Kneser-Hecke-operators in coding theory.

Gabriele Nebe

Lehrstuhl D für Mathematik, RWTH Aachen, 52056 Aachen, Germany,
nebe@math.rwth-aachen.de

Abstract

The Kneser-Hecke-operator is a linear operator defined on the complex vector space spanned by the equivalence classes of a family of self-dual codes of fixed length. It maps a linear self-dual code C over a finite field to the formal sum of the equivalence classes of those self-dual codes that intersect C in a codimension 1 subspace. The eigenspaces of this self-adjoint linear operator may be described in terms of a coding-theory analogue of the Siegel Φ-operator.
MSC: 94B05, 11F60

1   Introduction

The paper translates the lattice theoretic construction of certain Hecke-operators from [15] to coding theory. It only deals with linear self-dual codes over finite fields.

There is a beautiful analogy between most of the notions for lattices and codes provided by construction A (see for instance [5], [13], [19]). Theta-series of lattices correspond to weight-enumerators of codes. Whereas theta-series of unimodular lattices are modular forms for certain Siegel modular groups, weight-enumerators of self-dual codes are polynomials invariant under a certain finite group, called the associated Clifford-Weil group, and in fact the main result of [13] shows that these weight-enumerators generate the invariant ring. However, this generalized Gleason theorem is not true in such generality for lattices (see for instance [8]). One important tool in the theory of modular forms is Siegel's Φ-operator that maps the genus-m Siegel theta-series of a lattice to its Siegel theta-series of genus $m - 1$. An analogue of this Φ-operator was introduced in coding theory by Runge [19] to generalize Gleason's theorem to higher genus weight-enumerators of binary self-dual codes. Also theta-series with harmonic coefficients have a counterpart in coding theory (see [1], [2]). One missing concept in coding theory is that of Hecke-operators, which are an important tool in the theory of modular forms. Certain of these Hecke-operators may be expressed in terms of lattices (see [15], [14], [6]). The present paper translates this concept to coding theory. This also answers a question raised in 1977 in [3].

There are slight differences from the lattice case.
(1) For codes this method only yields p-local Hecke-operators, where p is the characteristic of the field, whereas for lattices Hecke-operators are defined for all primes.
(2) In the theory of modular forms, the Hecke-algebra is generated by certain double cosets of the Siegel modular group. For codes such a commutative algebra generated

1

by double cosets of the Clifford-Weil groups is examined in [9]. This maps onto the algebra generated by the Kneser-Hecke operator.

(3) The main result of the paper is that in the coding theory case, one can say much more about the resulting Kneser-Hecke-operator: The possible eigenvalues are known a priori and the corresponding eigenspaces are exactly the analogues of the spaces of Siegel cusp-forms.

2 The general setup.

Let $\mathcal{F}$ denote the family of self-dual codes of length N of a given Type. For a precise definition of Type the reader is referred to [13] or [12]. The present paper only deals with codes over finite fields $\mathbb{F}$ that are subspaces of $\mathbb{F}^N$, self-dual with respect to some non-degenerate bilinear or Hermitian form

$$b : \mathbb{F}^N \times \mathbb{F}^N \to \mathbb{F}, b(x,y) := \sum_{i=1}^{N} x_i \overline{y_i}$$

where $^{-} : \mathbb{F} \to \mathbb{F}$ is either the identity (in the bilinear case) or a non-trivial automorphism of order 2 (in the Hermitian case). The dimension of these codes is then $n := \frac{N}{2}$. The integers n and N will be fixed throughout the paper.

There are several possible notions of equivalence for these codes. This paper always uses permutation equivalence, which means that two codes are equivalent if and only if there is a permutation $\pi \in S_N$ of the coordinates mapping one code onto the other. Also the automorphism group

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

of a code is just the subgroup of the symmetric group S_N that preserves the code. The results may be easily generalized to coarser notions of equivalence (for instance allowing the Galois group to act) provided that one uses the same notion for automorphisms of codes and that one deals with the appropriate symmetrized weight-enumerators such that equivalent codes have the same genus-m weight-enumerator for all m.

Let $\mathcal{V}$ be the $\mathbb{C}$-vector space on the set of all equivalence classes $[C]$ with $C \in \mathcal{F}$. So the set

$$\mathcal{B} := \{[C] : C \in \mathcal{F}\}$$

is a $\mathbb{C}$-basis for $\mathcal{V}$.

Remark 1. *$\mathcal{V}$ has a Hermitian positive definite scalar product defined by*

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

.

