Invariable generation and totally deranged elements of simple groups

Scott Harper

University of Bristol

Simple Groups, Representations & Applications

Isaac Newton Institute, Cambridge

29 July 2022

Theorem (Steinberg | 1962 + CFSG)

Every finite simple group can be generated by two elements.

Theorem (Steinberg | 1962 + CFSG)

Every finite simple group can be generated by two elements.

Example

Let $n \geqslant 8$ be even. Then $A_n = \langle x_1, x_2 \rangle$ where

Theorem (Steinberg | 1962 + CFSG)

Every finite simple group can be generated by two elements.

Example

Let $n \geqslant 8$ be even. Then $A_n = \langle x_1, x_2 \rangle$ where

x_1 has cycle shape $(n-1, 1)$

x_2 has cycle shape $(n-k, k)$ for odd $k \in \{\frac{n}{2}-1, \frac{n}{2}-2\}$.

Theorem (Steinberg | 1962 + CFSG)

Every finite simple group can be generated by two elements.

Example

Let $n \geqslant 8$ be even. Then $A_n = \langle x_1, x_2 \rangle$ where

x_1 has cycle shape $(n-1, 1)$

x_2 has cycle shape $(n-k, k)$ for odd $k \in \{\frac{n}{2}-1, \frac{n}{2}-2\}$.

Observation

For all $g_1, g_2 \in A_n$ we still have $A_n = \langle x_1^{g_1}, x_2^{g_2} \rangle$.

Theorem (Steinberg | 1962 + CFSG)

Every finite simple group can be generated by two elements.

Example

Let $n \geqslant 8$ be even. Then $A_n = \langle x_1, x_2 \rangle$ where

- x_1 has cycle shape $(n-1, 1)$
- x_2 has cycle shape $(n-k, k)$ for odd $k \in \{\frac{n}{2}-1, \frac{n}{2}-2\}$.

Observation

For all $g_1, g_2 \in A_n$ we still have $A_n = \langle x_1^{g_1}, x_2^{g_2} \rangle$.

A group G is **invariably generated** by $\{x_1, \ldots, x_d\} \subseteq G$ if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for all choices of $g_1, \ldots, g_d \in G$.

A group G is **invariably generated** by $\{x_1, \ldots, x_d\} \subseteq G$ if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for all choices of $g_1, \ldots, g_d \in G$.

A group G is **invariably generated** by $\{x_1, \dots, x_d\} \subseteq G$ if $G = \langle x_1^{g_1}, \dots, x_d^{g_d} \rangle$ for all choices of $g_1, \dots, g_d \in G$.

Theorem (Kantor, Lubotzky & Shalev | 2011 // Guralnick & Malle | 2012)

Every finite simple group can be invariably generated by two elements.

A group G is **invariably generated** by $\{x_1, \ldots, x_d\} \subseteq G$ if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for all choices of $g_1, \ldots, g_d \in G$.

Theorem (Kantor, Lubotzky & Shalev | 2011 // Guralnick & Malle | 2012)

Every finite simple group can be invariably generated by two elements.

Example

Let $n \geqslant 8$ be even. Then A_n is invariably generated by $\{x_1, x_2\}$ where

- x_1 has cycle shape $(n-1, 1)$
- x_2 has cycle shape $(n-k, k)$ for odd $k \in \{\frac{n}{2} - 1, \frac{n}{2} - 2\}$.

A group G is **invariably generated** by $\{x_1, \dots, x_d\} \subseteq G$ if $G = \langle x_1^{g_1}, \dots, x_d^{g_d} \rangle$ for all choices of $g_1, \dots, g_d \in G$.

Theorem (Kantor, Lubotzky & Shalev | 2011 // Guralnick & Malle | 2012)

Every finite simple group can be invariably generated by two elements.

