Non-Existence of Sharply 2-Transitive Sets of Permutations in $\text{Sp}(2d, 2)$

Dominik Barth

University of Würzburg

May 14, 2016
Definitions

Let $\Omega$ be a finite set and $S \subseteq \text{Sym} \Omega$. 
Sharply Transitive Sets — Definitions

Definitions

Let $\Omega$ be a finite set and $S \subseteq \text{Sym} \Omega$.

- $S$ is **sharply transitive**, if for all $\alpha, \beta \in \Omega$ there is a unique $g \in S$ with $\alpha^g = \beta$. 

Observation (Witt)

Sharply 2-transitive subsets of $S_n$ correspond to projective planes of order $n$.

Problem (Hard)

Show the non-existence of sharply 2-transitive sets in 2-transitive subgroups of $S_n$. 
Definitions

Let $\Omega$ be a finite set and $S \subseteq \text{Sym} \Omega$.

- $S$ is **sharply transitive**, if for all $\alpha, \beta \in \Omega$ there is a unique $g \in S$ with $\alpha^g = \beta$.
- $S$ is **sharply 2-transitive**, if $S$ is sharply transitive on $\{(\omega_1, \omega_2) \in \Omega^2 \mid \omega_1 \neq \omega_2\}$.
Sharply Transitive Sets — Definitions

Definitions
Let $\Omega$ be a finite set and $S \subseteq \text{Sym}\,\Omega$.

- $S$ is **sharply transitive**, if for all $\alpha, \beta \in \Omega$ there is a unique $g \in S$ with $\alpha^g = \beta$.
- $S$ is **sharply 2-transitive**, if $S$ is sharply transitive on $\{(\omega_1, \omega_2) \in \Omega^2 \mid \omega_1 \neq \omega_2\}$.

Observation (Witt)
Sharply 2-transitive subsets of $S_n$ correspond to **projective planes** of order $n$. 

Definitions

Let $\Omega$ be a finite set and $S \subseteq \text{Sym} \Omega$.

- $S$ is **sharply transitive**, if for all $\alpha, \beta \in \Omega$ there is a unique $g \in S$ with $\alpha^g = \beta$.
- $S$ is **sharply 2-transitive**, if $S$ is sharply transitive on $\{(\omega_1, \omega_2) \in \Omega^2 \mid \omega_1 \neq \omega_2\}$.

Observation (Witt)

Sharply 2-transitive subsets of $S_n$ correspond to projective planes of order $n$.

Problem (Hard)

Show the non-existence of sharply 2-transitive sets in $S_n$. 
Sharply Transitive Sets — Definitions

Definitions
Let $\Omega$ be a finite set and $S \subseteq \text{Sym } \Omega$.

- $S$ is **sharply transitive**, if for all $\alpha, \beta \in \Omega$ there is a unique $g \in S$ with $\alpha^g = \beta$.
- $S$ is **sharply 2-transitive**, if $S$ is sharply transitive on $\{(\omega_1, \omega_2) \in \Omega^2 \mid \omega_1 \neq \omega_2\}$.

Observation (Witt)
Sharply 2-transitive subsets of $S_n$ correspond to projective planes of order $n$.

Problem (Easier)
Show the non-existence of sharply 2-transitive sets in subgroups of $S_n$. 
Sharply Transitive Sets — Definitions

**Definitions**

Let $\Omega$ be a finite set and $S \subseteq \text{Sym}\,\Omega$.

- $S$ is **sharply transitive**, if for all $\alpha, \beta \in \Omega$ there is a unique $g \in S$ with $\alpha^g = \beta$.
- $S$ is **sharply 2-transitive**, if $S$ is sharply transitive on $\{ (\omega_1, \omega_2) \in \Omega^2 \mid \omega_1 \neq \omega_2 \}$.

**Observation (Witt)**

Sharply 2-transitive subsets of $S_n$ correspond to projective planes of order $n$.

**Problem (Lorimer, 1970s)**

Show the non-existence of sharply 2-transitive sets in 2-transitive subgroups of $S_n$. 
Problem (Lorimer, 1970s)

Show the non-existence of sharply 2-transitive sets in 2-transitive subgroups of $S_n$. 
Sharply Transitive Sets — Results

Problem (Lorimer, 1970s)
Show the non-existence of sharply 2-transitive sets in 2-transitive subgroups of $S_n$.

Theorem (Lorimer, O’Nan, Grundhöfer, Müller, Nagy)
Suppose $G \leq S_n$ contains a sharply 2-transitive subset. Then:

- $G \leq AGL(e(F_p))$, $n = p^e$, or
- $G = A_n$, $n \equiv 0, 1 \mod 4$, or
- $G = S_n$, or
- $G = M_{24}$. 
Sharply Transitive Sets — Results

Problem (Lorimer, 1970s)
Show the non-existence of sharply 2-transitive sets in 2-transitive subgroups of $S_n$.

Theorem (Lorimer, O’Nan, Grundhöfer, Müller, Nagy)
Suppose $G \leq S_n$ contains a sharply 2-transitive subset. Then:
- $G \leq AGL_e(F_p), n = p^e$, or
Problem (Lorimer, 1970s)
Show the non-existence of sharply 2-transitive sets in 2-transitive subgroups of $S_n$.

