On automorphism groups of Type II codes.

Gabriele Nebe

Lehrstuhl D für Mathematik

Marseille, April 1, 2009

RWTH AACHEN UNIVERSITY

Binary Codes

A linear binary code of length n is a subspace $C \leq \mathbb{F}_2^n$.

$$C^\perp := \{v \in \mathbb{F}_2^n \mid v \cdot c = \sum_{i=1}^{n} v_i c_i = 0 \text{ for all } c \in C\}$$

Binary Codes

A linear binary code of length n is a subspace $C \leq \mathbb{F}_2^n$.

$$C^{\perp} := \{v \in \mathbb{F}_2^n \mid v \cdot c = \sum_{i=1}^{n} v_i c_i = 0 \text{ for all } c \in C\}$$

self-orthogonal means $C \subset C^{\perp}$ and self-dual means $C = C^{\perp}$.

Binary Codes

A linear binary code of length n is a subspace $C \leq \mathbb{F}_2^n$.

$$C^{\perp} := \{v \in \mathbb{F}_2^n \mid v \cdot c = \sum_{i=1}^{n} v_i c_i = 0 \text{ for all } c \in C\}$$

self-orthogonal means $C \subset C^{\perp}$ and self-dual means $C = C^{\perp}$.

$wt(c) := |\{1 \leq i \leq n \mid c_i \neq 0\}|$ is the Hamming weight of $c \in \mathbb{F}_2^n$
Clear: $C \subset C^{\perp} \Rightarrow \mathrm{wt}(c) \in 2\mathbb{Z}$ for all $c \in C$.

C is called Type II, if $C = C^{\perp}$ and $\mathrm{wt}(c) \in 4\mathbb{Z}$ for all $c \in C$.

Binary Codes

A linear binary code of length n is a subspace $C \leq \mathbb{F}_2^n$.

$$C^\perp := \{v \in \mathbb{F}_2^n \mid v \cdot c = \sum_{i=1}^{n} v_i c_i = 0 \text{ for all } c \in C\}$$

self-orthogonal means $C \subset C^\perp$ and self-dual means $C = C^\perp$.

$wt(c) := |\{1 \leq i \leq n \mid c_i \neq 0\}|$ is the Hamming weight of $c \in \mathbb{F}_2^n$
Clear: $C \subset C^\perp \Rightarrow \mathrm{wt}(c) \in 2\mathbb{Z}$ for all $c \in C$.

C is called Type II, if $C = C^\perp$ and $\mathrm{wt}(c) \in 4\mathbb{Z}$ for all $c \in C$.
Facts:

- $C = C^\perp \leq \mathbb{F}_2^n \Rightarrow n = 2\dim(C)$ is even.
- $C = C^\perp \leq \mathbb{F}_2^n \Rightarrow \mathbf{1} = (1, \ldots, 1) \in C$.
- $C \leq \mathbb{F}_2^n$ Type II $\Rightarrow n \in 8\mathbb{Z}$.

Automorphism groups.

The automorphism group of C is

$$P(C) := \{\pi \in S_n \mid \pi(C) = C\}.$$

Automorphism groups.

The automorphism group of C is

$$P(C) := \{\pi \in S_n \mid \pi(C) = C\}.$$

For a subgroup $G \leq S_n$ we let

$$\mathcal{C}(G) := \{C \leq \mathbb{F}_2^n \mid G \leq P(C)\}$$

the set of all $\mathbb{F}_2 G$-submodules of the permutation module $\mathbb{F}_2^n$.

Automorphism groups.

The automorphism group of C is

$$P(C) := \{\pi \in S_n \mid \pi(C) = C\}.$$

For a subgroup $G \leq S_n$ we let

$$\mathcal{C}(G) := \{C \leq \mathbb{F}_2^n \mid G \leq P(C)\}$$

the set of all $\mathbb{F}_2 G$-submodules of the permutation module $\mathbb{F}_2^n$.
Question:

- Is there $C = C^\perp \in \mathcal{C}(G)$?
- Is there a Type II code $C \in \mathcal{C}(G)$?

Group ring codes.

