Subset products and derangements

Aner Shalev
Hebrew University of Jerusalem, Israel
8th European Congress of Mathematics
Slovenia
21 June, 2021
Joint work with Michael Larsen and Pham Tiep

Products of subsets I: approximate subgroups

G a group, $A, B \subseteq G$, $AB := \{ab : a \in A, b \in B\}$.
Similarly for longer products ABC etc.

G finite, and often a (nonabelian) Finite Simple Group (FSG).

Natural Questions:
Study the product size. When is the product equal to G?
Approximate subgroups and the Product Theorem:
Breuillard-Green-Tao (2010-2011), Pyber-Szabó (2010-2016):
Let G be a finite simple group of Lie type of rank r. Then there exists $\epsilon > 0$ depending only on r such that, if $A \subseteq G$ generates G, then either $A^3 = G$, or

$$|A^3| \geq |A|^{1+\epsilon}.$$

Extends pioneering work by Helfgott (2006-2008) on $G = PSL_2(p)$.
Hrushovski (2007-2012) applied model theory to study approximate subgroups.

Product of subsets II: Quasi-random groups

G any finite group.
$m(G) :=$ the minimal degree of a non-trivial irreducible complex character $\chi \in IrrG$.

A family F of finite groups is called quasi-random if, for $G \in F$,

$$m(G) \to \infty \text{ as } |G| \to \infty.$$

Example: $F =$ all (nonabelian) FSG.

Gowers trick (Gowers 2008, Nikolov-Pyber 2011): If $A, B, C \subseteq G$ and $|A||B||C| \geq |G|^3/m(G)$, then

$$ABC = G.$$

Consequences:
(i) If $A \subseteq G$ and $|A| \geq m(G)^{-1/3}|G|$ then $A^3 = G$.
(ii) If F is quasi-random, $\epsilon > 0$, $G \in F$, and $A, B, C \subseteq G$ satisfy $|A|, |B|, |C| \geq \epsilon|G|$, then $ABC = G$ provided $|G| \gg 0$.
(iii) This applies for FSG.

The trouble with length two products

Can we extend results on products of length three to products of length two?
Usually not: no growth, no covering.
A rare yes: $A, B \subseteq G$, $|A|, |B| > |G|/2$ imply $AB = G$ (trivial).
Reason: A intersects gB^{-1} for all $g \in G$.
Best possible.

What if we deal with normal subsets $R, S \subseteq G$?
Liebeck-Schul-Sh (2016): For every $\epsilon > 0$ there is $\delta = \delta(\epsilon) > 0$ s.t., if G is a FSG, $R, S \subseteq G$ are normal subsets of size $\leq |G|^{\delta}$, then $|RS| \geq (|R||S|)^{1-\epsilon}$. Hence for $\delta = \delta(\epsilon/2) > 0$ and $|R| \leq |G|^{\delta}$ we have

$$|R^2| \geq |R|^{2-\epsilon}.$$

Unlike the Product Theorem, this holds for all FSG, and exhibits 2-step growth which is much faster than 3-step growth of non-normal (small, generating) subsets.
Yet, this says nothing about the 2-step growth or covering of large normal subsets.

Thompson Conjecture

Some 2-step covering problems by normal subsets are notoriously difficult and very much open:

Thompson Conjecture: Every FSG G has a conjugacy class C such that $C^2 = G$.
This implies Ore Conjecture (every element of a FSG is a commutator) proved in 2010 (Liebeck-O'Brien-Sh-Tiep);
it's still open for some FSG of Lie type over fields with ≤ 8 elements.

Approximations of Thompson Conjecture:
2008 Sh: Let G be a FSG, choose $x \in G$ at random and let $C = x^G$. Then, as $|G| \to \infty$, the random walk on G w.r.t. C has mixing time two. Consequently, for any fixed $\epsilon > 0$, $|C^2| \geq (1 - \epsilon)|G|$ almost surely.

2011 Larsen-Sh-Tiep: Every FSG G of size $> 2^{630}$ has conjugacy classes C_1, C_2 satisfying $C_1 C_2 \supseteq G \setminus \{e\}$.
2012 Guralnick-Malle: The above holds for all FSG.

Word maps

Let $w = w(x_1, \ldots, x_d)$ be a non-trivial word, namely $1 \neq w \in F_d$, 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 $w(G)$ denote the image of this map.
$w(G)$ is a normal subset of G.
Borel (1983): Word maps on simple algebraic groups are dominant.
Active project in the past 2-3 decades: Study word maps on FSG G.
Larsen (2004): They have large image.