Theorem (Lorimer, O’Nan, Grundhöfer, Müller, Nagy)
Suppose $G \leq S_n$ contains a sharply 2-transitive subset. Then:
- $G \leq AGL_e(\mathbb{F}_p)$, $n = p^e$, or
- $G = A_n$, $n \equiv 0, 1 \mod 4$, or
Problem (Lorimer, 1970s)

Show the non-existence of sharply 2-transitive sets in 2-transitive subgroups of $S_n$.

Theorem (Lorimer, O’Nan, Grundhöfer, Müller, Nagy)

Suppose $G \leq S_n$ contains a sharply 2-transitive subset. Then:

- $G \leq AGL_e(\mathbb{F}_p)$, $n = p^e$, or
- $G = A_n$, $n \equiv 0, 1 \mod 4$, or
- $G = S_n$, or
Problem (Lorimer, 1970s)

Show the non-existence of sharply 2-transitive sets in 2-transitive subgroups of $S_n$.

Theorem (Lorimer, O’Nan, Grundhöfer, Müller, Nagy)

Suppose $G \leq S_n$ contains a sharply 2-transitive subset. Then:

- $G \leq AGL_e(F_p)$, $n = p^e$, or
- $G = A_n$, $n \equiv 0, 1 \text{ mod } 4$, or
- $G = S_n$, or
- $G = M_{24}$. 
What methods can be used to prove the non-existence of sharply transitive sets?
What methods can be used to prove the non-existence of sharply transitive sets?

- “old”: (Modular) character theory (O’Nan 1984, Grundhöfer-Müller 2009)

Almost all “old” results were reproved using contradicting subsets. Exception: Non-existence of sharply 2-transitive sets in $Sp_{2d}(2, 2)$ of degree $2^d - 1 ± 2^{d-1}$.

(proved by Grundhöfer-Müller)

In this talk: Contradicting subsets for all $Sp_{2d}(2^d, 2^d)$, $d ≥ 4$. 

Groups and Topological Groups 2016 Dominik Barth
What *methods* can be used to prove the non-existence of sharply transitive sets?

- “old”: (Modular) character theory (O’Nan 1984, Grundhöfer-Müller 2009)
- “new”: Contradicting subsets (Müller-Nagy 2011)
What **methods** can be used to prove the non-existence of sharply transitive sets?

- “old”: (Modular) character theory (O’Nan 1984, Grundhöfer-Müller 2009)
- “new”: Contradicting subsets (Müller-Nagy 2011)

Almost all “old” results were **reproved** using contradicting subsets.
What **methods** can be used to prove the non-existence of sharply transitive sets?

- "old": (Modular) character theory (O'Nan 1984, Grundhöfer-Müller 2009)
- "new": Contradicting subsets (Müller-Nagy 2011)

Almost all "old" results were **reproved** using contradicting subsets.

**Exception**

Non-existence of sharply 2-transitive sets in Sp(2d, 2) of degree $2^{2d-1} \pm 2^{d-1}$.

(proved by Grundhöfer-Müller)
What methods can be used to prove the non-existence of sharply transitive sets?

- “old”: (Modular) character theory (O’Nan 1984, Grundhöfer-Müller 2009)
- “new”: Contradicting subsets (Müller-Nagy 2011)

Almost all “old” results were reproved using contradicting subsets.

**Exception**

Non-existence of sharply 2-transitive sets in Sp(2d, 2) of degree $2^{2d-1} \pm 2^{d-1}$.
(proved by Grundhöfer-Müller)

**In this talk**

Contradicting subsets for all Sp(2d, 2), $d \geq 4$
Contradicting Subsets

Lemma (Müller, Nagy)

Let \( S \subseteq \text{Sym}\,\Omega \) be sharply transitive and \( B, C \subseteq \Omega \) arbitrary. Then
Contradicting Subsets

Lemma (Müller, Nagy)

Let $S \subseteq \text{Sym} \Omega$ be \textit{sharply transitive} and $B, C \subseteq \Omega$ arbitrary. Then

$$|B||C| = \sum_{g \in S} |B \cap C^g|.$$
Lemma (Müller, Nagy)

Let $S \subseteq \text{Sym} \Omega$ be sharply transitive and $B, C \subseteq \Omega$ arbitrary. Then

$$|B||C| = \sum_{g \in S} |B \cap C^g|.$$ 

Proof.

Double counting of the set $\{(b, c, g) \in B \times C \times S \mid c^g = b\}$. 

\[ \square \]
Contradicting Subsets

Lemma (Müller, Nagy)
Let $S \subseteq \text{Sym} \Omega$ be sharply transitive and $B, C \subseteq \Omega$ arbitrary. Then

\[ |B||C| = \sum_{g \in S} |B \cap C^g|. \]

Proof.
Double counting of the set $\{(b, c, g) \in B \times C \times S \mid c^g = b\}$. \(\square\)

Definition
Subsets $B, C \subseteq \Omega$ are contradicting subsets (modulo $k$) for $G \leq \text{Sym} \Omega$, if:
Lemma (Müller, Nagy)

Let $S \subseteq \text{Sym} \Omega$ be sharply transitive and $B, C \subseteq \Omega$ arbitrary. Then

$$|B||C| = \sum_{g \in S} |B \cap C^g|.$$

Proof.

