Word maps on finite simple groups

Eamonn O'Brien

University of Auckland

April 2014

Word maps

Let $w = w(x_1, \ldots, x_k)$ be element of free group F_k on $x_1, \ldots, x_k$. The word map determined by w is the following:

$$\begin{array}{rcl} w : G^k & \longmapsto & G \\ (g_1, \ldots, g_k) & \longmapsto & w(g_1, \ldots, g_k) \end{array}$$

Word maps

Let $w = w(x_1, \ldots, x_k)$ be element of free group F_k on $x_1, \ldots, x_k$.
The word map determined by w is the following:

$$\begin{array}{rcl} w : G^k & \longmapsto & G \\ (g_1, \ldots, g_k) & \longmapsto & w(g_1, \ldots, g_k) \end{array}$$

Example

$w = x_1^m$, word map $g \mapsto g^m$
$w = [x_1, x_2]$, word map $(g, h) \mapsto [g, h]$.

Word maps

Let $w = w(x_1, \ldots, x_k)$ be element of free group F_k on $x_1, \ldots, x_k$.
The word map determined by w is the following:

$$\begin{array}{ccc} w : G^k & \longmapsto & G \\ (g_1, \ldots, g_k) & \longmapsto & w(g_1, \ldots, g_k) \end{array}$$

Example

$w = x_1^m$, word map $g \mapsto g^m$
$w = [x_1, x_2]$, word map $(g, h) \mapsto [g, h]$.

$w(G) = \{w(g_1, \ldots, g_k) : g_i \in G\}$ image of word map

$w(G)$ is a union of conjugacy classes of G, a normal subset.

How large is $w(G)$?

How large is $w(G)$?

Example

$G = A_5, w = [x_1, x_2], w(G) = G$

$G = A_5, w = x_1^2, \#w(G) = 45$, union of classes of order $1, 3, 5$.

How large is $w(G)$?

Example

$G = A_5, w = [x_1, x_2], w(G) = G$
$G = A_5, w = x_1^2, \#w(G) = 45$, union of classes of order $1, 3, 5$.

Let G be finite non-abelian simple group. Then $N := \langle w(G) \rangle \lhd G$, and so $N = 1$ or $N = G$.

How large is $w(G)$?

Example

$G = A_5, w = [x_1, x_2], w(G) = G$
$G = A_5, w = x_1^2, \#w(G) = 45$, union of classes of order $1, 3, 5$.

Let G be finite non-abelian simple group. Then $N := \langle w(G) \rangle \lhd G$, and so $N = 1$ or $N = G$.

Jones (1974): if $w \neq 1$ then there exists N_w such that $w(G) \neq 1$ for all simple groups G with $|G| > N_w$.

w-width

Let G be a finite simple group with $w(G) \neq 1$.

Question

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

w-width

Let G be a finite simple group with $w(G) \neq 1$.

Question

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

The w-width of G is $\min\{n : w(G)^n = G\}$.

Surjective words

If w-width is 1, then w is a surjective word on G.

Surjective words

If w-width is 1, then w is a surjective word on G.

Question

What words are surjective?

Surjective words

If w-width is 1, then w is a surjective word on G.

Question

What words are surjective?

Segal (2009): certain words are surjective on all groups – those in cosets of the form $x_1^{e_1} \ldots . x_k^{e_k} F_k'$ where the e_i are integers with $\gcd(e_1, \ldots, e_k) = 1$.

Surjective words

If w-width is 1, then w is a surjective word on G.

Question

What words are surjective?

Segal (2009): certain words are surjective on all groups – those in cosets of the form $x_1^{e_1} \ldots . x_k^{e_k} F_k'$ where the e_i are integers with $\gcd(e_1, \ldots, e_k) = 1$.

Example

$w = x_1$ or the result of applying Nielsen transformations to w, primitive words, elements of a free basis of F_k.

Surjective words

If w-width is 1, then w is a surjective word on G.

Question

What words are surjective?