Moreover, for every finite simple group G there exist elements $x_1, x_2 \in G$ such that $G = \langle x_1^{a_1}, x_2^{a_2} \rangle$ for all $a_1, a_2 \in \mathrm{Aut}(G)$

Example

Let $n \geqslant 8$ be even. Then A_n is invariably generated by $\{x_1, x_2\}$ where

- x_1 has cycle shape $(n-1, 1)$
- x_2 has cycle shape $(n-k, k)$ for odd $k \in \{\frac{n}{2} - 1, \frac{n}{2} - 2\}$.

A group G is **invariably generated** by $\{x_1, \ldots, x_d\} \subseteq G$ if $G = \langle x_1^{g_1}, \ldots, x_d^{g_d} \rangle$ for all choices of $g_1, \ldots, g_d \in G$.

Theorem (Kantor, Lubotzky & Shalev | 2011 // Guralnick & Malle | 2012)

Every finite simple group can be invariably generated by two elements.

Moreover, for every finite simple group G there exist elements $x_1, x_2 \in G$ such that $G = \langle x_1^{a_1}, x_2^{a_2} \rangle$ for all $a_1, a_2 \in \mathrm{Aut}(G)$ … except for $G = \mathrm{P}\Omega_8^+(2)$!

Example

Let $n \geqslant 8$ be even. Then A_n is invariably generated by $\{x_1, x_2\}$ where

- x_1 has cycle shape $(n-1, 1)$
- x_2 has cycle shape $(n-k, k)$ for odd $k \in \{\frac{n}{2} - 1, \frac{n}{2} - 2\}$.

A group G is **invariably generated** by $\{x_1, \dots, x_d\} \subseteq G$ if $G = \langle x_1^{g_1}, \dots, x_d^{g_d} \rangle$ for all choices of $g_1, \dots, g_d \in G$.

Theorem (Kantor, Lubotzky & Shalev | 2011 // Guralnick & Malle | 2012)

Every finite simple group can be invariably generated by two elements.

Moreover, for every finite simple group G there exist elements $x_1, x_2 \in G$ such that $G = \langle x_1^{a_1}, x_2^{a_2} \rangle$ for all $a_1, a_2 \in \mathrm{Aut}(G)$ … except for $G = \mathrm{P}\Omega_8^+(2)$!

Example

Let $n \geqslant 8$ be even. Then A_n is invariably generated by $\{x_1, x_2\}$ where

x_1 has cycle shape $(n-1, 1)$

x_2 has cycle shape $(n-k, k)$ for odd $k \in \{\frac{n}{2} - 1, \frac{n}{2} - 2\}$.

Question 1 (Garzoni | 2020)

Does there exist a nonabelian finite simple group G that has an invariable generating set $\{x, x^a\}$ where $x \in G$ and $a \in \mathrm{Aut}(G)$?

Example

Fix $G = \mathrm{GL}_n(\mathbb{C})$ and $H = \{\text{upper triangular matrices in } G\}$.

Example

Fix $G = \mathrm{GL}_n(\mathbb{C})$ and $H = \{\text{upper triangular matrices in } G\}$.

Every element of G is conjugate to an element of H

Example

Fix $G = \mathrm{GL}_n(\mathbb{C})$ and $H = \{\text{upper triangular matrices in } G\}$.

Every element of G is conjugate to an element of H

$\implies$ G has no invariable generating set.

Example

Fix $G = \mathrm{GL}_n(\mathbb{C})$ and $H = \{\text{upper triangular matrices in } G\}$.

Every element of G is conjugate to an element of H

$\implies$ G has no invariable generating set.

Every element of G is contained in a conjugate of H

Example

Fix $G = \mathrm{GL}_n(\mathbb{C})$ and $H = \{\text{upper triangular matrices in } G\}$.

Every element of G is conjugate to an element of H

$\implies$ G has no invariable generating set.

Every element of G is contained in a conjugate of H

$\implies$ G has no derangements in its action on G/H.

Example

Fix $G = \mathrm{GL}_n(\mathbb{C})$ and $H = \{\text{upper triangular matrices in } G\}$.

