Hecke operators for codes.

Gabriele Nebe, RWTH Aachen University

Vlora, April 30, 2008

This talk introduces Hecke operators for codes and therewith answers a question raised in 1977 by Michel Broué.

A **lattice** L in Euclidean N-space $E := (\mathbb{R}^N, (,))$ is the $\mathbb{Z}$-span of an $\mathbb{R}$-basis $B = (b_1, \ldots, b_N)$ of E

$$L = \langle b_1, \ldots, b_N \rangle_{\mathbb{Z}} = \{ \sum_{i=1}^{N} a_i b_i \mid a_i \in \mathbb{Z} \}.$$

The **dual lattice** of L is

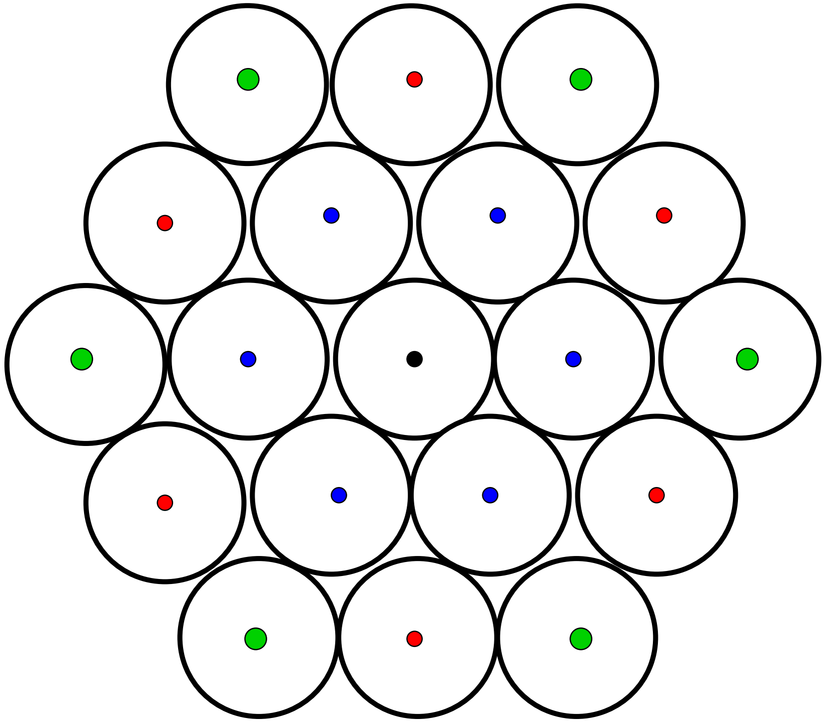
$$L^* := \{ v \in E \mid (v, \ell) \in \mathbb{Z} \forall \ell \in L \}.$$

L is called **integral**, if $L \subset L^*$ or equivalently $(\ell, m) \in \mathbb{Z}$ for all $\ell, m \in L$.
L is called **even**, if $(\ell, \ell) \in 2\mathbb{Z}$ for all $\ell \in L$.
L is called **unimodular**, if $L = L^*$.
The **theta series** of a lattice L is

$$\vartheta_L = \sum_{\ell \in L} q^{(\ell, \ell)}$$

where $q = \exp(\pi i z)$.

The hexagonal lattice.



$$\vartheta_L = 1 + 6q^2 + 6q^6 + 6q^8 + 12q^{14} + 6q^{18} + 6q^{24} + 12q^{26} + 6q^{32} + \ldots$$

Theorem. (Theta transformation formula)

$$\vartheta_{L^*}(z) = (\frac{z}{i})^{-k}\sqrt{\det(L)}\vartheta_L(-\frac{1}{z}) \qquad \text{(where } 2k = N = \dim(L))$$

Hecke's theorem. If $L = L^*$ then $\vartheta_L \in \mathcal{M}_k(\Theta)$ where

$$\Theta = \langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle$$

If $L = L^*$ and L is even, then $\vartheta_L \in \mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z}))$ where

$$\mathrm{SL}_2(\mathbb{Z}) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \rangle$$

We have

$$\mathcal{M}(\Theta) := \bigoplus_{k=0}^{\infty} \mathcal{M}_k(\Theta) = \mathbb{C}[\vartheta_{\mathbb{Z}^2}, \vartheta_{E_8}]$$

and

$$\mathcal{M}(\mathrm{SL}_2(\mathbb{Z})) = \bigoplus_{k=0}^{\infty} \mathcal{M}_{4k}(\Theta) = \mathbb{C}[\vartheta_{E_8}, \vartheta_{\Lambda_{24}}]$$

Construction A.

