$G$ finite group
$G' = \langle [x, y] : x, y \in G \rangle$ is the *subgroup* generated by commutators

Not every $g \in G'$ is a commutator $[x, y]$. 

Group $H$ of order 96, $|H'| = 32$ and contains 29 commutators.
**Commutators**

$G$ finite group

$G' = \langle [x, y] : x, y \in G \rangle$ is the *subgroup* generated by commutators

Not every $g \in G'$ is a commutator $[x, y]$. 

Group $H$ of order 96, $|H'| = 32$ and contains 29 commutators.
Commutators

$G$ finite group
$G' = \langle [x, y] : x, y \in G \rangle$ is the *subgroup* generated by commutators

Not every $g \in G'$ is a commutator $[x, y]$.

Group $H$ of order 96, $|H'| = 32$ and contains 29 commutators.
But every element $g$ of $G'$ is a product of commutators.
But every element $g$ of $G'$ is a **product** of commutators.

**Problem**

*Can we bound the length of such a product independently of $g$?*
But every element $g$ of $G'$ is a **product** of commutators.

**Problem**

*Can we bound the length of such a product independently of $g$?*

**Theorem (Nikolov & Segal, 2007)**

*There exists a function $f$ such that if $G$ is a $d$-generator finite group, then every element of $G'$ is a product of $f(d)$ commutators.*
But every element $g$ of $G'$ is a product of commutators.

**Problem**

*Can we bound the length of such a product independently of $g$?*

**Theorem (Nikolov & Segal, 2007)**

*There exists a function $f$ such that if $G$ is a $d$-generator finite group, then every element of $G'$ is a product of $f(d)$ commutators.*

Special interest: $G$ finite simple group.
Every element of a finite simple group is a commutator.
Every element of a finite simple group is a commutator.

Ore proved it for $A_n$: case by case, every relevant combination of cycles dealt with in turn.
The LOST result

Liebeck, O’B, Shalev, Tiep (JEMS, 2010)

**Theorem**

*If* $G$ *is a finite non-abelian simple group, then every* $g \in G$ *is a commutator.*
The LOST result

Liebeck, O’B, Shalev, Tiep (JEMS, 2010)

**Theorem**

*If $G$ is a finite non-abelian simple group, then every $g \in G$ is a commutator.*

In fact: every element of every quasisimple classical group is a commutator.
Not true for arbitrary quasi-simple groups: no element of order 12 in $3A_6$ is a commutator.
Not true for arbitrary quasi-simple groups: no element of order 12 in $3A_6$ is a commutator.

**Theorem**

The only quasisimple groups with non-central elements which are not commutators are covers of $A_6$, $A_7$, $L_3(4)$ and $U_4(3)$.

**Corollary**

Every element of every finite quasisimple group is a product of two commutators.
Overview of the lecture

- A broader context
- The basic approach
- A sketch of the proof
- Related questions
Waring type problems

Shalev et al.: program to express group elements as short products of values of fixed word $w$. 

Let $w = w(x_1, \ldots, x_d)$ be element of free group $F_d$ on $x_1, \ldots, x_d$. Consider word map $w: G_d \rightarrow G$: 

\[
\begin{align*}
G_d & \rightarrow \rightarrow \rightarrow \\
(g_1, \ldots, g_d) & \mapsto w(g_1, \ldots, g_d)
\end{align*}
\]

Set of all group elements $w(g_1, \ldots, g_d)$ is $W(G)$. How large is $W(G)$? Jones (1974) showed it's non-trivial for all $w \neq 1$ if $G$ is large enough.

Can we express $g \in G$ as short product of elements of $W(G)$?

Waring: express every integer as a sum of $f(k)$ $k$-th powers.
Shalev et al.: program to express group elements as short products of values of fixed word \( w \).

Let \( w = w(x_1, \ldots, x_d) \) be element of free group \( F_d \) on \( x_1, \ldots, x_d \).

Consider word map

\[
W_G : G^d \to G
\]

\[
(g_1, \ldots, g_d) \mapsto w(g_1, \ldots, g_d)
\]

Set of all group elements \( w(g_1, \ldots, g_d) \) is \( W(G) \).
Shalev et al.: program to express group elements as short products of values of fixed word $w$.

Let $w = w(x_1, \ldots, x_d)$ be element of free group $F_d$ on $x_1, \ldots, x_d$. Consider word map

$$w_G : G^d \rightarrow G$$

$$(g_1, \ldots, g_d) \mapsto w(g_1, \ldots, g_d)$$

Set of all group elements $w(g_1, \ldots, g_d)$ is $W(G)$.

