathcal{F} \mid D' \sim C \text{ and } D' \equiv D\}| \\ &= |\operatorname{Aut}(C)| \, |\{C' \in \mathcal{F} \mid C' \sim D \text{ and } C' \equiv C\}| = ([C], T([D])). \end{aligned}$$

Hence T is self-adjoint. The self-adjointness of T_R follows similarly. □

4.3. **Connected components of Γ_a.** Although it is known from [8] that Γ is a connected graph, it does not follow that the Γ_a are connected. In fact, it is not difficult to compute explicit examples in which the Γ_a have multiple connected components; one such example will appear in Section 5. Therefore, it is of interest to understand the size and composition of the connected components of the Γ_a. To do this, we will begin by studying some of the natural lifts of neighboring codes over R to codes over $\mathbb{F}_p$, as described in Definition 2.

Lemma 30. *Let $C, D \in \mathcal{F}_{a,b}$ be neighbors, $C \sim D$. Then Tor$(C) =$ Tor(D) and Res$(C) =$ Res(D).*

Proof. Let $C \sim D$ and put $E := C \cap D$. Then C/E and D/E are two distinct minimal submodules of $E^\perp/E$, and hence $E^\perp/E \cong S \oplus S$ is not cyclic.

It suffices to show that $C \cap pR^N = D \cap pR^N$ as this implies $\operatorname{Tor}(C) = \operatorname{Tor}(D)$. The equality of the residue codes then follow from Lemma 30.

Seeking for a contradiction we suppose that $C \cap pR^N \neq D \cap pR^N$, we get

$$C = C \cap pR^N + E,$$

so we may choose $x = pv \in C \cap pR^N$ such that $C = E \oplus \langle x \rangle$.

Next, we will show that for any $w \in E^\perp \setminus C$, it follows that $pw \notin pE$. To show this, suppose that $w \in E^\perp \setminus C$. Then $\langle w, x \rangle \neq 0$, or else it would follow that $\langle w, e + x \rangle = 0$ for every $e \in E$, and hence $w \in C = C^\perp$. Now suppose there is some $y \in E$ so that $pw = py$, then $\langle y, x \rangle = 0$, since $y \in E \subseteq C = C^\perp$. But then,

$$0 = \langle y, x \rangle = \langle y, pv \rangle = \langle py, v \rangle = \langle pw, v \rangle = \langle w, pv \rangle = \langle w, x \rangle \neq 0,$$

a contradiction.

Since $C \cap pR^N \neq D \cap pR^N$, we may similarly say that $D = E \oplus \langle pw \rangle$ for some $pw \in D \cap pR^N$. But then clearly $pw \in E^\perp \setminus C$. However,

$$p \cdot pw = p^2 w = 0 \in pE$$

contradicting what was established in the preceding paragraph. Therefore, we may conclude that $C \cap pR^N = D \cap pR^N$. □

Now we define the following set,

$$N(C) := \{D \in \mathcal{F}_{a,b} \mid \mathrm{Tor}(D) = \mathrm{Tor}(C)\},$$

noting that in view of Lemma 30, $N(C)$ contains all neighbors of C which are of the same module isomorphism type. Recalling Definition 2, we have

$$\mathrm{Res}(C) := (C + pR^N)/pR^N \leq (R/pR)^N = \mathbb{F}_p^N,$$

and so from Lemma 30, we also have

$$N(C) = \{D \in \mathcal{F}_{a,b} \mid \mathrm{Res}(D) = \mathrm{Res}(C)\}.$$

For any $D \in N(C)$ it is clear that $N(C) = N(D)$. Furthermore, for $D \in N(C)$ we have $D + pR^N = C + pR^N$ from Lemma 30. Hence, any such a family $N(C)$ defines a unique non-degenerate bilinear $\mathbb{F}_p$-vector space

$$W := C + pR^N / C \cap pR^N \cong \mathbb{F}_p^{2a},$$

with the bilinear form $\langle .,. \rangle : W \times W \to \mathbb{F}_p$ given by

$$\left\langle c + px + (C \cap pR^N), d + py + (C \cap pR^N) \right\rangle = \frac{1}{p} b(c + px, d + py).$$

