Words and Groups

Aner Shalev
Hebrew University Jerusalem
Erdős Centennial Conference
Budapest 2013

Classical Waring Type Problems

Additive Number Theory

- A classical result: every positive integer is a sum of 4 squares (Lagrange, 1770).

Classical Waring Type Problems

Additive Number Theory

- A classical result: every positive integer is a sum of 4 squares (Lagrange, 1770).
- Waring problem: Is it true that every natural number is a sum of $g(k)$ k-th powers, where g is a suitable function?

Classical Waring Type Problems

Additive Number Theory

- A classical result: every positive integer is a sum of 4 squares (Lagrange, 1770).
- Waring problem: Is it true that every natural number is a sum of $g(k)$ k-th powers, where g is a suitable function?
- Solutions for small k: $g(2) = 4$, $g(3) = 9$, $g(4) = 19$.

Classical Waring Type Problems

Additive Number Theory

- A classical result: every positive integer is a sum of 4 squares (Lagrange, 1770).
- Waring problem: Is it true that every natural number is a sum of $g(k)$ k-th powers, where g is a suitable function?
- Solutions for small k: $g(2) = 4$, $g(3) = 9$, $g(4) = 19$.
- In 1909 Hilbert solved the problem affirmatively.

Classical Waring Type Problems

Additive Number Theory

- A classical result: every positive integer is a sum of 4 squares (Lagrange, 1770).
- Waring problem: Is it true that every natural number is a sum of $g(k)$ k-th powers, where g is a suitable function?
- Solutions for small k: $g(2) = 4$, $g(3) = 9$, $g(4) = 19$.
- In 1909 Hilbert solved the problem affirmatively.
- Non-commutative analogues:
  Present group elements as short products of special elements: powers, or commutators, or values of a general word w, or elements of a given conjugacy class in the group.

Notation

- Let $w = w(x_1, \ldots, x_d)$ be a non-trivial word, namely a non-identity element of the free group F_d on $x_1, \ldots, x_d$.

Notation

- Let $w = w(x_1, \ldots, x_d)$ be a non-trivial word, namely a non-identity element of the free group F_d on $x_1, \ldots, x_d$.
- Let G be a group. The word map $w : G^d \to G$ is defined by substituting group elements $g_1, \ldots, g_d$ in $x_1, \ldots, x_d$ respectively.

Notation

- Let $w = w(x_1, \ldots, x_d)$ be a non-trivial word, namely a non-identity element of the free group F_d on $x_1, \ldots, x_d$.
- Let G be a group. The word map $w : G^d \to G$ is defined by substituting group elements $g_1, \ldots, g_d$ in $x_1, \ldots, x_d$ respectively.
- Let $w(G) \subseteq G$ denote the image of this map, and denote

$$w(G)^k = \{g_1 \cdot g_2 \cdot \ldots \cdot g_k \mid g_i \in w(G)\}.$$

FSG = Finite (non-abelian) Simple Group.
Assume CFSG (the Classification).

Theorem (Wilson, 1994)

Any element of a FSG is a product of c commutators, where c is some absolute constant. I.e., for $w = [x, y] = x^{-1}y^{-1}xy$,
$w(G)^c = G$. *(c unspecified)*

FSG = Finite (non-abelian) Simple Group.
Assume CFSG (the Classification).

Theorem (Wilson, 1994)

Any element of a FSG is a product of c commutators, where c is some absolute constant. I.e., for $w = [x, y] = x^{-1}y^{-1}xy$, $w(G)^c = G$. (c unspecified)

Theorem (Martinez-Zelmanov, 1996, Saxl-Wilson, 1997)

Let $w = x^k$. There exist $f(k)$ such that either $w(G) = 1$ or $w(G)^{f(k)} = G$ for any FSG G.

FSG = Finite (non-abelian) Simple Group.
Assume CFSG (the Classification).

Theorem (Wilson, 1994)

Any element of a FSG is a product of c commutators, where c is some absolute constant. I.e., for $w = [x, y] = x^{-1}y^{-1}xy$,
$w(G)^c = G$. *(c unspecified)*

Theorem (Martinez-Zelmanov, 1996, Saxl-Wilson, 1997)

Let $w = x^k$. *There exist* $f(k)$ *such that either* $w(G) = 1$ *or*
$w(G)^{f(k)} = G$ *for any FSG* G.

