Images of word maps in almost simple groups and quasisimple groups

Matthew Levy

Imperial College London, Supervisor: Nikolay Nikolov

Groups St Andrews 2013

Outline

Outline

1. Introduction
   - Word maps
   - Images of Word Maps
2. The Simple Groups
3. Other Groups
   - Almost Simple Groups
   - Symmetric Groups
   - Quasisimple Groups

Word maps

Let w be an element of the free group of rank k and let G be a group. We can define a *word map*, $w : G^k \to G$, by substitution:

$$w : G^k \longrightarrow G;$$
$$(g_1, ..., g_k) \longmapsto w(g_1, ..., g_k).$$

For example:

- $w(x) = x^n$;
- $w(x, y) = [x, y]$.

We will denote by G_w the *verbal image* of w over G:

$$G_w := \{w(g_1, ..., g_k) : g_i \in G\}.$$

Define the *verbal subgroup*, $w(G) = \langle G_w^{\pm 1} \rangle$.

Word maps

Let w be an element of the free group of rank k and let G be a group. We can define a *word map*, $w : G^k \to G$, by substitution:

$$w : G^k \longrightarrow G;$$
$$(g_1, ..., g_k) \longmapsto w(g_1, ..., g_k).$$

For example:

- $w(x) = x^n$;
- $w(x, y) = [x, y]$.

We will denote by G_w the *verbal image* of w over G:

$$G_w := \{w(g_1, ..., g_k) : g_i \in G\}.$$

Define the *verbal subgroup*, $w(G) = \langle G_w^{\pm 1} \rangle$.

Word maps

Let w be an element of the free group of rank k and let G be a group. We can define a *word map*, $w : G^k \to G$, by substitution:

$$\begin{aligned} w : G^k &\longrightarrow G; \\ (g_1, ..., g_k) &\longmapsto w(g_1, ..., g_k). \end{aligned}$$

For example:

- $w(x) = x^n$;
- $w(x, y) = [x, y]$.

We will denote by G_w the *verbal image* of w over G:

$$G_w := \{w(g_1, ..., g_k) : g_i \in G\}.$$

Define the *verbal subgroup*, $w(G) = \langle G_w^{\pm 1} \rangle$.

Outline

Images of Word Maps

Theorem (M. Kassabov & N. Nikolov, Dec 2011)

For every $n \geq 7$, $n \neq 13$ there is a word $w(x_1, x_2) \in F_2$ such that $Alt(n)_w$ consists of the identity and all 3-cycles. When $n = 13$ there is word $w(x_1, x_2, x_3) \in F_3$ with the same property.

Images of Word Maps

Theorem (M. Kassabov & N. Nikolov, Dec 2011)

For every $n \geq 7$, $n \neq 13$ there is a word $w(x_1, x_2) \in F_2$ such that Alt(n)$_w$ consists of the identity and all 3-cycles. When $n = 13$ there is word $w(x_1, x_2, x_3) \in F_3$ with the same property.

- Clearly holds for Alt(5), e.g. $w(x) = x^{10}$.
- Also holds for Sym(n).
- They go on to give other explicit examples e.g. all p-cycles with p prime $3 < p < n$.
- Similar results for SL(n, q).
- More examples can be found in [L.].

They were motivated by *verbal width*.

Images of Word Maps

Theorem (M. Kassabov & N. Nikolov, Dec 2011)

For every $n \geq 7$, $n \neq 13$ there is a word $w(x_1, x_2) \in F_2$ such that Alt(n)$_w$ consists of the identity and all 3-cycles. When $n = 13$ there is word $w(x_1, x_2, x_3) \in F_3$ with the same property.

- Clearly holds for Alt(5), e.g. $w(x) = x^{10}$.
- Also holds for Sym(n).
- They go on to give other explicit examples e.g. all p-cycles with p prime $3 < p < n$.
- Similar results for SL(n, q).
- More examples can be found in [L.].

They were motivated by *verbal width*.