Double counting of the set $\{(b, c, g) \in B \times C \times S \mid c^g = b\}$.

Definition

Subsets $B, C \subseteq \Omega$ are contradicting subsets (modulo $k$) for $G \leq \text{Sym} \Omega$, if:

- $k$ divides $|B \cap C^g|$ for all $g \in G$, but...
Lemma (Müller, Nagy)

Let $S \subseteq \text{Sym} \Omega$ be sharply transitive and $B, C \subseteq \Omega$ arbitrary. Then

$$|B||C| = \sum_{g \in S} |B \cap C^g|.$$ 

Proof.

Double counting of the set $\{(b, c, g) \in B \times C \times S \mid c^g = b\}$.

Definition

Subsets $B, C \subseteq \Omega$ are contradicting subsets (modulo $k$) for $G \leq \text{Sym} \Omega$, if:

- $k$ divides $|B \cap C^g|$ for all $g \in G$, but
- $k$ does not divide $|B||C|$.
Lemma (Müller, Nagy)

Let $S \subseteq \text{Sym } \Omega$ be sharply transitive and $B, C \subseteq \Omega$ arbitrary. Then

$$|B||C| = \sum_{g \in S} |B \cap C^g|.$$

Proof.

Double counting of the set $\{(b, c, g) \in B \times C \times S \mid c^g = b\}$. \hfill \square

Definition

Subsets $B, C \subseteq \Omega$ are contradicting subsets (modulo $k$) for $G \leq \text{Sym } \Omega$, if:

- $k$ divides $|B \cap C^g|$ for all $g \in G$, but
- $k$ does not divide $|B||C|$.

$\implies$ \# sharply transitive $S \subseteq G$
Let \((V = \mathbb{F}_2^{2d}, \varphi)\) be a symplectic space, i.e. \(\varphi : V \times V \to \mathbb{F}_2\) is alternating, bilinear, non-degenerate.
Let \((V = \mathbb{F}_2^{2d}, \varphi)\) be a symplectic space,

i.e. \(\varphi : V \times V \to \mathbb{F}_2\) is alternating, bilinear, non-degenerate.

Quadratic forms that polarize to \(\varphi\) :

\[
\Omega := \{\theta : V \to \mathbb{F}_2 \mid \theta(v + w) = \theta(v) + \theta(w) + \varphi(v, w) \quad \forall v, w \in V\}
\]
Let \(( V = \mathbb{F}_2^{2d}, \varphi )\) be a symplectic space,

i.e. \( \varphi : V \times V \rightarrow \mathbb{F}_2 \) is alternating, bilinear, non-degenerate.

Quadratic forms that polarize to \( \varphi \):

\[
\Omega := \{ \theta : V \rightarrow \mathbb{F}_2 \mid \theta(v + w) = \theta(v) + \theta(w) + \varphi(v, w) \quad \forall v, w \in V \}
\]

Singular vectors:

\[
V^0 := \{ v \in V \mid \theta(v) = 0, v \neq 0 \}
\]
Let \((V = \mathbb{F}_2^{2d}, \varphi)\) be a symplectic space,

i.e. \(\varphi : V \times V \to \mathbb{F}_2\) is alternating, bilinear, non-degenerate.

**Quadratic forms that polarize to \(\varphi\):**

\[
\Omega := \{\theta : V \to \mathbb{F}_2 \mid \theta(v + w) = \theta(v) + \theta(w) + \varphi(v, w) \quad \forall v, w \in V\}
\]

**Singular vectors:**

\[
V^0 := \{v \in V \mid \theta(v) = 0, v \neq 0\}
\]

**Observations**
Let \((V = \mathbb{F}_{2}^{2d}, \varphi)\) be a symplectic space, i.e. \(\varphi : V \times V \to \mathbb{F}_{2}\) is alternating, bilinear, non-degenerate.

Quadratic forms that polarize to \(\varphi\):

\[
\Omega := \{ \theta : V \to \mathbb{F}_{2} \mid \theta(v + w) = \theta(v) + \theta(w) + \varphi(v, w) \quad \forall v, w \in V \}
\]

Singular vectors:

\[
V^0 := \{ v \in V \mid \theta(v) = 0, v \neq 0 \}
\]

**Observations**

- \(\text{Sp}(V, \varphi)\) acts on \(\Omega\) via \(\theta^g(v) = \theta(v^g^{-1})\).
The 2-Transitive Actions of $\text{Sp}(2d, 2)$

Let $(V = \mathbb{F}_2^{2d}, \varphi)$ be a symplectic space, i.e. $\varphi : V \times V \to \mathbb{F}_2$ is alternating, bilinear, non-degenerate.