2

2.1 The filtration of $\mathcal{V}$.

The *genus-m complete weight-enumerator* of a code C is a homogeneous polynomial in $\mathcal{P}_m := \mathbb{C}[x_a : a \in \mathbb{F}^m]$ of degree N. For an m-tuple $\underline{c} := (c^{(1)}, \ldots, c^{(m)}) \in (\mathbb{F}^N)^m$ let

$$\mathrm{mon}(\underline{c}) = \prod_{v \in \mathbb{F}^m} x_v^{a_v(\underline{c})} \in \mathcal{P}_m$$

where for $v = (v_1, \ldots, v_m) \in \mathbb{F}^m$

$$a_v(\underline{c}) = |\{i \in \{1, \ldots, N\} : c_i^{(j)} = v_j \text{ for all } 1 \leq j \leq m\}|$$

is the number of columns of the $m \times N$-matrix defined by $\underline{c}$ that are equal to v. Then

$$\mathrm{cwe}_m(C) := \sum_{\underline{c} \in C^m} \mathrm{mon}(\underline{c}) \in \mathcal{P}_m$$

and $\mathrm{cwe}_0(C) := 1$. Note that $\mathrm{cwe}_m(C)$ only depends on the equivalence class of C and hence cwe_m may be extended to a linear map

$$\mathrm{cwe}_m : \mathcal{V} \to \mathcal{P}_m, \ \ \mathrm{cwe}_m(\sum v_C[C]) := \sum v_C \, \mathrm{cwe}_m(C).$$

For $m \in \mathbb{N}_0$ let

$$\mathcal{V}_m := \ker(\mathrm{cwe}_m) \leq \mathcal{V}.$$

To define an analogue of the Siegel Φ-operator one has to choose an embedding $\epsilon : \mathbb{F}^{m-1} \to \mathbb{F}^m, (a_1, \ldots, a_{m-1}) \mapsto (a_1, \ldots, a_{m-1}, 0)$. Then there are for all $m \in \mathbb{N}$ ring homomorphisms

$$\Phi : \mathcal{P}_m \to \mathcal{P}_{m-1}, \ \ x_a \mapsto \begin{cases} x_{\epsilon^{-1}(a)} & \text{if } a \in \epsilon(\mathbb{F}^{m-1}) \\ 0 & \text{else.} \end{cases}$$

Note that Φ respects the homogeneous components of the polynomial rings, i.e. if p is a homogeneous polynomial of degree N in $\mathcal{P}_m$, then $\Phi(p) \in \mathcal{P}_{m-1}$ is either 0 or homogeneous of the same degree N. Also $\Phi(\mathrm{cwe}_m(v)) = \mathrm{cwe}_{m-1}(v)$ for all $v \in \mathcal{V}$. Since the complete weight-enumerators of genus n of the basis $\mathcal{B}$ are linearly independent one gets a filtration

$$\mathcal{V} := \mathcal{V}_{-1} \geq \mathcal{V}_0 \geq \ldots \geq \mathcal{V}_n = \{0\}$$

with

$$\mathcal{V}_0 := \{ \sum_{[C] \in \mathcal{B}} v_C[C] : \sum_{[C] \in \mathcal{B}} v_C = 0 \}$$

of codimension 1 in $\mathcal{V}$. The dual filtration is obtained by letting $\mathcal{W}_i := \mathcal{V}_i^\perp$. Then

$$\mathcal{V} = \mathcal{W}_n \geq \mathcal{W}_{n-1} \geq \ldots \geq \mathcal{W}_0 \geq \mathcal{W}_{-1} = \{0\}.$$

The space W_0 is one-dimensional generated by

$$\sigma_N := \sum_{[C] \in \mathcal{B}} |\operatorname{Aut}(C)|^{-1}[C].$$

Using the Hermitian scalar product one obtains the orthogonal decomposition of $\mathcal{V}$ associated to this filtration by putting

$$\mathcal{Y}_m := \mathcal{W}_m \cap \mathcal{V}_{m-1} = \{w \in \mathcal{W}_m : (w, x) = 0 \text{ for all } x \in \mathcal{W}_{m-1}\}.$$

Then

$$\mathcal{V} = \perp_{m=0}^{n} \mathcal{Y}_m \tag{1}$$

with $\mathcal{Y}_0 = \mathcal{W}_0 = \langle \sigma_N \rangle$. Moreover the mapping cwe_m yields an isomorphism between $\mathcal{Y}_m$ and the kernel of the Φ-operator on $\operatorname{cwe}_m(\mathcal{V})$. One may think of the space $\mathcal{Y}_m$ (or the isomorphic space $\operatorname{cwe}_m(\mathcal{Y}_m)$) as the analogue of the space of Siegel cusp-forms of genus m. In Section 2.3 it is shown that the decomposition (1) is in fact the eigenspace decomposition of $\mathcal{V}$ under the Kneser-Hecke-operator T defined below.

2.2 Kneser-Hecke-operators.

Definition 2. For $0 \le k \le n$ two codes $C, D \in \mathcal{F}$ are called *k-neighbors*, written $C \sim_k D$, if $\dim(C \cap D) = \dim(C) - k$.
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 $\mathcal{F}$.
Let $T := T_1$ be the *Kneser-Hecke-operator* and call 1-neighbors simply *neighbors*.