Let p be a prime and $(b_1,\ldots,b_N)$ be a basis of E such that

$$(b_i,b_j)=\begin{cases} 0 & \text{if } i\neq j \\ 1/p & \text{if } i=j \end{cases}$$

Let $C\leq \mathbb{F}_p^N=\mathbb{Z}^N/p\mathbb{Z}^N$ be a code. Then the **codelattice** L_C is

$$L_C:=\{\sum_{i=1}^N a_ib_i \mid (a_1 \pmod p),\ldots,a_N \pmod p)\in C\}$$

Example. $L_{i_2}=\mathbb{Z}^2$, $L_{e_8}=E_8$ and
$\mathcal{M}(\Theta)=\mathbb{C}[\vartheta_{L_{i_2}},\vartheta_{L_{e_8}}]$, $\mathcal{M}(\mathrm{SL}_2(\mathbb{Z}))=\mathbb{C}[\vartheta_{L_{e_8}},\vartheta_{L_{g_{24}}}]$

Remark. (a) $L_C^*=L_{C^\perp}$, so L_C is unimodular, if C is self-dual.
(b) L_C is even unimodular, if $p=2$ and C is a Type II code.
(c) $\vartheta_{L_C}=\mathrm{cwe}_C(\vartheta_0,\ldots,\vartheta_{p-1})$ where $\vartheta_a=\vartheta_{(a+p\mathbb{Z})b_1}=\sum_{n=-\infty}^{\infty}q^{(a+pn)^2/p}$.

Parallels between lattices and codes.

code	lattice
self-dual code	unimodular lattice
doubly-even self-dual code	even unimodular lattice
weight enumerator	theta series
invariant polynomial	modular form
MacWilliams identity	Theta transformation formula
Gleason's theorem	Hecke's theorem
Molien's theorem	Selberg trace formula
Hamming code e_8	root lattice E_8
Golay code g_{24}	Leech lattice Λ_{24}
Runge's Φ-operator	Siegel's Φ-operator
Kneser-Hecke operators	Hecke operators

Motivation.

Determine linear relations between $\mathrm{cwe}_m(C)$ for $C \in M_N(T) = \{C \leq V^N \mid C \text{ of Type } T\}$.

$M_{16}(\mathrm{II}) = [e_8 \perp e_8] \cup [d_{16}^+]$ and these two codes have the same genus 1 and 2 weight enumerator, but $\mathrm{cwe}_3(e_8 \perp e_8)$ and $\mathrm{cwe}_3(d_{16}^+)$ are linearly independent.

$h(M_{24}(\mathrm{II})) = 9$ and only the genus 6 weight enumerators are linearly independent, there is one relation for the genus 5 weight enumerators.

$h(M_{32}(\mathrm{II})) = 85$ and here the genus 10 weight enumerators are linearly independent, whereas there is a unique relation for the genus 9 weight enumerators.

Three different approaches:

1) Determine all the codes and their weight enumerators.
If $\dim(C) = n = N/2$ there are $\prod_{i=0}^{d-1}(2^n - 2^i)/(2^d - 2^i)$ subspaces of dimension d in C.
$N = 32, d = 10$ yields more than 10^{18} subspaces.

2) Use Molien's theorem:
$\mathrm{Inv}_N(\mathcal{C}_m(\mathrm{II})) = \langle \mathrm{cwe}_m(C) \mid C \in M_N(\mathrm{II}) \rangle$
and if $a_N := \dim(\mathrm{Inv}_N(\mathcal{C}_m(\mathrm{II})))$ then

$$\sum_{N=0}^{\infty} a_N t^N = \frac{1}{|\mathcal{C}_m(\mathrm{II})|} \sum_{g \in \mathcal{C}_m(\mathrm{II})} (\det(1 - tg))^{-1}$$

Problem: $\mathcal{C}_{10}(\mathrm{II}) \leq \mathrm{GL}_{1024}(\mathbb{C})$ has order $> 10^{69}$.

