

Finite Weil-representations and associated Hecke-algebras.

Gabriele Nebe

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

Abstract

¹ An algebra $\mathcal{H}(G_m)$ of double-cosets is constructed for every finite Weil-representation G_m . For the Clifford-Weil groups $G_m = \mathcal{C}_m(\rho)$ associated to some classical Type ρ of self-dual codes over a finite field, this algebra is shown to be commutative. Then the eigenspace-decomposition of $\mathcal{H}(\mathcal{C}_m(\rho))$ acting on the space of degree N invariants of $\mathcal{C}_m(\rho)$ may be obtained from the kernels of powers of the coding theory analogue of the Siegel Φ -operator.

1 Introduction.

The present paper continues the investigation of the parallels between lattices and codes in particular those analogies that are reflected in the theory of modular forms and invariant theory of certain finite groups. Degree- m Siegel theta series of lattices are modular forms for certain subgroups of $\mathrm{Sp}_{2m}(\mathbb{R})$. Similarly degree- m complete weight-enumerators of (self-dual) codes of a given Type ρ are invariant under a certain finite complex matrix group $\mathcal{C}_m(\rho)$, the associated Clifford-Weil group. In fact [8] shows that these weight enumerators span the invariant ring of $\mathcal{C}_m(\rho)$. One important tool to investigate the ring of modular forms is the Siegel Φ -operator, which is a linear mapping between modular forms of degree m and degree $m-1$ and which maps the degree- m Siegel theta series of a lattice to its degree- $m-1$ Siegel theta series. A coding theory analogue of this Φ -operator was introduced by B. Runge [10] and provides a linear mapping between the invariant rings of finite matrix groups of different degree. In modular forms theory, the kernel of the Φ -operator is invariant under the Hecke algebra, an algebra generated by certain double cosets of the corresponding modular group. On the coding theory side, the existence of Hecke operators was an open question raised in 1977 in [1]. The recent paper [5] answers this question and translates a well-known construction of Hecke-operators acting on theta series of lattices to codes. For codes over finite fields the eigenspaces of the resulting Kneser-Hecke operator T can be characterized in terms of Runge's Φ -operator.

It is hence a natural question to obtain a group-theoretic interpretation of the Kneser-Hecke operator as a linear combination of certain double cosets of $\mathcal{C}_m(\rho)$. This paper proposes one possible answer motivated by the fact that the natural representation

¹MSC: primary 11F27, secondary 94B05, 11F60

of $\mathcal{C}_m(\rho)$ is a finite Weil-representation as explained in Section 2.1. Hence there is a Heisenberg group $\mathcal{E}_m \leq U_d(\mathbb{C})$ such that $\mathcal{C}_m(\rho)$ normalizes \mathcal{E}_m . The Siegel Φ -operator is a ring epimorphism from $\text{Inv}(\mathcal{C}_m(\rho))$ to $\text{Inv}(\mathcal{C}_{m-1}(\rho))$. Choosing a right inverse constructs a linear operator on $\text{Inv}(\mathcal{C}_m(\rho))$ which can be expressed as the action of the double coset

$$K_1 := \mathcal{C}_m(\rho)p_{\mathcal{U}_1}\mathcal{C}_m(\rho)$$

where \mathcal{U}_1 is a suitable abelian subgroup of \mathcal{E}_m and $p_{\mathcal{U}_1} \in \mathbb{C}^{d \times d}$ the orthogonal projection onto its fixed space.

The Hecke-algebra $\mathcal{H} := \mathcal{H}(\mathcal{C}_m(\rho))$ is the algebra generated by such double-cosets (see Definition 2). If the strong-transitivity condition (Definition 4) is satisfied, then this Hecke-algebra is commutative and the decomposition of the space of homogeneous degree- N invariants $\text{Inv}_N(\mathcal{C}_m(\rho))$ given by the kernels of powers of the Φ -operator is the eigenspace-decomposition of \mathcal{H} (Theorems 14 and 15).

The last section shows that the Clifford-Weil groups associated with the classical Types of codes over finite fields satisfy the strong-transitivity condition and hence here the algebra \mathcal{H} coincides with the one generated by the Kneser-Hecke operator.

ACKNOWLEDGEMENTS. I thank Prof. R. Schulze-Pillot for his encouragement and for sending me the preprint [4].

2 Finite Weil-representations.

The crucial point of the construction of a Hecke-algebra for the Clifford-Weil groups is that these groups normalize a certain Heisenberg group \mathcal{E}_m . The double cosets of the orthogonal projections onto the fixed space of certain abelian subgroups of \mathcal{E}_m then generate the associated Hecke-algebra. If the slightly technical strong transitivity condition from Definition 4 is satisfied, then Theorem 14 shows that this Hecke-algebra is commutative.

2.1 The Weil-representation.

Let V be a finite abelian group and consider for $m \in \mathbb{Z}_{\geq 0}$ the Hermitian space $M_m = \mathbb{C}[V^m]$ with orthonormal \mathbb{C} -basis $X_m := (x_{(v_1, \dots, v_m)} \mid v_i \in V)$.

Let $\beta : V \times V \rightarrow \mathbb{Q}/\mathbb{Z}$ be a non-degenerate bi-additive form (i.e. $x \mapsto (y \mapsto \beta(x, y))$) is an isomorphism between V and its dual $\text{Hom}(V, \mathbb{Q}/\mathbb{Z})$. Define the Heisenberg group

$$\mathcal{E}(\beta)_m := \mathcal{E}_m := V^m \times V^m \times \mathbb{Q}/\mathbb{Z}$$

where the multiplication on \mathcal{E}_m is given by

$$(v, v', a)(u, u', b) := (v + u, v' + u', a + b + \sum_{j=1}^m \beta(u'_j, v_j)) \text{ for all } (v, v', a), (u, u', b) \in \mathcal{E}_m.$$

Let $Z := \{(0, 0, a) \mid a \in \mathbb{Q}/\mathbb{Z}\}$ denote the center of \mathcal{E}_m . Then \mathcal{E}_m acts on M_m by unitary endomorphisms

$$(u, u', a)x_v := \exp(2\pi i(a + \sum_{j=1}^m \beta(v_j, u_j))x_{u'+v})$$

which gives an embedding of \mathcal{E}_m into the unitary group $U(M_m)$. It is easy to see that M_m is an irreducible \mathcal{E}_m -module and that any system of representatives of \mathcal{E}_m/Z maps onto \mathbb{C} -linearly independent matrices in $\text{End}(M_m)$. In fact the famous Stone-von Neumann theorem shows that M_m is the unique irreducible \mathcal{E}_m -module with the given central character. If G_m is a subgroup of $\text{Aut}(\mathcal{E}_m)$ centralizing the center of \mathcal{E}_m , then the action of G_m on \mathcal{E}_m gives rise to a projective representation of G_m on M_m . This representation is called the *Weil-representation* of G_m (see [11], [3], [4]). We call a subgroup $G_m \leq U(M_m)$ a *finite Weil-representation*, if G_m is a finite subgroup of the normalizer in $U(M_m)$ of \mathcal{E}_m .

2.2 An algebra of double-cosets of G_m .

Let G_m be a finite Weil-representation and define

$$\mathcal{U}_j := \{(u, 0, 0) \mid u = (0^{m-j}, u_1, \dots, u_j), u_i \in V\} \leq \mathcal{E}_m.$$

Then G_m acts on \mathcal{E}_m by conjugation. Let

$$\mathcal{S}_j := \{g\mathcal{U}_jg^{-1} \mid g \in G_m\}$$

denote the G_m -conjugacy class of \mathcal{U}_j . Let

$$p_{\mathcal{U}_j} := \frac{1}{|\mathcal{U}_j|} \sum_{u \in \mathcal{U}_j} u \in \text{End}(M_m)$$

be the orthogonal projection onto the fixed space of \mathcal{U}_j . Since β is non-degenerate, the image of $p_{\mathcal{U}_j}$ is generated by the $x_{(v_1, \dots, v_{m-j}, 0, \dots, 0)}$ with $v_i \in V$.