Theorem 3. *For $0 \le k \le n$ the operator T_k is a self-adjoint linear operator on the vector space $\mathcal{V}$.*

<u>Proof.</u> By definition T_k is linear. For basis vectors $[C], [D] \in \mathcal{B}$ one has

$$\frac{N!}{|\operatorname{Aut}(D)|} |\{C' \in \mathcal{F} : C' \sim_k D \text{ and } C' \cong C\}|$$
$$= \sum_{\tilde{D} \cong D} |\{C' \in \mathcal{F} : C' \sim_k \tilde{D} \text{ and } C' \cong C\}|$$
$$= \sum_{\tilde{C} \cong C} |\{D' \in \mathcal{F} : D' \sim_k \tilde{C} \text{ and } D' \cong D\}|$$
$$= \frac{N!}{|\operatorname{Aut}(C)|} |\{D' \in \mathcal{F} : D' \sim_k C \text{ and } D' \cong D\}|.$$

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

$$(T_k([C]), [D]) = |\operatorname{Aut}(D)| |\{D' \in \mathcal{F} : D' \sim_k C \text{ and } D' \cong D\}|$$
$$= |\operatorname{Aut}(C)| |\{C' \in \mathcal{F} : C' \sim_k D \text{ and } C' \cong C\}| = ([C], T_k([D])).$$

Hence T_k is self-adjoint. $\qquad \square$

Experiments suggest that the operators T_k are polynomials in $T = T_1$.

4

2.3 The main theorem.

The eigenvalue of T on the space $\mathcal{Y}_m$ depends on the geometry of the underlying space $(\mathbb{F}^N, b)$. To prove the main theorem some more notation is needed: Denote by

$$\mathcal{M}_m := \{ \prod_{a \in \mathbb{F}^m} x_a^{e_a} \: : \: \sum_{a \in \mathbb{F}^m} e_a = N \} \subseteq \mathcal{P}_m$$

the monomials in $\mathcal{P}_m$ of degree N.
For a monomial $X = \prod_{a \in \mathbb{F}^m} x_a^{e_a} \in \mathcal{M}_m$ define the *rank*

$$\mathrm{rk}(X) := \dim \langle a \: : \: e_a > 0 \rangle$$

and let

$$\mathcal{M}_m^* := \{ X \in \mathcal{M}_m \: : \: \mathrm{rk}(X) = m \}.$$

For $X \in \mathcal{M}_m$ and subset $C \subset \mathbb{F}^N$ define

$$a_X(C) := |\{ \underline{c} := (c^{(1)}, \ldots, c^{(m)}) \in C^m \: : \: \mathrm{mon}(\underline{c}) = X \}|.$$

Remark 4. *(i) $a_X(C)$ only depends on the equivalence class of the code $C \leq \mathbb{F}^N$.*
(ii) $\mathrm{cwe}_m(C) := \sum_{X \in \mathcal{M}_m} a_X(C) X$.
(iii) For $X \in \mathcal{M}_m$ extend a_X to a linear mapping

$$a_X : \mathcal{V} \to \mathbb{C}, \quad \sum_{[C] \in \mathcal{B}} v_C [C] \mapsto \sum_{[C] \in \mathcal{B}} v_C a_X(C).$$

Then $\mathcal{V}_m = \{ v \in \mathcal{V} \: : \: a_X(v) = 0 \text{ for all } X \in \mathcal{M}_m \}$.
(iv) $\mathcal{V}_m = \{ v \in \mathcal{V}_{m-1} \: : \: a_X(v) = 0 \text{ for all } X \in \mathcal{M}_m^* \}$.

In this language explicit generators for the spaces $\mathcal{W}_m$ are obtained by generalizing the construction of $\sigma_N = b_1$.

Remark 5. *For $X \in \mathcal{M}_m$ let*

$$b_X := \sum_{[C] \in \mathcal{B}} \frac{a_X(C)}{|\mathrm{Aut}(C)|} [C] \in \mathcal{V}.$$

Then for any $v \in \mathcal{V}$ the scalar product

$$(b_X, v) = a_X(v).$$

The vectors b_X, $X \in \mathcal{M}_m$ span the space $\mathcal{W}_m$.

