A Proof of the Hall-Paige Conjecture

Anthony B. Evans

Wright State University

December 21, 2011

Cayley Tables and Latin Squares

Definition

- The Cayley table of a group $G = \{g_1, \ldots, g_n\}$ is the $n \times n$ matrix with ijth entry $g_i g_j$.

Cayley Tables and Latin Squares

Definition

- The Cayley table of a group $G = \{g_1, \ldots, g_n\}$ is the $n \times n$ matrix with ijth entry $g_i g_j$.
- A latin square of order n, on a symbol set of order n, is an $n \times n$ matrix in which each symbol appears exactly once in each row, and exactly once in each column.

Cayley Tables and Latin Squares

Definition

- The Cayley table of a group $G = \{g_1, \ldots, g_n\}$ is the $n \times n$ matrix with ijth entry $g_i g_j$.
- A latin square of order n, on a symbol set of order n, is an $n \times n$ matrix in which each symbol appears exactly once in each row, and exactly once in each column.
- Two latin squares of the same order are orthogonal, or orthogonal mates, if, when superimposed, each ordered pair of symbols occurs exactly once.

Cayley Tables and Latin Squares

Definition

- The Cayley table of a group $G = \{g_1, \ldots, g_n\}$ is the $n \times n$ matrix with ijth entry $g_i g_j$.
- A latin square of order n, on a symbol set of order n, is an $n \times n$ matrix in which each symbol appears exactly once in each row, and exactly once in each column.
- Two latin squares of the same order are orthogonal, or orthogonal mates, if, when superimposed, each ordered pair of symbols occurs exactly once.

Observation

The Cayley table of a group is a latin square.

Cayley Tables and Latin Squares

Definition

- The Cayley table of a group $G = \{g_1, \ldots, g_n\}$ is the $n \times n$ matrix with ijth entry $g_i g_j$.
- A latin square of order n, on a symbol set of order n, is an $n \times n$ matrix in which each symbol appears exactly once in each row, and exactly once in each column.
- Two latin squares of the same order are orthogonal, or orthogonal mates, if, when superimposed, each ordered pair of symbols occurs exactly once.

Observation

The Cayley table of a group is a latin square.

Problem

Given a group, does its Cayley table have an orthogonal mate?

Orthogonal Latin Squares Based on $\mathbb{Z}_7$

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \end{pmatrix}$$

The Squares Superimposed

$$\begin{pmatrix} 00 & 11 & 22 & 33 & 44 & 55 & 66 \\ 13 & 24 & 35 & 46 & 50 & 61 & 02 \\ 26 & 30 & 41 & 52 & 63 & 04 & 15 \\ 31 & 42 & 53 & 64 & 05 & 16 & 20 \\ 45 & 56 & 60 & 01 & 12 & 23 & 34 \\ 54 & 65 & 06 & 10 & 21 & 32 & 43 \\ 62 & 03 & 14 & 25 & 36 & 40 & 51 \end{pmatrix}$$

The Squares Superimposed

$$\begin{pmatrix}
00 & 11 & 22 & 33 & 44 & 55 & 66 \\
13 & 24 & 35 & 46 & 50 & 61 & 02 \\
26 & 30 & 41 & 52 & 63 & 04 & 15 \\
31 & 42 & 53 & 64 & 05 & 16 & 20 \\
45 & 56 & 60 & 01 & 12 & 23 & 34 \\
54 & 65 & 06 & 10 & 21 & 32 & 43 \\
62 & 03 & 14 & 25 & 36 & 40 & 51
\end{pmatrix}$$

The Squares Superimposed

$$\begin{pmatrix} 00 & 11 & 22 & 33 & 44 & 55 & 66 \\ 13 & 24 & 35 & 46 & 50 & 61 & 02 \\ 26 & 30 & 41 & 52 & 63 & 04 & 15 \\ 31 & 42 & 53 & 64 & 05 & 16 & 20 \\ 45 & 56 & 60 & 01 & 12 & 23 & 34 \\ 54 & 65 & 06 & 10 & 21 & 32 & 43 \\ 62 & 03 & 14 & 25 & 36 & 40 & 51 \end{pmatrix}$$

A Complete Mapping of $\mathbb{Z}_7$

$$\begin{pmatrix} 0 & \color{red}{1} & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & \color{red}{6} & 0 \\ 2 & 3 & \color{red}{4} & 5 & 6 & 0 & 1 \\ \color{red}{3} & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & \color{red}{0} & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & \color{red}{2} & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & \color{red}{5} \end{pmatrix}$$

A Complete Mapping of $\mathbb{Z}_7$

$$\begin{pmatrix} 0 & \color{red}{1} & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & \color{red}{6} & 0 \\ 2 & 3 & \color{red}{4} & 5 & 6 & 0 & 1 \\ \color{red}{3} & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & \color{red}{0} & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & \color{red}{2} & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & \color{red}{5} \end{pmatrix}$$

- Define $\theta \colon \mathbb{Z}_7 \to \mathbb{Z}_7$ by $\theta(i) = j$ if the ijth entry is red.