Proposition 1. $G_m p_{\mathcal{U}_j} G_m = \dot{\bigcup}_{U \in \mathcal{S}_j} p_U G_m = \dot{\bigcup}_{U \in \mathcal{S}_j} G_m p_U$.

Proof. Clearly

$$G_m p_{\mathcal{U}_j} G_m = \bigcup_{g \in G} g p_{\mathcal{U}_j} g^{-1} G_m.$$

Moreover the element $g p_{\mathcal{U}_j} g^{-1} = p_{g\mathcal{U}_jg^{-1}}$ is an orthogonal projection and hence uniquely determined by its image. All elements in the right coset $g p_{\mathcal{U}_j} g^{-1} G_m$ have the same image, so $g p_{\mathcal{U}_j} g^{-1}$ is the unique orthogonal projection in its right coset. Therefore it remains to show that for $U, W = gUg^{-1} \in \mathcal{S}_j$ the two projections p_U and p_W are equal, if and only if $U = W$. This follows from the linear independence of \mathcal{E}_m/Z and the fact that $U \cap Z = W \cap Z = \{1\}$. \square

Definition 2. Let $G_m \leq U(M_m)$ be a finite Weil-representation. Then the algebra $\mathcal{H}(G_m)$ generated by the double-cosets

$$K_j := G_m p \mathcal{U}_j G_m$$

with $0 \leq j \leq m$ is called the *Hecke-algebra* of G_m .

The algebra $\mathcal{H}(G_m)$ is the set of all formal sums and products of the K_j . For $a \in \mathbb{Z}_{\geq 0}$ and a double-coset $G_m e G_m$ the multiple $a G_m e G_m$ denote the formal sum of a copies of $G_m e G_m$. The multiplication of double-cosets is for instance given in [2, Section (IV.1), p. 226 ff]: If $G_m e G_m = \dot{\cup}_{j=1}^a G_m e_j$ and $G_m f G_m = \dot{\cup}_{i=1}^b G_m f_i$ then

$$(G_m e G_m)(G_m f G_m) = \sum_{j,i} G_m e_j f_i G_m = \sum_k \alpha_k G_m g_k G_m$$

where the sums are formal linear combinations, g_k runs through a set of double-coset representatives, and

$$\alpha_k = |\{(j, i) \in \{1, \dots, a\} \times \{1, \dots, b\} \mid G_m e_j f_i = G_m g_k\}|.$$

The Hecke-algebra acts from the right on the polynomial ring

$$\mathbb{C}[X_m] := \mathbb{C}[x_v \mid v \in V^m] := \bigoplus_{N=0}^{\infty} \mathbb{C}[X_m]_N,$$

where $\mathbb{C}[X_m]_N$ is the subspace of homogeneous polynomials of degree N , via

$$p \cdot (G_m e G_m)(x) := |G_m|^{-2} \sum_{g,h \in G_m} p(geh x).$$

This action preserves the invariant ring

$$\text{Inv}(G_m) := \{p \in \mathbb{C}[X_m] \mid (p \cdot g)(x) := p(gx) = p(x) \text{ for all } g \in G_m\}$$

of G_m . Note that, if $G_m e G_m = \dot{\cup}_{j=1}^a G_m e_j$ and $p \in \text{Inv}(G_m)$ then $(p \cdot G_m e G_m)(x) = \frac{1}{a} \sum_{j=1}^a p(e_j x)$.

For any $r \in \mathbb{R}$ and $0 \leq j \leq m$ the double-coset

$$K_j(r) = G_m r p \mathcal{U}_j G_m \tag{1}$$

is stable under the involution \dagger , where $A^\dagger := \overline{A}^{\text{tr}}$. Therefore $\mathcal{H}(G_m)$ is commutative, if the products of the K_j are integral linear combinations of certain $K_i(r)$ ($r \in \mathbb{R}$, $0 \leq i \leq m$).

The action of the Hecke-algebra preserves the homogeneous components

$$\text{Inv}_N(G_m) := \{p \in \text{Inv}(G_m) \mid p \text{ is homogeneous of degree } N\}$$

which defines the representations

$$\Delta_N : \mathcal{H}(G_m) \rightarrow \text{End}(\text{Inv}_N(G_m)).$$

Clearly $\Delta_N(K_j(r)) = r^N \Delta_N(K_j)$.

Lemma 3. *Let A and B be finite abelian subgroups of $\text{GL}_d(\mathbb{C})$.*

a) *Let $X := AC_B(A)$. Assume that there is a subgroup $B_0 \leq B$ such that $B = C_B(A)B_0$ and $C_B(A) \cap B_0 = \{1\}$. Then*

$$p_{APB} = p_X p_{B_0} \text{ and } p_{BPA} = p_{B_0} p_X.$$

b) *If there is $a \in A$ and $1 \neq \zeta \in \mathbb{C}^*$ such that $\zeta a \in B$ then $p_{APB} = p_{BPA} = 0$.*

Proof. a) $|A| \cdot |B| p_{APB} =$

$$\sum_{a \in A, b \in B} ab = \sum_{a \in A, b \in C_B(A)} ab \sum_{b_0 \in B_0} b_0 = |A| \cdot |C_B(A)| p_X |B_0| p_{B_0} = |A| \cdot |B| p_X p_{B_0}.$$

The second equality follows similarly.

b) follows from a) since X has no fixed points if $\zeta I_d \in X$ and hence $p_X = 0$. \square

Definition 4. For $U \in \mathcal{S}_j$ and $W \in \mathcal{S}_\ell$ let $X(U, W) := \langle U, C_W(U) \rangle$. We say that the Weil-representation (G_m, \mathcal{E}_m) satisfies the *strong transitivity condition* if

- 1) for all $1 \leq j, \ell \leq m$ and all $U \in \mathcal{S}_j$ and $W \in \mathcal{S}_\ell$ there is some $0 \leq k \leq \ell$ and a subgroup $W \geq W_0 \in \mathcal{S}_k$ such that $W = W_0 C_W(U)$ and $W_0 \cap C_W(U) = \{1\}$,
- 2) for all $1 \leq j, \ell \leq m$ and all $U \in \mathcal{S}_j$ and $W \in \mathcal{S}_\ell$ either $p_{X(U, W)} = 0$ or there is some $j \leq k \leq m$ such that $X(U, W) \in \mathcal{S}_k$, and
- 3) for all $1 \leq j, \ell \leq m$ the group G_m acts transitively on the set

$$\mathcal{M}_{j, \ell} := \{(U, W) \in \mathcal{S}_j \times \mathcal{S}_\ell \mid C_W(U) = \{1\}\}.$$

3 Finite Siegel Φ -operators and invariant rings

This section introduces the coding theory analogue of the Siegel Φ -operator and the filtration of $\text{Inv}(G_m)$ defined by the kernels of these operators. In the theory of modular forms, the analogue filtration of the space of Siegel modular forms is invariant under the full Hecke algebra. A similar result is true here, if the Hecke algebra is commutative. In fact one motivation for the definition of the Hecke operators in Section 2 comes from this observation. The Hecke operator K_j has the same kernel as the Φ -operator $\Phi_{m, j}$ on the invariant ring of G_m .