<u>Proof.</u> Let $\mathcal{U}_m := \langle b_X \: : \: X \in \mathcal{M}_m \rangle$. Then

$$\mathcal{U}_m^\perp = \{ v \in \mathcal{V} \: : \: (b_X, v) = a_X(v) = 0 \text{ for all } X \in \mathcal{M}_m \} = \mathcal{V}_m = \mathcal{W}_m^\perp$$

and therefore $\mathcal{U}_m = \mathcal{W}_m$. $\qquad\qquad\square$

Remark 6. *Let* $\underline{c} := (c^{(1)}, \ldots, c^{(m)}) \in C^m$, $X := \mathrm{mon}(\underline{c})$, *and* $U := \langle c^{(1)}, \ldots, c^{(m)} \rangle \leq C$. *Then* $\dim(U) = \mathrm{rk}(X)$. *If* $\mathrm{rk}(X) = m$ *and* $\underline{b} := (b^{(1)}, \ldots, b^{(m)})$ *is another basis of* U, *then for all* $v \in \mathcal{V}$

$$a_X(v) = a_{\mathrm{mon}(\underline{b})}(v).$$

For the proof of the main theorem choose a suitable subset $\mathcal{M}_m^0 \subset \mathcal{M}_m^*$ such that

$$\mathcal{V}_m = \{v \in \mathcal{V}_{m-1} : a_X(v) = 0 \text{ for all } X \in \mathcal{M}_m^0\}. \tag{2}$$

Clearly the full set $\mathcal{M}_m^0 = \mathcal{M}_m^*$ satisfies condition (2), but there may be smaller sets.

Lemma 7. *Assume that all codes in* $\mathcal{F}$ *contain the all-ones vector* $\mathbf{1} := (1, \ldots, 1)$. *Then*

$$\mathcal{M}_m^0 = \mathcal{M}_m^1 := \{\mathrm{mon}(\underline{c}) : \dim\langle \mathbf{1}, c^{(1)}, \ldots, c^{(m)} \rangle = m + 1\}$$

satisfies condition (2).

<u>Proof.</u> For $C \in \mathcal{F}$ let $\underline{c} = (c^{(1)}, \ldots, c^{(m)}) \in C^m$ be such that $X := \mathrm{mon}(\underline{c}) \in \mathcal{M}_m^* \setminus \mathcal{M}_m^1$. Then $\mathbf{1} \in U := \langle c^{(1)}, \ldots, c^{(m)} \rangle$ and $\dim(U) = m$. By Remark 6 $a_X([C])$ is independent of the choice of the basis $\underline{c}$ of U one may assume w.l.o.g. that $c^{(m)} = \mathbf{1}$. Let $\underline{c}' := (c^{(1)}, \ldots, c^{(m-1)})$ and $Y := \mathrm{mon}(\underline{c}') \in \mathcal{M}_{m-1}^*$. Then

$$\underline{b}' := (b^{(1)}, \ldots, b^{(m-1)}) \mapsto \underline{b} := (b^{(1)}, \ldots, b^{(m-1)}, \mathbf{1})$$

establishes a bijection between

$$\{\underline{b}' \in C^{m-1} : \mathrm{mon}(\underline{b}') = Y\} \text{ and } \{\underline{b} \in C^m : \mathrm{mon}(\underline{b}) = X\}$$

showing that $a_X([C]) = a_Y([C])$ for all $[C] \in \mathcal{B}$. Therefore $a_X(v) = 0$ for all $v \in \mathcal{V}_{m-1} \subseteq \ker(a_Y)$. Hence

$$\begin{aligned}
\mathcal{V}_m &= \{v \in \mathcal{V}_{m-1} : a_X(v) = 0 \text{ for all } X \in \mathcal{M}_m^*\} \\
&= \{v \in \mathcal{V}_{m-1} : a_X(v) = 0 \text{ for all } X \in \mathcal{M}_m^1\}
\end{aligned}$$

which shows condition (2). □

Condition $\star$. In addition to condition (2), assume that for all codes $C \in \mathcal{F}$ and all $\underline{c} := (c^{(1)}, \ldots, c^{(m)}) \in C^m$ such that $\mathrm{mon}(\underline{c}) \in \mathcal{M}_m^0$ the sum

$$\alpha_m := \sum_{E \in \mathcal{E}_C(\underline{c})} \alpha_E$$

does not depend on $\underline{c}$ and C. Here

$$\mathcal{E}_C(\underline{c}) := \{E \leq C : \dim(E) = n - 1, \underline{c} \in E^m\}$$

and $\alpha_E = \alpha_E(C)$ is the number of codes $D \in \mathcal{F}$ with $D \cap C = E$.

