Spreading primitive groups of diagonal type do not exist

# Saul D. Freedman

#### The University of Western Australia

Joint work with John Bamberg and Michael Giudici

45th Australasian Combinatorics Conference December 15, 2023

Let G be a finite transitive permutation group on a finite set  $\Omega$ .

Let G be a finite transitive permutation group on a finite set  $\Omega$ .

G is primitive if  $\Omega$  has no nontrivial G-invariant partitions.

Let G be a finite transitive permutation group on a finite set  $\Omega$ .

G is primitive if  $\Omega$  has no nontrivial G-invariant partitions.

2-transitive (point stabiliser has two orbits on  $\Omega$ )  $\implies$  primitive.

Let G be a finite transitive permutation group on a finite set  $\Omega$ .

G is primitive if  $\Omega$  has no nontrivial G-invariant partitions.

2-transitive (point stabiliser has two orbits on  $\Omega$ )  $\implies$  primitive.

Araújo, Cameron and Steinberg's (2017) synchronisation hierarchy of permutation groups:

Let G be a finite transitive permutation group on a finite set  $\Omega$ .

G is primitive if  $\Omega$  has no nontrivial G-invariant partitions.

2-transitive (point stabiliser has two orbits on  $\Omega$ )  $\implies$  primitive.

Araújo, Cameron and Steinberg's (2017) synchronisation hierarchy of permutation groups:

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

Let G be a finite transitive permutation group on a finite set  $\Omega$ .

G is primitive if  $\Omega$  has no nontrivial G-invariant partitions.

2-transitive (point stabiliser has two orbits on  $\Omega$ )  $\implies$  primitive.

Araújo, Cameron and Steinberg's (2017) synchronisation hierarchy of permutation groups:

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

Synchronising and separating: conditions related to graphs defined on  $\boldsymbol{\Omega}$  and preserved by G.

Let G be a finite transitive permutation group on a finite set  $\Omega$ .

G is primitive if  $\Omega$  has no nontrivial G-invariant partitions.

2-transitive (point stabiliser has two orbits on  $\Omega$ )  $\implies$  primitive.

Araújo, Cameron and Steinberg's (2017) synchronisation hierarchy of permutation groups:

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

Synchronising and separating: conditions related to graphs defined on  $\boldsymbol{\Omega}$  and preserved by G.

Spreading: conditions related to sets and multisets of elements of  $\Omega$ .

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

O'Nan-Scott Theorem – Primitive groups are of almost simple, affine, diagonal, product or twisted wreath type.

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

O'Nan-Scott Theorem – Primitive groups are of almost simple, affine, diagonal, product or twisted wreath type.

2-transitive  $\implies$  almost simple or affine.

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

O'Nan-Scott Theorem – Primitive groups are of almost simple, affine, diagonal, product or twisted wreath type.

2-transitive  $\implies$  almost simple or affine.

Synchronising  $\implies$  almost simple, affine or diagonal (Araújo, Cameron & Steinberg, 2017).

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

O'Nan-Scott Theorem – Primitive groups are of almost simple, affine, diagonal, product or twisted wreath type.

2-transitive  $\implies$  almost simple or affine.

Synchronising  $\implies$  almost simple, affine or diagonal (Araújo, Cameron & Steinberg, 2017).

Where do diagonal groups fit in?

2-transitive  $\implies$  spreading  $\implies$  separating  $\implies$  synchronising  $\implies$  primitive.

O'Nan-Scott Theorem – Primitive groups are of almost simple, affine, diagonal, product or twisted wreath type.

2-transitive  $\implies$  almost simple or affine.

Synchronising  $\implies$  almost simple, affine or diagonal (Araújo, Cameron & Steinberg, 2017).

Where do diagonal groups fit in?

Bray, Cai, Cameron, Spiga & Zhang (2020): For affine and diagonal groups, synchronising  $\iff$  separating.

#### Theorem (Bray, Cai, Cameron, Spiga & Zhang, 2020)

Let G be a synchronising diagonal group. Then G has socle  $T \times T$  for some non-abelian finite simple group T.

#### Theorem (Bray, Cai, Cameron, Spiga & Zhang, 2020)

Let G be a synchronising diagonal group. Then G has socle  $T \times T$  for some non-abelian finite simple group T.

Let  $\Omega := T$ . The diagonal groups with socle  $T \times T$  are the groups G acting on  $\Omega$  where:

#### Theorem (Bray, Cai, Cameron, Spiga & Zhang, 2020)

Let G be a synchronising diagonal group. Then G has socle  $T \times T$  for some non-abelian finite simple group T.