Word Width (Annals): Liebeck-Sh (2001): $w(G)^{c(w)} = G$.
Nikolov-Segal (2007): Use word width to solve Serre's problem on profinite groups.
Let $1 \neq w_1, w_2, w_3 \in F_d$.
Sh (2009): $w_1(G)w_2(G)w_3(G) = G$ if $|G| \geq N(w_1, w_2, w_3)$.
Larsen-Sh-Tiep (2011): $w_1(G)w_2(G) = G$ if $|G| \geq N(w_1, w_2)$.
Larsen-Sh-Tiep (2019): If w_1, w_2 are disjoint words, then $w_1 w_2$ induces an almost uniform distribution on FSGs w.r.t. the L_1-norm.

Main Questions

Can we extend this to all large normal subsets?

Let S, T be normal subsets of a FSG G s.t. $|S|, |T| \geq \epsilon|G|$ $(\epsilon > 0)$.

Question 1: Does ST contain $G \setminus \{e\}$ if $|G|$ is sufficiently large?

Question 2: For $g \in G \setminus \{e\}$, is the number of solutions to $g = st$, $s \in S, t \in T$, $(1 + o_{|G|}(1))|S||T|/|G|$?

Question 3: What happens in the special case $S = T$?

Question 4: Applications?

Comments:

1. Excluding e in Questions 1 and 2 is necessary:
Every conjugacy class in $G \neq \{e\}$ has size $|G|/n$ for some $n \geq 2$, hence G has a normal subset S with $|G|/3 \leq |S| \leq 2|G|/3$. Setting $T = G \setminus S^{-1}$, we have $|T| \geq |G|/3$, and $e \notin ST$.

2. Assuming S, T are normal subsets in Questions 1 and 2 is necessary: If $G \neq \{e\}$, there are $S, T \subseteq G$ of size $\geq \lfloor |G|/2 \rfloor$ s.t. $ST \not\supseteq G \setminus \{e\}$; indeed, fix $g \in G \setminus \{e\}$, choose S of size $\lfloor |G|/2 \rfloor$, and let $T = G \setminus S^{-1}g$. Then $g \notin ST$.

3. A positive answer to Question 2 implies a positive answer to Question 1 (similarly when $S = T$).

Spoiler (main results)

Initially we tried to provide positive answers to Question 1 for all FSG.

Drawback: it's harder to prove wrong results.

Theorem (Larsen-Sh-Tiep 2020)

(i) The answers to Questions 1 and 2 are negative if G is ranges over all FSG, or even just over the alternating groups, or just over all projective special linear groups.

(ii) In the $S = T$ case, the answer to Question 2 is still negative for alternating groups.

(iii) In the $S = T$ case, the answer to Question 1 is positive for alternating groups.

(iv) If G is a group of Lie type of bounded rank, the answers to Questions 1 and 2 are both positive.

Alternating groups

Theorem

For every $s, t \geq 0$ with $s + t \leq 1$ there are normal subsets $S_n, T_n \subset A_n$ such that $|S_n|/|A_n| \to s$, $|T_n|/|A_n| \to t$, and $S_n T_n$ contains no 3-cycle.

Hence, for normal subsets $S, T \subset A_n$, the inequalities $|S|, |T| \geq (1/2 - o(1))|A_n|$ do not imply $ST \supseteq A_n \setminus \{e\}$.

What if $S = T$?

In this case we obtain a covering result even when $\epsilon \to 0$ rather fast:

Theorem

For every $0 < \alpha < 1/4$ there exists $N > 0$ such that, if $n \geq N$ and $T \subseteq A_n$ is a normal subset satisfying

$$|T| \geq \exp(-n^{\alpha}) \cdot |A_n|,$$

then $T^2 = A_n$.

Proof ideas

1. Applying exponential character bounds for S_n (Larsen-Sh): for each $\sigma \in S_n$ there is a well-defined $E(\sigma) \in [0,1]$ s.t.

$$|\chi(\sigma)| \leq \chi(1)^{E(\sigma)+o(1)} \text{ for all } \chi \in Irr S_n.$$

2. $E(\sigma) < 1/4$ implies $(\sigma^{S_n})^2 = A_n$ for all $n \gg 0$.

3. For every subset $T \subseteq A_n$ satisfying $|T| \geq \exp(-n^\alpha) \cdot |A_n|$ with $\alpha < 1/4$, a random $\sigma \in T$ satisfies $E(\sigma) < 1/4$ almost surely.