3) Use Hecke operators.

Fix a Type $T = (\mathbb{F}_q, \mathbb{F}_q, \beta, \Phi)$ of self-dual codes over a finite **field** with q elements.

$$M_N(T) = \{C \leq \mathbb{F}_q^N \mid C \text{ of Type } T\} = [C_1] \,\dot\cup\, \ldots \,\dot\cup\, [C_h]$$

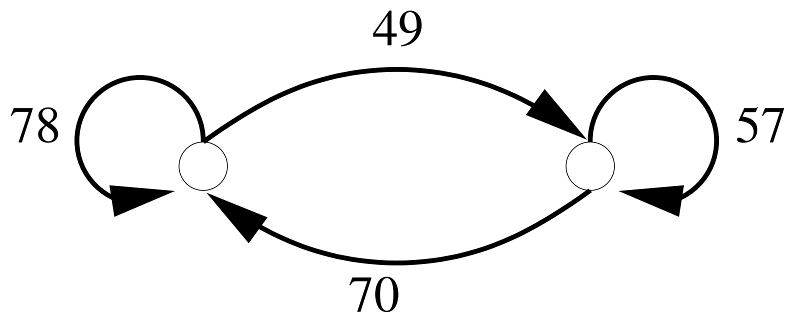
where $[C]$ denotes the **permutation equivalence** class of the code C. Then $n := \frac{N}{2} = \dim(C)$ for all $C \in M_N(T)$.
$C, D \in M_N(T)$ are called **neighbours**, if $\dim(C) - \dim(C \cap D) = 1$, $C \sim D$.

$$\mathcal{V} = \mathbb{C}[C_1] \oplus \ldots \oplus \mathbb{C}[C_h] \cong \mathbb{C}^h$$

$$K_N(T) \in \mathrm{End}(\mathcal{V}),\ K_N(T) : [C] \mapsto \sum_{D \in M_N(T), D \sim C} [D].$$

Kneser-Hecke operator.
(adjacency matrix of neighbouring graph)

Example. $M_{16}(\mathrm{II}) = [e_8 \perp e_8] \cup [d_{16}^{+}]$



$$K_{16}(\mathrm{II}) = \begin{pmatrix} 78 & 49 \\ 70 & 57 \end{pmatrix}$$

$\mathcal{V}$ has a Hermitian positive definite inner product defined by

$$\langle [C_i], [C_j] \rangle := |\operatorname{Aut}(C_i)| \delta_{ij}.$$

Theorem. (N. 2006)
The Kneser-Hecke operator K is a self-adjoint linear operator.

$$\langle v, Kw \rangle = \langle Kv, w \rangle \text{ for all } v, w \in \mathcal{V}.$$

Example. $\frac{7}{10} = \frac{|\operatorname{Aut}(e_8 \perp e_8)|}{|\operatorname{Aut}(d_{16}^+)|}$ hence

$$\operatorname{diag}(7, 10) K_{16}(\mathrm{II})^{\mathrm{Tr}} = K_{16}(\mathrm{II}) \operatorname{diag}(7, 10).$$

$$\mathsf{cwe}_m : \mathcal{V} \to \mathbb{C}[X], \sum_{i=1}^{h} a_i[C_i] \mapsto \sum_{i=1}^{h} a_i \,\mathsf{cwe}_m(C_i)$$

is a linear mapping with kernel

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

Then

$$\mathcal{V} =: \mathcal{V}_{-1} \geq \mathcal{V}_0 \geq \mathcal{V}_1 \geq \ldots \geq \mathcal{V}_n = \{0\}.$$

is a filtration of $\mathcal{V}$ yielding the orthogonal decomposition

$$\mathcal{V} = \bigoplus_{m=0}^{n} \mathcal{Y}_m \text{ where } \mathcal{Y}_m = \mathcal{V}_{m-1} \cap \mathcal{V}_m^{\perp}.$$

$$\mathcal{V}_0 = \{\sum_{i=1}^{h} a_i[C_i] \mid \sum a_i = 0\}$$

and

$$\mathcal{V}_0^{\perp} = \mathcal{Y}_0 = \langle \sum_{i=1}^{h} \frac{1}{|\operatorname{Aut}(C_i)|}[C_i] \rangle.$$

Theorem. (N. 2006)
The space $\mathcal{Y}_m = \mathcal{Y}_m(N)$ is the $K_N(T)$-eigenspace to the eigenvalue $\nu_N^{(m)}(T)$ with $\nu_N^{(m)}(T) > \nu_N^{(m+1)}(T)$ for all m.