How large is $W(G)$? Jones (1974) showed it’s non-trivial for all $w \neq 1$ if $G$ is large enough.
Shalev et al.: program to express group elements as short products of values of fixed word $w$. Let $w = w(x_1, \ldots, x_d)$ be element of free group $F_d$ on $x_1, \ldots, x_d$. Consider word map

$$w_G : G^d \rightarrow G$$

$$(g_1, \ldots, g_d) \mapsto w(g_1, \ldots, g_d)$$

Set of all group elements $w(g_1, \ldots, g_d)$ is $W(G)$. How large is $W(G)$? Jones (1974) showed it’s non-trivial for all $w \neq 1$ if $G$ is large enough. Can we express $g \in G$ as short product of elements of $W(G)$?
Waring type problems

Shalev et al.: program to express group elements as short products of values of fixed word \( w \).

Let \( w = w(x_1, \ldots, x_d) \) be element of free group \( F_d \) on \( x_1, \ldots, x_d \). Consider word map

\[
    w_G : G^d \mapsto G \\
    (g_1, \ldots, g_d) \mapsto w(g_1, \ldots, g_d)
\]

Set of all group elements \( w(g_1, \ldots, g_d) \) is \( W(G) \).

How large is \( W(G) \)? Jones (1974) showed it’s non-trivial for all \( w \neq 1 \) if \( G \) is large enough.

Can we express \( g \in G \) as short product of elements of \( W(G) \)?

Waring: express every integer as a sum of \( f(k) \) \( k \)-th powers.
Other much studied words: $x_1^k$ in Burnside-type problems, $x^p y^p$ where $p$ is prime.
Other much studied words: $x_1^k$ in Burnside-type problems, $x^p y^p$ where $p$ is prime.

**Theorem (Shalev, 2009)**

For each $w \neq 1$, there exists $N = N_w$ depending only on $w$ such that if $G$ is a finite simple group of order at least $N$ then $W(G)^3 = G$. 
Covering numbers

$G$ finite simple group, $C \neq \{1\}$ is a conjugacy class.
$G$ finite simple group, $C \neq \{1\}$ is a conjugacy class.

Then there exists $k \in \mathbb{P}$ such that $C^k = G$. 
$G$ finite simple group, $C \neq \{1\}$ is a conjugacy class.

Then there exists $k \in \mathbb{P}$ such that $C^k = G$.

Minimal such $k$ over all classes $C$ is covering number $c(G)$ of $G$. 
$G$ finite simple group, $C \neq \{1\}$ is a conjugacy class.

Then there exists $k \in \mathbb{P}$ such that $C^k = G$.

Minimal such $k$ over all classes $C$ is covering number $c(G)$ of $G$.

Ellers, Gordeev & Herzog (1999); Lawther & Liebeck (1998)

**Theorem**

- $c(A_n) = \lceil (n - 1)/2 \rceil$
- $c(G_r(q)) \leq mr$ for some absolute constant $m$. 
Covering numbers

$G$ finite simple group, $C \neq \{1\}$ is a conjugacy class.
Then there exists $k \in \mathbb{P}$ such that $C^k = G$.
Minimal such $k$ over all classes $C$ is covering number $c(G)$ of $G$.
Ellers, Gordeev & Herzog (1999); Lawther & Liebeck (1998)

Theorem

- $c(A_n) = \lceil (n - 1)/2 \rceil$
- $c(G_r(q)) \leq mr$ for some absolute constant $m$.

Theorem (Liebeck & Shalev, 2001)

$c(C, G) \leq m \log |G|/\log |C|$
Thompson’s conjecture (1985)

Every finite non-abelian simple group $G$ contains a conjugacy class $C$ with $C^2 = G$. 
Every finite non-abelian simple group $G$ contains a conjugacy class $C$ with $C^2 = G$. 

**Lemma**

*Thompson implies Ore.*
Every finite non-abelian simple group $G$ contains a conjugacy class $C$ with $C^2 = G$.

**Lemma**

*Thompson implies Ore.*

**Proof.**

Let $C = x^G$. Now $1 \in G = C^2$ so $x^{-1} \in C$ and $G = (x^{-1})^G x^G$. Hence every element of $G$ is a commutator.
Related probabilistic work

Shalev (2009): if \( g \) is a random element of finite simple group \( G \), then the probability that \( g \) is a commutator tends to 1 as \( |G| \to \infty \).