Let  $\Omega := T$ . The diagonal groups with socle  $T \times T$  are the groups G acting on  $\Omega$  where:

• 
$$T \times T \leq G \leq W(T) := \langle T \times T, \operatorname{Aut}(T), \sigma \rangle;$$

#### Theorem (Bray, Cai, Cameron, Spiga & Zhang, 2020)

Let G be a synchronising diagonal group. Then G has socle  $T \times T$  for some non-abelian finite simple group T.

Let  $\Omega := T$ . The diagonal groups with socle  $T \times T$  are the groups G acting on  $\Omega$  where:

• 
$$T \times T \leq G \leq W(T) := \langle T \times T, \operatorname{Aut}(T), \sigma \rangle;$$

• for  $(t_1, t_2) \in T \times T$  and  $s \in \Omega$ , we have  $s^{(t_1, t_2)} := t_1^{-1} s t_2$ ;

#### Theorem (Bray, Cai, Cameron, Spiga & Zhang, 2020)

Let G be a synchronising diagonal group. Then G has socle  $T \times T$  for some non-abelian finite simple group T.

Let  $\Omega := T$ . The diagonal groups with socle  $T \times T$  are the groups G acting on  $\Omega$  where:

• 
$$T \times T \leq G \leq W(T) := \langle T \times T, \operatorname{Aut}(T), \sigma \rangle;$$

• for  $(t_1, t_2) \in T \times T$  and  $s \in \Omega$ , we have  $s^{(t_1, t_2)} := t_1^{-1} s t_2$ ;

• Aut(T) acts naturally on  $\Omega$ ;

#### Theorem (Bray, Cai, Cameron, Spiga & Zhang, 2020)

Let G be a synchronising diagonal group. Then G has socle  $T \times T$  for some non-abelian finite simple group T.

Let  $\Omega := T$ . The diagonal groups with socle  $T \times T$  are the groups G acting on  $\Omega$  where:

- $T \times T \leq G \leq W(T) := \langle T \times T, \operatorname{Aut}(T), \sigma \rangle;$
- for  $(t_1, t_2) \in T \times T$  and  $s \in \Omega$ , we have  $s^{(t_1, t_2)} := t_1^{-1} s t_2$ ;
- Aut(T) acts naturally on  $\Omega$ ;
- and  $s^{\sigma} := s^{-1}$ .

#### Theorem (Bray, Cai, Cameron, Spiga & Zhang, 2020)

Let G be a synchronising diagonal group. Then G has socle  $T \times T$  for some non-abelian finite simple group T.

Let  $\Omega := T$ . The diagonal groups with socle  $T \times T$  are the groups G acting on  $\Omega$  where:

• 
$$T \times T \leq G \leq W(T) := \langle T \times T, \operatorname{Aut}(T), \sigma \rangle;$$

- for  $(t_1, t_2) \in T \times T$  and  $s \in \Omega$ , we have  $s^{(t_1, t_2)} := t_1^{-1} s t_2$ ;
- Aut(T) acts naturally on  $\Omega$ ;
- and  $s^{\sigma} := s^{-1}$ .

#### Theorem (Bamberg, Giudici, Lansdown & Royle, 2022)

The diagonal group  $PSL_2(q) \times PSL_2(q)$  is synchronising for q = 13 and q = 17, and non-spreading for all q.

Question: Do spreading groups of diagonal type exist?

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

J is trivial if  $\mu_J$  is constant on  $\Omega$ , or if  $\mu_J(\alpha) \neq 0$  for a unique  $\alpha$ .

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

J is trivial if  $\mu_J$  is constant on  $\Omega$ , or if  $\mu_J(\alpha) \neq 0$  for a unique  $\alpha$ .

#### Definition

A transitive permutation group G on  $\Omega$  is non-spreading if:

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

J is trivial if  $\mu_J$  is constant on  $\Omega$ , or if  $\mu_J(\alpha) \neq 0$  for a unique  $\alpha$ .

#### Definition

A transitive permutation group G on  $\Omega$  is non-spreading if:

 $\exists$  a nontrivial subset X of  $\Omega$  and a nontrivial multiset J of  $\Omega$  such that:

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

J is trivial if  $\mu_J$  is constant on  $\Omega$ , or if  $\mu_J(\alpha) \neq 0$  for a unique  $\alpha$ .

#### Definition

A transitive permutation group G on  $\Omega$  is non-spreading if:

 $\exists$  a nontrivial subset X of  $\Omega$  and a nontrivial multiset J of  $\Omega$  such that: |J| divides  $|\Omega|$ , and for all  $g \in G$ , the sum  $\sum_{\alpha \in X_F} \mu_J(\alpha)$  is constant.