Furthermore let
$$\beta_m := \frac{|\mathbb{F}|^m - 1}{|\mathbb{F}| - 1}$$

the number of $(m-1)$-dimensional subspaces of $\mathbb{F}^m$ and, if Condition $\star$ is satisfied,

$$\nu_m := \alpha_m - \beta_m.$$

Theorem 8. *Assume that Condition $\star$ is satisfied. Then the space $\mathcal{Y}_m$ is exactly the ν_m-eigenspace of T in $\mathcal{V}$.*

<u>Proof.</u> It is enough to show that T acts as ν_m id on $\mathcal{V}_{m-1}/\mathcal{V}_m$ which just means that for

$$v := \sum_{[C] \in \mathcal{B}} v_C[C] \in \mathcal{V}_{m-1} = \ker(\text{cwe}_{m-1})$$

the difference
$$T(v) - \nu_m v \in \mathcal{V}_m = \ker(\text{cwe}_m).$$

For this it is enough to show that

$$a_X(T(v)) = \nu_m a_X(v) \text{ for all } X \in \mathcal{M}_m^0.$$

Now
$$T(v) = \sum_{[C] \in \mathcal{B}} v_C T([C]) = \sum_{[C] \in \mathcal{B}} v_C \sum_{\substack{E \leq C \\ \dim(E) = n-1}} \sum_{\substack{D \in \mathcal{F} \\ E = D \cap C}} [D]$$

therefore we have to calculate for $X \in \mathcal{M}_m^0$ and a fixed $C \in \mathcal{F}$

$$\sum_{\substack{E \leq C \\ \dim(E) = n-1}} \sum_{\substack{D \in \mathcal{F} \\ E = D \cap C}} a_X([D]). \tag{3}$$

Let $\underline{c} := (c^{(1)}, \ldots, c^{(m)}) \in D^m$ for some neighbor D of C such that $\text{mon}(\underline{c}) = X \in \mathcal{M}_m^0$. Put $W := \langle c^{(1)}, \ldots, c^{(m)} \rangle$ and distinguish two cases:
(a) $W \leq C$: Then $\underline{c} \in D^m$, if and only if $\underline{c} \in (D \cap C)^m$ and by Condition $\star$ this yields a contribution $\alpha_m a_X(C)$ to the sum (3).
(b) $W \not\leq C$: Then $U := W \cap C$ has dimension $m-1$, and $E = W^\perp \cap C$ and $D = \langle E, W \rangle$ are uniquely determined by $\underline{c}$. Let $\underline{b} := (b^{(1)}, \ldots, b^{(m-1)})$ be a basis of U and let $Y := \text{mon}(\underline{b})$. Then by Remark 6 the value $a_Y(C)$ is independent of the choice of this basis. Note that W has exactly β_m such submodules U. Here the contribution to the sum (3) is

$$\sum_{Y \leq X} (f(X,Y)a_Y(C) - a_X(C)) = (\sum_{Y \leq X} f(X,Y)a_Y(C)) - \beta_m a_X(C) ,$$

7

where $f(X, Y)$ is the number of overcodes of U that are equivalent to W. By induction on m this argument shows that the subspaces $\mathcal{V}_m$ are T-invariant. Furthermore for $v \in \ker(\text{cwe}_{m-1})$ the sum

$$a_Y(v) = \sum_{[C] \in \mathcal{B}} v_C a_Y([C]) = 0 \text{ for all } Y \in \mathcal{M}_{m-1}.$$

Hence in total

$$a_X(T(v)) = \nu_m a_X(v)$$

for all $X \in \mathcal{M}_m^0$ and $v \in \mathcal{V}_{m-1}$. $\qquad\square$

Assume that Condition $\star$ is satisfied.

Corollary 9. σ_N *is an eigenvector of* T *with eigenvalue* ν_0.

For all k, the neighbor relation defines a graph Γ_k on the set $\mathcal{B}$ of equivalence classes of codes in $\mathcal{F}$. Two vertices $[C]$ and $[D]$ are joined by an edge in Γ_k, if there are codes $C' \in [C]$ and $D' \in [D]$ such that C' and D' are k-neighbors. The following general argument shows that this neighboring graph is connected.

Proposition 10. *If* ν_0 *is a simple eigenvalue of* T, *then the neighboring graph* Γ_1 *is connected.*

<u>Proof.</u> The eigenvalue ν_0 of the eigenvector σ_N is just the number of neighbors of any code $C \in \mathcal{F}$. By Condition $\star$ this number is independent of the choice of $C \in \mathcal{F}$. Assume that the neighboring graph is not connected. Then, reordering the elements in $\mathcal{B}$ if necessary, the matrix of T with respect to $\mathcal{B}$ is of the form $\begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix}$ for some non-trivial square matrices t_1 and t_2. The sum over the rows in t_1 and t_2 is the number of neighbors of the respective code $C \in [C] \in \mathcal{B}$ and hence equals ν_0. But then this eigenvalue has multiplicity at least 2, which is a contradiction. $\qquad\square$

3 Classical Types.

In this section it is shown that all classical Types of self-dual codes over finite fields $\mathbb{F} = \mathbb{F}_q$ satisfy Condition $\star$ of Section 2.3 and the eigenvalues of the operator T are determined. The Types are denoted by the names used in [18] and [13]:

q^E : Euclidean self-dual $\mathbb{F}_q$-linear codes in odd characteristic. So $\mathcal{F} = \{C = C^\perp \leq \mathbb{F}_q^N\}$ where the dual code $C^\perp = \{v \in \mathbb{F}_q^N : b(v, c) := \sum_{i=1}^N v_i c_i = 0 \text{ for all } (c_1, \dots, c_N) \in C\}$.