A Complete Mapping of $\mathbb{Z}_7$

$$\begin{pmatrix} 0 & \color{red}{1} & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & \color{red}{6} & 0 \\ 2 & 3 & \color{red}{4} & 5 & 6 & 0 & 1 \\ \color{red}{3} & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & \color{red}{0} & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & \color{red}{2} & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & \color{red}{5} \end{pmatrix}$$

- Define $\theta\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ by $\theta(i) = j$ if the ijth entry is red.
- The mapping $x \mapsto \theta(x)$ is a bijection.

A Complete Mapping of $\mathbb{Z}_7$

$$\begin{pmatrix} 0 & \color{red}{1} & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & \color{red}{6} & 0 \\ 2 & 3 & \color{red}{4} & 5 & 6 & 0 & 1 \\ \color{red}{3} & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & \color{red}{0} & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & \color{red}{2} & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & \color{red}{5} \end{pmatrix}$$

- Define $\theta\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ by $\theta(i) = j$ if the ijth entry is red.
- The mapping $x \mapsto \theta(x)$ is a bijection.
- The mapping $x \mapsto \theta(x) + x$ is a bijection.

A Complete Mapping of $\mathbb{Z}_7$

$$\begin{pmatrix} 0 & \color{red}{1} & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & \color{red}{6} & 0 \\ 2 & 3 & \color{red}{4} & 5 & 6 & 0 & 1 \\ \color{red}{3} & 4 & 5 & 6 & 0 & 1 & 2 \\ 4 & 5 & 6 & \color{red}{0} & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & \color{red}{2} & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & \color{red}{5} \end{pmatrix}$$

- Define $\theta\colon \mathbb{Z}_7 \to \mathbb{Z}_7$ by $\theta(i) = j$ if the ijth entry is red.
- The mapping $x \mapsto \theta(x)$ is a bijection.
- The mapping $x \mapsto \theta(x) + x$ is a bijection.
- θ is a complete mapping of $\mathbb{Z}_7$.

Complete Mappings of Groups

Definition

A *complete mapping* of a group G is a bijection $\theta\colon G \to G$ for which the mapping $x \mapsto x\theta(x)$ is also a bijection.

Complete Mappings of Groups

Definition

A *complete mapping* of a group G is a bijection $\theta\colon G \longrightarrow G$ for which the mapping $x \mapsto x\theta(x)$ is also a bijection.

Examples

Complete Mappings of Groups

Definition

A *complete mapping* of a group G is a bijection $\theta\colon G \to G$ for which the mapping $x \mapsto x\theta(x)$ is also a bijection.

Examples

1. If $G = GF(q)^+$, then $x \mapsto ax$ is a complete mapping if and only if $a \neq 0, -1$,

Complete Mappings of Groups

Definition

A *complete mapping* of a group G is a bijection $\theta\colon G \to G$ for which the mapping $x \mapsto x\theta(x)$ is also a bijection.

Examples

1. If $G = GF(q)^+$, then $x \mapsto ax$ is a complete mapping if and only if $a \neq 0, -1$, as then $x \mapsto ax$ and $x \mapsto (a+1)x$ are both bijections.

Complete Mappings of Groups

Definition

A *complete mapping* of a group G is a bijection $\theta\colon G \to G$ for which the mapping $x \mapsto x\theta(x)$ is also a bijection.

Examples

1. If $G = GF(q)^+$, then $x \mapsto ax$ is a complete mapping if and only if $a \neq 0, -1$, as then $x \mapsto ax$ and $x \mapsto (a+1)x$ are both bijections.
2. If $|G|$ is odd, then $x \mapsto x$ is a complete mapping,

Complete Mappings of Groups

Definition

A *complete mapping* of a group G is a bijection $\theta\colon G \to G$ for which the mapping $x \mapsto x\theta(x)$ is also a bijection.