4. Hence there is $\sigma \in T$ with $(\sigma^{S_n})^2 = A_n$ for $n \gg 0$.

5. Replacing σ^{S_n} with σ^{A_n} using Erdös-Turán's Statistical group theory. Conclude that $T^2 = A_n$ for $n \gg 0$.

Classical groups

Bad groups: e.g. $G = PSL_n(q)$ for q fixed and n unbounded and coprime to $q-1$. Here Question 1 has a negative answer: there are $S, T \subset G$ normal of size $\geq \epsilon|G|$ s.t. no transvection lies in ST. Passing to three normal subsets, Question 1 has a positive answer with a tiny $\epsilon = |G|^{-\delta}$:

Theorem

There exists a fixed $\delta > 0$ s.t., if G is a finite simple classical group, and $R, S, T \subseteq G$ are normal subsets of size $\geq |G|^{1-\delta}$, then $RST = G$.

This doesn't follow from Gowers trick:
for G of rank $r \gg 0$, $|G|^{-\delta} \sim q^{-ar^2}$ is much smaller than $m(G)^{-1/3} \sim q^{-br}$.
Main tools in the proof: Level theory of characters (Guralnick-Larsen-Tiep 2019): There is $\gamma > 0$ such that, if $|C_G(g)| \leq |G|^{\gamma}$, then $|\chi(g)| \leq \chi(1)^{1/4}$ for all $\chi \in Irr(G)$.
Witten zeta function $\zeta^G(s) = \sum_{\chi \in IrrG} \chi(1)^{-s}$ and its abscissa of convergence (Liebeck-Sh 2006).

The bounded rank theorem

Good groups: Lie type groups of bounded rank.
For normal subsets $R_1, \ldots, R_k$ of G and $g \in G$, let $P_{R_1,\ldots,R_k}(g)$ denote the probability that $x_1 \cdots x_k = g$, where $x_i \in R_i$ are randomly chosen.

Theorem

Let $G = X_r(q)$, a finite simple group of Lie type of rank r over F_q. Suppose r is bounded and $q \to \infty$. Fix $\epsilon > 0$ and let $S, T \subseteq G$ be normal subsets of size $\geq \epsilon|G|$. Then, for every $g \in G \setminus \{e\}$ we have

$$P_{S,T}(g) = (1 + o_{|G|}(1))|G|^{-1}.$$

Thus Question 2, and hence Questions 1-3, have affirmative answers for G.

Proof tools: Algebraic Geometry and Character Theory

The character connection:
Frobenius: $C_1, \ldots, C_k \subset G$ conjugacy classes, $g \in G$. Then

$$P_{C_1,\ldots,C_k}(g) = |G|^{-1} \sum_{\chi} \frac{\chi(C_1) \cdots \chi(C_k)\bar{\chi}(g)}{\chi(1)^{k-1}}.$$

Use the theory of exponential character bounds: $|\chi(g)| \leq \chi(1)^{\alpha(g)}$.
For S_n: Fomin-Lulov (1996), Liebeck-Sh (2004), Muller-Puchta (2007), Larsen-Sh (2008).
For For Lie type groups: Bezrukavnikov-Liebeck-Sh-Tiep (2018), Guralnick-Larsen-Tiep (2019, 2020), Taylor-Tiep (2020).

Tools from Algebraic Geometry:
Lang-Weil theorem estimating the number of q-rational points on varieties.
The existence of geometrically irreducible generic fibers and its connection with almost uniform word maps.

Applications I: word maps

For $w : G^d \to G$, $g \in G$, set $P_{w,G}(g) := |w^{-1}(g)|/|G|^d$.
Larsen-Sh-Tiep 2019: for every $\ell \geq 1$ there exists $N = N(\ell)$ such that, if $1 \neq w_1, \ldots, w_N \in F_d$ are pairwise disjoint words of length $\leq \ell$, G a FSG, then

$$\|P_{w_1 \cdots w_N, G} - U_G\|_\infty \to 0 \text{ as } |G| \to \infty.$$

Changing the probabilistic model and using the bounded rank theorem, we obtain an almost uniform distribution in L_∞ much faster:

Corollary

Let $1 \neq w_1, w_2 \in F_d$ and let G be a FSG of Lie type of bounded rank. Then

$$\|P_{w_1(G), w_2(G)} - U_G\|_\infty \to 0 \text{ as } |G| \to \infty.$$

A version for classical groups of unbounded rank (Nikolov-Pyber):

$$\|P_{w_1(G), w_2(G), w_3(G)} - U_G\|_\infty \to 0 \text{ as } |G| \to \infty.$$

Applications II: Derangements

$G \leq S_n$ a permutation group. A derangement is a fixed-point-free permutation $g \in G$.
The study of derangements goes back three centuries.
Monmort 1708: the proportion of derangements in S_n (in its natural action) tends to $1/e$ as $n \to \infty$.
Jordan 1870s: If G is transitive and $2 \leq n < \infty$ then there is a derangement $g \in G$.
Cameron-Cohen 1990: The proportion of derangements in G as above is $\geq 1/n$ (sharp).