Type	$\nu_N^{(m)}(T)$
q_{I}^E	$(q^{n-m} - q - q^m + 1)/(q-1)$
q_{II}^E	$(q^{n-m-1} - q^m)/(q-1)$
q^E	$(q^{n-m} - q^m)/(q-1)$
q_1^E	$(q^{n-m-1} - q^m)/(q-1)$
q^H	$(q^{n-m+1/2} - q^m - q^{1/2} + 1)/(q-1)$
q_1^H	$(q^{n-m-1/2} - q^m - q^{1/2} + 1)/(q-1)$

Corollary. The neighbouring graph is connected.
Proof. The maximal eigenvalue ν_0 of the adjacency matrix is simple with eigenspace $\mathcal{Y}_0$.

Example: $M_{16}(\mathrm{II}) = [e_8 \perp e_8] \cup [d_{16}^+]$
$(2^{8-m-1} - 2^m : m = 0, 1, 2, 3) = (127, 62, 28, 8)$

$$K_{16}(\mathrm{II}) = \begin{pmatrix} 78 & 49 \\ 70 & 57 \end{pmatrix}$$

has eigenvalues 127 and 8 with eigenvectors $(7, 10)$ and $(1, -1)$.
Hence

$$\mathcal{Y}_0 = \langle 7[e_8 \perp e_8] + 10[d_{16}^+] \rangle$$

$$\mathcal{Y}_1 = \mathcal{Y}_2 = 0$$

$$\mathcal{Y}_3 = \langle [e_8 \perp e_8] - [d_{16}^+] \rangle.$$

$M_{24}(\mathrm{II}) = [e_8^3] \cup [e_8 d_{16}] \cup [e_7^2 d_{10}] \cup [d_8^3] \cup [d_{24}] \cup [d_{12}^2] \cup [d_6^4] \cup [d_4^6] \cup [g_{24}]$

$K_{24}(\mathrm{II}) =$

$$\begin{pmatrix}
213 & 147 & 344 & 343 & 0 & 0 & 0 & 0 & 0 \\
70 & 192 & 896 & 490 & 7 & 392 & 0 & 0 & 0 \\
10 & 14 & 504 & 490 & 0 & 49 & 980 & 0 & 0 \\
1 & 3 & 192 & 447 & 0 & 36 & 1152 & 216 & 0 \\
0 & 990 & 0 & 0 & 133 & 924 & 0 & 0 & 0 \\
0 & 60 & 480 & 900 & 1 & 206 & 400 & 0 & 0 \\
0 & 0 & 72 & 216 & 0 & 3 & 1108 & 648 & 0 \\
0 & 0 & 0 & 45 & 0 & 0 & 720 & 1218 & 64 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1771 & 276
\end{pmatrix}$$

m	0	1	2	3	4	5	6
ν_m	2047	1022	508	248	112	32	-32
$\dim(\mathcal{Y}_m)$	1	1	1	2	2	1	1

$$\langle 99[e_8^3] - 297[e_8 d_{16}] - 3465[d_8^3] + 7[d_{24}] + 924[d_{12}^2]$$
$$+4928[d_6^4] - 2772[d_4^6] + 576[g_{24}]\rangle = \ker(\mathrm{cwe}_5) = \mathcal{V}_5$$

The Dimension of $\mathcal{Y}_m(N)$ for doubly-even binary self-dual codes.

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

The Molien series of $\mathcal{C}_m(\mathrm{II})$ is

$$1 + t^8 + a(m)t^{16} + b(m)t^{24} + c(m)t^{32} + \dots$$

where

m	1	2	3	4	5	6	7	8	9	≥ 10
a	1	1	2	2	2	2	2	2	2	2
b	2	3	5	7	8	9	9	9	9	9
c	2	4	9	19	34	55	73	81	84	85

$\dim(\mathcal{Y}_m(N))$ for binary self-dual codes.