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

J is trivial if  $\mu_J$  is constant on  $\Omega$ , or if  $\mu_J(\alpha) \neq 0$  for a unique  $\alpha$ .

#### Definition

A transitive permutation group G on  $\Omega$  is non-spreading if:

 $\exists$  a nontrivial subset X of  $\Omega$  and a nontrivial multiset J of  $\Omega$  such that: |J| divides  $|\Omega|$ , and for all  $g \in G$ , the sum  $\sum_{\alpha \in Xg} \mu_J(\alpha)$  is constant.

Otherwise, G is spreading.

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

J is trivial if  $\mu_J$  is constant on  $\Omega$ , or if  $\mu_J(\alpha) \neq 0$  for a unique  $\alpha$ .

#### Definition

A transitive permutation group G on  $\Omega$  is non-spreading if:

 $\exists$  a nontrivial subset X of  $\Omega$  and a nontrivial multiset J of  $\Omega$  such that:

|J| divides  $|\Omega|$ , and for all  $g \in G$ , the sum  $\sum_{\alpha \in X^g} \mu_J(\alpha)$  is constant.

Otherwise, G is spreading.

(X, J) is a witness to G being non-spreading.

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

J is trivial if  $\mu_J$  is constant on  $\Omega$ , or if  $\mu_J(\alpha) \neq 0$  for a unique  $\alpha$ .

#### Definition

A transitive permutation group G on  $\Omega$  is non-spreading if:

 $\exists$  a nontrivial subset X of  $\Omega$  and a nontrivial multiset J of  $\Omega$  such that: |J| divides  $|\Omega|$ , and for all  $g \in G$ , the sum  $\sum_{\alpha \in X^g} \mu_J(\alpha)$  is constant.

Otherwise, G is spreading.

(X, J) is a witness to G being non-spreading.

G non-spreading  $\implies$  all transitive subgroups of G are non-spreading.

Question: Do spreading groups of diagonal type exist?

 $\Omega$  – set; J – multiset of elements of  $\Omega$ ;  $\mu_J(\alpha)$  – multiplicity in J of  $\alpha \in \Omega$ .

J is trivial if  $\mu_J$  is constant on  $\Omega$ , or if  $\mu_J(\alpha) \neq 0$  for a unique  $\alpha$ .

#### Definition

A transitive permutation group G on  $\Omega$  is non-spreading if:  $\exists$  a nontrivial subset X of  $\Omega$  and a nontrivial multiset J of  $\Omega$  such that: |J| divides  $|\Omega|$ , and for all  $g \in G$ , the sum  $\sum_{\alpha \in X^g} \mu_J(\alpha)$  is constant. Otherwise, G is spreading.

(X, J) is a witness to G being non-spreading.

G non-spreading  $\implies$  all transitive subgroups of G are non-spreading.

#### Theorem (Bamberg, F. & Giudici, 2023+)

Each primitive group of diagonal type is non-spreading.

Bamberg, Giudici, Lansdown & Royle (2023+) provide a useful method of finding non-spreading witnesses. Using this, we prove:

Bamberg, Giudici, Lansdown & Royle (2023+) provide a useful method of finding non-spreading witnesses. Using this, we prove:

If a non-abelian finite simple group T satisfies

$$\exists B \triangleleft A \lneq T \text{ s.t. } A = B(A \cap A^{\tau}) \ \forall \tau \in \operatorname{Aut}(T), \tag{*}$$

Bamberg, Giudici, Lansdown & Royle (2023+) provide a useful method of finding non-spreading witnesses. Using this, we prove:

If a non-abelian finite simple group T satisfies

$$\exists B \trianglelefteq A \lneq T \text{ s.t. } A = B(A \cap A^{\tau}) \ \forall \tau \in \operatorname{Aut}(T), \tag{*}$$

then W(T) is non-spreading, with witness (A, T + |A : B|B - A), hence all diagonal groups with socle  $T \times T$  are non-spreading.

Bamberg, Giudici, Lansdown & Royle (2023+) provide a useful method of finding non-spreading witnesses. Using this, we prove:

If a non-abelian finite simple group T satisfies

$$\exists B \trianglelefteq A \lneq T \text{ s.t. } A = B(A \cap A^{\tau}) \ \forall \tau \in \operatorname{Aut}(T), \tag{*}$$

then W(T) is non-spreading, with witness (A, T + |A : B|B - A), hence all diagonal groups with socle  $T \times T$  are non-spreading.

#### Theorem (Bamberg, F., Giudici, & Royle, 2023+)

Let T be a non-abelian finite simple group.