q_1^E : Same as q^E but we additionally impose the condition that the all-ones vector $\mathbf{1} = (1, \dots, 1)$ be in all codes in $\mathcal{F}$.

q_{I}^E : Same as q^E but now q is even.

q_{II}^E : Same as q_{I}^E but additionally assuming that the codes in $\mathcal{F}$ are generalized doubly even as defined in [17], [10].

q^H : Hermitian self-dual $\mathbb{F}_q$-linear codes. Here $q = r^2$ is a square and $^{-} : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^r$ denotes the non-trivial Galois automorphism of $\mathbb{F}_q/\mathbb{F}_r$. Then the dual code is $C^\perp := \{v \in \mathbb{F}_q^N : \sum_{i=1}^N c_i \overline{v_i} = 0 \text{ for all } c \in C\}\}$.

$q_{\mathbf{1}}^H$: Same as q^H, but additionally assuming that $\mathbf{1}$ be in the codes in $\mathcal{F}$.

To show that these Types satisfy condition $\star$ from Section 2.3 we need to precise the set $\mathcal{M}_m^0$ and calculate the number α_m as defined there. Then the eigenvalue of T on $\mathcal{Y}_m$ is $\nu_m = \alpha_m - (q^m - 1)/(q - 1)$ according to Theorem 8.

Theorem 11. *The codes of the six Types listed above satisfy condition $\star$. The following table lists the set $\mathcal{M}_m^0$, the corresponding value for α_m and the eigenvalue ν_m (multiplied by $q - 1$ to avoid fractions):*

Type	$\mathcal{M}_m^0$	$\alpha_m(q-1)$	$\nu_m(q-1)$
q_{I}^E	$\mathcal{M}_m^1$	$q^{n-m} - q$	$q^{n-m} - q - q^m + 1$
q_{II}^E	$\mathcal{M}_m^1$	$q^{n-m-1} - 1$	$q^{n-m-1} - q^m$
q^E	$\mathcal{M}_m^*$	$q^{n-m} - 1$	$q^{n-m} - q^m$
q_1^E	$\mathcal{M}_m^1$	$q^{n-m-1} - 1$	$q^{n-m-1} - q^m$
q^H	$\mathcal{M}_m^*$	$\sqrt{q}(q^{n-m} - 1)$	$q^{n-m+1/2} - q^m - q^{1/2} + 1$
q_1^H	$\mathcal{M}_m^1$	$\sqrt{q}(q^{n-m-1} - 1)$	$q^{n-m-1/2} - q^m - q^{1/2} + 1$

<u>Proof.</u> By Lemma 7 the set $\mathcal{M}_m^1$ satisfies the condition (2) of Section 2.3 in the cases where the codes in $\mathcal{F}$ contain the all-ones vector.

Let $C \in \mathcal{F}$ be a self-dual code of one of the six Types and let $E \leq C$ be a subspace of codimension 1. First the number $\alpha_E := |\{D \in \mathcal{F} \mid C \cap D = E\}|$ is determined. The relevant codes D correspond to the one-dimensional isotropic subspaces $\neq C/E$ of $E^\perp/E$ with respect to the associated geometry. If $\mathbf{1} \in D$ for all $D \in \mathcal{F}$ (which is the case for $q_{\mathrm{I}}^E, q_{\mathrm{II}}^E, q_1^E, q_1^H$) and $\mathbf{1} \notin E$ then $C = \langle E, \mathbf{1} \rangle$ is the unique code in $\mathcal{F}$ that contains E. So here $\alpha_E = 0$ if $\mathbf{1} \notin E$.

Case q_{I}^E: Assume that we are in case q_{I}^E and that $\mathbf{1} \in E$. Then all elements $c = (c_1, \ldots, c_N) \in E^\perp$ satisfy

$$0 = b(\mathbf{1}, c) = \sum_{i=1}^N c_i = (\sum_{i=1}^N c_i)^2 = \sum_{i=1}^N c_i^2 = b(c, c),$$

because the characteristic of $\mathbb{F}$ is 2. Hence all $q + 1$ one-dimensional subspaces of $E^\perp/E$ are self-dual and $\alpha_E = q$. This proves that for $\underline{c} = (c^{(1)}, \ldots, c^{(m)}) \in C^m$ with $X := \mathrm{mon}(\underline{c}) \in \mathcal{M}_m^1$ the sum $\alpha_m := \sum_{E \in \mathcal{E}_C(\underline{c})} \alpha_E$ is q times the number

9

of $(n-1)$-dimensional subspaces of C that contain the $(m+1)$-dimensional space $\langle \mathbf{1}, c^{(1)}, \ldots, c^{(m)} \rangle$ hence $\alpha_m = q\beta_{n-m-1} = q\frac{q^{n-m-1}-1}{q-1}$.

