Hecke Operators in Coding Theory

Elisabeth Nossek

RWTH Aachen University

07/20/2009

Codes

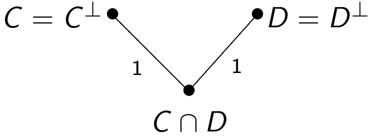
- $C \leq \mathbb{F}_q^N$ is called a linear code over $\mathbb{F}_q$ of length N.
- $b : \mathbb{F}_q^N \times \mathbb{F}_q^N \mapsto \mathbb{F}_q : (x, y) \mapsto \sum_{i=1}^N x_i \overline{y_i}$ be a bilinear or hermitian form.
- $C^\perp := \{v \in \mathbb{F}_q^N | b(c, v) = 0 \, \forall c \in C\}$ is the dual code of C.
- C is called selfdual if $C^\perp = C$, then $\dim(C) = N/2$.

Kneser-Neighbors

- C and D selfdual codes over $\mathbb{F}_q$ with length N are called (1)-neighbors $C \sim D$ iff $\dim(C/C \cap D) = 1$.
- neighboring graph Γ: vertices $\mathcal{F} := \{C \leq \mathbb{F}_q^N | C = C^\perp\}$ and edges between neighbors.
- A adjacency matrix of Γ.

Results about the neighboring graph

- **Theorem**:(Kneser) Γ is connected.
  Determine all selfdual Codes in $\mathcal{F}$ (or $\mathcal{F}$/equivalence) by going through the neighboring graph.



- **Theorem**:(Nebe)
  Description of eigenvalues and eigenspaces of A.

Higher Neighboring Relations

- C and D selfdual codes over $\mathbb{F}_q$ with length N are called k-neighbors $C \sim_k D$ iff $\dim(C/C \cap D) = k$.
- k-neighboring graph Γ_k, A_k adjacency matrix of Γ_k.
- **Question:** Are there polynomials $p_k \in \mathbb{Q}[X]$ such that $A_k = p_k(A)$?

Adjacency Matrices

The powers of adjacency matrices “count” paths through the graph

$$(A^m)_{ij} = |\{\text{paths of length m from i-th to j-th vertex}\}|.$$

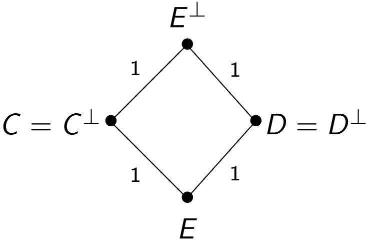
Isometry Group

- $G(\mathbb{F}_q^N, b)$ the group of isometries acts transitively on $\mathcal{F} = \{C \leq \mathbb{F}_q^N | C = C^\perp\}$ (Witt's theorem).
- $G(\mathbb{F}_q^N, b)$ preserves neighboring relations.
- Hence $|\{D \in \mathcal{F} | D \sim_k C\}|$ is independent of the choice of C.

Example

Let $C = C^\perp \leq \mathbb{F}_3^N$

- $G(\mathbb{F}_3^N, b) = O_N(\mathbb{F}_3)$.
- $|\{(N/2-1)\text{-dimensional subspaces of } C\}| = \frac{3^{N/2}-1}{2}$.
- Let E be a fixed $(N/2-1)$-dimensional subspaces of C $|\{D \in \mathcal{F} | E \leq D \leq E^\perp\}| = 2$.
- $|\{D \in \mathcal{F} | D \sim_1 C\}| = \frac{3^{N/2}-1}{2}$.



Decomposition of A^k

Theorem:
Let m_{kr} be the number of paths of length k between $C \sim_r D$ in Γ_1

$$A_1^k = \sum_{r=0}^{k} m_{kr} A_r$$

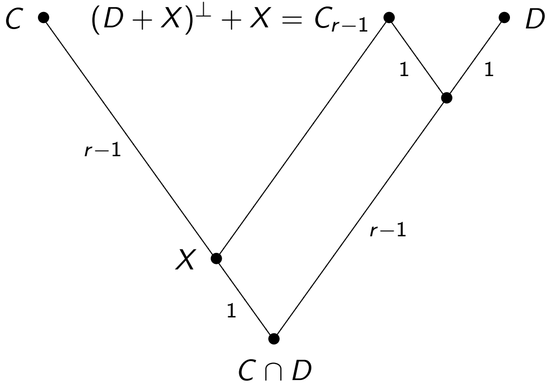
Recursive formula for m_{kr}:

$$m_{kr} = b_{r,r-1} m_{k-1,r-1} + b_{r,r} m_{k-1,r} + b_{r,r+1} m_{k-1,r+1}$$

where $b_{ij} := |\{E \in \mathcal{F} | E \sim_j C \text{ and } E \sim_1 D\}$ for $C \sim_i D$.