Then (\*) holds  $\iff T \notin \{J_1, M_{22}, J_3, McL, Th, \mathbb{M}\}.$ 

Bamberg, Giudici, Lansdown & Royle (2023+) provide a useful method of finding non-spreading witnesses. Using this, we prove:

If a non-abelian finite simple group T satisfies

$$\exists B \trianglelefteq A \lneq T \text{ s.t. } A = B(A \cap A^{\tau}) \ \forall \tau \in \operatorname{Aut}(T), \tag{*}$$

then W(T) is non-spreading, with witness (A, T + |A : B|B - A), hence all diagonal groups with socle  $T \times T$  are non-spreading.

#### Theorem (Bamberg, F., Giudici, & Royle, 2023+)

Let T be a non-abelian finite simple group.

Then (\*) holds  $\iff T \notin \{J_1, M_{22}, J_3, McL, Th, \mathbb{M}\}.$ 

 $\implies$ : GAP; Magma; Burness, O'Brien & Wilson (2010) for Th; Burness (2023) for M.
#### $\exists B \trianglelefteq A \lneq T \text{ s.t. } A = B(A \cap A^{\tau}) \ \forall \tau \in \operatorname{Aut}(T)$ (\*)

#### $\exists B \triangleleft A \lneq T \text{ s.t. } A = B(A \cap A^{\tau}) \ \forall \tau \in \operatorname{Aut}(T)$ (\*)

 $\Sigma_A$  – set of right cosets of A in T.

#### $\exists B \trianglelefteq A \lneq T \text{ s.t. } A = B(A \cap A^{\tau}) \ \forall \tau \in \operatorname{Aut}(T)$

 $\Sigma_A$  – set of right cosets of A in T.

Given A and B, (\*) holds if:

(P1) A and B have the same orbits in the action of T on  $\Sigma_A$ ;

(\*)

#### $\exists B \trianglelefteq A \lneq T \text{ s.t. } A = B(A \cap A^{\tau}) \ \forall \tau \in \operatorname{Aut}(T)$

 $\Sigma_A$  – set of right cosets of A in T.

Given A and B, (\*) holds if:

(P1) A and B have the same orbits in the action of T on  $\Sigma_A$ ; (P2) all Aut(T)-conjugates of A in T are conjugate in T. (\*)

#### $T = A_n$ , $n \ge 7$ ( $A_5 \cong PSL_2(4)$ and $A_6 \cong PSL_2(9)$ will be addressed later).

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

The action of T on  $\Gamma$  is transitive, and equivalent to its action on  $\Sigma_A$ .

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

The action of T on  $\Gamma$  is transitive, and equivalent to its action on  $\Sigma_A$ .

For  $\beta \in \Omega$  and  $x \in A$ , we have  $|\beta \cap \alpha| = |\beta^x \cap \alpha^x| = |\beta^x \cap \alpha|$ .

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

The action of T on  $\Gamma$  is transitive, and equivalent to its action on  $\Sigma_A$ .

For  $\beta \in \Omega$  and  $x \in A$ , we have  $|\beta \cap \alpha| = |\beta^x \cap \alpha^x| = |\beta^x \cap \alpha|$ .

A and B have the same orbits on  $\Gamma$ :  $\{\beta \in \Gamma \mid |\beta \cap \alpha| = i\}$  for  $i \in \{0, 1, 2, 3\}$ .

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

The action of T on  $\Gamma$  is transitive, and equivalent to its action on  $\Sigma_A$ .

For  $\beta \in \Omega$  and  $x \in A$ , we have  $|\beta \cap \alpha| = |\beta^x \cap \alpha^x| = |\beta^x \cap \alpha|$ .

A and B have the same orbits on  $\Gamma$ :  $\{\beta \in \Gamma \mid |\beta \cap \alpha| = i\}$  for  $i \in \{0, 1, 2, 3\}$ .  $\implies$  (P1).

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

The action of T on  $\Gamma$  is transitive, and equivalent to its action on  $\Sigma_A$ .

For  $\beta \in \Omega$  and  $x \in A$ , we have  $|\beta \cap \alpha| = |\beta^x \cap \alpha^x| = |\beta^x \cap \alpha|$ .

A and B have the same orbits on  $\Gamma$ : { $\beta \in \Gamma \mid |\beta \cap \alpha| = i$ } for  $i \in \{0, 1, 2, 3\}$ .  $\implies$  (P1).

For  $\tau \in S_n$ :  $A^{\tau} = T_{\alpha^{\tau}}$ 

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

The action of T on  $\Gamma$  is transitive, and equivalent to its action on  $\Sigma_A$ .