Question

Are there extensions of these results to general words w*?*

Theorem (Liebeck-Shalev, 2001)

For any word w there exists a positive integer $c = c_w$ such that, for any FSG G, either $w(G) = 1$ or $w(G)^c = G$.

Kassabov-Nikolov, Lubotzky, 2012: c_w genuinely depends on w.

Theorem (Liebeck-Shalev, 2001)

For any word w there exists a positive integer $c = c_w$ such that, for any FSG G, either $w(G) = 1$ or $w(G)^c = G$.

Kassabov-Nikolov, Lubotzky, 2012: c_w genuinely depends on w.
Surprise: For large G, c_w doesn't depend on w, and is very small:

Theorem (Liebeck-Shalev, 2001)

For any word w there exists a positive integer $c = c_w$ such that, for any FSG G, either $w(G) = 1$ or $w(G)^c = G$.

Kassabov-Nikolov, Lubotzky, 2012: c_w genuinely depends on w.
Surprise: For large G, c_w doesn't depend on w, and is very small:

Theorem (Shalev, 2009)

For any $w \neq 1$, there exists a positive integer $N = N_w$ such that

$$w(G)^3 = G$$

for every FSG G with $|G| \geq N$.

Proof uses probabilistic methods following Erdős
New proof by Nikolov-Pyber in 2011 using Gowers' trick.

Sharper results for some cases

Theorem (Liebeck-O'Brien-Shalev-Tiep, 2010: Ore Conjecture 1951)

For $w = [x, y]$ and G any FSG,

$$w(G) = G.$$

Sharper results for some cases

Theorem (Liebeck-O'Brien-Shalev-Tiep, 2010: Ore Conjecture 1951)

For $w = [x, y]$ and G any FSG,

$$w(G) = G.$$

Theorem (Liebeck-O'Brien-Shalev-Tiep, 2012)

For $w = x^2y^2$ and G any FSG,

$$w(G) = G.$$

Non-commutative analogue of Lagrange Theorem.

Sharper results for some cases

Theorem (Liebeck-O'Brien-Shalev-Tiep, 2010: Ore Conjecture 1951)

For $w = [x, y]$ and G any FSG,

$$w(G) = G.$$

Theorem (Liebeck-O'Brien-Shalev-Tiep, 2012)

For $w = x^2y^2$ and G any FSG,

$$w(G) = G.$$

Non-commutative analogue of Lagrange Theorem.
However, various words w are not surjective on all FSG, or even on almost all of them. E.g. x^n in not surjective whenever $(n, |G|) \neq 1$, so x^2 is never surjective on a FSG.

Hence, if $w(G)^2 = G$ for every word $w \neq 1$ and all large FSG, this would be the best possible solution.

Hence, if $w(G)^2 = G$ for every word $w \neq 1$ and all large FSG, this would be the best possible solution.

Theorem (Larsen-Shalev-Tiep, 2011)

Given $w \neq 1$, there exists a constant $N = N_w$ such that

$$w(G)^2 = G$$

for all FSG G of order at least N.

Proof involves Algebraic Geometry, Representation Theory and Probability

Hence, if $w(G)^2 = G$ for every word $w \neq 1$ and all large FSG, this would be the best possible solution.

Theorem (Larsen-Shalev-Tiep, 2011)

Given $w \neq 1$, there exists a constant $N = N_w$ such that

$$w(G)^2 = G$$

for all FSG G of order at least N.

Proof involves Algebraic Geometry, Representation Theory and Probability

Corollary

Given $k \geq 1$ there exists N_k such that, if G is a FSG satisfying $|G| \geq N_k$, then every element of G is a product of two k-th powers.

Better solution to Waring problem in the non-commutative world!

- A word w is called a power word if there exists some integer $r > 1$ and a word u such that $w = u^r$.

- A word w is called a power word if there exists some integer $r > 1$ and a word u such that $w = u^r$.
- If w is a power word, we cannot hope that w will be onto all large FSG.

- A word w is called a power word if there exists some integer $r > 1$ and a word u such that $w = u^r$.
- If w is a power word, we cannot hope that w will be onto all large FSG.

Question

Are power words the only case?

- A word w is called a power word if there exists some integer $r > 1$ and a word u such that $w = u^r$.

- If w is a power word, we cannot hope that w will be onto all large FSG.

Question

Are power words the only case?

NO!

Example (Jambor-Liebeck-O'Brien, 2013)

$w = x^2 \left[x^{-2}, y^{-1}\right]^k$ is not surjective on $\mathrm{PSL}_2(q)$ for infinitely many q.

