Finite simple groups

To establish uniform bounds that hold over all fnite simple groups, one usually breaks the problem into parts:

1) The *sporadic groups*, and maybe finitely many more small groups: these can be ignored.

2) *Groups of Lie type and small Lie rank*.

Algebraic geometry:

Proposition 1 (Larsen) *Let w be a non-trivial word. Then for each r there exists $c = c(w, r) >$ 0 such that for every finite simple group G of Lie type of Lie rank r we have*

$$\left|G_{+w}\right| > c\,|G|\,.$$

3a, 3b) *Groups of Lie type and large Lie rank; large alternating groups*.

Can often be dealt with by finding matrices, or permutations, of a nice form inside them.

Proposition 2 (Larsen) *Let w be a non-trivial word and let $\varepsilon > 0$. Then there exists N such that*

$$\left|G_{+w}\right| > |G|^{1-\varepsilon}$$

whenever $n > N$ and G is either $\mathrm{Alt}(n)$ *or a simple group of Lie type of Lie rank n.*

With CFSG, the two propositions imply

Theorem 1 (Larsen) *Let w be a non-trivial word and let $\varepsilon > 0$. Then $\left|G_{+w}\right| > |G|^{1-\varepsilon}$ for all sufficiently large finite simple groups G.*

A useful reduction:

Theorem 2 (Nikolov) *Let k be a perfect field and let $G = G(k)$ be a classical quasisimple group over k. Then G has a subgroup H isomorphic to $\mathsf{SL}_n(k_1)$ or $\mathsf{PSL}_n(k_1)$, for some n and a subfield k_1 of k, such that G is the product of 200 conjugates of H.*

It follows that if a word w has width m in $\mathsf{SL}_n(k_1)$, then it has width $200m$ in G.

The most general theorem about verbal width in finite simple groups is due to Aner Shalev:

Theorem 3 (Shalev) *Every word has positive width* 3 *in every sufficiently large finite simple group.*

Ore's conjecture:

Theorem 4 (LOST) *The commutator word* $[x, y]$ *has width one in* every *finite simple group.*

Proof involves character theory, algebraic geometry, number theory, computation (3 years CPU time)

A model-theoretic method

Consider simple groups of a fixed Lie type X.

Theorem 5 (F. Point) *Let $(F_n \mid n \in \mathbb{N})$ be a family of finite fields, let $\mathcal{U}$ be a non-principal ultrafilter on $\mathbb{N}$ and let $E = \prod_n F_n/\mathcal{U}$ be the corresponding ultraproduct. Then E is an infinite field and the ultraproduct of groups*

$$G = \prod_n X(F_n)/\mathcal{U}$$

is isomorphic to $X(E)$.

Now let w be a non-trivial word.
Suppose w does not have bounded width in $X(F)$ as F ranges over all finite fields.

Then there is an infinite sequence of finite fields (F_n) and for each $n \in \mathbb{N}$ an element

$$g_n \in w(X(F_n)) \setminus X(F_n)^{*n}_w.$$

Let $\tilde{g}$ be the image of $(g_n)_{n\in\mathbb{N}}$ in G.

Suppose $\tilde{g} \in w(G)$. Then $\tilde{g} \in G_w^{*m}$ for some finite m; this implies that some subset of $\{1, \ldots, m-1\}$ is a member of $\mathcal{U}$: FALSE! (a non-principal ultrafilter can't contain finite sets).

Therefore $w(G) < G$.

But $G \cong X(E)$ is simple! So $w(G) = 1$. Thus the first-order statement

$$w(x_1, \ldots, x_k) = 1 \ \forall x_1, \ldots, x_k \qquad (1)$$

holds in $\prod_n X(F_n)/\mathcal{U}$.

Łoś's theorem: (1) holds in $X(F_n)$ for each n in some member of $\mathcal{U}$.

So $g_n = 1$ for infinitely many n: contradiction!

Conclusion: *w has bounded width in $X(F)$ as F ranges over all finite fields.*

Theorem 6 *Let w be a non-trivial word. Then for each r there exists $m = m(w, r)$ such that w has width m in every finite simple group of Lie type and Lie rank at most r.*

A combinatorial method

$k(G)$ denotes *the minimal dimension of a non-trivial $\mathbb{R}$-linear representation of G.*

Theorem 7 (Gowers, Babai/Nikolov/Pyber) *Let $S_1, \ldots, S_t$ be subsets of a finite group G, where $t \geq 3$. If*

$$\prod_{i=1}^{t} |S_i| \geq \frac{|G|^t}{k(G)^{t-2}}$$

then $S_1 \cdot S_2 \cdot \ldots \cdot S_t = G$.