Garion & Shalev (2009): For finite simple group \( G \), the map \( \alpha : G \times G \to G \) defined by \( \alpha(x, y) = [x, y] \) is almost equidistributed, so almost all elements are commutators.

Applications to the product replacement algorithm.

Theorem (Shalev, 2009) There exists an absolute constant \( c \) such that every finite simple group \( G \) of order at least \( c \) has a conjugacy class \( C \) such that \( C^2 = G \). If \( x \in G \) is random, then probability that \( (xG)^3 = G \) tends to 1 as \( |G| \to \infty \).
Shalev (2009): if $g$ is a random element of finite simple group $G$, then the probability that $g$ is a commutator tends to 1 as $|G| \rightarrow \infty$.

If $G = G_q(r)$, a Lie type simple group of rank $r$ over field of size $q$, then probability is at least $1 - cq^{-2r}$ where $c$ is absolute constant.
Related probabilistic work

Shalev (2009): if $g$ is a random element of finite simple group $G$, then the probability that $g$ is a commutator tends to 1 as $|G| \to \infty$.

If $G = G_q(r)$, a Lie type simple group of rank $r$ over field of size $q$, then probability is at least $1 - cq^{-2r}$ where $c$ is absolute constant.

Garion & Shalev (2009): For finite simple group $G$, the map $\alpha : G \times G \to G$ defined by $\alpha(x, y) = [x, y]$ is almost equidistributed, so almost all elements are commutators.
Related probabilistic work

Shalev (2009): if $g$ is a random element of finite simple group $G$, then the probability that $g$ is a commutator tends to 1 as $|G| \to \infty$.

If $G = G_q(r)$, a Lie type simple group of rank $r$ over field of size $q$, then probability is at least $1 - cq^{-2r}$ where $c$ is absolute constant.

Garion & Shalev (2009): For finite simple group $G$, the map $\alpha : G \times G \to G$ defined by $\alpha(x, y) = [x, y]$ is almost equidistributed, so almost all elements are commutators.

Applications to the product replacement algorithm.

**Theorem (Shalev, 2009)**

There exists an absolute constant $c$ such that every finite simple group $G$ of order at least $c$ has a conjugacy class $C$ such that $C^2 = G$. If $x \in G$ is random, then probability that $(x^G)^3 = G$ tends to 1 as $|G| \to \infty$. 

Eamonn O'Brien
The Ore Conjecture
Theorem (Frobenius, 1896)

Let $G$ be a finite group, let $g$ be a fixed element of $G$, and for $1 \leq i \leq t$ let $C_i$ be a conjugacy class in $G$ with representative $x_i$. The number of solutions to the equation $\prod_{i=1}^{t} y_i = g$ with $y_i \in C_i$ is equal to

$$\frac{|C_1| \cdots |C_t|}{|G|} \sum_{\chi \in \text{Irr}(G)} \frac{\chi(x_1) \cdots \chi(x_t)\chi(g^{-1})}{\chi(1)^{t-1}},$$

where $\text{Irr}(G)$ is the set of ordinary irreducible characters of $G$.

Hence $g \in C^2$ if and only if

$$\sum_{\chi \in \text{Irr}(G)} \frac{\chi(C^2)\chi(g^{-1})}{\chi(1)} \neq 0$$
The Ore criterion

**Theorem (Frobenius, 1896)**

*For fixed* \( g \in G \),

\[
\#\{(x, y) \in G \times G \mid g = [x, y]\} = |G| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)}
\]
The Ore criterion

**Theorem (Frobenius, 1896)**

For fixed $g \in G$,

$$\# \{(x, y) \in G \times G \mid g = [x, y]\} = |G| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)}$$

To show $g \in G$ is commutator, suffices to show that
Theorem (Frobenius, 1896)

For fixed $g \in G$, 

$$\#\{(x, y) \in G \times G \mid g = [x, y]\} = |G| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)}$$

To show $g \in G$ is commutator, suffices to show that 

$$\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0$$
The Ore criterion

Theorem (Frobenius, 1896)

For fixed $g \in G,$

$$\# \{(x, y) \in G \times G \mid g = [x, y]\} = |G| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)}$$

To show $g \in G$ is commutator, suffices to show that

$$\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0$$

Or

$$\left| \sum_{\chi(1) > 1} \frac{\chi(g)}{\chi(1)} \right| < 1$$
The key step

\[ \sum_{\chi \in \text{Irr}(G)} |\chi(g)|^2 = |C_G(g)| \]
The key step

\[ \sum_{\chi \in \text{Irr}(G)} |\chi(g)|^2 = |C_G(g)| \]

Partition elements of \( G \) by centraliser size
The key step

\[ \sum_{\chi \in \text{Irr}(G)} |\chi(g)|^2 = |C_G(g)| \]

Partition elements of $G$ by centraliser size

If $G$ a finite simple group and $g \in G$ has small centraliser then main contribution to

\[ |G| \sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \]

comes from the trivial character $\chi = 1$. 