Quadratic forms that polarize to $\varphi$:

$$\Omega := \{ \theta : V \to \mathbb{F}_2 \mid \theta(v + w) = \theta(v) + \theta(w) + \varphi(v, w) \quad \forall v, w \in V \}$$

Singular vectors:

$$V^0 := \{ v \in V \mid \theta(v) = 0, v \neq 0 \}$$

Observations

- $\text{Sp}(V, \varphi)$ acts on $\Omega$ via $\theta^g(v) = \theta(v^{g^{-1}})$.
- 2-transitive on both orbits $\Omega_+$ (Witt index $d$) and $\Omega_-$ (Witt index $d - 1$).
The 2-Transitive Actions of $\text{Sp}(2d, 2)$

Let $(V = \mathbb{F}_2^{2d}, \varphi)$ be a symplectic space, i.e. $\varphi : V \times V \to \mathbb{F}_2$ is alternating, bilinear, non-degenerate.

Quadratic forms that polarize to $\varphi$:

$$\Omega := \{ \theta : V \to \mathbb{F}_2 \mid \theta(v + w) = \theta(v) + \theta(w) + \varphi(v, w) \quad \forall v, w \in V \}$$

Singular vectors:

$$V^0 := \{ v \in V \mid \theta(v) = 0, v \neq 0 \}$$

**Observations**

- $\text{Sp}(V, \varphi)$ acts on $\Omega$ via $\theta^g(v) = \theta(v^{g^{-1}})$.
- 2-transitive on both orbits $\Omega_+$ (Witt index $d$) and $\Omega_-$ (Witt index $d - 1$).
- Fix $\theta \in \Omega_\pm$. Actions of $\text{Sp}(V, \varphi)_\theta = \text{O}(V, \theta)$ on $\Omega_\pm \setminus \{ \theta \}$ and $V^0$ are equivalent.
Contradicting Subsets for $O^\pm(2d,2)$, $d \geq 4$

**Goal**

Show: No sharply 2-transitive sets in $Sp(V,\varphi)$ on both $\Omega_+$ and $\Omega_-$. 

Using contradicting subsets!

**Ingredients for the construction of contradicting subsets:**

- $V = F_2^{2d}$, $d \geq 4$, quadratic form $\theta$ with polar form $\varphi$ non-degenerate
- $U \leq V$ with $4 \leq \dim U \leq \dim V - 4$
- $W := U^\perp = \Rightarrow V = U^\perp W$
- A non-singular vector $c \in V$
Contradicting Subsets for $O^\pm(2d, 2)$, $d \geq 4$

Goal
Show: No sharply 2-transitive sets in $\text{Sp}(V, \varphi)$ on both $\Omega_+$ and $\Omega_-$. 

How to achieve it
Show: No sharply transitive sets in $O(V, \theta) = \text{Sp}(V, \varphi)_{\theta}$ on $V^0$. 

Groups and Topological Groups 2016
Dominik Barth
Contradicting Subsets for $O^\pm(2d,2)$, $d \geq 4$

Goal

Show: No sharply 2-transitive sets in $Sp(V, \varphi)$ on both $\Omega_+$ and $\Omega_-$. 

How to achieve it

Show: No sharply transitive sets in $O(V, \theta) = Sp(V, \varphi)_\theta$ on $V^0$. 

Using contradicting subsets!
Contradicting Subsets for $O^\pm(2d, 2)$, $d \geq 4$

**Goal**
Show: No sharply 2-transitive sets in $Sp(V, \varphi)$ on both $\Omega_+$ and $\Omega_-$. 

**How to achieve it**
Show: No sharply transitive sets in $O(V, \theta) = Sp(V, \varphi)\theta$ on $V^0$.

*Using contradicting subsets!*

**Ingredients for the construction of contradicting subsets:**

1. **Groups and Topological Groups 2016**
Dominik Barth
Contradicting Subsets for $O^\pm(2d, 2), \ d \geq 4$

**Goal**
Show: No sharply 2-transitive sets in $Sp(V, \varphi)$ on both $\Omega_+$ and $\Omega_-$. 

**How to achieve it**
Show: No sharply transitive sets in $O(V, \theta) = Sp(V, \varphi)_\theta$ on $V^0$. 
Using contradicting subsets!

**Ingredients for the construction of contradicting subsets:**
- $V = \mathbb{F}_2^{2d}, \ d \geq 4$, quadratic form $\theta$ with polar form $\varphi$
Contradicting Subsets for $O^\pm(2d, 2), \ d \geq 4$

**Goal**

Show: No sharply 2-transitive sets in $Sp(V, \varphi)$ on both $\Omega_+$ and $\Omega_-$.  

**How to achieve it**

Show: No sharply transitive sets in $O(V, \theta) = Sp(V, \varphi)_\theta$ on $V^0$.  

*Using contradicting subsets!*

**Ingredients for the construction of contradicting subsets:**

- $V = \mathbb{F}_2^{2d}, \ d \geq 4$, quadratic form $\theta$ with polar form $\varphi$
- non-degenerate $U \leq V$ with $4 \leq \dim U \leq \dim V - 4$
Contradicting Subsets for $O^\pm(2d,2)$, $d \geq 4$

Goal
Show: No sharply 2-transitive sets in $Sp(V,\varphi)$ on both $\Omega_+$ and $\Omega_-$.  

How to achieve it
Show: No sharply transitive sets in $O(V,\theta) = Sp(V,\varphi)_\theta$ on $V^0$.  
Using contradicting subsets!