The $\mathbb{F}_p$-bilinearity is clear as b is bilinear over R, and note that this product is well-defined because for all $c, d \in C$ and $x, y \in R^N$ we have

$$b(c + px, d + py) = b(c, d) + p(b(x, d) + b(c, y)) = p(b(x, d) + b(c, y)),$$

hence

$$\langle c + px + (C \cap pR^N), d + py + (C \cap pR^N) \rangle = b(x, d) + b(c, y) \pmod{p} \in \mathbb{F}_p,$$

and since $(C \cap pR^N) = (C + pR^N)^\perp$, this value is independent of choice of representative. Finally, the non-degeneracy follows from the fact that

$$\langle c + px + (C \cap pR^N), d + py + (C \cap pR^N) \rangle = 0$$

for all $d + py \in C + pR^N$, if and only if $c + px \in (C + pR^N)^\perp = C \cap pR^N$, and thus if and only if $c + px + (C \cap pR^N) = 0 \in W$.

Lemma 31. *$C/(C \cap pR^N)$ and $X := pR^N/(C \cap pR^N)$ are maximal isotropic subspaces of W with*

$$W = C/(C \cap pR^N) \oplus pR^N/(C \cap pR^N).$$

Proof. As $C = C^\perp$ and $pR^N = (pR^N)^\perp$ are maximal self-dual submodules of (R^N, b), their images are maximal self-dual subspaces of W. Note that both $\mathbb{F}_p$-vector spaces have dimension a and $2a = \dim(W)$. To see that the sum is direct, it is enough to show that their intersection is 0, but this is clear, as

$$C/(C \cap pR^N) \cap pR^N/(C \cap pR^N) = (C \cap pR^N)/(C \cap pR^N) = \{0\}.$$

□

Let $(e_1,\dots,e_a)$ be any $\mathbb{F}_p$-basis of $C/(C\cap pR^N)$. By the non-degeneracy of $\langle .,. \rangle$ there are elements $(f_1,\dots,f_a)\in X := pR^N/(C\cap pR^N)$ such that $\langle e_i,f_j\rangle=\delta_{ij}$. Then $(e_1,\dots,e_a,f_1,\dots,f_a)$ is a basis of W.

Let

$$M(C) := \{Y\le W \mid \langle Y,Y\rangle=\{0\}, W=Y\oplus X\}$$

denote the set of all totally isotropic complements of X in W.

Lemma 32. *The mapping $\varphi : N(C)\to M(C)$, $D\mapsto D/(C\cap pR^N)$ is a bijection.*

Proof. For any code $D\in N(C)$, we have that $C\cap pR^N = D\cap pR^N$ and $N(D)=N(C)$. As we have already seen in the previous lemma that $C/(C\cap pR^N)$ is a totally isotropic complement of X in W, the same is true for $D/(C\cap pR^N)$. So φ is well-defined.

That the map is a bijection follows from the homomorphism theorem: The map $R^N\to R^N/(C\cap pR^N)$, $x\mapsto x+(C\cap pR^N)$ is an R-module epimorphism with kernel $C\cap pR^N$, so it defines a bijection between the set of all submodules D of R^N that contain $C\cap pR^N$ and the submodules of $R^N/(C\cap pR^N)$. Such a submodule D lies in $N(C)$, if and only if $\dim(D/(C\cap pR^N))=a$, $D/(C\cap pR^N)$ is isotropic and $D\cap pR^N=C\cap pR^N$, and thus if and only if $D/(C\cap pR^N)$ lies in $M(C)$. □

Lemma 33. *Any $Y\in M(C)$ has a unique basis*

$$\left(e_1+\sum_{j=1}^{a} S_{1j}f_j,\dots,e_a+\sum_{j=1}^{a} S_{aj}f_j\right)$$

for some matrix $S\in\mathbb{F}_p^{a\times a}$ such that $S+S^{tr}=0$. Call this space $Y(S)$.