Thompson, Sloane, Willems and others treat group ring codes, so $G \leq S_G$ via its regular representation.

Then $\mathcal{C}(G) =: \mathcal{C}_{reg}(G)$ are the left ideals of $\mathbb{F}_2 G$.

Group ring codes.

Thompson, Sloane, Willems and others treat group ring codes, so $G \leq S_G$ via its regular representation.

Then $\mathcal{C}(G) =: \mathcal{C}_{reg}(G)$ are the left ideals of $\mathbb{F}_2 G$.

We find the famous and important cyclic codes, if G is cyclic.

Group ring codes.

Thompson, Sloane, Willems and others treat group ring codes, so $G \leq S_G$ via its regular representation.

Then $\mathcal{C}(G) =: \mathcal{C}_{reg}(G)$ are the left ideals of $\mathbb{F}_2 G$.

We find the famous and important cyclic codes, if G is cyclic.

Theorem 1 $\exists C = C^{\perp} \in \mathcal{C}_{reg}(G) \Leftrightarrow |G| \in 2\mathbb{Z}$.

Group ring codes.

Thompson, Sloane, Willems and others treat group ring codes, so $G \leq S_G$ via its regular representation.

Then $\mathcal{C}(G) =: \mathcal{C}_{reg}(G)$ are the left ideals of $\mathbb{F}_2 G$.

We find the famous and important cyclic codes, if G is cyclic.

Theorem 1 $\exists C = C^\perp \in \mathcal{C}_{reg}(G) \Leftrightarrow |G| \in 2\mathbb{Z}$.

Theorem 2 (Sloane, Thompson)
$\exists C = C^\perp \in \mathcal{C}_{reg}(G)$ of Type II
$\Leftrightarrow$
$|G| \in 8\mathbb{Z}$ and the Sylow 2-subgroups of G are not cyclic.

Proof of Theorem 1.

$\Rightarrow$: $C = C^{\perp} \leq \mathbb{F}_2 G \cong \mathbb{F}_2^{|G|}$, then $\dim(C) = \frac{|G|}{2}$, so $|G|$ is even.

Proof of Theorem 1.

$\Rightarrow$: $C = C^\perp \leq \mathbb{F}_2 G \cong \mathbb{F}_2^{|G|}$, then $\dim(C) = \frac{|G|}{2}$, so $|G|$ is even.

$\Leftarrow$: $1 \neq g \in G$, $g^2 = 1$. Then

$$C := \mathbb{F}_2 G(1+g) = C^\perp.$$

Proof of Theorem 1.

$\Rightarrow$: $C = C^{\perp} \leq \mathbb{F}_2 G \cong \mathbb{F}_2^{|G|}$, then $\dim(C) = \frac{|G|}{2}$, so $|G|$ is even.

$\Leftarrow$: $1 \neq g \in G$, $g^2 = 1$. Then

$$C := \mathbb{F}_2 G(1+g) = C^{\perp}.$$

More precisely, write $G = \dot{\bigcup} \{h_i, h_i g\}$, then with respect to $h_1, h_1 g, h_2, h_2 g, \ldots$ C is the rowspace of

$$\begin{array}{cccc} 1\,1 & 0\,0 & \ldots & 0\,0 \\ 0\,0 & 1\,1 & \ddots & 0\,0 \\ \ddots & \ddots & \ddots & \vdots \\ 0\,0 & 0\,0 & \ldots & 1\,1 \end{array}$$

General permutation representations

In joint work with Annika Günther we treat arbitrary permutation groups $G \leq S_n$.

Theorem A $\exists C = C^{\perp} \in \mathcal{C}(G) \Leftrightarrow$ condition (E) is satisfied.

(E) every simple $\mathbb{F}_2G$-module S with $S \cong S^* = \mathrm{Hom}(S, \mathbb{F}_2)$ occurs in $\mathbb{F}_2^n$ with even multiplicity.

General permutation representations

In joint work with Annika Günther we treat arbitrary permutation groups $G \leq S_n$.

Theorem A $\exists C = C^{\perp} \in \mathcal{C}(G) \Leftrightarrow$ condition (E) is satisfied.