Verbal Width

Say w has *finite width* in G if there exists m such that $w(G) = G_w^{*m} = \{g_1 \dots g_m : g_i \in G_w^{\pm 1}\}$.
Otherwise we say w has *infinite width*.
Define the *width* to be the least such m.
Clearly, if G is finite we always have finite width bounded by $|G|$.

Theorem (Larsen, Shalev, Tiep)

For any $w \neq 1$ we have $G = G_w G_w$ when G is a sufficiently large finite simple group.

The requirement of the size of G cannot be removed.

Corollary (Kassabov & Nikolov)

For any k, there exists a word w and a finite simple group G, such that w is not an identity in G, but $G \neq G_w^{*k}$.

Verbal Width

Say w has *finite width* in G if there exists m such that
$w(G) = G_w^{*m} = \{g_1 ... g_m : g_i \in G_w^{\pm 1}\}$.
Otherwise we say w has *infinite width*.
Define the *width* to be the least such m.
Clearly, if G is finite we always have finite width bounded by $|G|$.

Theorem (Larsen, Shalev, Tiep)

For any $w \neq 1$ we have $G = G_w G_w$ when G is a sufficiently large finite simple group.

The requirement of the size of G cannot be removed.

Corollary (Kassabov & Nikolov)

For any k, there exists a word w and a finite simple group G, such that w is not an identity in G, but $G \neq G_w^{*k}$.

Verbal Width

Say w has *finite width* in G if there exists m such that
$w(G) = G_w^{*m} = \{g_1 \dots g_m : g_i \in G_w^{\pm 1}\}$.
Otherwise we say w has *infinite width*.
Define the *width* to be the least such m.
Clearly, if G is finite we always have finite width bounded by $|G|$.

Theorem (Larsen, Shalev, Tiep)

For any $w \neq 1$ we have $G = G_w G_w$ when G is a sufficiently large finite simple group.

The requirement of the size of G cannot be removed.

Corollary (Kassabov & Nikolov)

For any k, there exists a word w and a finite simple group G, such that w is not an identity in G, but $G \neq G_w^{*k}$.

Verbal Width

Say w has *finite width* in G if there exists m such that $w(G) = G_w^{*m} = \{g_1 \ldots g_m : g_i \in G_w^{\pm 1}\}$.
Otherwise we say w has *infinite width*.
Define the *width* to be the least such m.
Clearly, if G is finite we always have finite width bounded by $|G|$.

Theorem (Larsen, Shalev, Tiep)

For any $w \neq 1$ we have $G = G_w G_w$ when G is a sufficiently large finite simple group.

The requirement of the size of G cannot be removed.

Corollary (Kassabov & Nikolov)

For any k, there exists a word w and a finite simple group G, such that w is not an identity in G, but $G \neq G_w^{*k}$.

Question

Fix a group G and let A be a subset of G. Does there exist a word w such that $G_w = A$? i.e. What are the verbal images of G?

Two necessary conditions:

- Clearly we must have $e \in A$ (since $w(e, ..., e) = e$).
- For every $\alpha \in \mathrm{Aut}(G)$, $\alpha(A) = A$ (since $\alpha(w(g_1, ..., g_k)) = w(\alpha(g_1), ..., \alpha(g_k))$.

If we assume G is a simple group, are these conditions sufficient?

Question

Fix a group G and let A be a subset of G. Does there exist a word w such that $G_w = A$? i.e. What are the verbal images of G?

Two necessary conditions:

- Clearly we must have $e \in A$ (since $w(e, ..., e) = e$).
- For every $\alpha \in \mathrm{Aut}(G)$, $\alpha(A) = A$ (since $\alpha(w(g_1, ..., g_k)) = w(\alpha(g_1), ..., \alpha(g_k))$.

If we assume G is a simple group, are these conditions sufficient?

Question

Fix a group G and let A be a subset of G. Does there exist a word w such that $G_w = A$? i.e. What are the verbal images of G?