Every element of G is conjugate to an element of H

$\implies$ G has no invariable generating set.

Every element of G is contained in a conjugate of H

$\implies$ G has no derangements in its action on G/H.

Recall: $g \in \mathrm{Sym}(\Omega)$ is a **derangement** if g fixes no point of Ω.

Example

Fix $G = \mathrm{GL}_n(\mathbb{C})$ and $H = \{\text{upper triangular matrices in } G\}$.

Every element of G is conjugate to an element of H

$\implies$ G has no invariable generating set.

Every element of G is contained in a conjugate of H

$\implies$ G has no derangements in its action on G/H.

Recall: $g \in \mathrm{Sym}(\Omega)$ is a **derangement** if g fixes no point of Ω.

Lemma

Let G be a group. Then

G has an invariable generating set $\iff$ for all transitive actions of G of degree $\geqslant 2$ G has a derangement.

Example

Fix $G = \mathrm{GL}_n(\mathbb{C})$ and $H = \{\text{upper triangular matrices in } G\}$.

Every element of G is conjugate to an element of H
$\implies$ G has no invariable generating set.

Every element of G is contained in a conjugate of H
$\implies$ G has no derangements in its action on G/H.

Recall: $g \in \mathrm{Sym}(\Omega)$ is a **derangement** if g fixes no point of Ω.

Lemma

Let G be a group. Then

G has an invariable generating set $\iff$ for all transitive actions of G of degree $\geqslant 2$ G has a derangement.

Theorem (Jordan | 1870)

Let G be a finite group acting transitively with degree at least 2.
Then G has a derangement.

Theorem (Jordan | 1870)

Let G be a finite group acting transitively with degree $\geqslant 2$.
Then there exists an element of G that does not fix a point.

Theorem (Jordan | 1870)

Let G be a finite group acting transitively with degree $\geqslant 2$.
Then there exists an element of G that does not fix a point.

Theorem (Serre | 2000)

Theorem (Jordan | 1870)

Let G be a finite group acting transitively with degree $\geqslant 2$.
Then there exists an element of G that does not fix a point.

Theorem (Serre | 2000)

(a) Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $\geqslant 2$.
Then there exists a prime p such that f does not have a root modulo p.

Theorem (Jordan | 1870)

Let G be a finite group acting transitively with degree $\geqslant 2$.
Then there exists an element of G that does not fix a point.

Theorem (Serre | 2000)

(a) Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $\geqslant 2$.
Then there exists a prime p such that f does not have a root modulo p.

(b) Let X be a top. space with path connected cover $p\colon C \to X$ of degree $\geqslant 2$.
Then there exists $f\colon S^1 \to X$ that does not lift to C.

Theorem (Jordan | 1870)

Let G be a finite group acting **transitively** with degree $\geqslant 2$.
Then there exists an element of G that does not fix a point.

Theorem (Serre | 2000)

(a) Let $f \in \mathbb{Z}[X]$ be an **irreducible** polynomial of degree $\geqslant 2$.
Then there exists a prime p such that f does not have a root modulo p.

(b) Let X be top. space with **path connected** cover $p\colon C \to X$ of degree $\geqslant 2$.
Then there exists $f\colon S^1 \to X$ that does not lift to C.

Theorem (Jordan | 1870)

Let G be a finite group acting **transitively** with **degree $\geqslant$ 2**.
Then there exists an element of G that does not fix a point.

Theorem (Serre | 2000)

(a) Let $f \in \mathbb{Z}[X]$ be an **irreducible** polynomial of **degree** $\geqslant 2$.
Then there exists a prime p such that f does not have a root modulo p.

(b) Let X be top. space with **path connected** cover $p\colon C \to X$ of **degree $\geqslant$ 2**.
Then there exists $f\colon S^1 \to X$ that does not lift to C.

Theorem (Jordan | 1870)

Let G be a finite group acting **transitively** with **degree $\geqslant$ 2**.
Then there **exists** an element of G that **does not** fix a point.