Eamonn O'Brien

The Ore Conjecture
If $g \in G$ has small centraliser, then

$$\#\{(x, y) \in G \times G \mid g = [x, y]\} = |G|(1 + o(1))$$

where $o(1) \rightarrow 0$ as $|G| \rightarrow \infty$ and $g$ is a commutator when $G$ is large enough.

So elements with small centralisers are commutators. Almost all elements of $G$ have small centralisers.
If $g \in G$ has small centraliser, then

$$\#\{(x, y) \in G \times G \mid g = [x, y]\} = |G|(1 + o(1))$$

where $o(1) \to 0$ as $|G| \to \infty$ and $g$ is a commutator when $G$ is large enough.

So elements with small centralisers are commutators.
If $g \in G$ has small centraliser, then

$$\#\{(x, y) \in G \times G \mid g = [x, y]\} = |G|(1 + o(1))$$

where $o(1) \rightarrow 0$ as $|G| \rightarrow \infty$ and $g$ is a commutator when $G$ is large enough.

So elements with small centralisers are commutators.

Almost all elements of $G$ have small centralisers.
• Ore (1951): conjectured and proved Ore for $A_n$.
• Hsü (1965): Thompson for $A_n$.
• R.C. Thompson (1962-63): Ore for $PSL_n(q)$. Use structure of $G$ to write $g = [x, y]$ based on various kinds of factorisations. Use similarity of matrices.
• Gow (1988): $PSp_n(q), q \equiv 1 \mod 4$. 
• Bonten (1993): $G$ Lie type, rank $r$. There exists a constant $q_0$ such that every element of $G_r(q)$ is a commutator for $q > q_0$. Exploited Frobenius and character ratios to obtain result for exceptionals of rank at most 4.

• Gow (2000): If $C$ is a class of regular semisimple real elements in simple group of Lie type, then $C^2 = G$. 

Theorem (Ellers & Gordeev, 1998) If Chevellay group $G$ has two regular semisimple elements $h_1$ and $h_2$ in a maximal split torus, then $G \setminus Z(G) \subset C_1 C_2$. Ore follows if $G$ has regular semisimple element $h$ in maximal split torus; Thompson if $h$ is real. Ore and Thompson hold for finite simple groups if $q \geq 8$. 

Eamonn O’Brien The Ore Conjecture
• Bonten (1993): $G$ Lie type, rank $r$. There exists a constant $q_0$ such that every element of $G_r(q)$ is a commutator for $q > q_0$. Exploited Frobenius and character ratios to obtain result for exceptionals of rank at most 4.

• Gow (2000): If $C$ is a class of regular semisimple real elements in simple group of Lie type, then $C^2 = G$.

**Theorem (Ellers & Gordeev, 1998)**

*If Chevellay group $G$ has two regular semisimple elements $h_1$ and $h_2$ in a maximal split torus, then $G \setminus Z(G) \subseteq C_1 C_2$.***
• Bonten (1993): $G$ Lie type, rank $r$. There exists a constant $q_0$ such that every element of $G_r(q)$ is a commutator for $q > q_0$. Exploited Frobenius and character ratios to obtain result for exceptionals of rank at most 4.

• Gow (2000): If $C$ is a class of regular semisimple real elements in simple group of Lie type, then $C^2 = G$.

---

Theorem (Ellers & Gordeev, 1998)

If Chevallay group $G$ has two regular semisimple elements $h_1$ and $h_2$ in a maximal split torus, then $G \setminus Z(G) \subset C_1 C_2$.

Ore follows if $G$ has regular semisimple element $h$ in maximal split torus; Thompson if $h$ is real.
• Bonten (1993): $G$ Lie type, rank $r$. There exists a constant $q_0$ such that every element of $G_r(q)$ is a commutator for $q > q_0$. Exploited Frobenius and character ratios to obtain result for exceptionals of rank at most 4.

• Gow (2000): If $C$ is a class of regular semisimple real elements in simple group of Lie type, then $C^2 = G$.