Examples

1. If $G = GF(q)^+$, then $x \mapsto ax$ is a complete mapping if and only if $a \neq 0, -1$, as then $x \mapsto ax$ and $x \mapsto (a+1)x$ are both bijections.
2. If $|G|$ is odd, then $x \mapsto x$ is a complete mapping, as $x \mapsto x$ and $x \mapsto x^2$ are both bijections.

Complete Mappings of Groups

Definition

A *complete mapping* of a group G is a bijection $\theta\colon G \to G$ for which the mapping $x \mapsto x\theta(x)$ is also a bijection.

Examples

1. If $G = GF(q)^+$, then $x \mapsto ax$ is a complete mapping if and only if $a \neq 0, -1$, as then $x \mapsto ax$ and $x \mapsto (a+1)x$ are both bijections.
2. If $|G|$ is odd, then $x \mapsto x$ is a complete mapping, as $x \mapsto x$ and $x \mapsto x^2$ are both bijections.
3. If $\alpha \in Aut(G)$, then $x \mapsto x^{-1}\alpha(x)$ is a complete mapping if and only if α is fixed-point-free.

The Problem Rewritten

Theorem

The Cayley table of a group has an orthogonal mate if and only if the group admits complete mappings.

The Problem Rewritten

Theorem

The Cayley table of a group has an orthogonal mate if and only if the group admits complete mappings.

Definition

A group is admissible if it admits complete mappings.

The Problem Rewritten

Theorem

The Cayley table of a group has an orthogonal mate if and only if the group admits complete mappings.

Definition

A group is **admissible** if it admits complete mappings.

The problem - Given a group, does its Cayley table have an orthogonal mate? - can be written as

The Problem Rewritten

Theorem

The Cayley table of a group has an orthogonal mate if and only if the group admits complete mappings.

Definition

A group is admissible if it admits complete mappings.

The problem - Given a group, does its Cayley table have an orthogonal mate? - can be written as

Problem

Which groups are admissible?

The Hall-Paige Theorem

Theorem (Hall and Paige, 1955)

A finite group with a nontrivial, cyclic Sylow 2-subgroup is not admissible.

The Hall-Paige Theorem

Theorem (Hall and Paige, 1955)

A finite group with a nontrivial, cyclic Sylow 2-subgroup is not admissible.

Proof

Assume G has a nontrivial, cyclic Sylow 2-subgroup,
$|G| = mn$, n odd, m a power of 2, and G admits a complete mapping θ.

The Hall-Paige Theorem

Theorem (Hall and Paige, 1955)

A finite group with a nontrivial, cyclic Sylow 2-subgroup is not admissible.

Proof

Assume G has a nontrivial, cyclic Sylow 2-subgroup,
$|G| = mn$, n odd, m a power of 2, and G admits a complete mapping θ.
There exists an epimorphism $\phi\colon G \to \mathbb{Z}_m$.

The Hall-Paige Theorem

Theorem (Hall and Paige, 1955)

A finite group with a nontrivial, cyclic Sylow 2-subgroup is not admissible.

Proof

Assume G has a nontrivial, cyclic Sylow 2-subgroup,
$|G| = mn$, n odd, m a power of 2, and G admits a complete mapping θ.
There exists an epimorphism $\phi\colon G \to \mathbb{Z}_m$.

$$\sum_{g\in G} \phi(g) = \sum_{g\in G} \phi(g\theta(g)) = \sum_{g\in G} (\phi(\theta(g)) + \phi(g)) = 2\sum_{g\in G} \phi(g)$$

The Hall-Paige Theorem

Theorem (Hall and Paige, 1955)

A finite group with a nontrivial, cyclic Sylow 2-subgroup is not admissible.

Proof

Assume G has a nontrivial, cyclic Sylow 2-subgroup,
$|G| = mn$, n odd, m a power of 2, and G admits a complete mapping θ.
There exists an epimorphism $\phi\colon G \to \mathbb{Z}_m$.

$$\sum_{g\in G} \phi(g) = \sum_{g\in G} \phi(g\theta(g)) = \sum_{g\in G} (\phi(\theta(g)) + \phi(g)) = 2\sum_{g\in G} \phi(g)$$

Thus $\sum_{g\in G} \phi(g) = 0$.

The Hall-Paige Theorem

Theorem (Hall and Paige, 1955)

A finite group with a nontrivial, cyclic Sylow 2-subgroup is not admissible.