3.1 Finite Siegel Φ -operators

The *finite Siegel Φ -operators* are linear operators

$$\Phi_{m,j} : M_m \rightarrow M_{m-j}, x_{(v_1, \dots, v_m)} \mapsto \begin{cases} x_{(v_1, \dots, v_{m-j})} & \text{if } v_{m-j+1} = \dots = v_m = 0 \\ 0 & \text{else} \end{cases}$$

for all $j \in \{0, \dots, m\}$. Their right inverses may be defined as

$$\varphi_{m,j} : M_{m-j} \rightarrow M_m, x_{(v_1, \dots, v_{m-j})} \mapsto x_{(v_1, \dots, v_{m-j}, 0, \dots, 0)}.$$

They satisfy $\Phi_{m,j} \circ \varphi_{m,j} = \text{id}_{M_{m-j}}$. In particular $\Phi_{m,j}$ is surjective and $\varphi_{m,j}$ is injective.

The idempotent endomorphism $\varphi_{m,j} \circ \Phi_{m,j} \in \text{End}(M_m)$ is self-adjoint with respect to the \mathcal{E}_m -invariant hermitian inner product. It is also a unique complex linear combination of matrices in \mathcal{E}_m/Z and since the image of the orthogonal projection $\varphi_{m,j} \circ \Phi_{m,j}$ is the fixed space of \mathcal{U}_j we have

$$\varphi_{m,j} \circ \Phi_{m,j} = p\mathcal{U}_j. \quad (2)$$

These linear operators may be extended to ring homomorphisms

$$\begin{aligned} \Phi_{m,j} : \mathbb{C}[X_m] &\rightarrow \mathbb{C}[X_{m-j}] \\ \varphi_{m,j} : \mathbb{C}[X_{m-j}] &\rightarrow \mathbb{C}[X_m] \end{aligned}$$

which respect the grading. The \mathcal{E}_m -invariant Hermitian form on M_m induces an \mathcal{E}_m -invariant positive definite symmetric Hermitian form on $\mathbb{C}[X_m]_N$ by letting

$$(p, q)_m := p\left(\frac{\partial}{\partial x} \mid x \in X_m\right)(\bar{q}) \text{ for } p, q \in \mathbb{C}[X_m]_N$$

where $p\left(\frac{\partial}{\partial x} \mid x \in X_m\right)$ is the differential operator obtained from the polynomial p by substituting each variable $x \in X_m$ by the partial derivative $\frac{\partial}{\partial x}$ and $\bar{q} \in \mathbb{C}[X_m]_N$ is the polynomial obtained from q by applying complex conjugation to its coefficients. Then the monomials of degree N form an orthogonal basis of $\mathbb{C}[X_m]_N$ and

$$\left(\prod_{v \in V^m} x_v^{n_v}, \prod_{v \in V^m} x_v^{n_v}\right)_m = \prod_{v \in V^m} (n_v!).$$

Explicit calculation and induction on j show the following lemma.

Lemma 5. *Let $m \in \mathbb{N}$ and $0 \leq j \leq m$.*

a) *The mappings $\varphi_{m,j} : \mathbb{C}[X_{m-j}]_N \rightarrow \varphi_{m,j}(\mathbb{C}[X_{m-j}]_N) \subset \mathbb{C}[X_m]_N$ and $\Phi_{m,j} : \ker(\Phi_{m,j})^\perp \rightarrow \mathbb{C}[X_{m-j}]_N$ are isometries.*

b) *For $p \in \mathbb{C}[X_m]_N, q \in \mathbb{C}[X_{m-j}]_N$ it holds that*

$$(\varphi_{m,j}(q), p)_m = (q, \Phi_{m,j}(p))_{m-j}.$$

c) $\varphi_{m,j} \circ \Phi_{m,j}$ is a self-adjoint idempotent in $\text{End}(\mathbb{C}[X_m]_N)$ and hence an orthogonal projection.

By the non-degeneracy of $(\cdot, \cdot)_{m-j}$ this implies

Corollary 6. *The image of $\varphi_{m,j}$ is the orthogonal complement of the kernel of $\Phi_{m,j}$.*

$$\begin{aligned} \mathbb{C}[X_m]_N &= \ker(\Phi_{m,1}) \perp \ker(\Phi_{m,1})^\perp = \ker(\Phi_{m,1}) \perp \varphi_{m,1}(\mathbb{C}[X_{m-1}]_N) = \\ &= \ker(\Phi_{m,1}) \perp \varphi_{m,1}(\ker(\Phi_{m-1,1})) \perp \varphi_{m,2}(\ker(\Phi_{m-2,1})) \perp \dots \perp \\ &= \varphi_{m,m-1}(\ker(\Phi_{1,1})) \perp \varphi_{m,m}(\mathbb{C}[X_0]_N) \end{aligned}$$

3.2 Restriction to invariant rings.

Let $G_m \leq \text{GL}(M_m)$ be a series of finite groups such that

$$\Phi_{m,j}(\text{Inv}(G_m)) = \text{Inv}(G_{m-j}) \text{ for all } m, j. \quad (3)$$

Then $\Phi_{m,j}$ induces an isometry between the orthogonal complement in $\text{Inv}(G_m)$ of $\ker(\Phi_{m,j})$ and $\text{Inv}(G_{m-j})$ of which we now aim to construct the inverse using the Reynolds operator

$$R_m : \mathbb{C}[X_m] \rightarrow \text{Inv}(G_m), p(x) \mapsto \frac{1}{|G_m|} \sum_{g \in G_m} p(gx).$$

Note that R_m respects the degree of the polynomials and its restriction to the degree N polynomials is the orthogonal projection of $\mathbb{C}[X_m]_N$ onto $\text{Inv}_N(G_m)$ with respect to $(\cdot, \cdot)_m$.

Lemma 7. *For $j \in \{1, \dots, m\}$ let*

$$\tilde{\varphi}_{m,j} : \text{Inv}(G_{m-j}) \rightarrow \text{Inv}(G_m), p \mapsto R_m(\varphi_{m,j}(p)).$$

If $\Phi_{m,j}(\text{Inv}_N(G_m)) = \text{Inv}_N(G_{m-j})$ then $\tilde{\varphi}_{m,j}$ is an isomorphism between the space of homogeneous invariants $\text{Inv}_N(G_{m-j})$ of degree N of G_{m-j} and $\ker(\Phi_{m,j})^\perp \cap \text{Inv}_N(G_m)$.

Proof. For $p \in \text{Inv}_N(G_m)$ and $q \in \text{Inv}_N(G_{m-j})$ one gets

$$(\tilde{\varphi}_{m,j}(q), p)_m = (R_m(\varphi_{m,j}(q)), p)_m = (\varphi_{m,j}(q), R_m(p))_m = (\varphi_{m,j}(q), p)_m = (q, \Phi_{m,j}(p))_{m-j}$$

since R_m is self-adjoint and p is invariant under G_m . The last equality follows from Lemma 5 (b). In particular

$$\begin{aligned} \tilde{\varphi}_{m,j}(\text{Inv}_N(G_{m-j})) &\subseteq \ker(\Phi_{m,j})^\perp \cap \text{Inv}_N(G_m) \text{ and} \\ \ker(\tilde{\varphi}_{m,j}) &\subseteq \Phi_{m,j}(\text{Inv}_N(G_m))^\perp \end{aligned}$$

Since $\Phi_{m,j}$ is surjective this implies that $\tilde{\varphi}_{m,j}$ is injective and hence an isomorphism onto $\ker(\Phi_{m,j})^\perp \cap \text{Inv}_N(G_m)$ by comparing dimensions. \square

As above this yields a decomposition of the space of homogeneous invariants.