Segal (2009): certain words are surjective on all groups – those in cosets of the form $x_1^{e_1} \ldots . x_k^{e_k} F_k'$ where the e_i are integers with $\gcd(e_1, \ldots, e_k) = 1$.

Example

$w = x_1$ or the result of applying Nielsen transformations to w, primitive words, elements of a free basis of F_k.

Example

$w = x_1^2$ is not surjective on any finite simple group: the map is not injective since there are always elements of order 2. More generally $w = x_1^k$ is not surjective on G if $|G|$ is not coprime to k.

Theorem (Liebeck - Shalev, 2001)

Let $w \neq 1$. There are constants $c(w)$ and N_w depending only on w such that $w(G)^{c(w)} = G$ for all finite simple groups G of order at least N_w.

Theorem (Liebeck - Shalev, 2001)

Let $w \neq 1$. There are constants $c(w)$ and N_w depending only on w such that $w(G)^{c(w)} = G$ for all finite simple groups G of order at least N_w.

Can we make $c(w)$ explicit? Yes.

Theorem (Liebeck - Shalev, 2001)

Let $w \neq 1$. There are constants $c(w)$ and N_w depending only on w such that $w(G)^{c(w)} = G$ for all finite simple groups G of order at least N_w.

Can we make $c(w)$ explicit? Yes.

Theorem (Larsen-Shalev-Tiep, 2009–2011)

For each $w \neq 1$, there exists N_w depending only on w such that if G is a finite simple group of order at least N_w then $w(G)^2 = G$.

2 is the best possible – power words are not surjective.

Is the commutator word surjective?

Is the commutator word surjective?

G finite group

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

Is the commutator word surjective?

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 $[x, y]$.

Is the commutator word surjective?

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.

Is the commutator word surjective?

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.

Is the commutator word surjective?

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.

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.

Ore Conjecture (1951)

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

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.

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 (JEMS, 2010)

Theorem

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

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 (JEMS, 2010)

Theorem

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

So the commutator word is surjective.

Thompson's conjecture (1985)

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

Thompson's conjecture (1985)

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

Lemma

Thompson implies Ore.

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. □

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

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

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

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

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

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

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

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

The Ore criterion

Theorem (Frobenius, 1896)

For fixed $g \in G$,

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

The Ore criterion

Theorem (Frobenius, 1896)

For fixed $g \in G$,

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

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

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

The Ore criterion

Theorem (Frobenius, 1896)

For fixed $g \in G$,

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

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

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

Or

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

Earlier work on Ore

- 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.
- Brenner (1983), Sourour (1986), Lev (1994): Thompson for $PSL_n(q)$.
- Neubüser, Pahlings, Cleuvers (1988): sporadics.
- Gow (1988): $PSp_n(q)$, $q \equiv 1 \bmod 4$.

- 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 $C^2 = G$.

- 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 $G \setminus Z(G) \subset C_1 C_2$.

- 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.

- 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 $q \geq 8$.

Sketch of LOST proof

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

Sketch of LOST proof

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

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

Sketch of LOST proof

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

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

or

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

The key step

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

The key step

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

Key: partition elements by centraliser size.

The key step

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

Key: partition elements by centraliser size.

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

$$|G| \sum_{\chi \in \mathrm{Irr(G)}} \frac{\chi(g)}{\chi(1)}$$

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

$|C_G(g)|$ is *small*

Use existing knowledge of chars, Deligne-Lusztig theory, and the theory of dual pairs and Weil characters of classical groups to construct *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 *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 $\sum_{\chi \in \mathrm{Irr(G)}} \chi(g)/\chi(1)$ comes from $\chi = 1$.

$|C_G(g)|$ is *small*

Use existing knowledge of chars, Deligne-Lusztig theory, and the theory of dual pairs and Weil characters of classical groups to construct *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 $\sum_{\chi \in \mathrm{Irr(G)}} \chi(g)/\chi(1)$ comes from $\chi = 1$.

Hence deduce that sum is positive, and so elements with small centralisers are commutators.

$|C_G(g)|$ is *large*

$|C_G(g)|$ is *large*

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

$|C_G(g)|$ 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.