(E) every simple $\mathbb{F}_2G$-module S with $S \cong S^* = \mathrm{Hom}(S, \mathbb{F}_2)$ occurs in $\mathbb{F}_2^n$ with even multiplicity.

Remark. Condition (E) is fulfilled, if $|N_G(H_i)/H_i|$ is even where $H_i := \mathrm{Stab}_G(i)$ for $i \in \{1, \ldots, n\}$.

Clear. Theorem A implies Theorem 1.

General permutation representations

In joint work with Annika Günther we treat arbitrary permutation groups $G \leq S_n$.

Theorem A $\exists C = C^{\perp} \in \mathcal{C}(G) \Leftrightarrow$ condition (E) is satisfied.

(E) every simple $\mathbb{F}_2 G$-module S with $S \cong S^* = \mathrm{Hom}(S, \mathbb{F}_2)$ occurs in $\mathbb{F}_2^n$ with even multiplicity.

Theorem B If $C = C^{\perp}$ is of Type II, then $P(C) \leq \mathrm{Alt}_n$.

General permutation representations

In joint work with Annika Günther we treat arbitrary permutation groups $G \leq S_n$.

Theorem A $\exists C = C^\perp \in \mathcal{C}(G) \Leftrightarrow$ condition (E) is satisfied.

(E) every simple $\mathbb{F}_2G$-module S with $S \cong S^* = \mathrm{Hom}(S, \mathbb{F}_2)$ occurs in $\mathbb{F}_2^n$ with even multiplicity.

Theorem B If $C = C^\perp$ is of Type II, then $P(C) \leq \mathrm{Alt}_n$.

Theorem C $\exists C = C^\perp \in \mathcal{C}(G)$ of Type II $\Leftrightarrow$
(a) $n \in 8\mathbb{Z}$,
(b) condition (E) is satisfied, and
(c) $G \leq \mathrm{Alt}_n$.

Theorem 2 follows from Theorem C

Remark: Theorem 2 follows from Theorem C:

Proof:

- Condition (E) for group ring codes is equivalent to even group order.
- The Sylow 2-subgroups of a group of even order are not cyclic precisely if the regular representation of G is contained in the alternating group.

Theorem 2 (Sloane, Thompson)
$\exists C = C^{\perp} \in \mathcal{C}_{reg}(G)$ of Type II
$\Leftrightarrow$
$|G| \in 8\mathbb{Z}$ and the Sylow 2-subgroups of G are not cyclic.

Theorem 2 follows from Theorem C

Remark: Theorem 2 follows from Theorem C:

Proof:

- Condition (E) for group ring codes is equivalent to even group order.
- The Sylow 2-subgroups of a group of even order are not cyclic precisely if the regular representation of G is contained in the alternating group.

Theorem C $\exists C = C^{\perp} \in \mathcal{C}(G)$ of Type II $\Leftrightarrow$
(a) $n \in 8\mathbb{Z}$,
(b) condition (E) is satisfied, and
(c) $G \leq \mathrm{Alt}_n$.

Proof of Theorem A

$\Rightarrow$: $\mathbb{F}_2^n/C^\perp \cong \mathrm{Hom}(C, \mathbb{F}_2)$, so if S is a composition factor of C, then S^* is a composition factor of $\mathbb{F}_2^n/C^\perp$.

$$\underbrace{\mathbb{F}_2^n \supseteq C^\perp}_{S^*} = \underbrace{C \supseteq \{0\}}_{S}$$

$\Leftarrow$: $C \subset C^\perp$ maximal self-orthogonal, then $C^\perp/C$ anisotropic and hence semi-simple,

$$C^\perp/C \cong \perp S_j \text{ with } S_j \cong S_j^* \forall j.$$

$S \perp S$ is hyperbolic since $\mathbb{F}_2 = \{x^2 \mid x \in \mathbb{F}_2\}$.

Theorem A $\exists C = C^\perp \in \mathcal{C}(G) \Leftrightarrow$ condition (E) is satisfied.

Orthogonal groups

Let K be any field, $V = K^{2m}$, $q : V \to K$ a non-degenerate quadratic form of Witt defect 0. This means that there is

$$U \leq V,\ \dim(U) = m,\ q(U) = \{0\}.$$

Fix such a maximal isotropic subspace U.