Theorem 8. *Assume that $\Phi_{m,j}(\text{Inv}_N(G_m)) = \text{Inv}_N(G_{m-j})$ for all j . Then*

$$\begin{aligned} \text{Inv}_N(G_m) = & \ker(\Phi_{m,1}) \perp \tilde{\varphi}_{m,1}(\ker(\Phi_{m-1,1})) \perp \tilde{\varphi}_{m,2}(\ker(\Phi_{m-2,1})) \perp \dots \perp \\ & \tilde{\varphi}_{m,m-1}(\ker(\Phi_{1,1})) \perp \tilde{\varphi}_{m,m}(\text{Inv}_N(G_0)) \end{aligned} \quad (4)$$

where the operators $\Phi_{j,1}$ are restricted to $\text{Inv}_N(G_j)$.

Since $\tilde{\varphi}_{m,j}(\ker(\Phi_{m-j,1}) \cap \text{Inv}_N(G_{m-j})) \subseteq R_m(\varphi_{m,j}(\ker(\Phi_{m-j,1})))$ for all j , the decomposition in Theorem 8 is the orthogonal projection under the operator R_m of the decomposition in Corollary 6.

Remark 9. *By Lemma 7 the orthogonal complement of $\ker(\Phi_{m,j})$ in $\text{Inv}_N(G_m)$ is $\tilde{\varphi}_{m,j}(\text{Inv}_N(G_{m-j}))$. Therefore the orthogonal decomposition in Theorem 8 is the one associated to the filtration of $\text{Inv}_N(G_m)$ by the kernels of $\Phi_{m,j}$:*

$$\text{Inv}_N(G_m) \supseteq \ker(\Phi_{m,m}) \supseteq \ker(\Phi_{m,m-1}) \supseteq \dots \supseteq \ker(\Phi_{m,2}) \supseteq \ker(\Phi_{m,1}) \supseteq \{0\}.$$

For $j \in \{0, \dots, m\}$ let

$$\psi_{m,j} := R_m \circ \varphi_{m,j} \circ \Phi_{m,j} : \text{Inv}(G_m) \rightarrow \text{Inv}(G_m)$$

where $\psi_{m,0} := \text{id}_{\text{Inv}(G_m)}$. Then for $p, q \in \text{Inv}_N(G_m)$

$$(\psi_{m,j}(p), q)_m = (R_m(\varphi_{m,j}(\Phi_{m,j}(p))), q)_m = (\varphi_{m,j}(\Phi_{m,j}(p)), q)_m$$

since R_m is self-adjoint and $q \in \text{Inv}(G_m)$. The latter equals

$$(\Phi_{m,j}(p), \Phi_{m,j}(q))_{m-j} = (p, \varphi_{m,j}(\Phi_{m,j}(q)))_m$$

by Lemma 5 (b) (applied twice). Again since p is invariant under G_m one sees that this equals $(p, \psi_{m,j}(q))_m$. This shows the following remark.

Remark 10. $\psi_{m,j}$ is a self-adjoint linear operator on $\text{Inv}_N(G_m)$. For any $p \in \text{Inv}(G_m)$

$$\psi_{m,j}(p)(x) = \frac{1}{|G_m|^2} \sum_{g \in G_m p U_j G_m} p(g(x)) = (p \cdot K_j)(x)$$

where K_j is the double-coset of G_m from Definition 2.

Proposition 11. *If $\Delta_N(\mathcal{H}(G_m)) \leq \text{End}(\text{Inv}_N(G_m))$ is commutative, then the decomposition (4) is invariant under $\Delta_N(\mathcal{H}(G_m))$.*

Proof. Since the generators (and hence all elements by commutativity) of $\Delta_N(\mathcal{H}(G_m))$ are self-adjoint, it is enough to show that the generators of $\Delta_N(\mathcal{H}(G_m))$ respect the filtration from Remark 9. Since $\tilde{\varphi}_{m,j}$ is injective, the kernel of $\psi_{m,j} = \tilde{\varphi}_{m,j} \circ \Phi_{m,j}$ equals $\ker(\Phi_{m,j})$. The assumed commutativity, $\psi_{m,j}\psi_{m,l} = \psi_{m,l}\psi_{m,j}$, yields that

$$\psi_{m,j}(\ker(\Phi_{m,l})) = \psi_{m,j}(\ker(\psi_{m,l})) \subset \ker(\psi_{m,l}) = \ker(\Phi_{m,l})$$

and hence $\mathcal{H}(G_m)$ respects the filtration in Remark 9. \square

4 Clifford-Weil groups and the Type of a code.

This section briefly recalls the construction of the Clifford-Weil group associated with a Type of codes. For details the reader is referred to [6], [7], [8], and the fundamental work [11] by A. Weil.

Let R be a finite ring and V be a finite left R -module. Let $\beta : V \times V \rightarrow \mathbb{Q}/\mathbb{Z}$ be a non-degenerate bi-additive form. Then β is called *admissible*, if the mapping $\psi : r \mapsto \beta^r$ is an isomorphism from R_R to the right R -module

$$M := \{\beta^r : (x, y) \mapsto \beta(x, ry) \mid r \in R\}$$

and if M closed under the involution

$$\tau : M \rightarrow M, \tau(\mu)(x, y) := \mu(y, x).$$

In this case τ induces an antiautomorphism ${}^J : R \rightarrow R$ on R defined by $\beta(x, r^J y) = \beta(rx, y)$ for all $x, y \in V, r \in R$. Let

$$\text{Quad}_0(V) := \{\phi : V \rightarrow \mathbb{Q}/\mathbb{Z} \mid \phi(x + y + z) + \phi(x) + \phi(y) + \phi(z) = \phi(x + y) + \phi(x + z) + \phi(y + z) \text{ for all } x, y, z \in V\}$$

be the group generated by all linear and quadratic forms from V to \mathbb{Q}/\mathbb{Z} . Then R acts (not linearly) on $\text{Quad}_0(V)$ by

$$(\phi r)(x) := \phi(rx) \text{ for all } r \in R, \phi \in \text{Quad}_0(V), x \in V.$$

Let Φ be a subgroup of $\text{Quad}_0(V)$ such that

- a) $\Phi R \subset \Phi$
- b) $\lambda(\Phi) \subset M$, where $\lambda(\phi)(x, y) := \phi(x + y) - \phi(x) - \phi(y)$
- c) $\{\mu\} \subset \Phi$, where $\{\mu\}(x) := \mu(x, x)$.

If β is admissible, then the tuple $\rho := (R, V, M, \Phi, \beta)$ is called a finite (representation of a) *form-ring*. The Clifford-Weil group $\mathcal{C}(\rho)$ associated with a form-ring ρ is the finite subgroup $\mathcal{C}(\rho)$ of $\text{GL}(\mathbb{C}[V])$ generated by

$$m_r \text{ with } r \in R^* \text{ where } m_r(x_v) = x_{rv} \text{ for all } v \in V,$$

$$d_\phi \text{ with } \phi \in \Phi \text{ where } d_\phi(x_v) = \exp(2\pi i \phi(v))x_v \text{ for all } v \in V, \text{ and}$$

$$h_\iota \text{ with } \iota^2 = \iota \in R \text{ is such that there are } e_\iota \in \iota R \iota^J, f_\iota \in \iota^J R \iota \text{ such that } e_\iota f_\iota = \iota \text{ and } f_\iota e_\iota = \iota^J \text{ where } h_\iota(x_v) = \sum_{w \in \iota V} \exp(2\pi i \beta(w, e_\iota v))x_{w+(1-\iota)v} \text{ for all } v \in V.$$

There is a natural notion of matrix ring of a form ring

$$\rho^{m \times m} := (R^{m \times m}, V^m, M^{m \times m}, \Phi^{(m)})$$

and the genus- m Clifford-Weil group

$$\mathcal{C}_m(\rho) := \mathcal{C}(\rho^{m \times m}) \leq \text{GL}(\mathbb{C}[V^m]) = \text{GL}(M_m)$$

acts linearly on M_m . This action is easily seen to normalize the one of $\mathcal{E}(\beta)_m$ (see for instance [8, Theorem 5.3.2]) and hence $\mathcal{C}_m(\rho)$ is a finite Weil-representation in the sense of Section 2.1 above.