Theorem (Serre | 2000)

(a) Let $f \in \mathbb{Z}[X]$ be an **irreducible** polynomial of **degree** $\geqslant 2$.
Then there **exists** a prime p such that f **does not** have a root modulo p.

(b) Let X be top. space with **path connected** cover $p\colon C \to X$ of **degree $\geqslant$ 2**.
Then there **exists** $f\colon S^1 \to X$ that **does not** lift to C.

Theorem (Jordan | 1870)

Let G be a finite group acting transitively with degree $\geqslant 2$.
Then there exists an element of G that does not fix a point.

Theorem (Serre | 2000)

(a) Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $\geqslant 2$.
Then there exists a prime p such that f does not have a root modulo p.

(b) Let X be a top. space with path connected cover $p\colon C \to X$ of degree $\geqslant 2$.
Then there exists $f\colon S^1 \to X$ that does not lift to C.

Theorem (Jordan | 1870)

Let G be a finite group acting transitively with degree $\geqslant 2$.
Then there exists an element of G that does not fix a point.

Theorem (Serre | 2000)

(a) Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $\geqslant 2$.
Then there exists a prime p such that f does not have a root modulo p.

(b) Let X be a top. space with path connected cover $p\colon C \to X$ of degree $\geqslant 2$.
Then there exists $f\colon S^1 \to X$ that does not lift to C.

Lots of recent work here, often reducing to faithful primitive actions of **almost simple groups**: G with $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for nonabelian simple G_0.

Theorem (Jordan | 1870)

Let G be a finite group acting transitively with degree $\geqslant 2$.
Then there exists an element of G that does not fix a point.

Theorem (Serre | 2000)

(a) Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree $\geqslant 2$.
Then there exists a prime p such that f does not have a root modulo p.

(b) Let X be a top. space with path connected cover $p\colon C \to X$ of degree $\geqslant 2$.
Then there exists $f\colon S^1 \to X$ that does not lift to C.

Lots of recent work here, often reducing to faithful primitive actions of **almost simple groups**: G with $G_0 \leqslant G \leqslant \mathrm{Aut}(G_0)$ for nonabelian simple G_0.

Question 2

Does there exist an almost simple group G with a **totally deranged element**: an element that is a derangement in every faithful primitive action of G?

Question 1 (Garzoni | 2020)

Does there exist a nonabelian finite simple group G that has an invariable generating set $\{x, x^a\}$ where $x \in G$ and $a \in \mathrm{Aut}(G)$?

Question 2

Does there exist an almost simple group G with a totally deranged element: an element that is a derangement in every faithful primitive action of G?

Question 1 (Garzoni | 2020)

Does there exist a nonabelian finite simple group G that has an invariable generating set $\{x, x^a\}$ where $x \in G$ and $a \in \mathrm{Aut}(G)$?

Question 2

Does there exist an almost simple group G with a totally deranged element: an element that is a derangement in every faithful primitive action of G?

Lemma

Let G be a group. Then

G has an invariable generating set $\iff$ for all transitive actions of degree $\geqslant 2$ G has a derangement.

Question 1 (Garzoni | 2020)

Does there exist a nonabelian finite simple group G that has an invariable generating set $\{x, x^a\}$ where $x \in G$ and $a \in \mathrm{Aut}(G)$?

Question 2

Does there exist an almost simple group G with a totally deranged element: an element that is a derangement in every faithful primitive action of G?

Lemma

Let G be a group. Then

G has an invariable generating set $\iff$ for all transitive actions of degree $\geqslant 2$ G has a derangement.

Lemma (H | 2022)

Let G_0 be a nonabelian finite simple group. Then

$\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariable generates G_0 $\implies$ x is a totally deranged element of $G = \langle G_0, a \rangle$.

Question 1 (Garzoni | 2020)

Does there exist a nonabelian finite simple group G that has an invariable generating set $\{x, x^a\}$ where $x \in G$ and $a \in \mathrm{Aut}(G)$?