Note: this applies to *any* finite group! Typical applications use:

If G is simple of Lie type over $\mathbb{F}_q$, of Lie rank r and dimension d, then

$$k(G) \geq cq^r,$$

$$|G| \sim q^d$$

(c is an absolute constant).

Proposition 3 (Larsen/Shalev, Nikolov/Pyber)
Let w be a non-trivial word. Then

$$\left|G_{+w}\right| \geq |G| / k(G)^{1/3}$$

for every simple group G of Lie type and sufficiently large order.

Taking $S_i = G_{+w_i}$ in theorem 7 now gives

Theorem 8 (Shalev) *Let w_1, w_2 and w_3 be non trivial words. Then*

$$G_{+w_1} G_{+w_2} G_{+w_3} = G$$

for every sufficiently large finite simple group G of Lie type.

Character theory

G denotes a finite group. χ ranges over all irreducible (complex) characters of G.

Given conjugacy classes $C_1, \ldots, C_s$ of G,

$$N(\mathbf{C}; g)$$

denotes the number of solutions to the equation

$$x_1 \cdot x_2 \cdot \ldots \cdot x_s = g$$
$$(x_1 \in C_1, \ldots, x_s \in C_s)$$

Theorem 9 *Let $a_i \in C_i$ for $i = 1, \ldots, s$. Then for $g \in G$ we have*

$$N(\mathbf{C}; g) = \frac{\prod |C_i|}{|G|} \sum_{\chi} \frac{\chi(a_1) \ldots \chi(a_s) \overline{\chi(g)}}{\chi(1)^{s-1}}.$$

General idea: to prove that $N(\mathbf{C}; g) \neq 0$ it suffices to show that $\chi(a)$ *is very small* for $a \in C_i$ and $\chi \neq \chi_1$.

Theorem 10 (Liebeck/Shalev) *There is an absolute constant c such that if G is any finite simple group and S is a normal subset of G with $|S|^t \geq |G|$ then*

$$m \geq ct \Longrightarrow S^{*m} = G.$$

Now let w be a non-trivial word, and let N be the number provided by Theorem 1 such that $\left|G_{+w}\right| > |G|^{1/2}$ for all finite simple groups G with $|G| > N$.

Suppose that G is a finite simple group with $w(G) \neq 1$, and set $S = G_{+w}$.
Then $|S|^t \geq |G|$ where $t = \max\{2, \ \log_2 N\}$;
take $m(w) = \lceil ct \rceil$:

Theorem 11 (Li/Sh) *For each word w there exists $m(w) \in \mathbb{N}$ such that w has positive width $m(w)$ in every finite simple group.*

Original proof: show that if G is sufficiently large then G_{+w} contains a relatively large conjugacy class of G.

Case 1. G is of Lie type and bounded Lie rank r. In this case, we have

$$|C|^{8r} \geq |G|$$

for *every* non-central conjugacy class C.

So done provided $G_{+w} \neq \{1\}$; this holds for all but finitely many simple groups G.

Case 2. $G = \mathrm{Alt}(n)$, where n is large.

There exists $s = s(w)$ such that $w(\mathrm{Alt}(s)) \neq 1$.

Write

$$n = ds + r \quad (0 \leq r < s).$$

Let $1 \neq \sigma \in \mathrm{Alt}(s)_{+w}$. Then G_{+w} contains the permutation

$$\tau = \sigma \times \sigma \times \cdots \times \sigma \times 1$$

which has support of size at least $3d$.

Lemma 1 (Li/Sh) *Let $\delta > 0$. Then for all sufficiently large n, if $\tau \in \mathrm{Alt}(n)$ has support of size m, the conjugacy class C of τ satisfies*

$$|C| \geq n^{(1/3-\delta)m}.$$

Taking $\delta = \frac{1}{12}$ and n sufficiently large we find that G_{+w} contains a conjugacy class C with

$$|C| \geq n^{n/2s} > |G|^{1/2s}.$$

Case 3. Groups of Lie type and large Lie rank. Suppose for example that $G = \mathsf{SL}_n(\mathbb{F}_q)$.