**Theorem (Ellers & Gordeev, 1998)**

*If Chevellay group $G$ has two regular semisimple elements $h_1$ and $h_2$ in a maximal split torus, then $G \setminus Z(G) \subset C_1 C_2$.*

Ore follows if $G$ has regular semisimple element $h$ in maximal split torus; Thompson if $h$ is real.

Ore and Thompson hold for finite simple groups if $q \geq 8$. 

Eamonn O'Brien  |  The Ore Conjecture
To show $g \in G$ is commutator, suffices to show that

$$\sum_{\chi \in \text{Irr}(G)} \chi(g) \chi(1) \neq 0 \quad \text{or} \quad |\sum_{\chi \in \text{Irr}(G)} \chi(g) \chi(1)| < 1.$$
To show \( g \in G \) is commutator, suffices to show that

\[
\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0
\]
To show $g \in G$ is commutator, suffices to show that

$$\sum_{\chi \in \text{Irr}(G)} \frac{\chi(g)}{\chi(1)} \neq 0$$

or

$$\left| \sum_{\chi(1) > 1} \frac{\chi(g)}{\chi(1)} \right| < 1$$

Key: partition elements by centraliser size.
Use existing knowledge of chars, Deligne-Lusztig theory, and the theory of dual pairs and Weil characters of classical groups to construct \textit{explicitly} irreducible characters of relatively small degrees, and to derive information on their character values.
$|C_G(g)|$ is small

Use existing knowledge of chars, Deligne-Lusztig theory, and the theory of dual pairs and Weil characters of classical groups to construct \textit{explicitly} irreducible characters of relatively small degrees, and to derive information on their character values.

Show $|\chi(g)|/\chi(1)$ is small for $\chi \neq 1$, so main contribution to $\sum_{\chi \in \text{Irr}(G)} \chi(g)/\chi(1)$ comes from $\chi = 1$. 

Hence deduce that sum is positive, and so elements with small centralisers are commutators.
Use existing knowledge of chars, Deligne-Lusztig theory, and the theory of dual pairs and Weil characters of classical groups to construct \textit{explicitly} irreducible characters of relatively small degrees, and to derive information on their character values.

Show \(|\chi(g)\)/\(\chi(1)\) is small for \(\chi \neq 1\), so main contribution to \(\sum_{\chi \in \text{Irr}(G)} \chi(g)/\chi(1)\) comes from \(\chi = 1\).

Hence deduce that sum is positive, and so elements with small centralisers are commutators.
$|C_G(g)|$ is large.

Reduce problem to groups of smaller rank and use induction. Usually such $g \in G$ has decomposition into Jordan blocks, and so lies in direct product of smaller classical groups.
$|C_G(g)|$ is large

Reduce problem to groups of *smaller rank* and use induction.
Reduce problem to groups of *smaller rank* and use induction.

Usually such $g \in G$ has decomposition into Jordan blocks, and so lies in direct product of smaller classical groups.
Let $G = Cl(V) = Sp(V), SU(V)$ or $\Omega(V)$.

**Definition**

$x \in G$ is *breakable* if there is a proper, nonzero, non-degenerate subspace $W$ of $V$ such that $x = (x_1, x_2) \in Cl(W) \times Cl(W^\perp)$, and one of the following holds:

- both factors $Cl(W)$ and $Cl(W^\perp)$ are perfect groups;
- $Cl(W)$ is perfect, and $x_2$ is a commutator in $Cl(W^\perp)$.

Otherwise, $x$ is *unbreakable*. 
Lemma

Suppose that whenever $W$ is a non-degenerate subspace of $V$ such that $\text{Cl}(W)$ is a perfect group, every unbreakable element of $\text{Cl}(W)$ is a commutator in $\text{Cl}(W)$. Then every element of the perfect group $G$ is a commutator.
Lemma

Suppose that whenever $W$ is a non-degenerate subspace of $V$ such that $\text{Cl}(W)$ is a perfect group, every unbreakable element of $\text{Cl}(W)$ is a commutator in $\text{Cl}(W)$. Then every element of the perfect group $G$ is a commutator.

Proof.

The proof goes by induction on $\dim V$. 
Lemma

Suppose that whenever $W$ is a non-degenerate subspace of $V$ such that $\text{Cl}(W)$ is a perfect group, every unbreakable element of $\text{Cl}(W)$ is a commutator in $\text{Cl}(W)$. Then every element of the perfect group $G$ is a commutator.

Proof.