$\underline{\text{Case } q_{\text{II}}^E}$: If $\mathbf{1} \in E$, the space $E^\perp/E$ is a non-singular quadratic space of dimension 2 with a maximal isotropic subspace C/E. Hence $E^\perp/E$ is a hyperbolic plane and has exactly two maximal isotropic subspaces. Therefore $\alpha_m = \beta_{n-m-1} = \frac{q^{n-m-1}-1}{q-1}$.

$\underline{\text{Case } q^E}$: Here q is odd and for any codimension 1 subspace $E \leq C \in \mathcal{F}$ the space $E^\perp/E$ is a hyperbolic plane with exactly two maximal isotropic subspaces. Therefore $\alpha_E = 1$ for all E and $\alpha_m = \beta_{n-m} = \frac{q^{n-m}-1}{q-1}$.

$\underline{\text{Case } q_1^E}$: By the argumentation above we only need to consider the subspaces E that contain $\mathbf{1}$. Again $E^\perp/E$ is a hyperbolic plane and $\alpha_m = \beta_{n-m-1} = \frac{q^{n-m-1}-1}{q-1}$.

$\underline{\text{Case } q^H}$: Let $E \leq C \in \mathcal{F}$ be a self-orthogonal subspace of dimension $n-1$. Then $E^\perp/E$ is a 2-dimensional non-degenerate Hermitian space over $\mathbb{F}_q$ hence isometric to $\mathbb{F}_q^2$ with the Hermitian form $((x_1, x_2), (y_1, y_2)) := x_1\overline{y_1} + x_2\overline{y_2}$. It follows easily that this space has exactly $\sqrt{q}+1$ one-dimensional isotropic subspaces. Since C/E is one of them $\alpha_E = r = \sqrt{q}$ and $\alpha_m = \sqrt{q}\beta_{n-m} = \sqrt{q}\frac{q^{n-m}-1}{q-1}$.

$\underline{\text{Case } q_1^H}$: Similar as for q^H but we only need to consider the subspaces E that contain $\mathbf{1}$. Therefore $\alpha_m = \sqrt{q}\beta_{n-m-1} = \sqrt{q}\frac{q^{n-m-1}-1}{q-1}$.

The eigenvalue ν_m of T now results from the general formula in Theorem 8. $\qquad\square$

Remark 12. *The eigenvalues ν_m are strictly decreasing. In particular the maximal eigenvalurs ν_0 is a simple eigenvalue which shows that the neighboring graph is connected.*

3.1 Explicit numerical results.

The neighboring method provides a quite efficient way to enumerate all equivalence classes of codes of a given Type. During this procedure, the Kneser-Hecke-operator T is calculated without difficulty. It is then easy to obtain the eigenvalues of T and the (dimensions of the) eigenspaces. With Theorem 8 this gives the dimension of all spaces $\text{cwe}_m(\mathcal{V})$ for all $m \in \mathbb{N}_0$, even if it might be quite difficult to obtain (enough terms of) the genus-m complete weight-enumerators of the codes in $\mathcal{F}$ to calculate this dimension directly. The calculations are performed with MAGMA [4] using a direct analogue of the Kneser-neighboring procedure described in [7] for lattices. Recall that $n := \frac{N}{2}$ denotes the dimension of the codes in $\mathcal{F}$. Starting with some code in $C \in \mathcal{F}$ (usually constructed as an orthogonal sum) we enumerate the orbits of the automorphism group on the $(n-1)$-dimensional subspaces $E \leq C$ (resp. those E that contain $\mathbf{1}$) and calculate the neighbors of C as preimages of the isotropic one-dimensional subspaces of $E^\perp/E$.

For the binary codes (where calculations could be performed without problems up to length $N = 32$) we have the following explicit results.

Table 1: The dimension of the space $\mathcal{Y}_m$ for Type 2_I.

10

N,m	0	1	2	3	4	5	6	7	8	9	10	11
2	1											
4	1											
6	1											
8	1	1										
10	1	1										
12	1	1	1									
14	1	1	1	1								
16	1	2	1	2	1							
18	1	2	2	2	2							
20	1	2	3	4	4	2						
22	1	2	3	6	7	4	2					
24	1	3	5	9	15	13	7	2				
26	1	3	6	12	23	29	20	8	1			
28	1	3	7	18	40	67	75	39	10	1		
30	1	3	8	23	65	142	228	189	61	10	1	
32	1	4	10	33	111	341	825	1176	651	127	15	1

Table 2: The dimension of the space $\mathcal{Y}_m$ for Type 2_{II}.