Proof. Let $Y\in M(C)$. Then Y is a complement of $X=\langle f_1,\dots,f_a\rangle$, and in particular, there are $b_1,\dots,b_a\in Y$, $z_1,\dots,z_a\in X$, such that $e_i=b_i-z_i$ for $i=1,\dots,a$. As $W=Y\oplus X$, these b_i and z_i are uniquely determined and $(b_1,\dots,b_a)$ is a basis of Y. Moreover there are unique $S_{ij}\in\mathbb{F}_p$ such that $z_i=\sum_{j=1}^{a} S_{ij}f_j$. That S is skew symmetric follows from the fact that Y is isotropic:

$$\langle b_i,b_k\rangle = \left\langle e_i+\sum_{j=1}^{a} S_{ij}f_j, e_k+\sum_{j=1}^{a} S_{kj}f_j\right\rangle = S_{ik}+S_{ki}=0.$$

□

Combining these two bijections we hence obtain a bijection

$$\mathrm{skew} : N(C)\to \left\{S\in\mathbb{F}_p^{a\times a} \mid S+S^{tr}=0\right\} = \mathrm{Skew}_a\,.$$

We note that then $\mathrm{skew}(C)=0$ since C maps to $C/(C\cap pR^N)$ which already has $(e_1,...,e_a)$ as a basis and consequently the S from Lemma 33 is the all zeros matrix.

Remark 34. *Everything is completely analogous if we work with quadratic forms for $p=2$, but then the image of* skew *lies in the space of alternating matrices, so that $S=S^{tr}\in\mathbb{F}_2^{a\times a}$, $S_{ii}=0$ for all i.*

Remark 35. *Let $D\in N(C)$. Then* $\dim(D/(D\cap C))=\dim(C/(D\cap C))=\dim(\varphi(D)/(\varphi(D)\cap\varphi(C)))=\dim(\varphi(C)/(\varphi(D)\cap\varphi(C)))=\mathrm{rank}(\mathrm{skew}(D))$.

Because the rank of an alternating matrix is always even, the code C has no neighbors in $N(C)$.

Corollary 36. *If p is odd or we deal with quadratic forms for $p = 2$ (i.e. doubly even quaternary codes), then $T_a = 0$ for all a.*

5. Some results for $\mathbb{Z}/4\mathbb{Z}$

In this section we turn our attention to the special case where $p = 2$, and $R = \mathbb{Z}/4\mathbb{Z}$. In this case we are able to compute the adjacency matrix, T, associated to the linear operator on $\mathcal{V}$. With these computations we make observations about the eigenvalues associated to each orthogonal component, T_a, and eventually describe the associated eigenspace. Before doing so, we establish the following results.

Lemma 37. *For any doubly-even binary code $H \leq \mathbb{F}_2^N$ of dimension a, there exists a code $C \in \mathcal{F}_{a,b}$ such that $Res(C) = H$. Hence, $N(C) = \{D \in \mathcal{F}_{a,b} \mid Res(D) = H\}$.*