An R -submodule $C \leq V^N$ is called a *code of Type ρ* for some finite form ring ρ as above, if

$C = C^\perp := \{v \in V^N \mid \sum_{j=1}^N \beta(v_j, c_j) = 0 \text{ for all } c = (c_1, \dots, c_N) \in C\}$ is self-dual and

For all $\phi \in \Phi$ and all $c \in C$ one has $\sum_{i=1}^N \phi(c_i) = 0$ (C is *isotropic* with respect to Φ).

The *genus- m complete weight enumerator* $\text{cwe}_m(C)$ of a code $C \leq V^N$ of Type ρ is a homogeneous polynomial of degree N in $\mathbb{C}[X_m]$ defined by

$$\text{cwe}_m(C) = \sum_{\underline{c} \in C^m} \prod_{v \in V^m} x_v^{a_v(\underline{c})}$$

where for $\underline{c} = (c^{(1)}, \dots, c^{(m)})$ and $v \in V^m$

$$a_v(\underline{c}) := |\{j \in \{1, \dots, m\} \mid c_j^{(i)} = v_i \text{ for all } 1 \leq i \leq m\}|.$$

For a code C of Type ρ the complete weight enumerator $\text{cwe}_m(C)$ is invariant under $\mathcal{C}_m(\rho)$. In fact the main theorem of [8] asserts that in many situations the invariant ring of $\mathcal{C}_m(\rho)$ is spanned by the genus- m complete weight enumerators of codes of Type ρ . Since $\Phi_{m,j}$ maps the genus- m weight enumerator of a code to its genus- $(m-j)$ weight enumerator this implies the surjectivity of the Φ -operators, which means that Equation (3) holds.

5 Hecke-algebras of Clifford-Weil groups.

This section proves the main result of this paper, namely that the Hecke-algebras of the Clifford-Weil groups are commutative, provided that the strong transitivity condition is satisfied. For the explicit calculations some specific elements in $\mathcal{C}_m(\rho)$ are needed.

Definition 12. For $1 \leq k \leq m$ let $h_k : \mathbb{C}[V^m] \rightarrow \mathbb{C}[V^m]$,

$$x_{(v_1, \dots, v_m)} \mapsto |V|^{-k/2} \sum_{(w_1, \dots, w_k) \in V^k} \exp(2\pi i \sum_{j=1}^k \beta(w_j, v_{m-k+j})) x_{(v_1, \dots, v_{m-k}, w_1, \dots, w_k)}$$

Then $h_k \in \mathcal{C}_m(\rho)$ is the MacWilliams transformation associated to the symmetric idempotent $\text{diag}(0^{m-k}, 1^k) \in R^{m \times m}$. Then

$$h_k^{-1} \mathcal{U}_k h_k = \mathcal{W}_k$$

where

$$\mathcal{W}_k := \{(0, u, 0) \mid u = (0^{m-k}, u_1, \dots, u_k), u_i \in V\} \leq \mathcal{E}_m$$

which follows from the equality

$$h_k^{-1}(u, 0, 0) h_k = ((u_1, \dots, u_{m-k}, 0^k), (0^{m-k}, u_{m-k+1}, \dots, u_m), 0) \text{ for all } u = (u_1, \dots, u_m) \in V^m.$$

Lemma 13. For $1 \leq k \leq j \leq m$ we have

$$p_{\mathcal{U}_j} p_{\mathcal{W}_k} = |V|^{-k/2} p_{\mathcal{U}_j} h_k$$

and

$$p_{\mathcal{W}_k} p_{\mathcal{U}_j} = |V|^{-k/2} h_k^{-1} p_{\mathcal{U}_j}.$$

Proof. The group \mathcal{W}_k permutes the basis elements x_v with $v \in V^m$, so $p_{\mathcal{W}_k}$ is the orthogonal projection

$$x_{(v_1, \dots, v_m)} \mapsto |V|^{-k} \sum_{(w_1, \dots, w_k) \in V^k} x_{(v_1, \dots, v_{m-k}, w_1, \dots, w_k)}.$$

The fixed space of \mathcal{U}_j is generated by $x_{(v_1, \dots, v_{m-j}, 0^j)}$ hence $p_{\mathcal{U}_j}$ maps x_v to x_v , if $v_{m-j+1} = \dots = v_m = 0$ and 0 else. Hence

$$p_{\mathcal{U}_j}(p_{\mathcal{W}_k}(x_{(v_1, \dots, v_m)})) = \begin{cases} |V|^{-k} x_{(v_1, \dots, v_{m-j}, 0^j)} & \text{if } v_{m-j+1} = \dots = v_{m-k} = 0 \\ 0 & \text{otherwise} \end{cases}$$

whereas

$$\begin{aligned} p_{\mathcal{U}_j}(h_k(x_{(v_1, \dots, v_m)})) &= |V|^{-k/2} \sum_{(w_1, \dots, w_{m-k}) \in V^{m-k}} \exp(2\pi i \sum_{l=1}^{m-k} \beta(w_l, v_{k+l})) p_{\mathcal{U}_j}(x_{(v_1, \dots, v_k, w_1, \dots, w_{m-k})}) \\ &= \begin{cases} |V|^{-k/2} x_{(v_1, \dots, v_{m-j}, 0^j)} & \text{if } v_{m-j+1} = \dots = v_{m-k} = 0 \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

The second equality follows by applying the involution \dagger to the first one and noting that $p_U^\dagger = p_U$ and $h_k^\dagger = h_k^{-1}$. \square

Theorem 14. Let $\mathcal{C}_m := \mathcal{C}_m(\rho)$ be a Clifford-Weil group associated to some finite form ring ρ . Assume that the finite Weil representation $(\mathcal{C}_m, \mathcal{E}(\beta)_m)$ satisfies the strong transitivity condition from Definition 4. Then

$$\mathcal{H}(\mathcal{C}_m(\rho)) = \langle K_j \mid j \in \{0, \dots, m\} \rangle$$

is a commutative subalgebra of $\text{End}(\text{Inv}(\mathcal{C}_m))$. The multiplication is given by

$$K_j K_\ell = \sum_{k=0}^j \sum_{i=\ell}^m c(j, \ell, i, k) K_i (|V|^{-k/2})$$

where

$$c(j, \ell, i, k) = |\{(U, W) \in \mathcal{S}_j \times \mathcal{S}_\ell \mid WC_U(W) = \mathcal{U}_i \text{ and } \dim(U/C_U(W)) = k\}|.$$

Proof. By Proposition 1 we have

$$K_j = \bigcup_{U \in \mathcal{S}_j} \mathcal{C}_m p_U$$

and hence

$$K_j K_\ell = \sum_{U \in \mathcal{S}_j} \sum_{W \in \mathcal{S}_\ell} \mathcal{C}_m p_U p_W \mathcal{C}_m = \sum_k \alpha_{j, \ell, k} \mathcal{C}_m g_k \mathcal{C}_m$$

where

$$\alpha_{j, \ell, k} = |\{(U, W) \in \mathcal{S}_j \times \mathcal{S}_\ell \mid \mathcal{C}_m p_U p_W = \mathcal{C}_m g_k\}|$$

and g_k runs through a system of representatives of the suitable double cosets. By Lemma 3 $p_U p_W = p_{U_0} p_X$ where $X = \langle W, C_U(W) \rangle$ and $U_0 \leq U$ is such that $U = C_U(W)U_0$ and $U_0 \cap C_U(W) = \{1\}$. By the strong transitivity condition, it is always possible to choose such $U_0 \in \mathcal{S}_k$ for some k . So one may assume that $C_U(W) = \{1\}$. Since \mathcal{C}_m acts transitively on the set $\mathcal{M}_{j, \ell}$ from Definition 4 we may assume that $U = U_0 = \mathcal{U}_k$ and $W = X = \mathcal{W}_{\ell'}$. The condition that $C_U(W) = \{1\}$ implies that $k \leq \ell'$ and hence by Lemma 13

$$\mathcal{C}_m p_U p_W = \mathcal{C}_m |V|^{-k/2} p_W.$$

Hence the product of the two generators $K_j K_\ell$ is the given formal linear combination of the $K_i (|V|^{-k/2})$. Since the $K_i(r)$ is stable under the involution \dagger for all i and all $r \in \mathbb{R}$, the commutativity of $\mathcal{H}(\mathcal{C}_m)$ follows by applying \dagger to the product of the generators $K_j K_\ell$. \square

Theorem 15. Under the condition of Theorem 14 the decomposition (4) given in Theorem 8 is the eigenspace decomposition of the $\mathcal{H}(\mathcal{C}_m)$ -module $\text{Inv}_N(\mathcal{C}_m)$.