N,m	0	1	2	3	4	5	6	7	8	9	10
8	1										
16	1	0	0	1							
24	1	1	1	2	2	1	1				
32	1	1	2	5	10	15	21	18	8	3	1

Application to Molien-series.

By [19] (see also [11]) there is a finite matrix group $\mathcal{C}_m \leq \mathrm{GL}_{2^m}(\mathbb{Q}[\sqrt{2}])$ called the *real Clifford-group of genus m*, such that the invariant ring of $\mathcal{C}_m$ is the image of cwe_m,

$$\mathrm{Inv}(\mathcal{C}_m) = \bigoplus_{N=0}^{\infty} \langle \mathrm{cwe}_m(C) \, : \, C = C^{\perp} \leq \mathbb{F}_2^N \rangle \ .$$

Corollary 13. *For $m \geq 1$ the Molien series of $\mathcal{C}_m$ is*

$$1 + t^2 + t^4 + t^6 + 2t^8 + 2t^{10} + \sum_{N=12}^{\infty} a_N(m) t^N$$

where for $N \leq 32$ the coefficients $a_N(m) = \dim \langle \mathrm{cwe}_m(C) \, : \, C = C^{\perp} \leq \mathbb{F}_2^N \rangle$ are given in the following table.

N	12	14	16	18	20	22	24	26	28	30	32
$m = 1$	2	2	3	3	3	3	4	4	4	4	5
$m = 2$	3	3	4	5	6	6	9	10	11	12	15
$m = 3$	3	4	6	7	10	12	18	22	29	35	48
$m = 4$	3	4	7	9	14	19	33	45	69	100	159
$m = 5$	3	4	7	9	16	23	46	74	136	242	500
$m = 6$	3	4	7	9	16	25	53	94	211	470	1325
$m = 7$	3	4	7	9	16	25	55	102	250	659	2501
$m = 8$	3	4	7	9	16	25	55	103	260	720	3152
$m = 9$	3	4	7	9	16	25	55	103	261	730	3279
$m = 10$	3	4	7	9	16	25	55	103	261	731	3294
$m \geq 11$	3	4	7	9	16	25	55	103	261	731	3295

Similarly the genus-m complete weight-enumerators of the doubly-even self-dual binary codes span the invariant ring of the *complex Clifford-group* $\mathcal{X}_m \leq \mathrm{GL}_{2^m}(\mathbb{Q}[\zeta_8])$ (see [19], [11]) and Table 2 above gives the first terms of the Molien series of those groups. The full Molien series of $\mathcal{C}_m$ and $\mathcal{X}_m$ are known for $m \leq 4$ (see [16], sequences number A008621, A008718, A024186, A110160, A008620, A028288, A039946, A051354 in [20]).

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. Cannon et al., *The Magma Computational Algebra System for Algebra, Number Theory and Geometry*, published electronically at http://magma.maths.usyd.edu.au/magma/.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, New York, 1998, 3rd. ed. 1998.

[6] M. Hentschel and A. Krieg, A Hermitian analog of the Schottky form. In *Automorphic forms and zeta functions – Proceedings of the conference in memory of Tsuneo Arakawa* – World Scientific, 2006.

[7] M. Kneser, Klassenzahlen definiter quadratischer Formen, *Archiv der Math.* **8** (1957), 241-250.

[8] W. Kohnen and R. Salvati Manni, Linear relations between theta series, *Osaka J. Math.* **41** (2004), 353–356.

[9] G. Nebe, Finite Weil-representations and associated Hecke-algebras. submitted (2006).

[10] G. Nebe, H.-G. Quebbemann, E. M. Rains and N. J. A. Sloane, Complete weight enumerators of generalized doubly-even self-dual codes, *Finite Fields Applic.*, **10** 2004, 540–550.

[11] G. Nebe, E. M. Rains and N. J. A. Sloane, The invariants of the Clifford groups, *Designs, Codes, and Cryptography* **24** (2001), 99–121.

[12] G. Nebe, E. M. Rains and N. J. A. Sloane, Codes and invariant theory, *Math. Nachrichten*, **274–275** (2004), 104–116.

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

[14] G. Nebe and M. Teider, Hecke actions on certain strongly modular genera of lattices. *Archiv der Math.*, **84** (1) (2005) 46–56.

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

[16] M. Oura, The dimension formula for the ring of code polynomials in genus 4, *Osaka J. Math.* (1997), **34**, pp. 53–72.

[17] H.-G. Quebbemann, On even codes, *Discrete Math.* **98** (1991), 29–34.

[18] E. M. Rains and N. J. A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, ed. V. S. Pless and W. C. Huffman, Elsevier, Amsterdam, 1998, pp. 177–294.

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

[20] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences* published electronically at www.research.att.com/∼njas/sequences/, 2005.