Proof. Suppose that $H \leq \mathbb{F}_2^N$ is a doubly-even binary code of dimension a with generator matrix $G \in \mathbb{F}_2^{a\times N}$. Then it is possible to lift G to an $a \times N$ matrix A over R. It is clear that $A \cdot A^{\mathrm{tr}} = 2Z$ for some $Z \in \mathbb{F}_2^{a\times a}$. Moreover, this matrix is symmetric with zeroes along the diagonal, since H is doubly-even. Now we will show that for a suitable choice of A, we have $Z = 0$, and consequently we will have the generating matrix for a self-dual code in R^N. Replacing A with $A+2B$ for some $B \in \mathbb{F}_2^{a\times N}$, we obtain $(A+2B)(A+2B)^{\mathrm{tr}} = 2Z + 2(A\cdot B^{\mathrm{tr}} + A^{\mathrm{tr}} \cdot B)$. But since A has rank a, its columns contain a basis for $\mathbb{F}_2^a$ and it is therefore possible to choose B so that $A \cdot B^{\mathrm{tr}} = [z_{ij}]$ where $z_{ij} = 0$ for $i \leq j$, and for $i > j$, z_{ij} is the entry in the i^{th} row and j^{th} column of Z. From here it is clear that $(A+2B)(A+2B)^{\mathrm{tr}} = 0$, and therefore $A + 2B$ is the generating matrix for a self-orthogonal code, say C_1, which is a free R-module of rank a. By Remark 6, there is a unique self-dual code $C = C_1 + 2C_1^{\perp} \in \mathcal{F}_{a,b}$ that contains C_1 as a maximal free submodule. □

Combining this lemma with the general discussion in the previous section we arrive at the following main results.

Theorem 38. *For $p = 2$, the connected components of the graph Γ_a are in bijection with the binary doubly-even codes of length N and dimension a.*

Proof. To begin, suppose that $C, D \in \mathcal{F}_{a,b}$, with $C \sim D$, and let $H = \mathrm{Res}(C)$. From Lemma 30, it follows that $C + 2R^N = D + 2R^N$, and hence $\mathrm{Res}(D) = H$. Extending this argument, we can easily see that for any $C, D \in \mathcal{F}_{a,b}$ which are connected by a path of neighbors in $\mathcal{F}_{a,b}$, all codes in that path will lift to H. This proves one direction of the claim.

Now, suppose we have two arbitrary codes $C, D \in \mathcal{F}_{a,b}$ with $\mathrm{Res}(C) = \mathrm{Res}(D) = H$ where $H \leq \mathbb{F}_2^N$ is a doubly-even binary code. From here we know that C and D are in $N(C)$, and from the general results in the previous section, including the bijectivity of the skew map, we can conclude that C and D are connected by a chain of neighbors. □

Clearly if H and H' are equivalent doubly-even codes then the equivalence between H and H' (which is just a permutation in S_N) gives rise to a simultaneous equivalence between any codes C and C' for which $\mathrm{Res}(C) = H$ and $\mathrm{Res}(C') = H'$. Recalling that the nodes of Γ_a are defined as the permutation equivalence classes of codes in $\mathcal{F}_{a,b}$, the entire discussion above holds up to permutation equivalence; that is to say, the equivalence classes of binary doubly-even codes of length N and dimension a precisely described the connected components of Γ.

Let $H_1, \dots, H_t$ be a system of representatives of equivalence classes of binary doubly even codes of length N and dimension a. When $a = N/2$ and N is not congruent to $0 \mod 8$, then it is an immediate consequence of Corollary 8 that $t = 0$, and therefore the associated eigenspace is trivial.

Corollary 39. *The maximal eigenvalue of T_a is $2^a - 1$. This occurs with multiplicity t and the eigenspace of T_a to the eigenvalue $2^a - 1$ has a basis $(\sigma_1, \dots, \sigma_t)$ where*

$$\sigma_i = \sum_{C \in \pi^{-1}(H_i)} \frac{1}{|\operatorname{Aut}(C)|}[C].$$

Proof. In view of Theorem 38, we know that counting the neighbors of C in $\mathcal{F}_{a,b}$ is equivalent to counting the number of elements in $M(C)$, which will be equal to the number of $(a-1)$-dimensional subspaces of $\mathbb{F}_2^a$. Consequently, Γ_a is (2^a-1)-regular, and therefore has the all ones eigenvector and $2^a - 1$ is an eigenvalue. Moreover, from the Peron-Frobenius Theorem we can be guaranteed that this is indeed the maximal eigenvalue.