Proof

Assume G has a nontrivial, cyclic Sylow 2-subgroup,
$|G| = mn$, n odd, m a power of 2, and G admits a complete mapping θ.
There exists an epimorphism $\phi\colon G \to \mathbb{Z}_m$.

$$\sum_{g \in G} \phi(g) = \sum_{g \in G} \phi(g\theta(g)) = \sum_{g \in G} (\phi(\theta(g)) + \phi(g)) = 2 \sum_{g \in G} \phi(g)$$

Thus $\sum_{g \in G} \phi(g) = 0$.
But

$$\sum_{g \in G} \phi(g) = n \sum_{i=0}^{m-1} i = nm(m-1)/2 = nm/2 \neq 0.$$

Special Cases of the Hall-Paige Theorem

Special Cases of the Hall-Paige Theorem

1. Euler (1779). Cyclic latin squares of even order do not have orthogonal mates. Later proofs given by Singer (1960) and Hedayat and Federer (1969).

Special Cases of the Hall-Paige Theorem

1. Euler (1779). Cyclic latin squares of even order do not have orthogonal mates. Later proofs given by Singer (1960) and Hedayat and Federer (1969).
2. Vijayaraghavan and Chowla (1948). If n has a primitive root, then the group of units of $\mathbb{Z}_n$ is not admissible. Extends a result of Hurwitz (1882).

Special Cases of the Hall-Paige Theorem

1. Euler (1779). Cyclic latin squares of even order do not have orthogonal mates. Later proofs given by Singer (1960) and Hedayat and Federer (1969).
2. Vijayaraghavan and Chowla (1948). If n has a primitive root, then the group of units of $\mathbb{Z}_n$ is not admissible. Extends a result of Hurwitz (1882).
3. Paige 1947. Finite abelian groups with unique involutions are not admissible.

Special Cases of the Hall-Paige Theorem

1. Euler (1779). Cyclic latin squares of even order do not have orthogonal mates. Later proofs given by Singer (1960) and Hedayat and Federer (1969).
2. Vijayaraghavan and Chowla (1948). If n has a primitive root, then the group of units of $\mathbb{Z}_n$ is not admissible. Extends a result of Hurwitz (1882).
3. Paige 1947. Finite abelian groups with unique involutions are not admissible.
4. Fleisher 1934. Cayley tables of groups of order $4n + 2$ do not have orthogonal mates. Later proofs given by Mann (1942) and Jungnickel (1980).

The Hall-Paige Conjecture

Conjecture (Hall and Paige, 1955)

A finite group with a trivial or noncyclic Sylow 2-subgroup is admissible.

Some Results

Some Results

Special Cases of the Hall-Paige Conjecture

This conjecture has been proved for several classes of groups including

- Abelian groups and groups of odd order - Paige (1947).

Some Results

Special Cases of the Hall-Paige Conjecture

This conjecture has been proved for several classes of groups including

- Abelian groups and groups of odd order - Paige (1947).
- Solvable groups - Hall and Paige (1955).

Some Results

Special Cases of the Hall-Paige Conjecture

This conjecture has been proved for several classes of groups including

- Abelian groups and groups of odd order - Paige (1947).
- Solvable groups - Hall and Paige (1955).
- A_n and S_n - Hall and Paige (1955).

Some Results

Special Cases of the Hall-Paige Conjecture

This conjecture has been proved for several classes of groups including

- Abelian groups and groups of odd order - Paige (1947).
- Solvable groups - Hall and Paige (1955).
- A_n and S_n - Hall and Paige (1955).
- Mathieu groups - Dalla Volta and Gavioli (1993).

Some Results

Special Cases of the Hall-Paige Conjecture

This conjecture has been proved for several classes of groups including

- Abelian groups and groups of odd order - Paige (1947).
- Solvable groups - Hall and Paige (1955).
- A_n and S_n - Hall and Paige (1955).
- Mathieu groups - Dalla Volta and Gavioli (1993).
- Suzuki groups and some unitary groups - Di Vicenzo (1989).

Some Results

Special Cases of the Hall-Paige Conjecture

This conjecture has been proved for several classes of groups including

- Abelian groups and groups of odd order - Paige (1947).
- Solvable groups - Hall and Paige (1955).
- A_n and S_n - Hall and Paige (1955).
- Mathieu groups - Dalla Volta and Gavioli (1993).
- Suzuki groups and some unitary groups - Di Vicenzo (1989).
- Many linear groups - Saeli (1989), Dalla Volta and Gavioli (1993, 1997), and Evans (1993, 2002, 2005).