- Engel words are words of the form $w_n = \underbrace{[\ldots[[[x,y],y],y],\ldots,y]}_{n \text{ times}}$.

- Engel words are words of the form
$w_n = \underbrace{[\dots[[[x,y],y],y],\dots,y]}_{n \text{ times}}$.

Theorem (Bandman-Garion-Grunewald, 2010)

Let w_n be the n-th Engel word. Then $w_n(G) = G$ for $G = \mathrm{PSL}_2(q)$ when $q \geq q_0(n)$.

- Engel words are words of the form
  $w_n = \underbrace{[\dots[[[x,y],y],y],\dots,y]}_{n \text{ times}}$.

Theorem (Bandman-Garion-Grunewald, 2010)

Let w_n be the n-th Engel word. Then $w_n(G) = G$ for $G = \mathrm{PSL}_2(q)$ when $q \geq q_0(n)$.

This, and computer experiments on other groups suggest:

Conjecture

Let G be a FSG. Let w_n be the n-th Engel word. Then $w_n(G) = G$.

Notation

For a conjugacy class C, we denote
$C^k = \{c_1 \cdot c_2 \cdot \ldots \cdot c_k \mid c_i \in C\}$.

Conjugacy classes and Thompson Conjecture

Notation

For a conjugacy class C, we denote
$C^k = \{c_1 \cdot c_2 \cdot \ldots \cdot c_k \mid c_i \in C\}$.

Conjecture (Thompson)

Every FSG G has a conjugacy class C such that $C^2 = G$.

This implies that every element in G is a commutator (Ore Conjecture – LOST Theorem). Known for A_n.

Conjugacy classes and Thompson Conjecture

Notation

For a conjugacy class C, we denote $C^k = \{c_1 \cdot c_2 \cdot \ldots \cdot c_k \mid c_i \in C\}$.

Conjecture (Thompson)

Every FSG G has a conjugacy class C such that $C^2 = G$.

This implies that every element in G is a commutator (Ore Conjecture – LOST Theorem). Known for A_n.

Theorem (Ellers-Gordeev, 1998)

Thompson conjecture holds for groups of Lie type over a finite field F_q, provided $q > 8$.

Probabilistic method:

Theorem (Shalev, 2008-2009)

For a random conjugacy class C of a FSG G we have $C^3 = G$, and $|C^2| = (1 - o(1))|G|$.

Probabilistic method:

Theorem (Shalev, 2008-2009)

For a random conjugacy class C of a FSG G we have $C^3 = G$, and $|C^2| = (1 - o(1))|G|$.

Theorem (Larsen-Shalev-Tiep, 2011)

Every large FSG G has two conjugacy classes C_1, C_2 with $C_1 C_2 \cup \{1\} = G$.

Probabilistic method:

Theorem (Shalev, 2008-2009)

For a random conjugacy class C of a FSG G we have $C^3 = G$, and $|C^2| = (1 - o(1))|G|$.

Theorem (Larsen-Shalev-Tiep, 2011)

Every large FSG G has two conjugacy classes C_1, C_2 with $C_1 C_2 \cup \{1\} = G$.

Theorem (Guralnick-Malle, 2012)

Every FSG G has two conjugacy classes C_1, C_2 with $C_1 C_2 \cup \{1\} = G$.

Till now we only asked which elements lie in $w(G)$ and in $w(G)^k$.
We can further ask about the distribution in which they occur.
Denote by $U_{w(G)}$ the uniform distribution on $w(G)$.

Till now we only asked which elements lie in $w(G)$ and in $w(G)^k$.
We can further ask about the distribution in which they occur.
Denote by $U_{w(G)}$ the uniform distribution on $w(G)$.
Denote by $U^{*k}_{w(G)}$ the distribution induced on $w(G)^k$ by a k-fold product:

$$U^{*k}_{w(G)}(g) = \mathrm{Prob}\left\{ g_1 g_2 \ldots g_k = g \;\middle|\; \begin{array}{c} g_1, \ldots, g_k \text{ distribute uniformly} \\ \text{and independently in } w(G) \end{array} \right\}.$$

This is the distribution induced on G by a k-step random walk on the (directed) Cayley graph of G with $w(G)$ as a generating set.