Question 2

Does there exist an almost simple group G with a totally deranged element: an element that is a derangement in every faithful primitive action of G?

Lemma

Let G be a group. Then

G has an invariable generating set	$\Longleftrightarrow$	for all transitive actions of degree $\geqslant 2$ G has a derangement.

Lemma (H | 2022)

Let G_0 be a nonabelian finite simple group. Then

$\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariable generates G_0	$\Longleftrightarrow$	x is a totally deranged element of $G = \langle G_0, a \rangle$.

Nonexample

Nonexample

The group $G = S_n$ has no totally deranged elements.

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$.

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

$\implies x \in S_k \times S_{n-k} < S_n$ (with $0 < k < \frac{n}{2}$)

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

$\implies x \in S_k \times S_{n-k} < S_n$ (with $0 < k < \frac{n}{2}$)

x is two $\frac{n}{2}$-cycles

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

$\implies x \in S_k \times S_{n-k} < S_n$ (with $0 < k < \frac{n}{2}$)

x is two $\frac{n}{2}$-cycles

$\implies x \in S_{n/2} \wr S_2 < S_n$

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

$$\implies x \in S_k \times S_{n-k} < S_n \text{ (with } 0 < k < \tfrac{n}{2}\text{)}$$

x is two $\frac{n}{2}$-cycles

$$\implies x \in S_{n/2} \wr S_2 < S_n$$

x is an n-cycle and $n = ab$ with $1 < a \leqslant b < n$

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

$\implies x \in S_k \times S_{n-k} < S_n$ (with $0 < k < \frac{n}{2}$)

x is two $\frac{n}{2}$-cycles

$\implies x \in S_{n/2} \wr S_2 < S_n$

x is an n-cycle and $n = ab$ with $1 < a \leqslant b < n$

$\implies x \in S_a \wr S_b < S_n$

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

$\implies x \in S_k \times S_{n-k} < S_n$ (with $0 < k < \frac{n}{2}$)

x is two $\frac{n}{2}$-cycles

$\implies x \in S_{n/2} \wr S_2 < S_n$

x is an n-cycle and $n = ab$ with $1 < a \leqslant b < n$

$\implies x \in S_a \wr S_b < S_n$

x is an n-cycle with n prime

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

$$\implies x \in S_k \times S_{n-k} < S_n \text{ (with } 0 < k < \tfrac{n}{2}\text{)}$$

x is two $\frac{n}{2}$-cycles

$$\implies x \in S_{n/2} \wr S_2 < S_n$$

x is an n-cycle and $n = ab$ with $1 < a \leqslant b < n$

$$\implies x \in S_a \wr S_b < S_n$$

x is an n-cycle with n prime

$$\implies x \in N_{S_n}(\langle x \rangle) = \mathrm{AGL}_1(n) < S_n$$

□

Nonexample

The group $G = S_n$ has no totally deranged elements.

Proof

Let $x \in G$. It suffices to find a corefree maximal subgroup of G containing x.

x is not an n-cycle or two $\frac{n}{2}$-cycles

$$\implies x \in S_k \times S_{n-k} < S_n \text{ (with } 0 < k < \tfrac{n}{2}\text{)}$$

x is two $\frac{n}{2}$-cycles

$$\implies x \in S_{n/2} \wr S_2 < S_n$$

x is an n-cycle and $n = ab$ with $1 < a \leqslant b < n$

$$\implies x \in S_a \wr S_b < S_n$$

x is an n-cycle with n prime

$$\implies x \in N_{S_n}(\langle x \rangle) = \mathrm{AGL}_1(n) < S_n$$

□

So $G_0 = A_n$ has no invariable generating set $\{x, x^a\}$ with $x \in G_0$ and $a \in G$.