Two necessary conditions:

- Clearly we must have $e \in A$ (since $w(e, ..., e) = e$).
- For every $\alpha \in \mathrm{Aut}(G)$, $\alpha(A) = A$ (since $\alpha(w(g_1, ..., g_k)) = w(\alpha(g_1), ..., \alpha(g_k))$.

If we assume G is a simple group, are these conditions sufficient?

The Simple Groups

Theorem (Lubotzky, June 2012)

Let G be a finite simple group and A a subset of G such that $e \in A$ and for every $\alpha \in Aut(G)$, $\alpha(A) = A$. Then there exists a word $w \in F_2$ such that $G_w = A$.

Proof (sketch)

Theorem (Lubotzky, June 2012)

Let G be a finite simple group and A a subset of G such that $e \in A$ and for every $\alpha \in Aut(G)$, $\alpha(A) = A$. Then there exists a word $w \in F_2$ such that $G_w = A$.

Key Theorem:

Theorem (Guralnick & Kantor)

Let G be a finite simple group. For every $e \neq a \in G$ there exists $b \in G$ such that $G = \langle a, b \rangle$.

Note this requires the classification of finite simple groups.

Proof (sketch)

Theorem (Lubotzky, June 2012)

Let G be a finite simple group and A a subset of G such that $e \in A$ and for every $\alpha \in Aut(G)$, $\alpha(A) = A$. Then there exists a word $w \in F_2$ such that $G_w = A$.

Key Theorem:

Theorem (Guralnick & Kantor)

Let G be a finite simple group. For every $e \neq a \in G$ there exists $b \in G$ such that $G = \langle a, b \rangle$.

Note this requires the classification of finite simple groups.

Proof (sketch)

Main idea:
Let $\Omega = \{(a_i, b_i) : i := 1, ..., |G|^2\}$ denote the set of all pairs of elements of G such that the first l pairs generate G and the remaining pairs generate proper subgroups of G. Let Ω_1 denote the set of the first l pairs and Ω_2 denote the set of the remaining pairs. Consider the homomorphism:

$$\phi_1 : F_2 \longrightarrow \prod_{\Omega_1} G, \tag{1}$$

$$w(x, y) \longmapsto (w(a_i, b_i))_{\Omega_1}. \tag{2}$$

The image $\phi_1(F_2)$ is a subdirect product.
It is well-known that $\phi_1(F_2)$ contains a 'diagonal' subgroup isomorphic to G^r where $r = l/|\mathrm{Aut}(G)|$.

Proof (sketch)

Main idea:
Let $\Omega = \{(a_i, b_i) : i := 1, ..., |G|^2\}$ denote the set of all pairs of elements of G such that the first l pairs generate G and the remaining pairs generate proper subgroups of G. Let Ω_1 denote the set of the first l pairs and Ω_2 denote the set of the remaining pairs. Consider the homomorphism:

$$\phi_1 : F_2 \longrightarrow \prod_{\Omega_1} G, \tag{1}$$

$$w(x, y) \longmapsto (w(a_i, b_i))_{\Omega_1}. \tag{2}$$

The image $\phi_1(F_2)$ is a subdirect product.
It is well-known that $\phi_1(F_2)$ contains a 'diagonal' subgroup isomorphic to G^r where $r = l/|\mathrm{Aut}(G)|$.

Proof (sketch)

Main idea:
Let $\Omega = \{(a_i, b_i) : i := 1, ..., |G|^2\}$ denote the set of all pairs of elements of G such that the first l pairs generate G and the remaining pairs generate proper subgroups of G. Let Ω_1 denote the set of the first l pairs and Ω_2 denote the set of the remaining pairs. Consider the homomorphism:

$$\phi_1 : F_2 \longrightarrow \prod_{\Omega_1} G, \tag{1}$$

$$w(x, y) \longmapsto (w(a_i, b_i))_{\Omega_1}. \tag{2}$$

The image $\phi_1(F_2)$ is a subdirect product.
It is well-known that $\phi_1(F_2)$ contains a 'diagonal' subgroup isomorphic to G^r where $r = l/|\mathrm{Aut}(G)|$.