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

The Molien series of $\mathcal{C}_m(\mathrm{I})$ is

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

where

$$a_N(m) := \dim\langle\ \mathrm{cwe}_m(C) : C = C^\perp \leq \mathbb{F}_2^N \rangle$$

is given in the following table:

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

A group theoretic interpretation of the Kneser-Hecke operator.

In modular forms theory, Hecke operators are double cosets of the modular group. So I tried to find a similar interpretation for the Kneser-Hecke operator.

Let $T = (R, V, \beta, \Phi)$ be a Type. Then the invariant ring $\mathrm{Inv}(\mathcal{C}_m(T)) = \langle \mathrm{cwe}_m(C) \mid C \text{ of Type } T \rangle$

The finite Siegel Φ-operator

$$\Phi_m : \mathrm{Inv}(\mathcal{C}_m(T)) \to \mathrm{Inv}(\mathcal{C}_{m-1}(T)), \mathrm{cwe}_m(C) \mapsto \mathrm{cwe}_{m-1}(C)$$

defines a surjective graded $\mathbb{C}$-algebra homomorphism between invariant rings of complex matrix groups of different degree. Φ is given by the variable substitution:

$$x_{(v_1,\ldots,v_m)} \mapsto \begin{cases} x_{(v_1,\ldots,v_{m-1})} & \text{if } v_m = 0 \\ 0 & \text{else} \end{cases}$$

Explanation:

$\mathrm{cwe}_{m-1}(C)$ is obtained from $\mathrm{cwe}_m(C)$ by counting only those matrices

$$\begin{array}{cccccc} c_1^{(1)} & c_2^{(1)} & \dots & c_j^{(1)} & \dots & c_N^{(1)} \\ c_1^{(2)} & c_2^{(2)} & \dots & c_j^{(2)} & \dots & c_N^{(2)} \\ \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ c_1^{(m)} & c_2^{(m)} & \dots & c_j^{(m)} & \dots & c_N^{(m)} \\ & & & \uparrow & & \\ & & & v \in V^m & & \end{array}$$

in which the last row is zero.

This is expressed by the variable substitution

$$x_{(v_1,\dots,v_m)} \mapsto \begin{cases} x_{(v_1,\dots,v_{m-1})} & \text{if } v_m = 0 \\ 0 & \text{else} \end{cases}$$

$$(p,q)_m := p(\frac{\partial}{\partial x})(\overline{q}) \text{ for } p,q \in \mathbb{C}[x_v : v \in V^m]_N$$

defines a positive definite Hermitian form on the homogeneous component $\mathbb{C}[x_v : v \in V^m]_N$.

The monomials of degree N form an orthogonal basis and

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

Then $\Phi_m : \ker(\Phi_m)^{\perp} \to \mathrm{Inv}(\mathcal{C}_{m-1}(T))$ is an isomorphism with inverse

$$\varphi_m : \mathrm{Inv}(\mathcal{C}_{m-1}(T)) \to \mathrm{Inv}(\mathcal{C}_m(T)), x_{(v_1,\ldots,v_{m-1})} \mapsto R(x_{(v_1,\ldots,v_{m-1},0)})$$

where $R(p) = \frac{1}{|\mathcal{C}_m(T)|}\sum_{g\in\mathcal{C}_m(T)} p(gx)$ is the **Reynolds operator** (the orthogonal projection onto the invariant ring).
Note that R is not a ring homomorphism.