Ingredients for the construction of contradicting subsets:

- $V = \mathbb{F}_2^{2d}$, $d \geq 4$, quadratic form $\theta$ with polar form $\varphi$
- non-degenerate $U \leq V$ with $4 \leq \dim U \leq \dim V - 4$
- $W := U^\perp \implies V = U \perp W$. 

Contradicting Subsets for $O^\pm(2d, 2)$, $d \geq 4$

**Goal**
Show: No sharply 2-transitive sets in $\text{Sp}(V, \varphi)$ on both $\Omega_+$ and $\Omega_-$. 

**How to achieve it**
Show: No sharply transitive sets in $O(V, \theta) = \text{Sp}(V, \varphi)_\theta$ on $V^0$.

**Using contradicting subsets!**

**Ingredients for the construction of contradicting subsets:**

- $V = \mathbb{F}_2^{2d}$, $d \geq 4$, quadratic form $\theta$ with polar form $\varphi$
- non-degenerate $U \leq V$ with $4 \leq \dim U \leq \dim V - 4$
- $W := U^\perp \implies V = U \perp W$
- a non-singular vector $c \in V$
Contradicting Subsets for $\text{O}^\pm(2d, 2)$, $d \geq 4$

Reminder: $V = U \perp W \quad \text{dim } U, W \geq 4 \quad \theta(c) = 1$

**Theorem (B.)**

Setting
Contradicting Subsets for $O^\pm(2d, 2), \; d \geq 4$

Reminder: $V = U \perp W \quad \dim U, W \geq 4 \quad \theta(c) = 1$

Theorem (B.)

Setting

- $B := U^1 + W^1 = \{u + w \mid u \in U, w \in W, \theta(u) = \theta(w) = 1\} \subseteq V^0$
Contradicting Subsets for $\text{O}^\pm(2d, 2), \ d \geq 4$

Reminder: $V = U \perp W \quad \text{dim } U, W \geq 4 \quad \theta(c) = 1$

**Theorem (B.)**

**Setting**

- $B := U^1 + W^1 = \{u + w \mid u \in U, w \in W, \theta(u) = \theta(w) = 1\} \subseteq V^0$
- $C := V^0 \cap c^\perp = \{v \in V \mid \theta(v) = \varphi(v, c) = 0\} \setminus \{0\}$
Contradicting Subsets for $\text{O}^\pm(2d, 2)$, $d \geq 4$

Reminder: $V = U \perp W$ \quad $\dim U, W \geq 4$ \quad $\theta(c) = 1$

### Theorem (B.)

**Setting**

- $B := U^1 + W^1 = \{u + w \mid u \in U, w \in W, \theta(u) = \theta(w) = 1\} \subseteq V^0$
- $C := V^0 \cap c^\perp = \{v \in V \mid \theta(v) = \varphi(v, c) = 0\} \setminus \{0\}$

we have:
**Contradicting Subsets for \(O^\pm(2d, 2), \ d \geq 4\)**

Reminder: \(V = U \bot W\) \(\dim U, W \geq 4\) \(\theta(c) = 1\)

### Theorem (B.)

**Setting**

- \(B := U^1 + W^1 = \{u + w \mid u \in U, w \in W, \theta(u) = \theta(w) = 1\} \subseteq V^0\)
- \(C := V^0 \cap c^\perp = \{v \in V \mid \theta(v) = \varphi(v, c) = 0\} \setminus \{0\}\)

we have:

- \(2^{d-1}\) divides \(|B \cap C^g|\) for all \(g \in O^\pm(2d, 2)\), but
Contradicting Subsets for $O^\pm(2d, 2)$, $d \geq 4$

Reminder: $V = U \perp W$, $\dim U, W \geq 4$, $\theta(c) = 1$

Theorem (B.)

Setting

- $B := U^1 + W^1 = \{u + w \mid u \in U, w \in W, \theta(u) = \theta(w) = 1\} \subseteq V^0$
- $C := V^0 \cap c^\perp = \{v \in V \mid \theta(v) = \varphi(v, c) = 0\} \setminus \{0\}$

we have:

- $2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$, but
- $2^{d-1}$ is no divisor of $|B||C|$. 
Contradicting Subsets for $O^\pm(2d, 2), \ d \geq 4$

Reminder: $V = U \perp W \quad \text{dim } U, W \geq 4 \quad \theta(c) = 1$

**Theorem (B.)**

**Setting**

- $B := U^1 + W^1 = \{u + w \mid u \in U, w \in W, \theta(u) = \theta(w) = 1\} \subseteq V^0$
- $C := V^0 \cap c^\perp = \{v \in V \mid \theta(v) = \varphi(v, c) = 0\} \setminus \{0\}$

we have:

- $2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$, but
- $2^{d-1}$ is no divisor of $|B||C|$.

Thus $B, C$ are contradicting subsets for $O^\pm(2d, 2)$ on $V^0$. 

Contradicting Subsets for $O^\pm(2d, 2)$, $d \geq 4$

Reminder: $V = U \perp W$ \hspace{1cm} dim $U, W \geq 4$ \hspace{1cm} $\theta(c) = 1$

**Theorem (B.)**

Setting

- $B := U^1 + W^1 = \{u + w \mid u \in U, w \in W, \theta(u) = \theta(w) = 1\} \subseteq V^0$
- $C := V^0 \cap c^\perp = \{v \in V \mid \theta(v) = \varphi(v, c) = 0\} \setminus \{0\}$

we have:

- $2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$, but
- $2^{d-1}$ is no divisor of $|B||C|$.