The proof goes by induction on $\text{dim} \ V$.

The inductive hypothesis holds for all perfect subgroups of $G$ of the form $\text{Cl}(X)$ with $X$ a non-degenerate subspace of $V$. 
Lemma

*Suppose that whenever* $W$ *is a non-degenerate subspace of* $V$ *such that* $Cl(W)$ *is a perfect group, every unbreakable element of* $Cl(W)$ *is a commutator in* $Cl(W)$. *Then every element of the perfect group* $G$ *is a commutator.*

Proof.

The proof goes by induction on $\dim V$.

The inductive hypothesis holds for all perfect subgroups of $G$ of the form $Cl(X)$ with $X$ a non-degenerate subspace of $V$.

If $x \in G$ is unbreakable, then it is a commutator by hypothesis.
Lemma

Suppose that whenever $W$ is a non-degenerate subspace of $V$ such that $Cl(W)$ is a perfect group, every unbreakable element of $Cl(W)$ is a commutator in $Cl(W)$. Then every element of the perfect group $G$ is a commutator.

Proof.

The proof goes by induction on $\dim V$.

The inductive hypothesis holds for all perfect subgroups of $G$ of the form $Cl(X)$ with $X$ a non-degenerate subspace of $V$.

If $x \in G$ is unbreakable, then it is a commutator by hypothesis.

Otherwise $x$ is breakable, so $x = (x_1, x_2) \in Cl(W) \times Cl(W^\perp)$ satisfies (1) or (2).
Lemma

Suppose that whenever $W$ is a non-degenerate subspace of $V$ such that $\text{Cl}(W)$ is a perfect group, every unbreakable element of $\text{Cl}(W)$ is a commutator in $\text{Cl}(W)$. Then every element of the perfect group $G$ is a commutator.

Proof.

The proof goes by induction on $\dim V$.

The inductive hypothesis holds for all perfect subgroups of $G$ of the form $\text{Cl}(X)$ with $X$ a non-degenerate subspace of $V$.

If $x \in G$ is unbreakable, then it is a commutator by hypothesis.

Otherwise $x$ is breakable, so $x = (x_1, x_2) \in \text{Cl}(W) \times \text{Cl}(W^\perp)$ satisfies (1) or (2).

In either case, by induction $x_1, x_2$ are commutators in $\text{Cl}(W), \text{Cl}(W^\perp)$ respectively, and so $x$ is a commutator, as required.
Difficulties with reduction

Some blocks may lie in a group which is not perfect, such as $\text{Sp}_2(2), \text{Sp}_2(3), \text{Sp}_4(2), \Omega^+_4(2)$; or in orthogonal case blocks may have determinant $-1$.

Unitary groups: Jordan blocks can have many different determinants. e.g. 8 possible values for $\text{PSU}_n(7)$.

Instead solve certain equations in unitary groups, and establish certain properties of unitary matrices in small dimensions.
Difficulties with reduction

- Some blocks may lie in a group which is not perfect, such as $Sp_2(2)$, $Sp_2(3)$, $Sp_4(2)$, $\Omega^+_4(2)$; or in orthogonal case blocks may have determinant $-1$. 

Unitary groups: Jordan blocks can have many different determinants. E.g. 8 possible values for $PSU_n(7)$. Instead solve certain equations in unitary groups, and establish certain properties of unitary matrices in small dimensions.
Difficulties with reduction

- Some blocks may lie in a group which is not perfect, such as $Sp_2(2)$, $Sp_2(3)$, $Sp_4(2)$, $\Omega_4^+(2)$; or in orthogonal case blocks may have determinant $-1$.

- Unitary groups: Jordan blocks can have many different determinants. e.g. 8 possible values for $PSU_n(7)$. 

Eamonn O’Brien  The Ore Conjecture
Difficulties with reduction

- Some blocks may lie in a group which is not perfect, such as $Sp_2(2)$, $Sp_2(3)$, $Sp_4(2)$, $\Omega_4^+(2)$; or in orthogonal case blocks may have determinant $-1$.

- Unitary groups: Jordan blocks can have many different determinants. e.g. 8 possible values for $PSU_n(7)$.

Instead solve certain equations in unitary groups, and establish certain properties of unitary matrices in small dimensions.
Enough to prove that unbreakable $g \in G = Cl(V)$ is commutator.

- If $g$ unbreakable, then $|C_G(g)|$ is small.
Enough to prove that unbreakable $g \in G = Cl(V)$ is commutator.