Difficulties with reduction

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.

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 $PSU_n(7)$.

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.

The induction base

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

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.

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 $Sp_{16}(2)$.

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.

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.

Related results

Related results

Theorem (LOST 2012)

Let G be a finite quasisimple group not on a known list of 15 exceptions. Every element of G is a commutator.

Related results

Theorem (LOST 2012)

Let G be a finite quasisimple group not on a known list of 15 exceptions. Every element of G is a commutator.

Smallest exception: no element of order 12 in $3A_6$ is a commutator.

Related results

Theorem (LOST 2012)

Let G be a finite quasisimple group not on a known list of 15 exceptions. Every element of G is a commutator.

Smallest exception: no element of order 12 in $3A_6$ is a commutator.

Guralnick and Malle (2012); LOST (2012)

Theorem

Every element of every finite non-abelian simple group is a product of two p-th powers for prime p. In other words, $x^p y^p$ is surjective.

Non-surjective words?

Non-surjective words?

Conjecture (Shalev, 2009)

If $w(x_1, x_2)$ is not a proper power of a non-trivial word, then the corresponding word map is surjective on $\mathrm{PSL}_2(q)$ for all sufficiently large q.

Non-surjective words?

Conjecture (Shalev, 2009)

If $w(x_1, x_2)$ is not a proper power of a non-trivial word, then the corresponding word map is surjective on $\mathrm{PSL}_2(q)$ for all sufficiently large q.

Theorem (Jambor, Liebeck, O'B, 2014)

Let $w = x_1^2[x_1^{-2}, x_2^{-1}]^2$. The word map is non-surjective on $\mathrm{PSL}(2, p^{2r+1})$ for all non-negative integers r and all odd primes $p \neq 5$ such that $p^2 \not\equiv 1 \bmod 16$ and $p^2 \not\equiv 1 \bmod 5$.

So for example it is non-surjective for $\mathrm{PSL}(2, 3^{2r+1})$

Non-surjective words?

Conjecture (Shalev, 2009)

If $w(x_1, x_2)$ is not a proper power of a non-trivial word, then the corresponding word map is surjective on $\mathrm{PSL}_2(q)$ for all sufficiently large q.

Theorem (Jambor, Liebeck, O'B, 2014)

Let $w = x_1^2[x_1^{-2}, x_2^{-1}]^2$. The word map is non-surjective on $\mathrm{PSL}(2, p^{2r+1})$ for all non-negative integers r and all odd primes $p \neq 5$ such that $p^2 \not\equiv 1 \bmod 16$ and $p^2 \not\equiv 1 \bmod 5$.

So for example it is non-surjective for $\mathrm{PSL}(2, 3^{2r+1})$

First example of word map non-surjective on an infinite family of finite non-abelian simple groups.

Method of proof

Method of proof

Investigate traces of 2×2 matrices in $\mathrm{SL}(2, q)$.

Method of proof

Investigate traces of 2×2 matrices in $\mathrm{SL}(2, q)$.

Fricke-Klein showed that for any w, there is a polynomial P_w such that for all $x, y \in G$

$$Tr(w(x, y)) = P_w(Tr(x), Tr(y), Tr(xy)) = P_w(s, t, u)$$

Method of proof

Investigate traces of 2×2 matrices in $\mathrm{SL}(2, q)$.

Fricke-Klein showed that for any w, there is a polynomial P_w such that for all $x, y \in G$

$$Tr(w(x, y)) = P_w(Tr(x), Tr(y), Tr(xy)) = P_w(s, t, u)$$

Get polynomial of degree 10 in three variables

Method of proof

Investigate traces of 2×2 matrices in $\mathrm{SL}(2, q)$.

Fricke-Klein showed that for any w, there is a polynomial P_w such that for all $x, y \in G$

$$Tr(w(x, y)) = P_w(Tr(x), Tr(y), Tr(xy)) = P_w(s, t, u)$$

Get polynomial of degree 10 in three variables

We prove: $P_w \neq 0$ for all $s, t, u \in F$