Since the neighboring relation is symmetric, the connected components of Γ_a are strongly connected, therefore the multiplicity of the eigenvalue $2^a - 1$ is the same as the number of connected components, namely, t. □

Now we will compute an explicit example when $N = 8$. Using Magma, we compute the permutation equivalence classes of the codes. There are 29 distinct permutation equivalence classes when $N = 8$, which we will enumerate by module isomorphism type, where $[4^a 2^b]_n$ will denote the n^{th} permutation equivalence class of codes isomorphic to $R^a \oplus S^b$ as R-submodules. Then we have

$$[4^0 2^8]_1$$

$$[4^1 2^6]_n \text{ where } 1 \le n \le 4$$

$$[4^2 2^4]_n \text{ where } 1 \le n \le 8$$

$$[4^3 2^2]_n \text{ where } 1 \le n \le 9$$

$$[4^4 2^0]_n \text{ where } 1 \le n \le 7$$

Using Magma we compute the adjacency matrix associated to T and its component block matrices, the T_a, which we give below.

$$T_0 = \begin{bmatrix} 0 \end{bmatrix}, T_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, T_2 = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \end{bmatrix},$$

$$T_3 = \begin{bmatrix} 6 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 7 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 3 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 4 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 4 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 4 & 0 & 2 & 1 & 0 \end{bmatrix}, T_4 = \begin{bmatrix} 6 & 0 & 6 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 8 & 0 & 7 \\ 8 & 0 & 5 & 1 & 0 & 1 & 0 \\ 0 & 0 & 6 & 0 & 8 & 1 & 0 \\ 7 & 1 & 0 & 7 & 0 & 0 & 0 \\ 8 & 0 & 6 & 1 & 0 & 0 & 0 \\ 8 & 1 & 0 & 0 & 0 & 0 & 6 \end{bmatrix}.$$

Now we can view the graphs Γ_a associated to each T_a, in particular we take a closer look at T_2. Figure 1 is the graph associated to Γ_2, whose nodes are precisely the permutation equivalence classes of codes isomorphic to $R^2 \oplus S^4$.

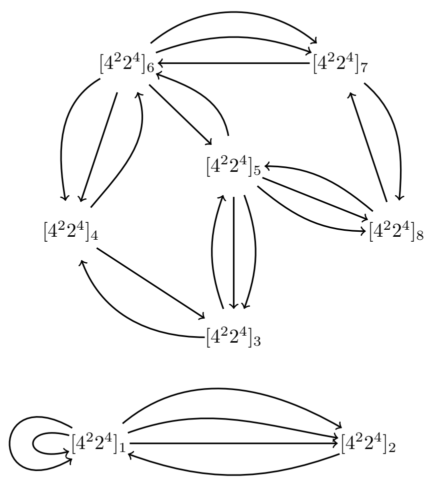

FIGURE 1. Graph of Γ_2

The two distinct connected components of Γ_2 are determined by the two distinct permutation equivalence classes of binary doubly-even codes of length 8 and dimension 2, namely those with generator matrices

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \text{ and } H' = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

The equivalence classes $[4^22^4]_1$ and $[4^22^4]_2$ contain codes with the following generator matrices,

$$G_1 = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \end{bmatrix} \text{ and } G_2 = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 3 \\ 0 & 0 & 1 & 1 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \end{bmatrix},$$

respectively. Let C_1 be the code with generator matrix G_1, and C_2 the code with generator matrix G_2. Then it's clear that both C_1 and C_2 lift to H'. Similarly, it can be shown each of the codes in the remaining permutation equivalence classes lift to H.