Some Results

Special Cases of the Hall-Paige Conjecture

This conjecture has been proved for several classes of groups including

- Abelian groups and groups of odd order - Paige (1947).
- Solvable groups - Hall and Paige (1955).
- A_n and S_n - Hall and Paige (1955).
- Mathieu groups - Dalla Volta and Gavioli (1993).
- Suzuki groups and some unitary groups - Di Vicenzo (1989).
- Many linear groups - Saeli (1989), Dalla Volta and Gavioli (1993, 1997), and Evans (1993, 2002, 2005).

Aschbacher's Reduction

Aschbacher (1990). Any minimal counterexample to the Hall-paige conjecture must be "close" to being simple.

A Proof of the Hall-Paige Conjecture

The proof has three parts.

A Proof of the Hall-Paige Conjecture

The proof has three parts.

1. Reduction to simple groups.

A Proof of the Hall-Paige Conjecture

The proof has three parts.

1. Reduction to simple groups.
   Wilcox (2009).

A Proof of the Hall-Paige Conjecture

The proof has three parts.

1. Reduction to simple groups.
   Wilcox (2009).
2. The proof for groups of Lie type.

A Proof of the Hall-Paige Conjecture

The proof has three parts.

1. Reduction to simple groups.
   Wilcox (2009).
2. The proof for groups of Lie type.
   Wilcox (2009): all except the Tits group.

A Proof of the Hall-Paige Conjecture

The proof has three parts.

1. Reduction to simple groups.
   Wilcox (2009).
2. The proof for groups of Lie type.
   Wilcox (2009): all except the Tits group.
   Evans (2009): The Tits group.

A Proof of the Hall-Paige Conjecture

The proof has three parts.

1. Reduction to simple groups.
   Wilcox (2009).
2. The proof for groups of Lie type.
   Wilcox (2009): all except the Tits group.
   Evans (2009): The Tits group.
3. The proof for sporadic simple groups.

A Proof of the Hall-Paige Conjecture

The proof has three parts.

1. Reduction to simple groups.
   Wilcox (2009).
2. The proof for groups of Lie type.
   Wilcox (2009): all except the Tits group.
   Evans (2009): The Tits group.
3. The proof for sporadic simple groups.
   Evans (2009): all but J_4.

A Proof of the Hall-Paige Conjecture

The proof has three parts.

1. Reduction to simple groups.
   Wilcox (2009).
2. The proof for groups of Lie type.
   Wilcox (2009): all except the Tits group.
   Evans (2009): The Tits group.
3. The proof for sporadic simple groups.
   Evans (2009): all but J_4.
   Bray (Personal Communication): J_4.

Wilcox's Reduction

Theorem (Wilcox, 2009)

Any minimal counterexample to the Hall-Paige conjecture, if such exists, must be a nonabelian simple group.

Wilcox's Reduction

Theorem (Wilcox, 2009)

Any minimal counterexample to the Hall-Paige conjecture, if such exists, must be a nonabelian simple group.

Main idea – Suppose that G has noncyclic Sylow 2-subgroups and $H \trianglelefteq G$.

Wilcox's Reduction

Theorem (Wilcox, 2009)

Any minimal counterexample to the Hall-Paige conjecture, if such exists, must be a nonabelian simple group.

Main idea – Suppose that G has noncyclic Sylow 2-subgroups and $H \trianglelefteq G$.

Special Case

If $H \cong \mathbb{Z}_2$ and G/H is admissible, then G is admissible.

Wilcox's Reduction

Theorem (Wilcox, 2009)

Any minimal counterexample to the Hall-Paige conjecture, if such exists, must be a nonabelian simple group.

Main idea – Suppose that G has noncyclic Sylow 2-subgroups and $H \trianglelefteq G$.

Special Case

If $H \cong \mathbb{Z}_2$ and G/H is admissible, then G is admissible.

Special Case

If $G/H \cong \mathbb{Z}_2$ and H is admissible, then G is admissible.

Wilcox's Reduction

Theorem (Wilcox, 2009)

Any minimal counterexample to the Hall-Paige conjecture, if such exists, must be a nonabelian simple group.

Main idea – Suppose that G has noncyclic Sylow 2-subgroups and $H \trianglelefteq G$.

Special Case

If $H \cong \mathbb{Z}_2$ and G/H is admissible, then G is admissible.

Special Case

If $G/H \cong \mathbb{Z}_2$ and H is admissible, then G is admissible.
Proved by showing that technical conditions in a result of Evans (1992) hold.

W-systems

Let G be a finite group acting on X. Let $H = G_x$ for some $x \in X$.
$\mathcal{D} = \{HgH \mid g \in G\}$ is the set of double cosets for H in G.