Proof. That the decomposition (4) is invariant under $\Delta_N(\mathcal{H}(\mathcal{C}_m))$ follows from Theorem 14 together with Proposition 11. For $0 \leq j \leq m$ and $k \in \mathbb{Z}$ one has

$$\Delta_N(K_j(|V|^{-k/2})) = |V|^{-kN/2} \Delta_N(K_j).$$

So the multiplication given in Theorem 14 yields

$$\Delta_N(K_j) \Delta_N(K_l) = \sum_{k=0}^j \sum_{i=l}^m c(j, l, i, k) |V|^{-kN/2} \Delta_N(K_i).$$

In particular the images $\Delta_N(K_j)$, $0 \leq j \leq m$ generate the image $\Delta_N(\mathcal{H}(\mathcal{C}_m)) \leq \text{End}(\text{Inv}_N(\mathcal{C}_m))$ as a \mathbb{C} -vector space. For $0 \leq j \leq m$ let $V_j := \ker(\Delta_N(K_j))$ and $V_{m+1} := \text{Inv}_N(\mathcal{C}_m)$. Then $V_j \subseteq V_{j+1}$ and

$$(\Delta_N(K_j)|_{V_{j+1}})^2 = c_j \Delta_N(K_j)|_{V_{j+1}}$$

for $c_j := \sum_{k=0}^j c(j, j, j, k) |V|^{-kN/2}$. Therefore K_j acts on V_{j+1}/V_j as c_j times the identity. Note that $c_j > 0$ since $(\mathcal{U}_j, \mathcal{U}_j)$ contributes at least 1 to $c(j, j, j, 0)$ and all summands are nonnegative. For $0 \leq j \leq m$ let

$$\mathcal{H}_j := \langle \Delta_N(K_m), \dots, \Delta_N(K_j) \rangle$$

be the subalgebra generated by the last $m - j + 1$ generators of $\Delta_N(\mathcal{H}(\mathcal{C}_m))$.

$$\underline{\text{Claim:}} \dim(\mathcal{H}_j) = |\{i \mid j \leq i \leq m \text{ and } V_{i+1} \neq V_i\}|.$$

The proof of this claim proceeds by induction over j .

For $j = m$ the claim is clearly true, because $c_m \neq 0$.

Assume that the claim is true for all $i \geq j+1$. If $V_j \neq V_{j+1}$ then $\dim(\mathcal{H}_j) = \dim(\mathcal{H}_{j+1}) + 1$ since $c_j \neq 0$. If $V_j = V_{j+1}$ we have to show that $\Delta_N(K_j) \in \mathcal{H}_{j+1}$. Since $\Delta_N(K_j)$ acts as 0 on V_{j+1} this is equivalent to showing that $\Delta_N(K_j)$ acts as a scalar on V_{l+1}/V_l for all $j+1 \leq l \leq m$. If $V_{l+1} = V_l$ then this is trivially satisfied. If $V_{l+1} \neq V_l$ then $\Delta_N(K_l)$ acts as the scalar $c_l \neq 0$ on V_{l+1}/V_l . Hence it suffices to show that $\Delta_N(K_j) \Delta_N(K_l)$ acts as a scalar on V_{l+1}/V_l . By Theorem 14 this product is

$$\Delta_N(K_j) \Delta_N(K_l) = \sum_{k=0}^j \sum_{i=l}^m c(j, l, i, k) |V|^{-kN/2} \Delta_N(K_i).$$

Since $\Delta_N(K_i)$ is 0 on V_{l+1} for all $i \geq l+1$ this product is a multiple of $\Delta_N(K_l)$ and therefore scalar on V_{l+1}/V_l . This proves the Claim.

In particular the dimension of $\mathcal{H}_0 = \Delta_N(\mathcal{H}(\mathcal{C}_m))$ equals the number of non-zero direct summands in the decomposition (4). Therefore $\Delta_N(\mathcal{H}(\mathcal{C}_m))$ has to act as a scalar on each of the direct summands. \square

6 Codes over finite fields.

The results of this section show that the Clifford-Weil groups associated to the classical Types of self-dual codes over finite fields satisfy the strong transitivity condition. Since the decomposition (4) is the eigenspace decomposition of $\text{Inv}_N(\mathcal{C}_m)$ under the Kneser-Hecke-operator T constructed in [5] this implies that $\Delta_N(\mathcal{H}(\mathcal{C}_m))$ is the subalgebra of $\text{End}(\text{Inv}_N(\mathcal{C}_m))$ generated by T .

A more precise description of the Types is found in [8, Chapter 2] and the structure of the associated Clifford-Weil groups is given in [8, Chapter 7]. The following Types of codes over finite fields $R = V = \mathbb{F}_q$, $q = p^f$ are considered:

q^E : Euclidean self-dual \mathbb{F}_q -linear codes in odd characteristic. Here $\beta : \mathbb{F}_q \times \mathbb{F}_q \rightarrow \mathbb{Q}/\mathbb{Z}$, $\beta(x, y) := \frac{1}{p} \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(xy)$ and the genus m Clifford-Weil group $\mathcal{C}_m(q^E)$ is $\mathcal{C}_m(q^E) \cong Z_a \cdot \text{Sp}_{2m}(q)$ where $a = \gcd(q+1, 4)$.

q_1^E : Same as q^E but additionally imposing the condition that the all-ones vector $\mathbf{1} = (1, \dots, 1)$ be in the self-dual isotropic codes. Then $\mathcal{C}_m(q_1^E) \cong Z_a \cdot p_+^{1+2mf} \cdot \text{Sp}_{2m}(q)$ where $a = \gcd(q+1, 4)$.

q_I^E : Same as q^E but now $p = 2$. Then $\mathcal{C}_m(q_I^E) \cong 2_+^{1+2mf} \cdot O_{2m}^+(2^f)$.

q_{II}^E : Same as q_I^E but additionally assuming that the codes are generalized doubly even as defined in [9]. Then the associated Clifford-Weil group is $\mathcal{C}_m(q_{II}^E) \cong Z_8 Y 2^{1+2mf} \cdot \text{Sp}_{2m}(2^f)$.

q^H : Hermitian self-dual \mathbb{F}_q -linear codes. Here $q = r^2$ is a square and $\bar{\cdot} : \mathbb{F}_q \rightarrow \mathbb{F}_q$, $x \mapsto x^r$ denotes the non-trivial Galois automorphism of $\mathbb{F}_q/\mathbb{F}_r$. Then $\beta : \mathbb{F}_q \times \mathbb{F}_q \rightarrow \mathbb{Q}/\mathbb{Z}$, $\beta(x, y) := \frac{1}{p} \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x\bar{y})$ is hermitian and $\mathcal{C}_m(q^H) \cong Z_2 \cdot \text{GU}_{2m}(q)$ is a central extension of the general unitary group.

q_1^H : Same as q^H , but additionally assuming that $\mathbf{1}$ be in the self-dual isotropic codes. Then $\mathcal{C}_m(q_1^H) = Z_a \times p_+^{1+2mf} \cdot \text{GU}_{2m}(q)$ where $a = \gcd(2, p+1)$.

