

Solving Equations in ~~Finite~~ Simple Groups

Michael Larsen

2008 Spring Central Section

Bloomington, April 5, 2008

Equations

A typical equation:

$$xyx^{-1}y^{-1} = g$$

in unknowns $x, y \in G$ where $g \in G$ is constant.

- For which groups G can this always be solved?
- Given G , for how many $g \in G$ can it be solved?
- Given G and g , how many solutions are there?

Why Simple Groups?

- The simplest case: cannot solve an equation over G if it has no solutions over some quotient of G .
- History: over fifty years of work on the simple case.
- Classification: problem divides into explicit list of cases.

Classification of Compact Simple Lie Groups

- Finite simple groups
- Classical groups
 - $\text{PSU}(n + 1)$, $n \geq 1$.
 - $\text{SO}(2n + 1)$, $n \geq 2$.
 - $\text{PSp}(2n)$, $n \geq 3$.
 - $\text{PSO}(2n)$, $n \geq 4$.
- Exceptional groups
 - E_n , $6 \leq n \leq 8$.
 - F_4 .
 - G_2 .

Classification of Finite Simple Groups

- Alternating groups A_n , $n \geq 5$.
- Groups of Lie type
 - $\text{PSL}_{n+1}(\mathbb{F}_q)$, $\text{PSU}_{n+1}(\mathbb{F}_q)$, $n \geq 1$.
 - $\text{PSpin}_{n,n+1}(\mathbb{F}_q)$, $n \geq 2$; ${}^2B_2(\mathbb{F}_{2^{2f+1}})$.
 - $\text{PSp}_{2n}(\mathbb{F}_q)$, $n \geq 3$.
 - $\text{PSpin}_{n,n}(\mathbb{F}_q)$, $\text{PSpin}_{n+1,n-1}(\mathbb{F}_q)$, $n \geq 4$;
 ${}^3D_4(\mathbb{F}_q)$.
 - $E_6(\mathbb{F}_q)$, ${}^2E_6(\mathbb{F}_q)$, $E_7(\mathbb{F}_q)$, $E_8(\mathbb{F}_q)$.
 - $F_4(\mathbb{F})$, ${}^2F_4(\mathbb{F}_{2^{2f+1}})$.
 - $G_2(\mathbb{F})$, ${}^2G_2(\mathbb{F}_{3^{2f+1}})$.
- Sporadic groups.

Ore's Conjecture

Conjecture (Ore, 1951). Every element of every finite simple group is a commutator.

Theorem (Hsu, 1965; Cleavers-Neubuser-Pahlings, 1984; Ellers-Gordeev, 1998). Ore's conjecture holds except possibly for classical groups over fields with ≤ 8 elements.

Theorem (Gotô, 1949). Every element of every compact simple group of dimension > 0 is a commutator.

Extracting Square Roots

When does the equation $x^2 = g$ have a solution in S_n ?

$$(1\ 2\ 3 \cdots 2n)^2 = (1\ 3\ 5 \cdots 2n-1)(2\ 4\ 6 \cdots 2n).$$

$$(1\ 2\ 3 \cdots 2n+1)^2 = (1\ 3\ 5 \cdots 2n+1\ 2\ 4 \cdots 2n).$$

$1^{a_1} 2^{a_2} \cdots k^{a_k}$ is a square $\Leftrightarrow a_{2i} \in 2\mathbb{Z}$ for all i .

Theorem. The probability that a random permutation has a square root grows like $n^{-1/2}$.

Power-free Words

Definition. A word w is *power-free* if it is not of the form w_0^k for any $k \geq 2$.

Question. If w is power-free, is $w(G) = G$ whenever $|G|$ is sufficiently large?

Algebraic Groups and General Word Maps

Theorem (Borel, 1983) If w is a word and G is a simple algebraic group, then $w(G)$ is Zariski-dense in G .