Example

Example

$G = \mathrm{O}_{16}^{+}(q)$ and $G_0 = \Omega_{16}^{+}(q)$ with $q = 2^f$

Example

$G = \mathrm{O}_{16}^{+}(q)$ and $G_0 = \Omega_{16}^{+}(q)$ with $q = 2^f$

$a \in \mathrm{O}_{16}^{+}(q) \setminus \Omega_{16}^{+}(q)$

Example

$G = \mathrm{O}_{16}^{+}(q)$ and $G_0 = \Omega_{16}^{+}(q)$ with $q = 2^f$

$a \in \mathrm{O}_{16}^{+}(q) \setminus \Omega_{16}^{+}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

Example

$G = \mathrm{O}^+_{16}(q)$ and $G_0 = \Omega^+_{16}(q)$ with $q = 2^f$

$a \in \mathrm{O}^+_{16}(q) \setminus \Omega^+_{16}(q)$ $\quad$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

Example

$G = \mathrm{O}_{16}^{+}(q)$ and $G_0 = \Omega_{16}^{+}(q)$ with $q = 2^f$

$a \in \mathrm{O}_{16}^{+}(q) \setminus \Omega_{16}^{+}(q)$ $\quad$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Example

$G = \mathrm{O}_{16}^{+}(q)$ and $G_0 = \Omega_{16}^{+}(q)$ with $q = 2^f$

$a \in \mathrm{O}_{16}^{+}(q) \setminus \Omega_{16}^{+}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

Example

$G = \mathrm{O}^+_{16}(q)$ and $G_0 = \Omega^+_{16}(q)$ with $q = 2^f$

$a \in \mathrm{O}^+_{16}(q) \setminus \Omega^+_{16}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

G_U

Example

$G = \mathrm{O}^+_{16}(q)$ and $G_0 = \Omega^+_{16}(q)$ with $q = 2^f$

$a \in \mathrm{O}^+_{16}(q) \setminus \Omega^+_{16}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

$$G_U \quad G_{U^*}$$

Example

$G = \mathrm{O}_{16}^{+}(q)$ and $G_0 = \Omega_{16}^{+}(q)$ with $q = 2^f$

$a \in \mathrm{O}_{16}^{+}(q) \setminus \Omega_{16}^{+}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

$$G_U \quad G_{U^*} \quad G_{U \oplus U^*}$$

Example

$G = \mathrm{O}^+_{16}(q)$ and $G_0 = \Omega^+_{16}(q)$ with $q = 2^f$

$a \in \mathrm{O}^+_{16}(q) \setminus \Omega^+_{16}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

$$G_U \quad G_{U^*} \quad G_{U \oplus U^*} \quad \mathrm{O}^+_8(q^2).2 \quad \mathrm{GU}_8(q).2.$$

Example

$G = \mathrm{O}_{16}^{+}(q)$ and $G_0 = \Omega_{16}^{+}(q)$ with $q = 2^f$

$a \in \mathrm{O}_{16}^{+}(q) \setminus \Omega_{16}^{+}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathrm{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

$$G_U \quad G_{U^*} \quad G_{U \oplus U^*} \quad \mathrm{O}_8^{+}(q^2).2 \quad \mathrm{GU}_8(q).2.$$

(None are conjugate to themselves or each other under an element of $G \setminus G_0$.)

Example

$G = \mathrm{O}^+_{16}(q)$ and $G_0 = \Omega^+_{16}(q)$ with $q = 2^f$

$a \in \mathrm{O}^+_{16}(q) \setminus \Omega^+_{16}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathrm{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

$$G_U \quad G_{U^*} \quad G_{U \oplus U^*} \quad \mathrm{O}^+_8(q^2).2 \quad \mathrm{GU}_8(q).2.$$

(None are conjugate to themselves or each other under an element of $G \setminus G_0$.)