For  $\beta \in \Omega$  and  $x \in A$ , we have  $|\beta \cap \alpha| = |\beta^x \cap \alpha^x| = |\beta^x \cap \alpha|$ .

A and B have the same orbits on  $\Gamma$ :  $\{\beta \in \Gamma \mid |\beta \cap \alpha| = i\}$  for  $i \in \{0, 1, 2, 3\}$ .  $\implies$  (P1).

For 
$$\tau \in S_n$$
:  $A^{\tau} = T_{\alpha^{\tau}}$   
=  $T_{\alpha^s}$  for some  $s \in T$  (transitivity of  $T$ )

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

The action of T on  $\Gamma$  is transitive, and equivalent to its action on  $\Sigma_A$ .

For  $\beta \in \Omega$  and  $x \in A$ , we have  $|\beta \cap \alpha| = |\beta^x \cap \alpha^x| = |\beta^x \cap \alpha|$ .

A and B have the same orbits on 
$$\Gamma$$
:  
 $\{\beta \in \Gamma \mid |\beta \cap \alpha| = i\}$  for  $i \in \{0, 1, 2, 3\}$ .  
 $\implies$  (P1).

For 
$$\tau \in S_n$$
:  $A^{\tau} = T_{\alpha^{\tau}}$   
=  $T_{\alpha^s}$  for some  $s \in T$  (transitivity of  $T$ )  
=  $A^s \implies$  (P2).

 $T = A_n$ ,  $n \ge 7$  ( $A_5 \cong PSL_2(4)$  and  $A_6 \cong PSL_2(9)$  will be addressed later).

Let  $\Gamma$  be the set of 3-subsets of  $\{1, \ldots, n\}$ , and  $\alpha \in \Gamma$ .

Let  $A := T_{\alpha} = (S_3 \times S_{n-3}) \cap T$  and  $B := A_3 \times A_{n-3}$ .

The action of T on  $\Gamma$  is transitive, and equivalent to its action on  $\Sigma_A$ .

For  $\beta \in \Omega$  and  $x \in A$ , we have  $|\beta \cap \alpha| = |\beta^x \cap \alpha^x| = |\beta^x \cap \alpha|$ .

A and B have the same orbits on 
$$\Gamma$$
:  
 $\{\beta \in \Gamma \mid |\beta \cap \alpha| = i\}$  for  $i \in \{0, 1, 2, 3\}$ .  
 $\implies$  (P1).

For 
$$\tau \in S_n$$
:  $A^{\tau} = T_{\alpha^{\tau}}$   
=  $T_{\alpha^s}$  for some  $s \in T$  (transitivity of  $T$ )  
=  $A^s \implies$  (P2).

(P1) and (P2)  $\implies$  (\*)  $\implies$  W(T) is non-spreading.

*T* − a simple group of Lie type  ${}^{r}X_{\ell}(q)$ :  $r \in \{1, 2, 3\}, X \in \{A, B, C, D, E, F, G\}, \ell \ge 1, q$  a power of a prime *p*.

- $\begin{array}{l} T \mbox{ a simple group of Lie type } {}^{r}X_{\ell}(q) \mbox{:} \\ r \in \{1,2,3\}, \ X \in \{{\rm A,B,C,D,E,F,G}\}, \ \ell \geqslant 1, \ q \ \mbox{a power of a prime } p. \end{array}$
- U Sylow *p*-subgroup of *T*.

T - a simple group of Lie type  ${}^{r}X_{\ell}(q)$ :  $r \in \{1, 2, 3\}, X \in \{A, B, C, D, E, F, G\}, \ell \ge 1, q$  a power of a prime p.

- U Sylow *p*-subgroup of T.
- $N_T(U)$  and a subgroup N of T form a (B, N)-pair for T. (†)

*T* − a simple group of Lie type  ${}^{r}X_{\ell}(q)$ :  $r \in \{1, 2, 3\}, X \in \{A, B, C, D, E, F, G\}, \ell \ge 1, q$  a power of a prime *p*.

U – Sylow *p*-subgroup of *T*.

 $N_T(U)$  and a subgroup N of T form a (B, N)-pair for T. (†)

If  $r \ge 2$  or  $q \ge 3$ : let  $A := N_T(U) > U$  and B := U. Then (P2) holds.

T - a simple group of Lie type  ${}^{r}X_{\ell}(q)$ :  $r \in \{1, 2, 3\}, X \in \{A, B, C, D, E, F, G\}, \ell \ge 1, q$  a power of a prime p.

U – Sylow *p*-subgroup of T.

 $N_T(U)$  and a subgroup N of T form a (B, N)-pair for T.