Proof (sketch)

Main idea:
Let $\Omega = \{(a_i, b_i) : i := 1, ..., |G|^2\}$ denote the set of all pairs of elements of G such that the first l pairs generate G and the remaining pairs generate proper subgroups of G. Let Ω_1 denote the set of the first l pairs and Ω_2 denote the set of the remaining pairs. Consider the homomorphism:

$$\phi_1 : F_2 \longrightarrow \prod_{\Omega_1} G, \quad (1)$$

$$w(x, y) \longmapsto (w(a_i, b_i))_{\Omega_1}. \quad (2)$$

The image $\phi_1(F_2)$ is a subdirect product.
It is well-known that $\phi_1(F_2)$ contains a 'diagonal' subgroup isomorphic to G^r where $r = l/|\mathrm{Aut}(G)|$.

Proof (sketch)

Main idea:
Let $\Omega = \{(a_i, b_i) : i := 1, ..., |G|^2\}$ denote the set of all pairs of elements of G such that the first l pairs generate G and the remaining pairs generate proper subgroups of G. Let Ω_1 denote the set of the first l pairs and Ω_2 denote the set of the remaining pairs. Consider the homomorphism:

$$\phi_1 : F_2 \longrightarrow \prod_{\Omega_1} G, \quad (1)$$

$$w(x, y) \longmapsto (w(a_i, b_i))_{\Omega_1}. \quad (2)$$

The image $\phi_1(F_2)$ is a subdirect product.
It is well-known that $\phi_1(F_2)$ contains a 'diagonal' subgroup isomorphic to G^r where $r = l/|\mathrm{Aut}(G)|$.

Other Groups

How about other groups? Almost Simple Groups? Quasisimple Groups?

Outline

Almost Simple Groups

Let G be an almost simple group, i.e. $S \leq G \leq \mathrm{Aut}(S)$ where S is a non-abelian finite simple group.
Suppose further that $G \trianglelefteq \mathrm{Aut}(S)$.

Theorem (L., 2012)

Let G and S be as above. Let A be a subset of S such that $e \in A$ and A is closed under the action of $\mathrm{Aut}(G)$. Then there exists a word $w \in F_2$ such that $G_w = A$.

It remains to describe the situation where $A \not\leq S$.

Almost Simple Groups

Let G be an almost simple group, i.e. $S \leq G \leq \mathrm{Aut}(S)$ where S is a non-abelian finite simple group.
Suppose further that $G \trianglelefteq \mathrm{Aut}(S)$.

Theorem (L., 2012)

Let G and S be as above. Let A be a subset of S such that $e \in A$ and A is closed under the action of Aut(G). Then there exists a word $w \in F_2$ such that $G_w = A$.

It remains to describe the situation where $A \not\leq S$.

Almost Simple Groups

Let G be an almost simple group, i.e. $S \leq G \leq \mathrm{Aut}(S)$ where S is a non-abelian finite simple group.
Suppose further that $G \trianglelefteq \mathrm{Aut}(S)$.

Theorem (L., 2012)

Let G and S be as above. Let A be a subset of S such that $e \in A$ and A is closed under the action of Aut(G). Then there exists a word $w \in F_2$ such that $G_w = A$.

It remains to describe the situation where $A \not\leq S$.

Almost Simple Groups

Let G be an almost simple group, i.e. $S \leq G \leq \mathrm{Aut}(S)$ where S is a non-abelian finite simple group.
Suppose further that $G \trianglelefteq \mathrm{Aut}(S)$.

Theorem (L., 2012)

Let G and S be as above. Let A be a subset of S such that $e \in A$ and A is closed under the action of Aut(G). Then there exists a word $w \in F_2$ such that $G_w = A$.

It remains to describe the situation where $A \not\leq S$.

Note that if we do not require that $w \in F_2$ we can immediately deduce this from the proof of the Ore Conjecture, the fact that the group of outer automorphisms of a finite simple group has derived length at most 3 and from Lubotzky's Theorem.