Images of Word Maps

Theorem (L., 2004). If w is a word map, G is any finite simple group, and $\epsilon > 0$,

$$|w(G)| > c_{w,\epsilon} |G|^{1-\epsilon}.$$

Theorem (L.-Shalev). If G is a finite simple group of Lie type but not of the form $\mathrm{PSL}_{r+1}(\mathbb{F}_q)$ or $\mathrm{PSU}_{r+1}(\mathbb{F}_q)$, then

$$|w(G)| > c_w \frac{|G|}{r} > c_w \frac{|G|}{\log |G|}.$$

Question. Is there always an estimate

$$|w(G)| > c_w \frac{|G|}{\log |G|}?$$

Images of Word Maps for A_n

Theorem (L.-Shalev). For any non-trivial w ,

$$|w(A_n)| > c_{w,\epsilon} n^{-29/9-\epsilon} |A_n|.$$

1. Embed $\mathrm{PSL}_3(\mathbb{F}_p)$ in A_{p^2+p+1} .
2. Prove that for a large set S of primes p $w(A_{p^2+p+1})$ contains a $p^2 + p + 1$ -cycle.
3. Choose primes $p_1 \gg p_2 \gg p_3 \gg \dots$ in S such that $n = \sum_i (p_i^2 + p_i + 1)$.
4. Estimate the size of the A_n -conjugacy class of a cycle of type

$$(p_1^2 + p_1 + 1)^1 (p_2^2 + p_2 + 1)^1 \dots$$

.

Images of Word Maps for Compact Lie Groups

Theorem (Lindenstrauss) There exists a sequence w_1, w_2, \dots such that for every compact simple group G and every neighborhood U of the identity in G , $w_i(G) \subset U$ for all i sufficiently large.

Question. Given a word w , is $w(G) = G$ for all compact simple G of sufficiently large dimension?

“Waring’s Problem”

Question. Can every element of G be written as a product of two squares?

Theorem (Shalev, 2008). Given w , for $|G|$ sufficiently large,

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

Theorem (L.-Shalev). Given w_1, w_2, w_3 , for $|G|$ sufficiently large

$$G = w_1(G)w_2(G)w_3(G).$$

Question. Is

$$G = w_1(G)w_2(G)?$$

Waring's Problem for Algebraic Groups

Theorem (L.-Shalev). Let $w = w_1 w_2$ be a product of words in disjoint variables and G a simply connected algebraic group which is simple modulo its finite center Z . Then $w^{-1}(g)$ is a non-empty irreducible variety for all $g \notin Z$.

Basic Fact. If $f(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$ is irreducible in every \mathbb{F}_{q^n} then

$$f(x_1, \dots, x_n) = 0$$

has solutions in \mathbb{F}_q if q is large compared to d and n .

Cautionary Example. $x^2 + 1 = 0$ has no solutions (mod p) if $p \equiv 3 \pmod{4}$.

Products of Conjugacy Classes

Given conjugacy classes $C_1, C_2, C_3 \subset G$, when is $C_3 \subset C_1C_2$?

Several approaches:

- Combinatorics.
- Character theory.
- Algebraic geometry.

Thompson's Conjecture

Conjecture. For every finite simple group G , there exists a conjugacy class $C \subset G$ such that $C^2 = G$.

Thompson's conjecture implies Ore's.

Waring's Problem for Alternating Groups

Theorem (L.-Shalev). Let $w = w_1w_2$ be a product of words in disjoint variables. Then $w(A_n) = A_n$ for all $n > c_w$.

- Characterize conjugacy classes C in A_n such that $C^2 = A_n$.
- Find such a C appearing in both $w_1(A_n)$ and $w_2(A_n)$.

Strong Thompson Conjecture for Alternating Groups

Theorem (L.-Shalev). If $C \subset A_n$ has less than $n^{1/4-\epsilon}$ cycles and $n > N_\epsilon$, then $C^2 = A_n$.

- Fomin-Lulov strength estimates for character values of inhomogeneous elements
- Explicit constructions of classes with many cycles inside C^2 .

Waring's Problem for Compact Groups

Theorem. There exists a constant k such that if $w = w_1 \cdots w_k$, then $w(G) = G$ for all compact simple groups of sufficiently high dimension.

Question. What is the minimum value of k ?