- If $g$ unbreakable, then $|C_G(g)|$ is small.
- For unbreakable $g$ and $n > n_0$, prove that $g$ is a commutator.
Enough to prove that unbreakable $g \in G = Cl(V)$ is commutator.

- If $g$ unbreakable, then $|C_G(g)|$ is small.
- For unbreakable $g$ and $n > n_0$, prove that $g$ is a commutator.
- Induction base: prove Ore for $Cl_n(q)$ for $n \leq n_0$. 
Lemma

Assume \( n \geq 7 \), and let \( x \) be an unbreakable element of \( G = \text{Sp}(V) = \text{Sp}_{2n}(2) \). Then \( |C_G(x)| < 2^{2n+15} \).

Based on detailed analysis of Jordan forms of elements.
Lemma

Assume \( n \geq 7 \), and let \( x \) be an unbreakable element of \( G = \text{Sp}(V) = \text{Sp}_{2n}(2) \). Then \( |C_G(x)| < 2^{2n+15} \).

Based on detailed analysis of Jordan forms of elements.

Let \( k(G) \) be number of conjugacy classes of \( G \).

Theorem (Fulman & Guralnick, 2009)

\( k(\text{Sp}_{2n}(q)) \leq 12q^n \) if \( q \) is odd, and \( k(\text{Sp}_{2n}(q)) \leq 17q^n \) if \( q \) is even.
Theorem (Guralnick & Tiep, 2004)

Let $G = \text{Sp}_{2n}(q)$ with $q$ even, $n \geq 4$. There is a collection $\mathcal{W}$ of $q + 3$ irreducible characters of $G$, such that

- $\chi(1) \geq \frac{(q^n-1)(q^n-q)}{2(q+1)}$ if $\chi \in \mathcal{W}$,
- $\chi(1) \geq \frac{1}{2}(q^{2n} - 1)(q^{n-1} - 1)(q^{n-1} - q^2)/(q^4 - 1)$ for $1 \neq \chi \in \text{Irr}(G)\backslash \mathcal{W}$.

Partition sum of non-trivial char values for unbreakable $g \in G$ as

$$S_1(g) = \sum_{\chi \in \mathcal{W}} \frac{\chi(g)}{\chi(1)}, \quad S_2(g) = \sum_{1 \neq \chi \in \text{Irr}(G)\backslash \mathcal{W}} \frac{\chi(g)}{\chi(1)},$$

and show $|S_1(g)| + |S_2(g)| < 1$. 

Eamonn O'Brien
The Ore Conjecture
Some facts

- \( \sum_{\chi \in \text{Irr}(G)} |\chi(g)| \leq k(G)^{1/2}|C_G(g)|^{1/2} \)
Some facts

- \[ \sum_{\chi \in \text{Irr}(G)} |\chi(g)| \leq k(G)^{1/2} |C_G(g)|^{1/2} \]

- If \( \chi_1, \ldots, \chi_k \in \text{Irr}(G) \) are distinct characters of degree \( \geq N \), then

\[
\sum_{\chi \in \text{Irr}(G), \chi(1) \geq N} \frac{|\chi(g)|}{\chi(1)} \leq \frac{k(G)^{1/2} |C_G(g)|^{1/2}}{N}.
\]
We can readily bound $S_2(x)$.

**Lemma**

*Suppose $n \geq 7$. If $|C_G(x)| < 2^{2n+15}$, then $|S_2(x)| < 0.6$.***
We can readily bound $S_2(x)$.

**Lemma**

Suppose $n \geq 7$. If $|C_G(x)| < 2^{2n+15}$, then $|S_2(x)| < 0.6$.

**Proof.**

$S_2(x)$ is sum over at most $k(G)$ characters, each of degree at least

$$\frac{1}{30}(2^{2n} - 1)(2^{n-1} - 1)(2^{n-1} - 4).$$
We can readily bound $S_2(x)$.

**Lemma**

*Suppose $n \geq 7$. If $|C_G(x)| < 2^{2n+15}$, then $|S_2(x)| < 0.6$.***

**Proof.**

$S_2(x)$ is sum over at most $k(G)$ characters, each of degree at least

$$\frac{1}{30}(2^{2n} - 1)(2^{n-1} - 1)(2^{n-1} - 4).$$

Deduce that

$$|S_2(x)| < \frac{30\sqrt{17} \cdot 2^{n/2} |C_G(x)|^{1/2}}{(2^{2n} - 1)(2^{n-1} - 1)(2^{n-1} - 4)}.$$
We can readily bound $S_2(x)$.

