

**Hecke operators for codes.**

Gabriele Nebe, RWTH Aachen University

Ankara, August 29, 2008

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

## 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 $\Lambda_{24}$
Runge's $\Phi$ -operator	Siegel's $\Phi$ -operator
<b>Kneser-Hecke operators</b>	Hecke operators

## Motivation.

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

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

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

$h(M_{32}(\text{II})) = 85$  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:

$\text{Inv}_N(\mathcal{C}_m(\mathbb{II})) = \langle \text{cwe}_m(C) \mid C \in M_N(\mathbb{II}) \rangle$

and if  $a_N := \dim(\text{Inv}_N(\mathcal{C}_m(\mathbb{II})))$  then

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

Problem:  $\mathcal{C}_{10}(\mathbb{II}) \leq \text{GL}_{1024}(\mathbb{C})$  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.

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

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  $\dim(C) - \dim(C \cap D) = 1$ ,  $C \sim D$ .

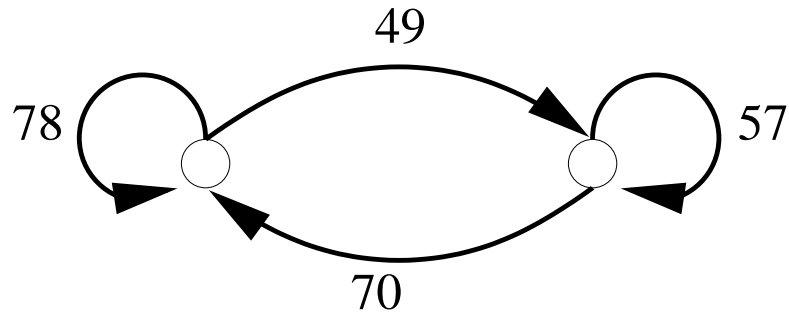
$$\mathcal{V} = \mathbb{C}[C_1] \oplus \dots \oplus \mathbb{C}[C_h] \cong \mathbb{C}^h$$

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

**Kneser-Hecke operator.**

(adjacency matrix of neighbouring graph)

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



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

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

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

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

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

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

is a linear mapping with kernel

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

Then

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

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

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

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

and

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

**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  $\nu_0$  of the adjacency matrix is simple with eigenspace  $\mathcal{Y}_0$ .

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

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

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

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

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

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

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

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

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

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

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

**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	$\geq 10$
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  $\mathcal{C}_m(\text{II})$  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	$\geq 10$
$a$	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  $\mathcal{C}_m(\mathbb{I})$  is

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

where

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

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
$\geq 11$	3	4	7	9	16	25	55	103	261	731	3295

The Kneser-Hecke operator  $K_N(T)$  acts  $\mathbb{C}$ -linearly on

$$\text{Inv}_N(\mathcal{C}_m(T)) = \langle \text{cwe}_m(C) \mid C \in M_N(T) \rangle$$

Call this action  $\Delta_m(K_N(T)) : \text{cwe}_m(C) \mapsto \text{cwe}_m(K_N(T)([C]))$ .

### Hecke operators as double cosets.

Let  $T := (R, V, \beta, \Phi)$  be a Type.

The associated extraspecial group

$$\begin{aligned} \mathcal{E}_m(V, \beta) &:= (V^m \times V^m) : \mathbb{Q}/\mathbb{Z}, \quad \text{with multiplication} \\ (a, b, q)(a', b', q') &= (a + a', b + b', q + q' + \beta(b', a)) \end{aligned}$$

acts irreducibly on  $\mathbb{C}[V^m] = \langle x_v : v \in V^m \rangle_{\mathbb{C}}$  via

$$(a, b, q)x_v := \exp(2\pi i(q + \beta(v, a)))x_{v+b}$$

**Remark.** The associated Clifford-Weil group  $\mathcal{C}_m \leq \text{GL}(\mathbb{C}[V^m])$  normalizes  $\mathcal{E}_m$ .

$\mathcal{U}_j := \{(a, 0, 0) \mid a = (0^{m-j}, a_1, \dots, a_j) \in V^m\} \leq \mathcal{E}_m$  and  $\mathcal{T}_j = \mathcal{C}_m p_{\mathcal{U}_j} \mathcal{C}_m$  where for  $U \leq \mathcal{E}_m$  the endomorphism

$$p_U := \frac{1}{|U|} \sum_{u \in U} u$$

denotes the orthogonal projection onto the fixed space of  $U$ . Note that  $p_U = 0$  if  $U \cap Z \neq \{(0, 0, 0)\}$  where  $Z = \{(0, 0, q) \mid q \in \mathbb{Q}/\mathbb{Z}\} = Z(\mathcal{E}_m)$ .

**Theorem.** (N. 2006) If  $V = R = \mathbb{F}_q$  is a finite field, then

$$\mathcal{H}(\mathcal{C}_m) = \langle \mathcal{T}_j \mid 0 \leq j \leq m \rangle_{\mathbb{C}\text{-algebra}} = \mathbb{C}[\mathcal{T}_1]$$

is a commutative subalgebra of  $\text{End}(\text{Inv}(\mathcal{C}_m))$  consisting of self-adjoint linear operators acting on the subspace of degree  $N$  invariants via, say,  $\delta_N$ .

Then there are explicit constants  $c, d$  (depending on  $q$ , the Type  $T$ , the genus  $m$  and the length  $N$ ) such that

$$\delta_N(\mathcal{T}_1) = c \text{id} + d \Delta_m(K_N(T)).$$