Theorem (Liebeck, O'Brian, Shalev, Tiep)

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

$w = [[[x_1, x_2], [x_3, x_4]], [[x_5, x_6], [x_7, x_8]]]$ has image precisely S where $S \leq G \leq \mathrm{Aut}(S)$.

Outline

Symmetric Groups

Fix $n \geq 5$ and consider S_n, an almost simple group ($\mathrm{A}_n \leq \mathrm{S}_n \leq \mathrm{Aut}(\mathrm{A}_n)$).

Corollary (L., 2012)

The verbal images of S_n are either:

- *an $Aut(S_n)$-invariant subset of A_n including the identity or;*
- *any $Aut(S_n)$-invariant subset of S_n containing C, where C is the set of all 2-elements of S_n and the identity.*

Symmetric Groups

Fix $n \geq 5$ and consider S_n, an almost simple group ($\mathrm{A}_n \leq \mathrm{S}_n \leq \mathrm{Aut}(\mathrm{A}_n)$).

Corollary (L., 2012)

The verbal images of S_n are either:

- *an $Aut(S_n)$-invariant subset of A_n including the identity or;*
- *any $Aut(S_n)$-invariant subset of S_n containing C, where C is the set of all 2-elements of S_n and the identity.*

Outline

Quasisimple Groups

A group S is quasisimple if $S/Z(S)$ is simple and S is perfect.

Theorem (L., 2012)

There exists a constant C with the following property: Let S be a universal quasisimple group with $|S| > C$ and let A be a subset of S such that $e \in A$ and A is closed under the action of the automorphism group of S. Then there exists a word $w \in F_2$ such that $S_w = A$.

In fact, if S is the universal cover of an alternating group then the condition of sufficiently large can be removed.

Quasisimple Groups

A group S is quasisimple if $S/Z(S)$ is simple and S is perfect.

Theorem (L., 2012)

There exists a constant C with the following property: Let S be a universal quasisimple group with $|S| > C$ and let A be a subset of S such that $e \in A$ and A is closed under the action of the automorphism group of S. Then there exists a word $w \in F_2$ such that $S_w = A$.

In fact, if S is the universal cover of an alternating group then the condition of sufficiently large can be removed.

References I

M. Kassabov and N. Nikolov
Words with few values in finite simple groups.
Q. J. Math, June 2012.

M. Levy
Word maps with small image in finite simple groups.
arχiv, (1206.1206v1), 2012.

M. Levy
Images of word maps in almost simple groups and quasisimple groups.
arχiv, (1301.7188v1), 2012.

References II

A. Lubotzky
Images of word maps in finite simple groups.
arχiv, (1211.6575v1), 2012.

Miklós Abért
On the probability of satisfying a word in a group.
J. Group Theory, 9(5):665-694,, 2006.

Robert M. Guralnick and William M. Kantor
Probabilistic generation of finite simple groups.
J. Algebra, 234(2):743-792, 2000.

References III

Jason Fulman and Robert Guralnick
Bounds on the number and sizes of conjugacy classes in finite chevalley groups with applications to derangements.
Trans. Amer. Math. Soc., 364(6):3023-3070, 2012.

W. M. Kantor and A. Lubotzky
The probability of generating a finite classical group.
Geom. Dedicata, 36(1):67-87, 1990.

Martin Liebeck and Aner Shalev
The probability of generating a finite simple group.
Geom. Dedicata, 56(1):103-113, 1995.

References IV

M. W. Liebeck, E. A. O'Brian, A. Shalev, P. H. Tiep
The Ore Conjecture.
J. Eur. Math. Soc., 12 (2010) 939-1950, 1995.

M. Larsen, A. Shalev, P. H. Tiep
The Waring problem for finite simple groups.
Ann. Math., 174 (2011), 1885-1950 1995.

Attila Maróti
Bounding the number of conjugacy classes of a permutation group.
J. Group Theory, 8(3):273-289, 2005.

References V

Attila Maróti and M. Chiara Tamburini
Bounds for the probability of generating the symmetric and alternating groups.
Arch. Math. (Basel), 96(2):115-121, 2011.