Thus $B, C$ are contradicting subsets for $O^\pm(2d, 2)$ on $V^0$.

**Corollary (Grundhöfer, Müller)**

The symplectic groups $Sp(2d, 2)$, $d \geq 4$, in their actions of degrees $2^{2d-1} \pm 2^{d-1}$, have no sharply 2-transitive subsets.
Proof of the Theorem

Let $V$ be a $2d$-dimensional non-degenerate orthogonal space over $F_2$. Then:

(i) $|V_0| = 2^{2d} - 1 \pm 2^{2d-1} - 1$ and $|V_1| = 2^{2d} - 1 \mp 2^{2d-1} - 1$.

(ii) For $v \in V_1$ we have $|V_1 \cap v^\perp| = |(V_0 \cap v^\perp) \cup \{0\}| = 2^{2d-2}$.

(iii) For $v \in V_1$ we have $|V_1 \setminus v^\perp| = 2^{2d-2} \mp 2^{2d-1}$.

(iv) For $v \in V_0$ we have $|V_1 \setminus v^\perp| = 2^{2d-2}$.

(v) For $v \in V_0$ we have $|V_1 \cap v^\perp| = 2^{2d-2} \mp 2^{2d-1}$.
Proof of the Theorem

Combinatorical building blocks

Let $V$ be a $2d$-dimensional non-degenerate orthogonal space over $F_2$. Then:

(i) $|V_0| = 2^{2d-1} \pm 2^{d-1}$ and $|V_1| = 2^{2d-1}.$

(ii) For $v \in V_1$ we have $|V_1 \cap v^\perp| = |(V_0 \cap v^\perp) \cup \{0\}| = 2^{2d-2}$.

(iii) For $v \in V_1$ we have $|V_1 \setminus v^\perp| = 2^{2d-2} \mp 2^{d-1}$.

(iv) For $v \in V_0$ we have $|V_1 \setminus v^\perp| = 2^{2d-2}$.

(v) For $v \in V_0$ we have $|V_1 \cap v^\perp| = 2^{2d-2} \mp 2^{d-1}$.
Proof of the Theorem

Combinatorical building blocks

Let $V$ be a $2d$-dimensional non-degenerate orthogonal space over $\mathbb{F}_2$. Then:

(i) $|V_0| = 2^{2d-1} \pm V_2^{d-1}$ and $|V_1| = 2^{2d-1} \mp V_2^{d-1}$.

(ii) For $v \in V_1$ we have $|V_1 \cap v^\perp| = |(V_0 \cap v^\perp) \cup \{0\}| = 2^{2d-2}$.

(iii) For $v \in V_1$ we have $|V_1 \setminus v^\perp| = 2^{2d-2} \mp V_2^{d-1}$.

(iv) For $v \in V_0$ we have $|V_1 \setminus v^\perp| = 2^{2d-2}$.

(v) For $v \in V_0$ we have $|V_1 \cap v^\perp| = 2^{2d-2} \mp V_2^{d-1}$.
Combinatorical building blocks

Let \( V \) be a \( 2d \)-dimensional non-degenerate orthogonal space over \( \mathbb{F}_2 \). Then:

(i) \( |V^0| = 2^{2d-1} \pm_v 2^{d-1} - 1 \) and \( |V^1| = 2^{2d-1} \mp_v 2^{d-1} \).

(ii) For \( v \in V^1 \) we have \( |V^1 \cap v^\perp| = |(V^0 \cap v^\perp) \cup \{0\}| = 2^{2d-2} \).

(iii) For \( v \in V^1 \) we have \( |V^1 \setminus v^\perp| = 2^{2d-2} \mp_v 2^{d-1} \).

(iv) For \( v \in V^0 \) we have \( |V^1 \setminus v^\perp| = 2^{2d-2} \).

(v) For \( v \in V^0 \) we have \( |V^1 \cap v^\perp| = 2^{2d-2} \mp_v 2^{d-1} \).
Proof of the Theorem

Combinatorical building blocks

Let $V$ be a $2d$-dimensional non-degenerate orthogonal space over $\mathbb{F}_2$. Then:

(i) $|V^0| = 2^{2d-1} \pm 2^{d-1} - 1$ and $|V^1| = 2^{2d-1} \mp 2^{d-1}$.

(ii) For $v \in V^1$ we have $|V^1 \cap v^\perp| = |(V^0 \cap v^\perp) \cup \{0\}| = 2^{2d-2}$.

(iii) For $v \in V^1$ we have $|V^1 \setminus v^\perp| = 2^{2d-2} \mp 2^{d-1}$.

(iv) For $v \in V^0$ we have $|V^1 \setminus v^\perp| = 2^{2d-2}$.

(v) For $v \in V^0$ we have $|V^1 \cap v^\perp| = 2^{2d-2} \mp 2^{d-1}$.

Proof.

Simple: One-two-line proofs for each statement.
Proof of the Theorem

Lemma

$|B| |C|$ is not divisible by $2^{d-1}$.
Proof of the Theorem

Lemma

\(|B||C| \text{ is not divisible by } 2^{d-1}.