If  $r \ge 2$  or  $q \ge 3$ : let  $A := N_T(U) > U$  and B := U. Then (P2) holds.

(†) and  $T = ANB \implies AsA = AsB \forall s \in T \implies$  (P1).

 $(\dagger)$ 

*T* − a simple group of Lie type  ${}^{r}X_{\ell}(q)$ :  $r \in \{1, 2, 3\}, X \in \{A, B, C, D, E, F, G\}, \ell \ge 1, q$  a power of a prime *p*. *U* − Sylow *p*-subgroup of *T*.

 $N_T(U)$  and a subgroup N of T form a (B, N)-pair for T. (†)

If  $r \ge 2$  or  $q \ge 3$ : let  $A := N_T(U) > U$  and B := U. Then (P2) holds.

(†) and  $T = ANB \implies AsA = AsB \forall s \in T \implies$  (P1).

If r = 1 and q = 2: May assume  $\ell \ge 3$ .

*T* − a simple group of Lie type  ${}^{r}X_{\ell}(q)$ :  $r \in \{1, 2, 3\}, X \in \{A, B, C, D, E, F, G\}, \ell \ge 1, q$  a power of a prime *p*. *U* − Sylow *p*-subgroup of *T*.

 $N_T(U)$  and a subgroup N of T form a (B, N)-pair for T. (†)

If  $r \ge 2$  or  $q \ge 3$ : let  $A := N_T(U) > U$  and B := U. Then (P2) holds.

(†) and  $T = ANB \implies AsA = AsB \quad \forall s \in T \implies$  (P1).

If r = 1 and q = 2: May assume  $\ell \ge 3$ . PSL<sub>2</sub>(2)  $\cong S_3$ .

*T* − a simple group of Lie type  ${}^{r}X_{\ell}(q)$ :  $r \in \{1, 2, 3\}, X \in \{A, B, C, D, E, F, G\}, \ell \ge 1, q$  a power of a prime *p*. *U* − Sylow *p*-subgroup of *T*.

 $N_T(U)$  and a subgroup N of T form a (B, N)-pair for T.

If  $r \ge 2$  or  $q \ge 3$ : let  $A := N_T(U) > U$  and B := U. Then (P2) holds.

(†) and  $T = ANB \implies AsA = AsB \forall s \in T \implies$  (P1).

If r = 1 and q = 2: May assume  $\ell \ge 3$ .

 $PSL_2(2) \cong S_3.$ 

Can choose A to be a parabolic subgroup  $K \rtimes (M \times S_3)$  and  $B := K \rtimes (M \times C_3)$ , with K a 2-group and M a subgroup of Lie type.

 $(\dagger)$ 

*T* − a simple group of Lie type  ${}^{r}X_{\ell}(q)$ :  $r \in \{1, 2, 3\}, X \in \{A, B, C, D, E, F, G\}, \ell \ge 1, q$  a power of a prime *p*. *U* − Sylow *p*-subgroup of *T*.

 $N_T(U)$  and a subgroup N of T form a (B, N)-pair for T.

If  $r \ge 2$  or  $q \ge 3$ : let  $A := N_T(U) > U$  and B := U. Then (P2) holds.

(†) and  $T = ANB \implies AsA = AsB \forall s \in T \implies$  (P1).

If r = 1 and q = 2: May assume  $\ell \ge 3$ .

 $\mathrm{PSL}_2(2) \cong S_3.$ 

Can choose A to be a parabolic subgroup  $K \rtimes (M \times S_3)$  and  $B := K \rtimes (M \times C_3)$ , with K a 2-group and M a subgroup of Lie type.

We consider how the elements of N conjugate certain involutions of  $A \setminus B$ .

 $(\dagger)$ 

T – one of the 26 sporadic simple groups, or the Tits group  ${}^{2}F_{4}(2)'$ .

T – one of the 26 sporadic simple groups, or the Tits group  ${}^{2}F_{4}(2)'$ .

For  $A \leq T$ , let fix(s) := set of points in  $\Sigma_A$  fixed by  $s \in T$ .

T – one of the 26 sporadic simple groups, or the Tits group  ${}^{2}F_{4}(2)'$ .

For  $A \leq T$ , let fix(s) := set of points in  $\Sigma_A$  fixed by  $s \in T$ .

Cauchy–Frobenius Lemma: For  $C \leq T$ , the number of orbits of C on  $\Sigma_A$  is  $\lambda_C := \frac{1}{|C|} \sum_{s \in C} |\operatorname{fix}(s)|$ .

T – one of the 26 sporadic simple groups, or the Tits group  ${}^{2}F_{4}(2)'$ .