Furthermore, for each a we compute the eigenvalues, λ, associated to each T_a, and their multiplicities t, which we give in the table below, noting that in any case the largest eigenvalue corresponds to $2^a - 1$.

a	$\langle \lambda, t \rangle$
0	$\langle 0, 1 \rangle$
1	$\langle 1, 2 \rangle$, $\langle -1, 2 \rangle$
2	$\langle 3, 2 \rangle$, $\langle 1, 2 \rangle$, $\langle -1, 3 \rangle$, $\langle -3, 1 \rangle$
3	$\langle 7, 2 \rangle$, $\langle 3, 2 \rangle$, $\langle -1, 4 \rangle$, $\langle -5, 1 \rangle$
4	$\langle 15, 1 \rangle$, $\langle 7, 2 \rangle$, $\langle -1, 3 \rangle$, $\langle -9, 1 \rangle$

References

[1] C. Bachoc, On harmonic weight enumerators of binary codes, *Designs, Codes, and Cryptography* **18** (1999), 11–28

[2] C. Bachoc, Harmonic weight enumerators of non-binary codes and MacWilliams identities, in *Codes and association schemes (Piscataway, NJ, 1999)*, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., **56**, Amer. Math. Soc., Providence, RI, 2001; pp. 1–23

[3] M. Broué, Codes correcteurs d'erreurs auto-orthogonaux sur le corps à deux éléments et formes quadratiques entières définies positives à discriminant +1. *Discrete Math.* **17** (1977), no. 3, 247–269.

[4] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, Springer Grundlehren **290**, 1988, 1993, 1999.

[5] S. T. Dougherty, J.-L. Kim and H. Liu, *Constructions of self-dual codes over finite commutative chain rings*, Int. J. Inform. and Coding Theory, **1**, 2/2010, 170–190.

[6] W. Ebeling, *Lattices and Codes*, Springer, 2013.

[7] M. Kneser, *Quadratische Formen*, Springer, 2002.

[8] A. Meyer, *Automorphism groups of self-dual codes,* PhD thesis, RWTH Aachen University, (2009).

[9] G. Nebe and B. B. Venkov, On Siegel modular forms of weight 12, *J. Reine Angew. Math.* **531** (2001), 49–60.

[10] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-dual codes and invariant theory*, Springer (2006).

[11] G. Nebe, *Kneser-Hecke-operators in coding theory,* Abh. Math. Sem. Univ. Hamburg 76 (2006) 79–90

[12] G. Nebe, *Finite Weil-representations and associated Hecke-algebras*, J. Number Theory **129** (2009) 588–603.

[13] G. H. Norton and A. Salagean, *On the structure of linear and cyclic codes over finite chain rings,* Applicable Algebra in engineering, communication and computing, **10**, 2000, 489–506.

[14] E. Nossek, *Kneser-Hecke-Operatoren in der Codierungstheorie*, Diplomathesis, RWTH Aachen, (2009). `http://www.math.rwth-aachen.de/~Gabriele.Nebe/dipl.html`

[15] V. Pless, *On Witt's theorem for nonalternating symmetric bilinear forms over a field of characteristic 2*, Proc. AMS **15** (1964) 979–983.

[16] B. Runge, Codes and Siegel modular forms, *Discrete Math.* **148** (1996), 175–204.

[17] J. A. Wood, *Extension theorems for linear codes over finite rings,* Apploed algebra, algebraic algorithms and error-correcting codes, (Toulouse,1997), 329-340, Lecture Notes in Comput. Sci., 1255, Springer, Berlin (1997).

[18] J. A. Wood, *Witt's extension theorem for mod four valued quadratic forms*, Transactions AMS **336** (1993) 445–461.

Amy Feaver, Department of Mathematics and Computing Science, The King's University, 9125 50 St NW, Edmonton, AB T6B 2H3
E-mail address: amy.feaver@kingsu.ca

Anna Haensch, Department of Mathematics and Computer Science, Duquesne University, Pittsburgh, PA 15282, USA.
E-mail address: haenscha@duq.edu

Jingbo Liu, Department of Mathematics and Computer Science, Wesleyan University, Middletown, CT 06459, USA
E-mail address: jliu02@wesleyan.edu

Gabi Nebe, Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany
E-mail address: nebe@math.rwth-aachen.de