Orthogonal groups

Let K be any field, $V = K^{2m}$, $q : V \to K$ a non-degenerate quadratic form of Witt defect 0. This means that there is

$$U \leq V,\ \dim(U) = m,\ q(U) = \{0\}.$$

Fix such a maximal isotropic subspace U.

$$O(V,q) := \{g \in \mathrm{GL}(V) \mid q(g(v)) = q(v) \text{ for all } v \in V\}.$$

Orthogonal groups

Let K be any field, $V = K^{2m}$, $q : V \to K$ a non-degenerate quadratic form of Witt defect 0. This means that there is

$$U \leq V, \ \dim(U) = m, \ q(U) = \{0\}.$$

Fix such a maximal isotropic subspace U.

$$O(V,q) := \{g \in \mathrm{GL}(V) \mid q(g(v)) = q(v) \text{ for all } v \in V\}.$$

Dickson homomorphism

$$D : O(V,q) \to \{1,-1\}, g \mapsto (-1)^{m-\dim(U \cap Ug)}$$

is a well defined (independent from U) homomorphism.

Orthogonal groups

Let K be any field, $V = K^{2m}$, $q : V \to K$ a non-degenerate quadratic form of Witt defect 0. This means that there is

$$U \leq V,\ \dim(U) = m,\ q(U) = \{0\}.$$

Fix such a maximal isotropic subspace U.

$$O(V,q) := \{g \in \mathrm{GL}(V) \mid q(g(v)) = q(v) \text{ for all } v \in V\}.$$

Dickson homomorphism

$$D : O(V,q) \to \{1,-1\}, g \mapsto (-1)^{m-\dim(U \cap Ug)}$$

is a well defined (independent from U) homomorphism.

$\mathrm{char}(K) \neq 2 \Rightarrow D(g) = \det(g).$

Orthogonal groups

Let K be any field, $V = K^{2m}$, $q : V \to K$ a non-degenerate quadratic form of Witt defect 0. This means that there is

$$U \leq V,\ \dim(U) = m,\ q(U) = \{0\}.$$

Fix such a maximal isotropic subspace U.

$$O(V,q) := \{g \in \mathrm{GL}(V) \mid q(g(v)) = q(v) \text{ for all } v \in V\}.$$

Dickson homomorphism

$$D : O(V,q) \to \{1,-1\}, g \mapsto (-1)^{m-\dim(U\cap Ug)}$$

is a well defined (independent from U) homomorphism.

$\mathrm{char}(K) \neq 2 \Rightarrow D(g) = \det(g)$.

Theorem. $\mathrm{Stab}_{O(V,q)}(U) \leq \ker(D)$

Proof of Theorem B

Let $n \in 8\mathbb{Z}$.

$$V := \mathbf{1}^\perp / \langle \mathbf{1} \rangle = \{x + \langle \mathbf{1} \rangle \mid x \in \mathbb{F}_2^n, \mathrm{wt}(x) \in 2\mathbb{Z}\}$$

$$q : V \to \mathbb{F}_2, q(x + \langle \mathbf{1} \rangle) := \frac{\mathrm{wt}(x)}{2} + 2\mathbb{Z}.$$

Proof of Theorem B

Let $n \in 8\mathbb{Z}$.

$$V := \mathbf{1}^{\perp}/\langle \mathbf{1} \rangle = \{x + \langle \mathbf{1} \rangle \mid x \in \mathbb{F}_2^n, \mathrm{wt}(x) \in 2\mathbb{Z}\}$$

$$q : V \to \mathbb{F}_2, q(x + \langle \mathbf{1} \rangle) := \frac{\mathrm{wt}(x)}{2} + 2\mathbb{Z}.$$

- q is a well-defined, non-degenerate quadratic form.
- Its associated bilinear form is $\sum x_i y_i$.
- (V, q) has Witt defect 0.