Proof.
Proof of the Theorem

**Lemma**

$|B| |C|$ is not divisible by $2^{d-1}$.

**Proof.**

- $|C| = |V^0 \cap c^\perp| = $
Proof of the Theorem

<table>
<thead>
<tr>
<th>Lemma</th>
</tr>
</thead>
</table>

$|B| |C|$ is **not** divisible by $2^{d-1}$.

<table>
<thead>
<tr>
<th>Proof.</th>
</tr>
</thead>
</table>

- $|C| = |V^0 \cap c^\perp| = 2^{2d-2} - 1$ is odd.
Proof of the Theorem

Lemma

$|B||C|$ is not divisible by $2^{d-1}$.

Proof.

- $|C| = |V^0 \cap c^\perp| = 2^{2d-2} - 1$ is odd.
- Let $\dim U = 2a$, $\dim W = 2b$. Then
Proof of the Theorem

Lemma

\(|B| |C| \) is not divisible by \(2^{d-1}\).

Proof.

- \(|C| = |V^0 \cap c^\perp| = 2^{2d-2} - 1\) is odd.
- Let \(\dim U = 2a\), \(\dim W = 2b\). Then

\[
|B| = |U^1 + W^1| = |U^1||W^1| = (2^{2a-1} \uplus U 2^{a-1})(2^{2b-1} \uplus W 2^{b-1})
\]
Proof of the Theorem

Lemma

$|B||C|$ is not divisible by $2^{d-1}$.

Proof.

- $|C| = |V^0 \cap c^\perp| = 2^{2d-2} - 1$ is odd.
- Let dim $U = 2a$, dim $W = 2b$. Then

  $$|B| = |U^1 + W^1| = |U^1||W^1| = (2^{2a-1} \oplus_U 2^{a-1})(2^{2b-1} \oplus_W 2^{b-1})$$

  is not divisible by $2^{d-1}$ (using $a + b = d$).
Proof of the Theorem

Lemma

$|B||C|$ is not divisible by $2^{d-1}$.

Proof.

- $|C| = |V^0 \cap c^\perp| = 2^{2d-2} - 1$ is odd.
- Let $\dim U = 2a$, $\dim W = 2b$. Then

$$|B| = |U^1 + W^1| = |U^1||W^1| = (2^{2a-1} \oplus_U 2^{a-1})(2^{2b-1} \oplus_W 2^{b-1})$$

is not divisible by $2^{d-1}$ (using $a + b = d$).

- Together: $|B||C|$ is not divisible by $2^{d-1}$.
Proof of the Theorem

Lemma

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$. 

Proof.

Note that $B \cap C^g = B \cap (V_0 \cap c_\perp^g) = B \cap (c_\perp^g)$ and decompose $c_\perp^g = x + y$ with $x \in U, y \in W$. Then:

$|B \cap C^g| = |B \cap (c_\perp^g) \perp| = \{|u + w| : u \in U_1, w \in W_1, \varphi(u + w, c_\perp^g) = 0\}| = \{|(u, w) \in U_1 \times W_1 | \varphi(u, x + y) + \varphi(w, x + y) = 0\}| = \{|(u, w) \in U_1 \times W_1 | \varphi(u, x) + \varphi(w, y) = 0\}| = |U_1 \cap x_\perp \cdot |W_1 \cap y_\perp| + |U_1 \setminus x_\perp \cdot |W_1 \setminus y_\perp|.$

Building blocks $\Rightarrow$ this term is divisible by $2^{d-1}$. 

Groups and Topological Groups 2016 Dominik Barth
Proof of the Theorem

Lemma

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$.

Proof.

Note that

$$B \cap C^g = B \cap (V^0 \cap c^\perp)^g = B \cap (c^g)^\perp.$$
Lemma

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$.

Proof.

Note that

$$B \cap C^g = B \cap (V^0 \cap c^\perp)^g = B \cap (c^g)^\perp$$

and decompose $c^g = x + y$ with $x \in U$, $y \in W$. Then:
Proof of the Theorem

Lemma

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$.

Proof.

Note that

$$B \cap C^g = B \cap (V^0 \cap c^\perp)^g = B \cap (c^g)^\perp$$

and decompose $c^g = x + y$ with $x \in U$, $y \in W$. Then:

$$|B \cap C^g| = |B \cap (c^g)^\perp| = |\{u + w \mid u \in U^1, w \in W^1, \varphi(u + w, c^g) = 0\}|$$
Proof of the Theorem

Lemma

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$.

Proof.

Note that

$$B \cap C^g = B \cap (V^0 \cap c^\perp)^g = B \cap (c^g)^\perp$$

and decompose $c^g = x + y$ with $x \in U$, $y \in W$. Then:

$$|B \cap C^g| = |B \cap (c^g)^\perp| = |\{u + w \mid u \in U^1, w \in W^1, \varphi(u + w, c^g) = 0\}|$$

$$= |\{(u, w) \in U^1 \times W^1 \mid \varphi(u, c^g) + \varphi(w, c^g) = 0\}|$$
Proof of the Theorem

Lemma

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$.

Proof.