For  $A \leq T$ , let fix(s) := set of points in  $\Sigma_A$  fixed by  $s \in T$ .

Cauchy–Frobenius Lemma: For  $C \leq T$ , the number of orbits of C on  $\Sigma_A$  is  $\lambda_C := \frac{1}{|C|} \sum_{s \in C} |\operatorname{fix}(s)|$ .

Calculations using the GAP Character Table Library:  $T \notin \{J_1, M_{22}, J_3, McL, Th, \mathbb{M}\} \implies \exists B \trianglelefteq A \underset{max}{<} T \text{ s.t. } \lambda_A = \lambda_B$  $\implies$  (P1).

T – one of the 26 sporadic simple groups, or the Tits group  ${}^{2}F_{4}(2)'$ .

For  $A \leq T$ , let fix(s) := set of points in  $\Sigma_A$  fixed by  $s \in T$ .

Cauchy–Frobenius Lemma: For  $C \leq T$ , the number of orbits of C on  $\Sigma_A$  is  $\lambda_C := \frac{1}{|C|} \sum_{s \in C} |\operatorname{fix}(s)|$ .

Calculations using the GAP Character Table Library:  $T \notin \{J_1, M_{22}, J_3, McL, Th, \mathbb{M}\} \implies \exists B \trianglelefteq A \underset{max}{<} T \text{ s.t. } \lambda_A = \lambda_B$  $\implies$  (P1).

If also  $T \neq O'N$ , then (P2) holds. So (\*) holds.

T – one of the 26 sporadic simple groups, or the Tits group  ${}^{2}F_{4}(2)'$ .

For  $A \leq T$ , let fix(s) := set of points in  $\Sigma_A$  fixed by  $s \in T$ .

Cauchy–Frobenius Lemma: For  $C \leq T$ , the number of orbits of C on  $\Sigma_A$  is  $\lambda_C := \frac{1}{|C|} \sum_{s \in C} |\operatorname{fix}(s)|$ .

Calculations using the GAP Character Table Library:  $T \notin \{J_1, M_{22}, J_3, McL, Th, \mathbb{M}\} \implies \exists B \trianglelefteq A \underset{max}{<} T \text{ s.t. } \lambda_A = \lambda_B$  $\implies$  (P1).

If also  $T \neq O'N$ , then (P2) holds. So (\*) holds.

For O'N, we consider the right cosets of A in Aut(T), instead of in T.

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\exists$  pairwise non-conjugate  $r, s_1, s_2 \in T$  such that (i)  $r^{-1} \in r^T$ ;

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\exists$  pairwise non-conjugate  $r, s_1, s_2 \in T$  such that (i)  $r^{-1} \in r^T$ ; (ii)  $|s_1^T| = |s_2^T|$ ; and

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\exists \text{ pairwise non-conjugate } r, s_1, s_2 \in T \text{ such that (i) } r^{-1} \in r^T;$ (ii)  $|s_1^T| = |s_2^T|$ ; and

(iii)  $\chi(r^{\tau}) = 0 \quad \forall \tau \in \operatorname{Aut}(T), \quad \forall \chi \in \operatorname{Irr}(T) \text{ s.t. } \chi(s_1) \neq \chi(s_2).$ 

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\exists \text{ pairwise non-conjugate } r, s_1, s_2 \in T \text{ such that (i) } r^{-1} \in r^T;$ (ii)  $|s_1^T| = |s_2^T|;$  and (iii)  $\chi(r^\tau) = 0 \quad \forall \tau \in \text{Aut}(T), \quad \forall \chi \in \text{Irr}(T) \text{ s.t. } \chi(s_1) \neq \chi(s_2).$ 

Let  $X := r^T$ ,  $g \in W(T)$ . By (i),  $\exists \tau \in Aut(T), u \in T$  s.t.  $X^g = (r^{\tau})^T u$ .
$\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\exists \text{ pairwise non-conjugate } r, s_1, s_2 \in T \text{ such that (i) } r^{-1} \in r^T;$ (ii)  $|s_1^T| = |s_2^T|$ ; and
(iii)  $\chi(r^\tau) = 0 \quad \forall \tau \in \operatorname{Aut}(T), \quad \forall \chi \in \operatorname{Irr}(T) \text{ s.t. } \chi(s_1) \neq \chi(s_2).$ Let  $X := r^T, g \in W(T)$ . By (i),  $\exists \tau \in \operatorname{Aut}(T), u \in T \text{ s.t. } X^g = (r^\tau)^T u.$ Let  $J := \Omega + s_1^T - s_2^T$ . Then  $|J| = |\Omega|$ , and  $\sum_{\alpha \in X^g} \mu_J(\alpha) = |X| + |X^g \cap s_1^T| - |X^g \cap s_2^T|.$ 