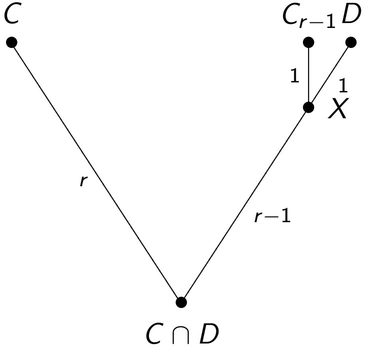
Example continued

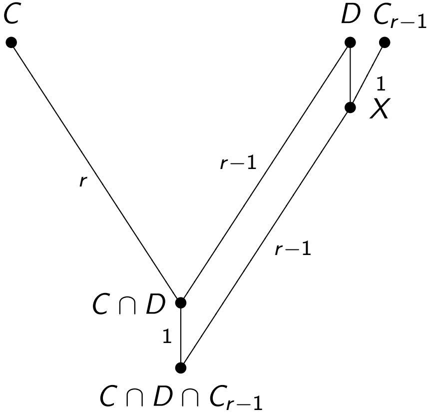
$b_{r,r-1} = \frac{3^r - 1}{2}$



Example continued

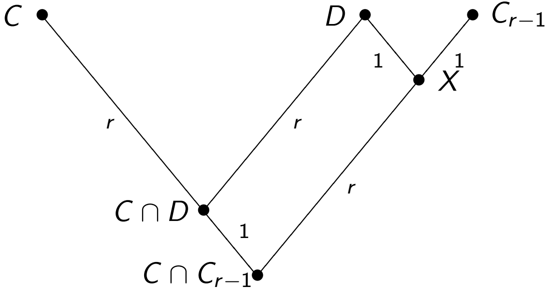
$b_{r,r} = 0$





Example continued

$$b_{r,r+1} = \frac{3^{N/2-r}-1}{2}\left(\frac{3^r-1}{2} - \frac{3^{r-1}-1}{2}\right) = \frac{3^{N/2+1}-3^{r-1}}{2}$$



$$\boxed{m_{kr} = \frac{3^r-1}{2} m_{k-1,r-1} + \frac{3^{N/2+1}-3^{r-1}}{2} m_{k-1,r+1}}$$

Polynomial for A_k

Theorem:
Let $P = (p_{ij})_{0 \leq i,j \leq k} := M^{-1}$ with $M = (m_{ij})_{0 \leq i,j \leq k}$

$$A_k = p_k(A) := \sum_{j=0}^{k} p_{kj} A^j$$

$G(\mathbb{F}_q^N, b)$-linearity

Let $\mathcal{V} := \mathbb{C}^{\mathcal{F}} = \langle e_C | C \in \mathcal{F} \rangle_{\mathbb{C}}$ be a complex vector space:

- $\mathcal{V}$ is a $G(\mathbb{F}_q^N, b)$-permutation module through the action of $G(\mathbb{F}_q^N, b)$ on $\mathcal{F}$
- $$A_k : \mathcal{V} \to \mathcal{V} : e_C \mapsto \sum_{D \sim_k C} e_D$$
- A_k is a $G(\mathbb{F}_q^N, b)$-linear endomorphism on $\mathcal{V}$.
- **Theorem:** $\mathrm{End}_{\mathbb{C}G(\mathbb{F}_q^N, b)}(\mathcal{V}) = \mathbb{C}[A_1]$

Hecke-Operators

Let S_N act on $\mathbb{F}_q^N$ by permuting the components.

- Let $[C]$ be the orbit under the induced action on $\mathcal{F}$
- $\overline{\mathcal{V}} := \langle [C] | C \in \mathcal{F} \rangle$
- Hecke operator:

$$T_k : \overline{\mathcal{V}} \to \overline{\mathcal{V}} : [C] \mapsto \sum_{D \sim_k C} [D]$$

$$A_k : \mathcal{V} \to \mathcal{V} : e_C \mapsto \sum_{D \sim_k C} e_D$$

- **Corollary**: $p_k(T_1) = T_k$

Hecke-Operators

Let S_N act on $\mathbb{F}_q^N$ by permuting the components.

- Let $[C]$ be the orbit under the induced action on $\mathcal{F}$
- $\overline{\mathcal{V}} := \langle [C] | C \in \mathcal{F} \rangle$
- Hecke operator:

$$T_k : \overline{\mathcal{V}} \to \overline{\mathcal{V}} : [C] \mapsto \sum_{D \sim_k C} [D]$$

$$A_k : \mathcal{V} \to \mathcal{V} : e_C \mapsto \sum_{D \sim_k C} e_D$$

- **Corollary**: $p_k(T_1) = T_k$

Example for T_k

- $\mathbb{F}_2$, $N = 8$
- 2 equivalence classes: $[e_8]$ and $[i_2^4]$.
- $T_1 = \begin{bmatrix} 7 & 7 \\ 2 & 12 \end{bmatrix}$.

$$T_2 = \frac{1}{3} T_1^2 - \frac{1}{3} T_1 - \frac{14}{3} I_2$$
$$T_3 = \frac{1}{27} T_1^3 - \frac{4}{21} T_1^2 - \frac{47}{21} T_1 + 2 I_2$$