This yields an orthogonal decomposition of the space of degree N invariants of $\mathcal{C}_m(T)$

$$\mathrm{Inv}_N(\mathcal{C}_m(T)) = \ker(\Phi_m) \perp \varphi_m^{-1}(\mathrm{Inv}_N(\mathcal{C}_{m-1}(T))) =$$

$$\ker(\Phi_m) \perp \varphi_m^{-1}(\ker(\Phi_{m-1}) \perp \varphi_{m-1}^{-1}(\mathrm{Inv}_N(\mathcal{C}_{m-2})(T))) =$$

$$Y_m \perp Y_{m-1} \perp \ldots \perp Y_0$$

such that for all $0 \leq k \leq m$ the mapping

$$\mathrm{cwe}_m : \mathcal{Y}_k \to Y_k.$$

is an isomorphism of vector spaces.

$$\begin{array}{rccccccccc}
\mathcal{V} = & \mathcal{Y}_n & \perp \ldots \perp & \mathcal{Y}_{m+1} & \perp & \mathcal{Y}_m & \perp & \mathcal{Y}_{m-1} & \perp \ldots \perp & \mathcal{Y}_0 \\
\mathrm{cwe}_m & \downarrow & \ldots & \downarrow & & \downarrow & & \downarrow & \ldots & \downarrow \\
\mathrm{Inv}_N(\mathcal{C}_m(T)) = & 0 & \perp \ldots \perp & 0 & \perp & Y_m & \perp & Y_{m-1} & \perp \ldots \perp & Y_0
\end{array}$$

The Kneser-Hecke operator $K_N(T)$ acts on $\mathrm{Inv}_N(\mathcal{C}_m(T))$ as $\delta_m(K_N(T))$ having $Y_m \perp Y_{m-1} \perp \ldots \perp Y_0$ as the eigenspace decomposition.

$$\mathcal{C}_m(T) = \underbrace{S.(\ker(\lambda) \times \ker(\lambda))}_{\mathcal{E}_m(T)} .\mathcal{G}_m(T)$$

Choose a suitable subgroup $\mathcal{U}_1$ of $\mathcal{E}_m(T)$ that corresponds to a 1-dimensional subspace of $(\ker(\lambda) \times \ker(\lambda))$ and let

$$p_1 := \frac{1}{q} \sum_{u \in \mathcal{U}_1} u \in \mathbb{C}^{q^m \times q^m}$$

be the orthogonal projection onto the fixed space of $\mathcal{U}_1$ and let

$$H_m(T) := \mathcal{C}_m(T) p_1 \mathcal{C}_m(T) = \dot{\bigcup}_{U \in X} p_U \mathcal{C}_m(T)$$

then this double coset acts on $\mathrm{Inv}_N(\mathcal{C}_m(T))$ via

$$\Delta_N(H_m(T)) : f \mapsto \frac{1}{|X|} \sum_{U \in X} f(x p_U)$$

Theorem. (N. 2006)

$$(q-1)\delta_m(K_N(T)) = q^{n-m-e}((q-1)\Delta_N(H_m(T))+\mathrm{id})-(q^m+a)\,\mathrm{id}$$

where $n = N/2$ and e, a are as follows:

T	q^E	q_{I}^E	q_1^E	q_{II}^E	q_1^H	q^H
a	0	$q-1$	0	0	$\sqrt{q}-1$	$\sqrt{q}-1$
e	0	0	1	1	$1/2$	$-1/2$

- formal notion of Type $T = (R, V, \beta, \Phi)$.
- self-dual code C of Type T.
- automorphisms and equivalences of codes of a given Type
- mass formula, classifications with Kneser's neighbouring method.
- the associated Clifford-Weil group $\mathcal{C}_m(T)$, a finite complex matrix group of degree $|V|^m$ such that

$$\text{Inv}_N(\mathcal{C}_m(T)) = \langle \text{cwe}_m(C) \mid C = C^\perp \leq V^N \text{ of Type } T \rangle$$

- In particular the scalar subgroup $\mathcal{C}_m(T) \cap \mathbb{C}^* \text{id}$ is cyclic of order

$$\min\{N \mid \text{ there is a code } C \leq V^N \text{ of Type } T\}.$$

- $\mathcal{C}_m(T)$ has a nice group theoretic structure.
- $\Phi_m : \text{Inv}(\mathcal{C}_m(T)) \to \text{Inv}(\mathcal{C}_{m-1}(T))$
- if R is a field then:
- As in modular forms theory, the invariant ring of $\mathcal{C}_m(T)$ can be investigated using Hecke operators.
- The Hecke algebra is generated by the incidence matrix of the Kneser neighbouring graph.
- Obtain linear relations between weight enumerators.