All subgroups of G containing x are contained in G_0

Example

$G = \mathrm{O}^+_{16}(q)$ and $G_0 = \Omega^+_{16}(q)$ with $q = 2^f$

$a \in \mathrm{O}^+_{16}(q) \setminus \Omega^+_{16}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)
Every proper subgroup of G that contains x is G_0 or is contained in one of

$$G_U \quad G_{U^*} \quad G_{U \oplus U^*} \quad \mathrm{O}^+_8(q^2).2 \quad \mathrm{GU}_8(q).2.$$

(None are conjugate to themselves or each other under an element of $G \setminus G_0$.)

All subgroups of G containing x are contained in G_0

$\implies$ x is a totally deranged element of G.

Example

$G = \mathrm{O}^+_{16}(q)$ and $G_0 = \Omega^+_{16}(q)$ with $q = 2^f$

$a \in \mathrm{O}^+_{16}(q) \setminus \Omega^+_{16}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

$$G_U \quad G_{U^*} \quad G_{U \oplus U^*} \quad \mathrm{O}^+_8(q^2).2 \quad \mathrm{GU}_8(q).2.$$

(None are conjugate to themselves or each other under an element of $G \setminus G_0$.)

All subgroups of G containing x are contained in G_0

$\implies$ x is a totally deranged element of G.

For all $H < G_0$ and $g \in G_0$, if $x \in H$ then $x^{ag} \notin H$

Example

$G = \mathrm{O}^+_{16}(q)$ and $G_0 = \Omega^+_{16}(q)$ with $q = 2^f$

$a \in \mathrm{O}^+_{16}(q) \setminus \Omega^+_{16}(q)$ [e.g. a transvection, with Jordan form (J_2, J_1^{14})]

$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \in G_0$ stabilising $U \oplus U^*$ for a totally singular 8-space U

↰ Singer cycle s transitively permutes the $q^8 - 1$ vectors of $U \setminus 0$

Proposition (H | 2022)

Every proper subgroup of G that contains x is G_0 or is contained in one of

$$G_U \quad G_{U^*} \quad G_{U \oplus U^*} \quad \mathrm{O}^+_8(q^2).2 \quad \mathrm{GU}_8(q).2.$$

(None are conjugate to themselves or each other under an element of $G \setminus G_0$.)

All subgroups of G containing x are contained in G_0
$\implies$ x is a totally deranged element of G.

For all $H < G_0$ and $g \in G_0$, if $x \in H$ then $x^{ag} \notin H$
$\implies$ $\{x, x^a\}$ invariably generates G_0.

Theorem (H | 2022)

Theorem (H | 2022)

Let G_0 be a nonabelian finite simple group. The following are equivalent

Theorem (H | 2022)

Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

Theorem (H | 2022)

Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

Theorem (H | 2022)

Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c)

Theorem (H | 2022)

Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \quad \mathrm{P}\Omega_n^+(q) \quad$ with $n = 2^k \geqslant 8$

Theorem (H | 2022)

Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \quad \mathrm{P}\Omega_n^+(q) \quad$ with $n = 2^k \geqslant 8$

$a \in \mathrm{Aut}(G_0)$ induces a graph automorphism

Theorem (H | 2022)

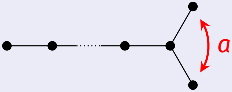
Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \quad \mathrm{P\Omega}_n^+(q) \quad$ with $n = 2^k \geqslant 8$

$a \in \mathrm{Aut}(G_0)$ induces a graph automorphism



Theorem (H | 2022)

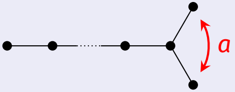
Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \quad \mathrm{P}\Omega_n^+(q) \quad$ with $n = 2^k \geqslant 8$

$a \in \mathrm{Aut}(G_0)$ induces a graph automorphism



$$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} \quad \text{with } |s| = q^{n/2} - 1$$

Theorem (H | 2022)

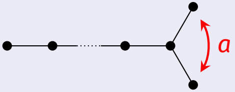
Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \quad \mathrm{P}\Omega_n^+(q) \quad$ with $n = 2^k \geqslant 8$