Theorem (Larsen-Schul-Shalev, 2008-9)

For $w \neq 1$, $\left\| U_{w(G)}^{*2} - U_G \right\|_1 \to 0$ *as* $|G| \to \infty$ *and* G *is FSG.*
Thus the mixing time of the random walk on G *with respect to* $w(G)$ *as a generating set is 2.*

Larsen-Shalev (2008) - alternating groups
Schul-Shalev (2009) - groups of Lie type.

Theorem (Larsen-Schul-Shalev, 2008-9)

For $w \neq 1$, $\left\| U^{*2}_{w(G)} - U_G \right\|_1 \to 0$ *as* $|G| \to \infty$ *and* G *is FSG.*
Thus the mixing time of the random walk on G *with respect to* $w(G)$ *as a generating set is 2.*

Larsen-Shalev (2008) - alternating groups
Schul-Shalev (2009) - groups of Lie type.

Corollary

If $w \neq 1$ *then* $\frac{|w(G)^2|}{|G|} \to 1$ *as* $|G| \to \infty$ *(*G *FSG).*

Another natural distribution induced on G by a word map:

$$P_{w,G}(g) = \text{Prob}\left\{ w(g_1, \ldots, g_d) = g \;\middle|\; \begin{array}{c} g_1 \ldots g_d \text{ distribute uniformly} \\ \text{and independently in } G \end{array} \right\}.$$

How small is $P_{w,G}(g)$?

Another natural distribution induced on G by a word map:

$$P_{w,G}(g) = \mathrm{Prob}\left\{ w(g_1, \ldots, g_d) = g \;\middle|\; \begin{array}{c} g_1 \ldots g_d \text{ distribute uniformly} \\ \text{and independently in } G \end{array} \right\}.$$

How small is $P_{w,G}(g)$?

Theorem (Larsen-Shalev, 2012)

For any word $w \neq 1$ there exists $\epsilon = \epsilon_w > 0$ such that for all large FSG G and $g \in G$, we have $P_{w,G}(g) \leq |G|^{-\epsilon}$.

Best possible bound. Applications to Subgroup Growth and to Representation Varieties.

Another natural distribution induced on G by a word map:

$$P_{w,G}(g) = \text{Prob}\left\{ w(g_1, \ldots, g_d) = g \;\middle|\; \begin{array}{c} g_1 \ldots g_d \text{ distribute uniformly} \\ \text{and independently in } G \end{array} \right\}.$$

How small is $P_{w,G}(g)$?

Theorem (Larsen-Shalev, 2012)

For any word $w \neq 1$ there exists $\epsilon = \epsilon_w > 0$ such that for all large FSG G and $g \in G$, we have $P_{w,G}(g) \leq |G|^{-\epsilon}$.

Best possible bound. Applications to Subgroup Growth and to Representation Varieties.

$P_{w,G}$ is a class function on G, hence a linear combination of irreducible characters: $P_{w,G} = |G|^{-1} \sum_\chi a_\chi \chi$. (Fourier expansion)

Hence character methods are highly relevant.

Theorem (Garion-Shalev, 2009)

For FSG G, $\left\|P_{[x,y],G} - U_G\right\|_1 \to 0$ as $|G| \to \infty$.

Sketch of proof:
(i) $\left\|P_{[x,y],G} - U_G\right\|_1 \leq \sum_{\chi \neq 1} \chi(1)^{-2}$.
(ii) $\sum_{\chi \neq 1} \chi(1)^{-2} \to 0$ as $|G| \to \infty$.
Application to Product Replacement Algorithm. Similar result for $x^2 y^2$.

Theorem (Garion-Shalev, 2009)

For FSG G, $\|P_{[x,y],G} - U_G\|_1 \to 0$ *as* $|G| \to \infty$.

Sketch of proof:
(i) $\|P_{[x,y],G} - U_G\|_1 \leq \sum_{\chi \neq 1} \chi(1)^{-2}$.
(ii) $\sum_{\chi \neq 1} \chi(1)^{-2} \to 0$ as $|G| \to \infty$.
Application to Product Replacement Algorithm. Similar result for x^2y^2.

Theorem (Larsen-Shalev, 2013)

Fix $n, m \geq 1$. *Then for FSG G,* $\|P_{x^m y^n,G} - U_G\|_1 \to 0$ *as* $|G| \to \infty$.

Work in progress: Same for $w_1 w_2$, where $w_1, w_2 \neq 1$ are words in disjoint variables.

For $w = x$ we have: $P_{x,G} \equiv \frac{1}{|G|}$ for every finite group G.