There exists s such that $w(\mathsf{SL}_s(\mathbb{F}_q)) \neq 1$; again write $n = ds + r$ where $0 \leq r < s$, and let $1 \neq \sigma \in \mathsf{SL}_s(\mathbb{F}_q)_{+w}$.

Then G_{+w} contains a block-diagonal matrix τ having d identical blocks σ;
let C be the conjugacy class of τ, let ρ be a power of σ with prime order, and denote the conjugacy class of ρ by C_1.
Obviously $|C| \geq |C_1|$. And

$$|C_1| \geq c\,|G|^{1/6s},$$

$c > 0$ an absolute constant.

The same technique is applied to the other classical groups. Alternatively: quote Theorem 2.

Sharper results due to Larsen and Shalev

1) Let $G = G_r(q)$ be a finite simple group of Lie type, of Lie rank r over $\mathbb{F}_q$, and let C_1, C_2 and C_3 be conjugacy classes in G.

Proposition 4 (Shalev) (i) *If $|G|$ is sufficiently large and C_1, C_2 and C_3 consist of regular semisimple elements, or*

(ii) *if r is sufficiently large and*

$$|C_1|\,|C_2|\,|C_3| \geq q^{-15/4}\,|G|^3\,,$$

then $C_1C_2C_3 = G$.

Proposition 5 (Shalev) *Let w be a non-trivial word. If r is sufficiently large then G_{+w} contains a conjugacy class C with $|C| > q^{-5r/4}\,|G|$.*

Proposition 6 (Guralnick/Lübeck) *The number of regular semisimple elements in G is at least* $(1-aq^{-1})\,|G|$*, where a is an absolute constant.*

Now let w_1, w_2 and w_3 be non trivial words, and put $S_i = G_{+w_i}$ for each i.

If r is large and G is sufficiently large, Proposition 5 together with Proposition 4(ii) shows that $S_1S_2S_3 = G$.

If r is small and G is sufficiently large, Proposition 6 and Proposition 1 together imply that each S_i contains a regular semisimple element, and then Proposition 4(i) shows again that $S_1S_2S_3 = G$.

– Original proof of Theorem 8

2) Alternating groups.

For $\sigma \in \mathrm{Alt}(n)$ denote by $\mathrm{cyc}(\sigma)$ the number of orbits of $\langle\sigma\rangle$ in $\{1, \ldots, n\}$.

Proposition 7 (Larsen/Shalev) *Let $k \in \mathbb{N}$. For all sufficiently large n, if $\sigma \in \mathrm{Alt}(n)$ and $\mathrm{cyc}(\sigma) \leq k$ then the conjugacy class C of σ satisfies $C^{*2} = \mathrm{Alt}(n)$.*

The application to verbal mappings is made via

Proposition 8 (LaSh) *There exists a sequence (σ_n) of permutations with $\sigma_n \in \mathrm{Alt}(n)$ such that*

(i) $\mathrm{cyc}(\sigma_n) \leq 23$ *for each n, and*

(ii) *if w is a non-trivial word then $\sigma_n \in \mathrm{Alt}(n)_{+w}$ for all sufficiently large n.*

Let C_n denote the conjugacy class of σ_n in $\mathrm{Alt}(n)$, let w_1 and w_2 be non trivial words and set $S_i = G_{+w_i}$ for each i. The two last propositions together imply that for all sufficiently large n we have

$$S_1 S_2 \supseteq C_n^{*2} = \mathrm{Alt}(n).$$

Hence:

Theorem 12 (LaSh) *Let u and w be non trivial words. Then for all sufficiently large n,*

$$\mathrm{Alt}(n)_{+u}\mathrm{Alt}(n)_{+w} = \mathrm{Alt}(n).$$

Thm. 3 follows from Thms. 8 and 12, with CFSG.

Conjecture (LaSh) *Let u and w be non trivial words. Then*

$$G_{+u}G_{+w} = G$$

for all sufficiently large finite simple groups G.

Larsen and Shalev prove this for the case of Lie-type groups of bounded Lie rank, so only the case of classical groups of large rank remains open.