**Lemma**

Suppose $n \geq 7$. If $|C_G(x)| < 2^{2n+15}$, then $|S_2(x)| < 0.6$.

**Proof.**

$S_2(x)$ is sum over at most $k(G)$ characters, each of degree at least

$$\frac{1}{30}(2^{2n} - 1)(2^{n-1} - 1)(2^{n-1} - 4).$$

Deduce that

$$|S_2(x)| < \frac{30\sqrt{17} \cdot 2^n/2|C_G(x)|^{1/2}}{(2^{2n} - 1)(2^{n-1} - 1)(2^{n-1} - 4)}.$$

This is less than 0.6 when $|C_G(x)| < 2^{2n+15}$ and $n \geq 7$. □
Suppose $n \geq 7$. If $|C_G(x)| < 2^{2n+15}$, then $|S_1(x)| < 0.2$.

Bound for $S_1$ based on a detailed analysis of the characters in $\mathcal{W}$, taken from Guralnick & Tiep (2004).
Some very hard base cases where Ore must be verified directly: e.g. $Sp(12, q)$, $\Omega_{11}(3)$, $SU_6(7)$
The induction base

Some very hard base cases where Ore must be verified directly: e.g. $Sp(12, q)$, $\Omega_{11}(3)$, $SU_6(7)$

In most cases, directly verified the conjecture by constructing character table using Unger algorithm as implemented in Magma.
Some very hard base cases where Ore must be verified directly:
e.g. $Sp(12, q)$, $\Omega_{11}(3)$, $SU_6(7)$

In most cases, directly verified the conjecture by constructing character table using Unger algorithm as implemented in Magma.

Variations needed for $Sp_{16}(2)$. 
Some very hard base cases where Ore must be verified directly: e.g. $Sp(12, q), \Omega_{11}(3), SU_6(7)$

In most cases, directly verified the conjecture by constructing character table using Unger algorithm as implemented in Magma.

Variations needed for $Sp_{16}(2)$.

For unitary groups: certain equations solved explicitly by finding elements which satisfy these.
Some very hard base cases where Ore must be verified directly:
e.g. $Sp(12, q), \Omega_{11}(3), SU_6(7)$

In most cases, directly verified the conjecture by constructing
character table using Unger algorithm as implemented in Magma.

Variations needed for $Sp_{16}(2)$.

For unitary groups: certain equations solved explicitly by finding
elements which satisfy these.

About 3 years of CPU time.
Every element is a commutator:
Every element is a commutator:

Goto (1949): in a connected compact semisimple group.
The infinite context

Every element is a commutator:

Goto (1949): in a connected compact semisimple group.

Pasiencier & Wang (1962): in a semisimple algebraic group over $\mathbb{C}$. 

Eamonn O'Brien  The Ore Conjecture
Every element is a commutator:

Goto (1949): in a connected compact semisimple group.

Pasiencier & Wang (1962): in a semisimple algebraic group over $\mathbb{C}$.

Ree (1964): in a connected semisimple algebraic group defined over an algebraically closed field.
A related question

Problem

*Can every element of a finite simple group be obtained as a commutator of a generating pair?*

No! Only 44 of the elements of $A_5$ can be obtained in this way; 146 elements of $PSL(2,7)$.

McCullough & Wanderley: true for $PSL(2,q)$ for $q \geq 11$.

Garrion & Shalev (2009): “almost every” element is obtained as commutator of a generating pair.
Can every element of a finite simple group be obtained as a commutator of a generating pair?

No! Only 44 of the elements of $A_5$ can be obtained in this way; 146 elements of $PSL(2, 7)$. 

McCullough & Wanderley: true for $PSL(2, q)$ for $q \geq 11$.

Garrion & Shalev (2009): “almost every” element is obtained as commutator of a generating pair.
A related question

Problem

Can every element of a finite simple group be obtained as a commutator of a generating pair?

No! Only 44 of the elements of $A_5$ can be obtained in this way; 146 elements of $PSL(2, 7)$.

McCullough & Wanderley: true for $PSL(2, q)$ for $q \geq 11$. 
Problem

*Can every element of a finite simple group be obtained as a commutator of a generating pair?*

No! Only 44 of the elements of $A_5$ can be obtained in this way; 146 elements of $PSL(2, 7)$.

McCullough & Wanderley: true for $PSL(2, q)$ for $q \geq 11$.

Garrion & Shalev (2009): “almost every” element is obtained as commutator of a generating pair.