W-systems

Let G be a finite group acting on X. Let $H = G_x$ for some $x \in X$.
$\mathcal{D} = \{HgH \mid g \in G\}$ is the set of double cosets for H in G.

Theorem (W-system)

If H is admissible and there exist bijections $\phi, \psi\colon \mathcal{D} \to \mathcal{D}$ satisfying $|D| = |\psi(D)| = |\phi(D)|$ and

$$\psi(D) \subseteq D\phi(D) \quad \text{for all} \quad D \in \mathcal{D},$$

then G is admissible.

W-systems

Let G be a finite group acting on X. Let $H = G_x$ for some $x \in X$. $\mathcal{D} = \{HgH \mid g \in G\}$ is the set of double cosets for H in G.

Theorem (W-system)

If H is admissible and there exist bijections $\phi, \psi \colon \mathcal{D} \to \mathcal{D}$ satisfying $|D| = |\psi(D)| = |\phi(D)|$ and

$$\psi(D) \subseteq D\phi(D) \quad \text{for all} \quad D \in \mathcal{D},$$

then G is admissible.

Corollary (Simple W-system)

If H is admissible and

$$D \subseteq D^2 \quad \text{for all} \quad D \in \mathcal{D},$$

then G is admissible.

Groups of Lie Type

Groups of Lie Type

Theorem

No finite simple group of Lie type, with the possible exception of the Tits group, can be a minimal counterexample to the Hall-Paige conjecture.

Groups of Lie Type

Theorem

No finite simple group of Lie type, with the possible exception of the Tits group, can be a minimal counterexample to the Hall-Paige conjecture.

The proof uses (B, N)-pairs and parabolic subgroups, which yield partitions of the element set of a group of Lie type into double cosets.

The Tits Group

Theorem

The Tits group $T = {}^2F_4(2)'$ is not a minimal counterexample to the Hall-Paige conjecture.

The proof uses a rank-4 permutation representation of degree 1,600 and MAGMA.

Doubly Transitive Groups

Theorem

If H is a point-stabilizer in a doubly transitive permutation representation of a finite simple group G and H is admissible, then G is admissible.

Doubly Transitive Groups

Theorem

If H is a point-stabilizer in a doubly transitive permutation representation of a finite simple group G and H is admissible, then G is admissible.

Proof

The double cosets are H and $D = G \setminus H$.

Doubly Transitive Groups

Theorem

If H is a point-stabilizer in a doubly transitive permutation representation of a finite simple group G and H is admissible, then G is admissible.

Proof

The double cosets are H and $D = G \setminus H$.
$H \subseteq H^2$

Doubly Transitive Groups

Theorem

If H is a point-stabilizer in a doubly transitive permutation representation of a finite simple group G and H is admissible, then G is admissible.

Proof

The double cosets are H and $D = G \setminus H$.
$H \subseteq H^2$
If $D \not\subseteq D^2$, then $g^2 \in H$ for all $g \in G$.

Doubly Transitive Groups

Theorem

If H is a point-stabilizer in a doubly transitive permutation representation of a finite simple group G and H is admissible, then G is admissible.

Proof

The double cosets are H and $D = G \setminus H$.

$H \subseteq H^2$

If $D \not\subseteq D^2$, then $g^2 \in H$ for all $g \in G$.

If $|g|$ is odd, then $g \in H$.

Doubly Transitive Groups

Theorem

If H is a point-stabilizer in a doubly transitive permutation representation of a finite simple group G and H is admissible, then G is admissible.

Proof

The double cosets are H and $D = G \setminus H$.
$H \subseteq H^2$
If $D \not\subseteq D^2$, then $g^2 \in H$ for all $g \in G$.
If $|g|$ is odd, then $g \in H$.
Then K, the subgroup of G generated by the set of odd-order elements of G, is a nontrivial characteristic subgroup of G contained in H.

Doubly Transitive Groups

Theorem

If H is a point-stabilizer in a doubly transitive permutation representation of a finite simple group G and H is admissible, then G is admissible.

Proof

The double cosets are H and $D = G \setminus H$.
$H \subseteq H^2$
If $D \not\subseteq D^2$, then $g^2 \in H$ for all $g \in G$.
If $|g|$ is odd, then $g \in H$.
Then K, the subgroup of G generated by the set of odd-order elements of G, is a nontrivial characteristic subgroup of G contained in H.
A contradiction.

