

The Ore Conjecture

Eamonn O'Brien

University of Auckland

November 2009

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.

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.

The Ore Conjecture (1951)

Every element of a finite non-abelian simple group is a commutator.

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

Liebeck, O'B, Shalev, Tiep (To appear, JEMS)

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.

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

$$\begin{aligned}w_G : G^d &\longmapsto G \\(g_1, \dots, g_d) &\longmapsto w(g_1, \dots, g_d)\end{aligned}$$

Set of all group elements $w(g_1, \dots, g_d)$ 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.

Another much-studied word: x_1^k in Burnside-type problems.

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 $W(G)^3 = G$.

G finite non-abelian 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 $C^2 = G$.

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 $|G| \mapsto \infty$.

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 $\alpha : G \times G \mapsto G$ 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 $|G| \mapsto \infty$.

The Thompson criterion

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 $g \in G$,

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

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

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

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 $\chi = 1$.

If $g \in G$ has small centraliser, then

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

where $o(1) \mapsto 0$ as $|G| \mapsto \infty$ 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 and similarity of matrices.
- Brenner (1983), Sourour (1986), Lev (1994): Thompson for $PSL_n(q)$.
- Neubüser, Pahlings, Cleavers (1988): sporadics.
- Gow (1988): $PSp_n(q)$, $q \equiv 1 \pmod{4}$.

- Bonten (1993): 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 Chevella 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 $q \geq 8$.

Sketch of LOST proof

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 *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.

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 $G = CI(V) = Sp(V)$, $SU(V)$ or $\Omega(V)$.

Definition

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

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

Otherwise, x is *unbreakable*.

Lemma

Suppose that whenever W is a non-degenerate subspace of V such that $CI(W)$ is a perfect group, every unbreakable element of $CI(W)$ is a commutator in $CI(W)$. 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 $CI(X)$ 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 $x = (x_1, x_2) \in CI(W) \times CI(W^\perp)$ satisfies (1) or (2).

In either case, by induction x_1, x_2 are commutators in $CI(W)$, $CI(W^\perp)$ respectively, and so x is a commutator, as required. \square

- 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.

Proving Ore for unbreakable elements

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 $G = Sp(V) = Sp_{2n}(2)$. 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)

$k(Sp_{2n}(q)) \leq 12q^n$ if q is odd, and $k(Sp_{2n}(q)) \leq 17q^n$ if q is even.

Theorem (Guralnick & Tiep, 2004)

Let $G = Sp_{2n}(q)$ 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 $1 \neq \chi \in \text{Irr}(G) \setminus \mathcal{W}$.

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

$$\mathcal{S}_1(g) = \sum_{\chi \in \mathcal{W}} \frac{\chi(g)}{\chi(1)}, \quad \mathcal{S}_2(g) = \sum_{1 \neq \chi \in \text{Irr}(G) \setminus \mathcal{W}} \frac{\chi(g)}{\chi(1)},$$

and show $|\mathcal{S}_1(g)| + |\mathcal{S}_2(g)| < 1$.

- $\sum_{\chi \in \text{Irr}(G)} |\chi(g)| \leq k(G)^{1/2} |C_G(g)|^{1/2}$
- If $\chi_1, \dots, \chi_k \in \text{Irr}(G)$ 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 $\mathcal{S}_2(x)$.

Lemma

Suppose $n \geq 7$. If $|C_G(x)| < 2^{2n+15}$, then $|\mathcal{S}_2(x)| < 0.6$.

Proof.

$\mathcal{S}_2(x)$ 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

$$|\mathcal{S}_2(x)| < \frac{30\sqrt{17} \cdot 2^{n/2} |C_G(x)|^{1/2}}{(2^{2n} - 1)(2^{n-1} - 1)(2^{n-1} - 4)}.$$

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

Lemma

Suppose $n \geq 7$. If $|C_G(x)| < 2^{2n+15}$, then $|\mathcal{S}_1(x)| < 0.2$.

Bound for \mathcal{S}_1 based on a detailed analysis of the characters in \mathcal{W} , taken from Guralnick & Tiep (2004).

▶ Skip to induction

The orthogonal groups

Assume $G = \Omega_{2n}^{\pm}(q)$ where $n \geq 6$.

If $g \in \Omega_{2n}(q)$ is unbreakable, then $|C_G(g)| < 2^{10} \cdot q^{2n+6}$.

Use estimates for $k(G)$ to deduce that

$$|\mathcal{S}_2| \leq \frac{(2^{20} q^{(3n+3)})^{1/2}}{q^{4n-10}} < 0.1$$

where \mathcal{S}_2 is set of chars of degree $> q^{4n-10}$.

Use Deligne-Lusztig theory, theory of dual pairs and Weil characters to construct *explicitly* the characters and their values in complement \mathcal{S}_1 and deduce that $|\mathcal{S}_1| < 0.8$.

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.

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.

▶ Skip to query

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.

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.