Conjecture (Boston-Sh 1990s)

The proportion of derangements in any finite simple transitive permutation group is $\geq \epsilon$ for some fixed $\epsilon > 0$.

$D(G) :=$ the set of derangements in G. $D(G) = D(G)^{-1}$ is a normal subset of G. The conjecture states that $|D(G)| \geq \epsilon |G|$.
For G transitive with a point-stabilizer H, $D(G) = G \setminus \cup_{g \in G} H^g$.

Derangements width I

Theorem (Fulman-Guralnick 2002-2018)

The conjecture holds. If $|G| \gg 0$ we may take $\epsilon = 0.016$.

Since FSGs are quasi-random, the above theorem, combined with Gowers trick, yields:

Corollary

For all sufficiently large transitive simple permutation groups G, every permutation in G is a product of three derangements.

Can we replace three by two?

Theorem

Let G be a finite simple transitive permutation group which is alternating or of Lie type of bounded rank. If $|G| \gg 0$ then every element of G is a product of two derangements.

Indeed, we proved for the groups above that $T^2 = G$ for normal subsets T of size $\geq \epsilon|G|$. Take $T := D(G)$.

Derangements width II

It remains to deal with classical groups G of unbounded rank. We may assume primitive action, i.e. a point-stabilizer H is a maximal subgroup.

Cameron Conjecture: Almost all permutations in S_n ($n \to \infty$) do not lie in a proper transitive subgroup (not containing A_n).

1993 Łuczak-Pyber: Cameron Conjecture holds. They also posed a similar problem for $GL_n(p)$ (p fixed).

1998 Sh: Almost all matrices in $GL_n(q)$ (q fixed, $n \to \infty$) do not lie in a proper irreducible subgroup (not containing $SL_n(q)$).

2018 Fulman-Guralnick: A similar result for all classical groups of rank $\to \infty$ (q arbitrary); if $G = Sp_{2r}(2^k)$ we exclude the subgroups $O^{\pm}_{2r}(2^k)$.

Corollary

$G \in Cl_n(q)$ has derangement width two when $n \gg 0$ and the point-stabilizer H is irreducible and not $O^{\pm}_n(2^k)$ when $G = Sp_n(2^k)$.

Proof: The union $X(G)$ of the above subgroups has size $< |G|/2$ for $n \gg 0$. $\cup_{g \in G} H^g \subseteq X(G)$ implies $|D(G)| \geq |G| - |X(G)| > |G|/2$, hence $D(G)^2 = G$.

There are absolute constants c_1, c_2 s.t. the following holds. Let $G \in Cl_n(q)$ be a finite simple classical primitive permutation group with point-stabilizer H. Assume $(G, H) \neq (Sp_n(2^k), O_n^{\pm}(2^k))$, $n \geq c_1$ and the action is not a subspace action on subspaces of dimension $k \leq c_2$. Then G has derangements width two.

Indeed, we may assume that H is reducible, namely G acts in subspace action, say on subspaces of dimension $k \leq n/2$. Results of Fulman and Guralnick show that, as $k \to \infty$, the proportion of derangements in G is $1 - O(k^{-0.005})$, which tends to 1. The result follows as before.

In the remaining cases, character methods are often useful; the method of Malle-Saxl-Weigel 1994 and its extensions, e.g. LST 2011, use weakly orthogonal tori T_1, T_2 and regular s.s. elements $t_i \in T_i$ s.t. only few (unipotent) characters $\chi \in IrrG$ satisfy $\chi(t_1)\chi(t_2) \neq 0$, which helps showing that $t_1^G t_2^G \supseteq G \setminus \{e\}$.

Upshot

This completes the proof of:

Theorem

Let G be a finite simple transitive permutation group. If G is sufficiently large, then every element of G is a product of two derangements.

Are there any exceptions?
Conjecture: NO
O'Brien: positive computational evidence

Thank you and good health!