Note that

$$B \cap C^g = B \cap (V^0 \cap c^\perp)^g = B \cap (c^g)^\perp$$

and decompose $c^g = x + y$ with $x \in U$, $y \in W$. Then:

$$|B \cap C^g| = |B \cap (c^g)^\perp| = |\{u + w | u \in U^1, w \in W^1, \varphi(u + w, c^g) = 0\}|$$

$$= |\{(u, w) \in U^1 \times W^1 | \varphi(u, c^g) + \varphi(w, c^g) = 0\}|$$

Building blocks $\Rightarrow$ this term is divisible by $2^{d-1}$. 

Groups and Topological Groups 2016 Dominik Barth
Proof of the Theorem

**Lemma**

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$.

**Proof.**

Note that

$$B \cap C^g = B \cap (V^0 \cap c^\perp)^g = B \cap (c^g)^\perp$$

and decompose $c^g = x + y$ with $x \in U$, $y \in W$. Then:

$$|B \cap C^g| = |B \cap (c^g)^\perp| = |\{u + w \mid u \in U^1, w \in W^1, \varphi(u + w, c^g) = 0\}|$$

$$= |\{(u, w) \in U^1 \times W^1 \mid \varphi(u, c^g) + \varphi(w, c^g) = 0\}|$$

$$= |\{(u, w) \in U^1 \times W^1 \mid \varphi(u, x + y) + \varphi(w, x + y) = 0\}|$$

$$= |\{(u, w) \in U^1 \times W^1 \mid \varphi(u, x) + \varphi(w, y) = 0\}|$$
Proof of the Theorem

Lemma

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$.

Proof.

Note that

$$B \cap C^g = B \cap (V^0 \cap c^\perp)^g = B \cap (c^g)^\perp$$

and decompose $c^g = x + y$ with $x \in U$, $y \in W$. Then:

$$|B \cap C^g| = |B \cap (c^g)^\perp| = \{|u + w \mid u \in U^1, w \in W^1, \varphi(u + w, c^g) = 0\}|$$

$$= \{|(u, w) \in U^1 \times W^1 \mid \varphi(u, c^g) + \varphi(w, c^g) = 0\}|$$

$$= \{|(u, w) \in U^1 \times W^1 \mid \varphi(u, x + y) + \varphi(w, x + y) = 0\}|$$

$$= \{|(u, w) \in U^1 \times W^1 \mid \varphi(u, x) + \varphi(w, y) = 0\}|$$

$$= |U^1 \cap x^\perp| \cdot |W^1 \cap y^\perp| + |U^1 \setminus x^\perp| \cdot |W^1 \setminus y^\perp|.$$
Proof of the Theorem

Lemma

$2^{d-1}$ divides $|B \cap C^g|$ for all $g \in O^\pm(2d, 2)$.

Proof.

Note that

$$B \cap C^g = B \cap (V^0 \cap c^\perp)^g = B \cap (c^g)^\perp$$

and decompose $c^g = x + y$ with $x \in U$, $y \in W$. Then:

$$|B \cap C^g| = |B \cap (c^g)^\perp| = |\{u + w \mid u \in U^1, w \in W^1, \varphi(u + w, c^g) = 0\}|$$

$$= |\{(u, w) \in U^1 \times W^1 \mid \varphi(u, c^g) + \varphi(w, c^g) = 0\}|$$

$$= |\{(u, w) \in U^1 \times W^1 \mid \varphi(u, x + y) + \varphi(w, x + y) = 0\}|$$

$$= |\{(u, w) \in U^1 \times W^1 \mid \varphi(u, x) + \varphi(w, y) = 0\}|$$

$$= |U^1 \cap x^\perp| \cdot |W^1 \cap y^\perp| + |U^1 \setminus x^\perp| \cdot |W^1 \setminus y^\perp|.$$

Building blocks $\implies$ this term is divisible by $2^{d-1}$. 

\[\square\]
Contradicting subsets for $O^\pm(2d, 2)$, $d \geq 4$, and therefore for $Sp(2d, 2)$.
Summary and Outlook

- Contradicting subsets for $O^{\pm}(2d, 2)$, $d \geq 4$, and therefore for $Sp(2d, 2)$
- Still open: $A_n$, $S_n$, $M_{24}$.
Summary and Outlook

- Contradicting subsets for $O^\pm(2d, 2), d \geq 4$, and therefore for $Sp(2d, 2)$
- Still open: $A_n, S_n, M_{24}$.
- Unfortunately, contradicting subsets (probably) won’t help here:
  Non-existence of contradicting subsets for $S_n$ of degree $n(n-1)$ for all $n \leq 100$
For Further Reading

Thank you for your attention!

P. Lorimer.
Finite projective planes and sharply 2-transitive subsets of finite groups.

M. O’Nan.
Sharply 2-transitive sets of permutations.

T. Grundhöfer and P. Müller.
Sharply 2-transitive sets of permutations and groups of affine projectivities.

P. Müller and G. P. Nagy.
On the non-existence of sharply transitive sets of permutations in certain finite permutation groups.

D. B.
The non-existence of sharply 2-transitive sets of permutations in $\text{Sp}(2d, 2)$ of degree $2^{2d-1} \pm 2^{d-1}$