Some Doubly Transitive Simple Groups

Corollary

HS and Co_3 are not minimal counterexamples to the Hall-Paige conjecture.

Some Doubly Transitive Simple Groups

Corollary

HS and Co_3 are not minimal counterexamples to the Hall-Paige conjecture.

Corollary

A_n, $n \geq 5$, is not a minimal counterexample to the Hall-Paige conjecture.

Some Doubly Transitive Simple Groups

Corollary

HS and Co_3 are not minimal counterexamples to the Hall-Paige conjecture.

Corollary

A_n, $n \geq 5$, is not a minimal counterexample to the Hall-Paige conjecture.

Corollary

The Mathieu groups are not minimal counterexamples to the Hall-Paige conjecture.

Rank-3 Groups

Theorem

Let G be an even-order group and let H be a point-stabilizer in a rank 3 permutation representation of G with parameters (n, k, l, λ, μ). If H is admissible, $\lambda > 0$, and $l - k + \mu - 1 > 0$, then G is admissible.

Rank-3 Groups

Theorem

Let G be an even-order group and let H be a point-stabilizer in a rank 3 permutation representation of G with parameters (n, k, l, λ, μ). If H is admissible, $\lambda > 0$, and $l - k + \mu - 1 > 0$, then G is admissible.

Corollary

J_2, McL, Ru, Suz, Co_2, Fi_{22}, Fi_{23}, and Fi'_{24} are not minimal counterexamples to the Hall-Paige conjecture.

Parameters for Rank-3 Groups

G	H	n	k	l	λ	μ
J_2	$U_3(3)$	100	36	63	14	12
McL	$U_4(3)$	275	112	162	30	56
Ru	${}^2F_4(2)$	4,060	1,755	2,304	730	780
Suz	$G_2(4)$	1,782	416	1,365	100	96
Co_2	$U_6(2){:}2$	2,300	891	1,408	378	324
Fi_{22}	$2^{\cdot}U_6(2)$	3,510	693	2,816	180	126
	$O_7(3)$	14,080	3,159	10,920	918	648
Fi_{23}	$2^{\cdot}Fi_{22}$	31,671	3,510	28, 160	693	351
	$O_8^+(3){:}S_3$	137,632	28,431	109,200	6,030	5,832
Fi'_{24}	Fi_{23}	306,936	31,671	275,264	3,510	3,240

Collapsed Adjacency Matrices

Collapsed Adjacency Matrices

G acts on X.

Collapsed Adjacency Matrices

G acts on X.
H point-stabilizer.

Collapsed Adjacency Matrices

G acts on X.
H point-stabilizer.
$O_1, \ldots, O_r$ orbits of H on X.

Collapsed Adjacency Matrices

G acts on X.
H point-stabilizer.
$O_1, \ldots, O_r$ orbits of H on X.
$a_1, \ldots, a_r$ representatives of $O_1, \ldots, O_r$.

Collapsed Adjacency Matrices

G acts on X.
H point-stabilizer.
$O_1, \ldots, O_r$ orbits of H on X.
$a_1, \ldots, a_r$ representatives of $O_1, \ldots, O_r$.
$E_1, \ldots, E_r$ orbits of G on $X \times X$.

Collapsed Adjacency Matrices

G acts on X.
H point-stabilizer.
$O_1, \ldots, O_r$ orbits of H on X.
$a_1, \ldots, a_r$ representatives of $O_1, \ldots, O_r$.
$E_1, \ldots, E_r$ orbits of G on $X \times X$.
$D_1, \ldots, D_r$ double cosets of H in G.

Collapsed Adjacency Matrices

G acts on X.
H point-stabilizer.
$O_1, \ldots, O_r$ orbits of H on X.
$a_1, \ldots, a_r$ representatives of $O_1, \ldots, O_r$.
$E_1, \ldots, E_r$ orbits of G on $X \times X$.
$D_1, \ldots, D_r$ double cosets of H in G.

Entries of Collapsed Adjacency matrices

$A_{ij}^k = |\{y \in O_j \mid (a_i, y) \in E_k\}|$.

Results from Collapsed Adjacency Matrices

Results from Collapsed Adjacency Matrices

Lemma

If $A_{kk}^{k} \neq 0$, *then* $D_k \subseteq D_k^2$.

Results from Collapsed Adjacency Matrices

Lemma

If $A^k_{kk} \neq 0$*, then* $D_k \subseteq D^2_k$*.*

Lemma

If $A^k_{kj} \neq 0$*, then* $D^2_k \supseteq D_j$*.*

Results from Collapsed Adjacency Matrices

Lemma

If $A^k_{kk} \neq 0$, then $D_k \subseteq D^2_k$.