Theorem (Puder-Parzanchevski, 2011)

$P_{w,G} \equiv \frac{1}{|G|}$ for every finite group G if and only if w is a primitive word (there exists $\varphi \in \mathrm{Aut}(F_d)$ with $\varphi(w) = x$).

For $w = x$ we have: $P_{x,G} \equiv \frac{1}{|G|}$ for every finite group G.

Theorem (Puder-Parzanchevski, 2011)

$P_{w,G} \equiv \frac{1}{|G|}$ for every finite group G if and only if w is a primitive word (there exists $\varphi \in \mathrm{Aut}(F_d)$ with $\varphi(w) = x$).

For any $w \in F_d$ and $\varphi \in \mathrm{Aut}(F_d)$, $P_{w,G} \equiv P_{\varphi(w),G}$ for every finite group G.
(since $\varphi(w)(h_1, \dots, h_d) = w(g_1, \dots, g_d)$, where $h_i = \varphi^{-1}(x_i)(g_1, \dots g_d)$).

For $w = x$ we have: $P_{x,G} \equiv \frac{1}{|G|}$ for every finite group G.

Theorem (Puder-Parzanchevski, 2011)

$P_{w,G} \equiv \frac{1}{|G|}$ for every finite group G if and only if w is a primitive word (there exists $\varphi \in \mathrm{Aut}(F_d)$ with $\varphi(w) = x$).

For any $w \in F_d$ and $\varphi \in \mathrm{Aut}(F_d)$, $P_{w,G} \equiv P_{\varphi(w),G}$ for every finite group G.
(since $\varphi(w)(h_1, \ldots, h_d) = w(g_1, \ldots, g_d)$, where $h_i = \varphi^{-1}(x_i)(g_1, \ldots g_d)$).

Question

Given $w, w' \in F_d$ such that $P_{w,G} = P_{w',G}$ for every finite group G, is there $\varphi \in \mathrm{Aut}(F_d)$ with $\varphi(w) = w'$?

Extensions to Infinite Groups

G semisimple, simply connected, algebraic group over $\mathbb{Q}$.
Consider the p-adic group $G(\mathbb{Z}_p)$, and the arithmetic group $G(\mathbb{Z})$.
Can we extend results from finite simple groups to infinite p-adic and arithmetic groups?

Extensions to Infinite Groups

G semisimple, simply connected, algebraic group over $\mathbb{Q}$.
Consider the p-adic group $G(\mathbb{Z}_p)$, and the arithmetic group $G(\mathbb{Z})$.
Can we extend results from finite simple groups to infinite p-adic and arithmetic groups?

Theorem (Avni-Gelander-Kassabov-Shalev, 2013)

For any word $w \neq 1$ there exists a number N_w such that, if $p \geq N_w$ is a prime, then $w(G(\mathbb{Z}_p))^3 = G(\mathbb{Z}_p)$.

Condition on p necessary. Not true for $w(G(\mathbb{Z}_p))^2$.

Extensions to Infinite Groups

G semisimple, simply connected, algebraic group over $\mathbb{Q}$.
Consider the p-adic group $G(\mathbb{Z}_p)$, and the arithmetic group $G(\mathbb{Z})$.
Can we extend results from finite simple groups to infinite p-adic and arithmetic groups?

Theorem (Avni-Gelander-Kassabov-Shalev, 2013)

For any word $w \neq 1$ there exists a number N_w such that, if $p \geq N_w$ is a prime, then $w(G(\mathbb{Z}_p))^3 = G(\mathbb{Z}_p)$.

Condition on p necessary. Not true for $w(G(\mathbb{Z}_p))^2$.

Theorem (Avni-Gelander-Kassabov-Shalev, 2013)

If n is a proper divisor of $p-1$ then every element of $\mathrm{PSL}_n(\mathbb{Z}_p)$ is a commutator.

Ore Conjecture for p-adic and arithmetic groups:

Question

Suppose $n > 2$. Is every element of $\mathrm{SL}_n(\mathbb{Z}_p)$ a commutator?
Is every element of $\mathrm{SL}_n(\mathbb{Z})$ a commutator?

Ore Conjecture for p-adic and arithmetic groups:

Question

Suppose $n > 2$. Is every element of $\mathrm{SL}_n(\mathbb{Z}_p)$ a commutator?
Is every element of $\mathrm{SL}_n(\mathbb{Z})$ a commutator?

Thank you!