Proof of Theorem B

Let $n \in 8\mathbb{Z}$.

$$V := \mathbf{1}^{\perp}/\langle \mathbf{1} \rangle = \{x + \langle \mathbf{1} \rangle \mid x \in \mathbb{F}_2^n, \mathrm{wt}(x) \in 2\mathbb{Z}\}$$

$$q : V \to \mathbb{F}_2, q(x + \langle \mathbf{1} \rangle) := \frac{\mathrm{wt}(x)}{2} + 2\mathbb{Z}.$$

- q is a well-defined, non-degenerate quadratic form.
- Its associated bilinear form is $\sum x_i y_i$.
- (V, q) has Witt defect 0.
- The maximal isotropic subspaces of (V, q) are precisely the images of the Type II codes in $\mathbb{F}_2^n$.

Proof of Theorem B

Let $n \in 8\mathbb{Z}$.

$$V := \mathbf{1}^{\perp}/\langle \mathbf{1} \rangle = \{x + \langle \mathbf{1} \rangle \mid x \in \mathbb{F}_2^n, \mathrm{wt}(x) \in 2\mathbb{Z}\}$$

$$q : V \to \mathbb{F}_2, q(x + \langle \mathbf{1} \rangle) := \frac{\mathrm{wt}(x)}{2} + 2\mathbb{Z}.$$

- q is a well-defined, non-degenerate quadratic form.
- Its associated bilinear form is $\sum x_i y_i$.
- (V, q) has Witt defect 0.
- The maximal isotropic subspaces of (V, q) are precisely the images of the Type II codes in $\mathbb{F}_2^n$.
- S_n fixes $\mathbf{1}$ and preserves the weight hence embeds into $O(V, q)$.
- The restriction of the Dickson homomorphism $D : S_n \to \{1, -1\}$ is the sign.

Generalization of Theorem B

This shows more general:
Theorem B'. Let $C \leq \mathbb{F}_{2^d}^n$ be a self-dual generalized doubly-even code. Then $P(C) \leq \mathrm{Alt}_n$.

Generalization of Theorem B

This shows more general:
Theorem B'. Let $C \leq \mathbb{F}_{2^d}^n$ be a self-dual generalized doubly-even code. Then $P(C) \leq \mathrm{Alt}_n$.

For odd characteristic, the weight preserving mappings that preserve orthogonality are all permutations and sign changes

$$\{\pm 1\}^n : S_n$$

and one obtains

Theorem B". Let $p > 2$ and $C = C^{\perp} \leq \mathbb{F}_{p^d}^n$. Then $\det(\mathrm{Aut}(C)) = \{1\}$.

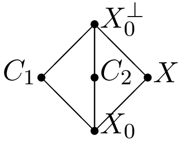
Proof of Theorem C

$\Leftarrow$: Condition (E) $\Rightarrow \exists\, X = X^\perp \in \mathcal{C}(G)$.
X doubly-even, then done ,

Proof of Theorem C

$\Leftarrow$: Condition (E) $\Rightarrow \exists\ X = X^{\perp} \in \mathcal{C}(G)$.
X doubly-even, then done , else

$$X_0 := \{x \in X \mid \mathrm{wt}(x) \in 4\mathbb{Z}\}$$

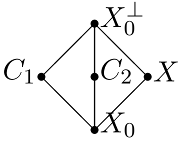


Then $X_0^{\perp}/X_0 \cong \mathbb{F}_2 \oplus \mathbb{F}_2$.

Proof of Theorem C

$\Leftarrow$: Condition (E) $\Rightarrow \exists\ X = X^\perp \in \mathcal{C}(G)$.
X doubly-even, then done , else

$$X_0 := \{x \in X \mid \mathrm{wt}(x) \in 4\mathbb{Z}\}$$



Then $X_0^\perp / X_0 \cong \mathbb{F}_2 \oplus \mathbb{F}_2$.

- C_1 and C_2 are doubly-even.
- $\dim(C_1) - \dim(C_1 \cap C_2) = 1$ is odd.
- $G \leq P(X) \leq P(X_0)$ acts on $\{C_1, C_2\}$.
- $D(G) = \{1\}$ so $C_i g = C_i$ for all $g \in G$, $i = 1, 2$.
- $C_i \in \mathcal{C}(G)$ are Type II.