Theorem 16. *In these six cases $(\mathcal{C}_m, \mathcal{E}(\beta)_m)$ satisfies the strong transitivity condition.*

Proof. Let \mathcal{C}_m be one of these groups. Then the conjugation action of \mathcal{C}_m on $\mathcal{E}_m := \mathcal{E}(\beta)_m$ respects the commutator $[(u, u', a), (v, v', b)] = (0, 0, \sum_{i=1}^m \beta(v'_i, u_i) - \beta(u'_i, v_i))$ for (u, u', a) and $(v, v', b) \in \mathcal{E}_m$. Hence this induces a form $\tilde{\beta}$ on $\mathcal{E}_m/Z \cong \mathbb{F}_q^{2m}$ given by

$$\tilde{\beta}((u, u'), (v, v')) := \sum_{i=1}^m \beta(v'_i, u_i) - \beta(u'_i, v_i).$$

In the first four cases, this form is alternating and for the hermitian cases q^H and q_1^H , the form $\tilde{\beta}$ is skew-hermitian (hence can be turned into a hermitian form).

In the case q_I^E , the Clifford-Weil group fixes the subgroup

$$\mathcal{E}_m^{(2)} := \{(u, u', a) \in \mathcal{E}_m \mid a \in \frac{1}{2}\mathbb{Z}/\mathbb{Z}\} \leq \mathcal{E}_m.$$

Since $\mathcal{U}_j \leq \mathcal{E}_m^{(2)}$ for all j , the set \mathcal{S}_j consists of subgroups of $\mathcal{E}_m^{(2)}$. The $O_{2m}^+(2^f)$ -invariant quadratic form qf on $\mathcal{E}_m^{(2)}$ is given by squaring

$$\text{qf}((u, u', a)Z) := \sum_{i=1}^m \beta(u_i, u'_i)$$

and the elements of \mathcal{S}_j , being elementary abelian, map onto totally isotropic subspaces of \mathcal{E}_m/Z .

Any abelian subgroup $U \leq \mathcal{E}_m$ with $U \cap Z = \{1\}$ can be thought of as a pair (\bar{U}, χ) where $\bar{U} \leq \mathcal{E}_m/Z$ is self-orthogonal with respect to $\tilde{\beta}$ (and isotropic w.r.t. qf in case 2) and $\chi : \bar{U} \rightarrow Z$ is a mapping such that $U = \{(u, \chi(u)) \mid u \in \bar{U}\}$ is an abelian subgroup of \mathcal{E}_m .

Since the natural representation of \mathcal{E}_m is absolutely irreducible, the kernel of the conjugation action of \mathcal{C}_m on \mathcal{E}_m is the subgroup S of scalar matrices in \mathcal{C}_m . Therefore the action of the *hyperbolic co-unitary group* $\mathcal{U}_m(R, \Phi) \cong \mathcal{C}_m/S$ is faithful. This group consists of the pairs of matrices

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix} \right) \in R^{2m \times 2m} \times \Phi^{(2m)} \quad (5)$$

such that

$$\begin{pmatrix} c^J a & c^J b \\ d^J a - 1 & d^J b \end{pmatrix} = (\psi^{2m \times 2m})^{-1} \begin{pmatrix} \lambda^{m \times m}(\phi_1) & \mu \\ \tau(\mu) & \lambda^{m \times m}(\phi_2) \end{pmatrix}. \quad (6)$$

The group law is given by matrix multiplication and the natural action of $\text{GL}_{2m}(R)$ on $\Phi^{(2m)}$ (see [8, Chapter 5]). The action of $\mathcal{U}_m(R, \Phi)$ on \mathcal{E}_m is given by

$$\left(\begin{pmatrix} ab \\ cd \end{pmatrix}, \begin{pmatrix} \phi_1 & \mu \\ & \phi_2 \end{pmatrix} \right)(x, y, q) := (ax + by, cx + dy, q + \phi_1(x) + \phi_2(y) + \mu(x, y) + \mu(y, x)).$$

The projection π to the first component of the elements in $\mathcal{U}_m(R, \Phi)$ is a group homomorphism into $\text{GL}_{2m}(R)$ whose kernel is an abelian group isomorphic to $\ker(\lambda^{m \times m}) \times \ker(\lambda^{m \times m})$. The image of π is isomorphic to the full isometry group of $(\mathcal{E}_m/Z, \tilde{\beta})$ (resp. of $(\mathcal{E}_m^{(2)}/\{\pm 1\}, \text{qf})$ in the third case). The kernel of π acts trivially on \mathcal{E}_m/Z . In all cases, where this group is not trivial, it acts transitively on the set of possible characters for any isotropic subspace $\bar{U} \leq \mathcal{E}_m/Z$. Therefore in these cases

$$\mathcal{S}_j = \{U \leq \mathcal{E}_m \mid UZ/Z \text{ is a } j\text{-dimensional isotropic } \mathbb{F}_q\text{-subspace of } \mathcal{E}_m/Z \text{ and } U \cap Z = \{1\}\}$$

and the cardinality of \mathcal{S}_j is q^j times the number of totally isotropic subspaces of dimension j in \mathcal{E}_m/Z and the strong transitivity condition is satisfied by Witt's theorem and the fact that the groups in \mathcal{S}_j are elementary abelian, so there is no problem to find complements.

We now assume that π is injective. Then the stabilizer of \mathcal{U}_j in $\mathcal{U}_m(R, \Phi)$ consists of matrices as in (5) for which the last j columns of c are 0. Then equation (6) yields that also the last j rows of ϕ_1 lie in the kernel of $\lambda^{j \times m}$. Since λ is assumed to be injective, this implies that these rows are 0 which shows that the stabilizer of \mathcal{U}_j acts as the group $\text{GL}_j(R)$ on the set of possible characters. In particular it stabilizes the trivial character, used to define \mathcal{U}_j . Since $\mathcal{U}_m(R, \Phi)$ is transitive on the set of isotropic subspaces $\overline{U} \leq \mathcal{E}_m/Z$ of dimension j one concludes that for all those \overline{U} there is a unique character χ such that $U = \{(u, \chi(u)) \mid u \in \overline{U}\} \in \mathcal{S}_j$.