Lemma

If $A^k_{kj} \neq 0$, then $D^2_k \supseteq D_j$.

Theorem

He, $O'N$, HN, Ly, Th, Co_1, B, and M are not minimal counterexamples to the Hall-Paige conjecture.

Results from Collapsed Adjacency Matrices

Lemma

If $A^k_{kk} \neq 0$, then $D_k \subseteq D^2_k$.

Lemma

If $A^k_{kj} \neq 0$, then $D^2_k \supseteq D_j$.

Theorem

He, $O'N$, HN, Ly, Th, Co_1, B, and M are not minimal counterexamples to the Hall-Paige conjecture.

Group	He	$O'N$	HN	Ly	Th	Co_1	B	M
Rank	5	5	9	5	11	4	10	9
W-simple?	N	Y	Y	Y	N	Y	Y	Y

Three Janko Groups

Lemma

Let H be a subgroup of G, and $\mathcal{D}$ the set of double cosets of H in G. If $D \in \mathcal{D}$ contains an element of order 3, then $D \subseteq (D^{(-1)})^2$ and $D^{(-1)} \subseteq D^2$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$.

Three Janko Groups

Lemma

Let H be a subgroup of G, and $\mathcal{D}$ the set of double cosets of H in G. If $D \in \mathcal{D}$ contains an element of order 3, then $D \subseteq (D^{(-1)})^2$ and $D^{(-1)} \subseteq D^2$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$.

Theorem

J_1 and J_3 are not minimal counterexamples to the Hall-Paige conjecture.

Three Janko Groups

Lemma

Let H be a subgroup of G, and $\mathcal{D}$ the set of double cosets of H in G. If $D \in \mathcal{D}$ contains an element of order 3, then $D \subseteq (D^{(-1)})^2$ and $D^{(-1)} \subseteq D^2$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$.

Theorem

J_1 and J_3 are not minimal counterexamples to the Hall-Paige conjecture.

The proof uses the 3-element Lemma, a rank-22 permutation representation of J_1, a rank-14 permutation representation of J_3, and MAGMA.

Three Janko Groups

Lemma

Let H be a subgroup of G, and $\mathcal{D}$ the set of double cosets of H in G. If $D \in \mathcal{D}$ contains an element of order 3, then $D \subseteq (D^{(-1)})^2$ and $D^{(-1)} \subseteq D^2$, where $D^{(-1)} = \{d^{-1} \mid d \in D\}$.

Theorem

J_1 and J_3 are not minimal counterexamples to the Hall-Paige conjecture.

The proof uses the 3-element Lemma, a rank-22 permutation representation of J_1, a rank-14 permutation representation of J_3, and MAGMA.

Theorem (Bray, Personal Communication)

J_4 is not minimal counterexample to the Hall-Paige conjecture.

The proof is obtained by constructing collapsed adjacency matrices for a degree 3,980,549,947 permutation representation of J_4.

Summary: The Last 22 Groups; part a

G	H	Index	Rank
J_1	$A_5 \times 2$	$1,463$	22
J_2	$U_3(3)$	100	3
$^2F_4(2)'$	$L_3(3):2$	1,600	4
HS	$U_3(5):2$	176	2
J_3	$L_2(19)$	$14,688$	14
McL	$U_4(3)$	275	3
He	$S_4(4):2$	$2,058$	5
Ru	$^2F_4(2)$	$4,060$	3
Suz	$G_2(4)$	$1,782$	3
$O'N$	$L_3(7):2$	$122,760$	5
Co_3	$McL:2$	276	2

Summary: The Last 22 Groups; part b

G	H	Index	Rank
Co_2	$U_6(2):2$	$2,300$	3
Fi_{22}	$2^{\cdot}U_6(2)$	$3,510$	3
HN	$2.HS.2$	$1,539,000$	9
Ly	$G_2(5)$	$8,835,156$	5
Th	$2^5.L_5(2)$	$283,599,225$	11
Fi_{23}	$2^{\cdot}Fi_{22}$	$31,671$	3
Co_1	Co_2	$98,280$	4
J_4	$2_+^{1+12}{}^{\cdot}3M_{22}:2$	$3,980,549,947$	?
Fi_{24}'	Fi_{23}	$306,936$	3
B	$2_+^{1+22}.Co_2$	$11,707,448,673,375$	10
M	$2.B$	$97,239,461,142,009,186,000$	9