$a \in \mathrm{Aut}(G_0)$ induces a graph automorphism



$x = \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix}$ with $|s| = q^{n/2} - 1$ or a small power

Theorem (H | 2022)

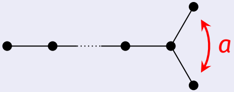
Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \quad \mathrm{P\Omega}_n^+(q) \quad$ with $n = 2^k \geqslant 8$

$a \in \mathrm{Aut}(G_0)$ induces a graph automorphism



$$x = \begin{cases} \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} & \text{with } |s| = q^{n/2} - 1 \\ \begin{bmatrix} s & & {}^{1} \\ & {}_{1}\,\cdot^{\cdot^{\cdot}} & \\ & & s^{-\mathsf{T}} \end{bmatrix} & \text{with } |s| = q^{n/4} + 1 \text{ \& } q \text{ odd} \end{cases}$$

or a small power.

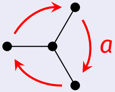
Theorem (H | 2022)

Let G_0 be a nonabelian finite simple group. The following are equivalent

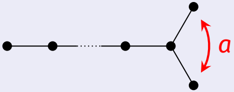
(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \mathrm{P\Omega}_n^+(q)$ with $n = 2^k \geqslant 8$



$a \in \mathrm{Aut}(G_0)$ induces a graph automorphism



$$x = \begin{cases} \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} & \text{with } |s| = q^{n/2} - 1 \\ \begin{bmatrix} s & & 1 \\ & \iddots & \\ 1 & & s^{-\mathsf{T}} \end{bmatrix} & \text{with } |s| = q^{n/4} + 1 \text{ \& } q \text{ odd} \end{cases}$$

or a small power.

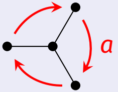
Theorem (H | 2022)

Let G_0 be a nonabelian finite simple group. The following are equivalent

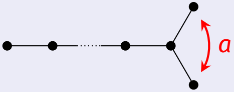
(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \begin{cases} \mathrm{P}\Omega_n^+(q) & \text{with } n = 2^k \geqslant 8 \\ \mathrm{Sp}_4(q) & \text{with } n = 4 \text{ \& } q \text{ even} \end{cases}$



$a \in \mathrm{Aut}(G_0)$ induces a graph automorphism



$$x = \begin{cases} \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} & \text{with } |s| = q^{n/2} - 1 \\ \begin{bmatrix} s & & 1 \\ & 1 & \\ & & s^{-\mathsf{T}} \end{bmatrix} & \text{with } |s| = q^{n/4} + 1 \text{ \& } q \text{ odd} \end{cases}$$

or a small power.

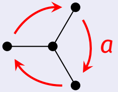
Theorem (H | 2022)

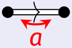
Let G_0 be a nonabelian finite simple group. The following are equivalent

(a) $\{x, x^a\}$ with $x \in G_0$ and $a \in \mathrm{Aut}(G_0)$ invariably generates G_0

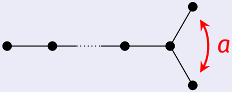
(b) x is a totally deranged element of $G = \langle G_0, a \rangle$

(c) $G_0 = \begin{cases} \mathrm{P}\Omega_n^+(q) & \text{with } n = 2^k \geqslant 8 \\ \mathrm{Sp}_4(q) & \text{with } n = 4 \text{ \& } q \text{ even} \end{cases}$





$a \in \mathrm{Aut}(G_0)$ induces a graph automorphism



$$x = \begin{cases} \begin{bmatrix} s & \\ & s^{-\mathsf{T}} \end{bmatrix} & \text{with } |s| = q^{n/2} - 1 \\ \begin{bmatrix} s & & 1 \\ & 1 & \\ & & s^{-\mathsf{T}} \end{bmatrix} & \text{with } |s| = q^{n/4} + 1 \text{ \& } q \text{ odd} \end{cases}$$

or a small power.