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\exists$  pairwise non-conjugate  $r, s_1, s_2 \in T$  such that (i)  $r^{-1} \in r^T$ : (ii)  $|s_1^T| = |s_2^T|$ ; and (iii)  $\chi(r^{\tau}) = 0 \ \forall \tau \in \operatorname{Aut}(T), \ \forall \chi \in \operatorname{Irr}(T) \text{ s.t. } \chi(s_1) \neq \chi(s_2).$ Let  $X := r^T$ ,  $g \in W(T)$ . By (i),  $\exists \tau \in Aut(T), u \in T$  s.t.  $X^g = (r^\tau)^T u$ . Let  $J := \Omega + s_1^T - s_2^T$ . Then  $|J| = |\Omega|$ , and  $\sum_{\alpha \in \mathbf{X}^g} \mu_I(\alpha) = |X| + |X^g \cap s_1^T| - |X^g \cap s_2^T|.$ For  $i \in \{1,2\}$ :  $|X^g \cap s_i^T| = \frac{|r^T||s_i^T|}{|T|} \sum_{\chi(1)} \frac{\chi(r^{\tau})\chi(u)\overline{\chi(s_i)}}{\chi(1)}$ .  $\chi \in \operatorname{Irr}(T)$ 

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\exists$  pairwise non-conjugate  $r, s_1, s_2 \in T$  such that (i)  $r^{-1} \in r^T$ : (ii)  $|s_1^T| = |s_2^T|$ ; and (iii)  $\chi(r^{\tau}) = 0 \ \forall \tau \in \operatorname{Aut}(T), \ \forall \chi \in \operatorname{Irr}(T) \text{ s.t. } \chi(s_1) \neq \chi(s_2).$ Let  $X := r^T$ ,  $g \in W(T)$ . By (i),  $\exists \tau \in Aut(T), u \in T$  s.t.  $X^g = (r^\tau)^T u$ . Let  $J := \Omega + s_1^T - s_2^T$ . Then  $|J| = |\Omega|$ , and  $\sum_{\alpha \in \mathbf{X}^g} \mu_I(\alpha) = |X| + |X^g \cap s_1^T| - |X^g \cap s_2^T|.$ For  $i \in \{1,2\}$ :  $|X^g \cap s_i^T| = \frac{|r^T||s_i^T|}{|T|} \sum_{\substack{\chi(r^\tau)\chi(u) \overline{\chi(s_i)} \\ \chi(1)}} \sum_{\chi(1)} \frac{\chi(r^\tau)\chi(u) \overline{\chi(s_i)}}{\chi(1)}$ .  $\chi \in \operatorname{Irr}(T)$ (ii) & (iii)  $\implies |X^g \cap s_1^T| = |X^g \cap s_2^T| \quad \forall g \in W(T).$ 

 $\mathcal{T} \in \{\mathrm{J}_1, \mathrm{M}_{22}, \mathrm{J}_3, \mathrm{McL}, \mathrm{Th}, \mathbb{M}\}.$ 

Irr(T) – set of irreducible complex characters of T.

 $\exists$  pairwise non-conjugate  $r, s_1, s_2 \in T$  such that (i)  $r^{-1} \in r^T$ : (ii)  $|s_1^T| = |s_2^T|$ ; and (iii)  $\chi(r^{\tau}) = 0 \ \forall \tau \in \operatorname{Aut}(T), \ \forall \chi \in \operatorname{Irr}(T) \text{ s.t. } \chi(s_1) \neq \chi(s_2).$ Let  $X := r^T$ ,  $g \in W(T)$ . By (i),  $\exists \tau \in Aut(T), u \in T$  s.t.  $X^g = (r^\tau)^T u$ . Let  $J := \Omega + s_1^T - s_2^T$ . Then  $|J| = |\Omega|$ , and  $\sum_{\alpha \in \mathbf{X}^g} \mu_I(\alpha) = |X| + |X^g \cap s_1^T| - |X^g \cap s_2^T|.$ For  $i \in \{1,2\}$ :  $|X^g \cap s_i^T| = \frac{|r^T||s_i^T|}{|T|} \sum_{\substack{\chi(r^\tau)\chi(u)\overline{\chi(s_i)}\\ \chi(1)}}$ .  $\chi \in \operatorname{Irr}(T)$ (ii) & (iii)  $\implies |X^g \cap s_1^T| = |X^g \cap s_2^T| \quad \forall g \in W(T).$  $\implies$  (X, J) is a witness to W(T) being non-spreading.