The stabilizer of \mathcal{U}_j acts transitively on the subgroups of \mathcal{U}_j of given dimension. Therefore the union of the sets \mathcal{S}_i is closed under taking subgroups and it remains to show property 2) of the strong transitivity condition. Let $U \in \mathcal{S}_j$, $W \in \mathcal{S}_\ell$ and $X := X(U, W) = \langle U, C_W(U) \rangle$. We may assume that $U = \mathcal{U}_j$ and $W = g\mathcal{U}_\ell$ for some $g \in \mathcal{U}(R, \Phi)$. Since $\overline{X} \leq \mathcal{E}_m/Z$ is a totally isotropic subspace that contains \overline{U} , there is an element $h \in \mathcal{U}(R, \Phi)$ stabilizing \overline{U} and mapping \overline{X} onto a subgroup of $\overline{\mathcal{U}_m}$. Then ${}^h C_W(U)$ is a subgroup of ${}^h g\mathcal{U}_\ell$ that maps onto a subspace of $\overline{\mathcal{U}_m}$. This means that its elements are of the form $(0, dy, \phi_2(y))$ with $\lambda^{m \times m}(\phi_2) = 0$. Since λ is injective the associated character is trivial and therefore ${}^h X \in \mathcal{S}_k$ for some k . \square

Remark 17. *Similar investigations can be done for other Types of codes over finite fields. However for codes over more general Galois rings part (1) of the strong transitivity condition fails in general since the groups \mathcal{U}_j are no longer elementary abelian. Experiments show that already for codes over $\mathbb{Z}/4\mathbb{Z}$ the associated Hecke algebra is not commutative. It would be interesting to generalize the approach to arbitrary finite Galois rings.*

[5] defines the Kneser-Hecke operator T acting on the space \mathcal{V} of formal linear combinations of isometry classes of self-dual isotropic codes of a given Type ρ and length N . Taking the degree- m -complete weight enumerator defines a linear mapping onto the space $\text{Inv}_N(\mathcal{C}_m(\rho))$ with kernel, say, \mathcal{V}_m . For the six cases treated in Theorem 16 the eigenspace decomposition of T on \mathcal{V} is

$$\mathcal{V} = \perp_{k=0}^N Y_k$$

where $Y_k = \mathcal{V}_{k-1} \cap \mathcal{V}_k^\perp$. The linear mapping cwe_m maps this decomposition to the one given in Theorem 8, which is hence the eigenspace decomposition of the linear operator $\delta_m(T)$ on $\text{Inv}_N(\mathcal{C}_m(\rho))$. Therefore $\Delta_N(\mathcal{H}(\mathcal{C}_m(\rho))) = \mathbb{C}[\delta_m(T)]$ by Theorem 16. More precise calculations allow to obtain $\delta_m(T)$ as explicit linear combination of the Hecke operators $\Delta_N(K_1)$ and the identity.

Proposition 18. *The eigenvalue of $\Delta_N(K_1)$ on the space*

$$\text{cwe}_m(Y_{m-\ell}) = \tilde{\varphi}_{m,\ell}(\ker(\Phi_{m-\ell,1})) = \ker(\Delta_N(K_\ell))^\perp \cap \ker(\Delta_N(K_{\ell+1}))$$

in decomposition (4) is

$$c(1, \ell, \ell, 0) + q^{-n}c(1, \ell, \ell, 1) = \frac{q^\ell - 1}{q - 1} + q^{-n} \frac{q^\ell - 1}{q - 1} q^{2m-\ell+e}$$

where $n = N/2$ and $e = 0$ for the cases q^E and q_I^E , $e = 1$ for q_1^E , q_{II}^E , $e = 1/2$ for q_1^H and $e = -1/2$ for q_H .

Proof. Theorem 14 says that

$$K_1 K_\ell = c(1, \ell, \ell, 0)K_\ell + c(1, \ell, \ell, 1)K_\ell\left(\frac{1}{\sqrt{q}}\right) + S$$

where S is a linear combination of $K_j(r)$ with $j > \ell$. In particular $\Delta_N(S)$ acts as 0 on $\text{cwe}_m(Y_{m-\ell})$. Since $\Delta_N(K_\ell)$ acts as a scalar on $\text{cwe}_m(Y_{m-\ell})$ and $\Delta_N(K_\ell(\frac{1}{\sqrt{q}})) = q^{-n}\Delta_N(K_\ell)$ the eigenvalue of $\Delta_N(K_1)$ on this space is $c(1, \ell, \ell, 0) + q^{-n}c(1, \ell, \ell, 1)$ and it remains to calculate $c(1, \ell, \ell, 0)$ and $c(1, \ell, \ell, 1)$. By Theorem 14,

$$c(1, \ell, \ell, 0) = |\{(U, W) \in \mathcal{S}_1 \times \mathcal{S}_\ell \mid WC_U(W) = \mathcal{U}_\ell \text{ and } U = C_U(W)\}|.$$

Since $|W| = |\mathcal{U}_\ell|$ we have $W = \mathcal{U}_\ell$ and U is an arbitrary 1-dimensional subspace of \mathcal{U}_ℓ , so $c(1, \ell, \ell, 0) = \frac{q^\ell - 1}{q - 1}$. Similarly

$$c(1, \ell, \ell, 1) = |\{(U, W) \in \mathcal{S}_1 \times \mathcal{S}_\ell \mid WC_U(W) = \mathcal{U}_\ell \text{ and } C_U(W) = \{1\}\}|.$$

Hence again $W = \mathcal{U}_\ell$ and $U/Z = \langle x + y \rangle$ where $\langle x \rangle$ runs through the 1-dimensional subspaces of $\langle f_1, \dots, f_\ell \rangle$ and y is an arbitrary vector in $\langle e_1, \dots, e_m, f_{\ell+1}, \dots, f_m \rangle$ such that $x + y$ is isotropic with respect to qf in the case q_I^E and with respect to the Hermitian form in the cases q^H and q_1^H . Hence there are

$$\frac{q^\ell - 1}{q - 1} q^{2m-\ell+e'}$$

possibilities for U/Z where $e' = -1, 0, 0, 0, -1/2, -1/2$ in the six cases $q_I^E, q_{II}^E, q^E, q_1^E, q^H, q_1^H$. In the cases q_I^E, q_{II}^E, q_1^E and q_1^H there are q groups $U \in \mathcal{S}_1$ with the same U/Z , in the other two cases there is a unique such U . Hence $c(1, \ell, \ell, 1) = \frac{q^\ell - 1}{q - 1} q^{2m-\ell+e}$ where $e = 0, 1, 0, 1, -1/2, 1/2$ as stated in the theorem. \square

Comparing these eigenvalues with the ones of the Kneser-Hecke operator T from [5] one gets the following corollary.

Corollary 19. *Let n and e be as in Proposition 18. Then*

$$(q - 1)\delta_m(T) = q^{n-m-e}((q - 1)\Delta_N(K_1) + \text{id}) - (q^m + a)\text{id}$$

where a is $q - 1$ for q_I^E , $\sqrt{q} - 1$ for q^H and q_1^H and 0 in the other three cases.

Proof. By [5, Theorem 9] the eigenvalue of $(q - 1)T$ on Y_k is given as $q^{n-k-e} - q^k - a$ where n , e and a are as above. Comparing these with the eigenvalues of K_1 given in Proposition 18 yields the stated formula. \square

References

- [1] 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.
- [2] E. Freitag, *Siegelsche Modulformen*, Springer-Verlag, New York, 1983.
- [3] P. Gérardin, Weil-representations associated to finite fields. *J. Algebra* **46** (1977) 54–101.
- [4] R. Howe, Invariant theory and duality for classical groups over finite fields, with applications to their singular representation theory. Yale Univ., New Haven, Conn. (197?) (unpublished)
- [5] G. Nebe, Kneser-Hecke-operators in coding theory. *Abh. Math. Sem. Univ. Hamburg* (to appear)
- [6] G. Nebe, E. M. Rains and N. J. A. Sloane, The invariants of the Clifford groups, *Designs, Codes, and Cryptography* **24** (2001), 99–121.
- [7] G. Nebe, E. M. Rains and N. J. A. Sloane, Codes and invariant theory, *Math. Nachrichten*, **274–275** (2004), 104–116.
- [8] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-dual codes and invariant theory*. Springer-Verlag ACM 17 (2006).
- [9] H.-G. Quebbemann, On even codes, *Discrete Math.* **98** (1991), 29–34.
- [10] B. Runge, Codes and Siegel modular forms, *Discrete Math.* **148** (1996), 175–204.
- [11] A. Weil, Sur certaines groupes d’opérateurs unitaires, *Acta Math.* **111** (1964), 143–211. *Oeuvres Scientifiques III*, Springer-Verlag, 1979, pp. 1–69.