Asymptotics of Powers in Finite Reductive Groups

Anupam Singh (IISER Pune, India)

email : anupam@iiserpune.ac.in

IISER PUNE

Word maps

- G a finite group.
- A word w is an element of the free group F_d in d variables $X_1, \ldots, X_d$.
- For example, $w = X_{i_1}^{j_1} \cdots X_{i_k}^{j_k}$.
- **Word map**

  $$w \colon G^d \to G$$

  given by

  $$(g_1, \ldots, g_d) \mapsto w(g_1, \ldots, g_d).$$

- w is said to be non-trivial if $w(G) \neq \{1\}$.

Broad questions

- How big is the image $w(G) := w(G^d) \subset G$?
- In particular, is w surjective?
- What's the width of $< w(G) >$ with respect to $w(G)$?
- For example, determine the diameter of the Cayley graph of G with respect to the set $w(G)$ when w is surjective?
- When G is finite, estimate $\frac{|w(G)|}{|G|}$?

Some classic examples

1. **Commutator map:** When $w(X_1, X_2) = X_1 X_2 X_1^{-1} X_2^{-1}$ the map

$$w \colon G \times G \to G$$

given by

$$(g, h) \mapsto ghg^{-1}h^{-1}$$

is called a commutator map.

Some classic examples

1. **Commutator map:** When $w(X_1, X_2) = X_1 X_2 X_1^{-1} X_2^{-1}$ the map

$$w\colon G \times G \to G$$

given by

$$(g, h) \mapsto ghg^{-1}h^{-1}$$

is called a commutator map.

2. **Power map:** When $w(X) = X^M$ the map $w\colon G \to G$ given by

$$g \mapsto g^M$$

is called a power map.

Motivation

Ore's conjecture

Ore, in 1951, conjectured that the commutator map is surjective for all non-Abelian finite simple groups.

Ore's conjecture

Ore, in 1951, conjectured that the commutator map is surjective for all non-Abelian finite simple groups.

Now this conjecture is proved in affirmative.

- Ore himself proved it for the alternating groups in 1951.
- Thompson for SL_n in 1961.
- Ellers and Gordeev proved for all finite simple groups of Lie type (except some small size) in 1998.
- Liebeck, O'Brien, Shalev and Tiep completed the proof in 2010.

Waring-like problem

The Waring problem in number theory:

Given $k > 1$, does there exist $g(k)$ such that every natural number is a sum of $g(k)$ many k-th powers of natural numbers.

That is, find $g(k)$ (smallest) such that $X_1^2 + \cdots + X_{g(k)}^2$ is surjective on $\mathbb{N}$.

Waring-like problem

The Waring problem in number theory:

For example, the four square theorem says $g(2) = 4$, i.e, every positive integer is a sum of four squares.

$g(3) = 9$, $g(4) = 19$, $g(5) = 37$, $g(6) = 73$ etc.

This has some well known contribution of R. Balasubramanian.

Conjecture: $g(k) = 2^k + \lfloor (3/2)^k \rfloor - 2$**.**

Waring-like problem

Waring-like problem for non-Abelian finite simple (and quasi-simple) groups:

Given n, does there exist $f(n)$ such that, the word map

$$X_1^n \cdots X_{f(n)}^n$$

is surjective on all non-Abelian finite simple (quasi-simple) groups?

In other words, consider the set $S = \{g^n \mid g \in G\}$ where G is a FSG. Does S generate G and determine the width of G with respect to the set S?

Borel dominance theorem (Borel 1983)

G a simple algebraic group and $w \in F_d$, a non-trivial word.

Then, the word map defined by w is a dominant morphism.

Thus, for simple algebraic groups, $f(k) = 2$.

♣ P. Chatterjee and Steinberg have studied surjectivity of power map for algebraic groups.

Work done on Waring-like problem

Notation: G a **non-abelian finite simple group (FSG)**, w a non-trivial word.

Work done on Waring-like problem

Notation: G a **non-abelian finite simple group (FSG)**, w a non-trivial word.

- Martinez and Zelmanov (1996), Saxl and Wilson (1997) proved the existence of $f(k)$.

Work done on Waring-like problem

Notation: G a **non-abelian finite simple group (FSG)**, w a non-trivial word.

- Martinez and Zelmanov (1996), Saxl and Wilson (1997) proved the existence of $f(k)$.
- Liebeck & Shalev (Annals of Math 2001) : there exists c such that $w(G)^c = G$.

Work done on Waring-like problem

Notation: G a **non-abelian finite simple group (FSG)**, w a non-trivial word.

- Martinez and Zelmanov (1996), Saxl and Wilson (1997) proved the existence of $f(k)$.
- Liebeck & Shalev (Annals of Math 2001) : there exists c such that $w(G)^c = G$.
- Shalev (Annals of Math 2009) : there exists N such that when $|G| > N$, we have $w(G)^3 = G$.

Work done on Waring-like problem

Notation: G a **non-abelian finite simple group (FSG)**, w a non-trivial word.

- Martinez and Zelmanov (1996), Saxl and Wilson (1997) proved the existence of $f(k)$.
- Liebeck & Shalev (Annals of Math 2001) : there exists c such that $w(G)^c = G$.
- Shalev (Annals of Math 2009) : there exists N such that when $|G| > N$, we have $w(G)^3 = G$.
- Larsen, Shalev & Tiep (Annals of Math 2011) : there exists N such that when $|G| > N$, we have $w(G)^2 = G$.

Work done on Waring-like problem

Mainly from the work of Larsen, Shalev and Tiep, it follows that for **large enough** G, we have

- $f(w(G)) = 2$ when G is finite simple and
- $f(w(G)) = 3$ when G is finite quasi-simple.

♣ See the survey article by Shalev titled “Some results and problems in the theory of word maps”.

Surjectivity of certain maps on FSG

In a series of four papers by Liebeck, O'Brien, Shalev and Tiep and another paper together with Guralnick the following results are proved:

- Every element of every FSG is a product of two squares.
- Every element of every FSG is a product of two nth powers where $n = p^k$ or $p^a q^b$. It is not true when n is a product of three prime powers.

Lie groups and Chevalley groups

Hui, Larsen and Shalev, in 2015, proved similar results for certain Lie groups and Chevalley groups.

- There exists N such that if G is a classical connected real compact Lie group of rank at least N then $w(G)^2 = G$.
- Over $\mathbb{R}$ or $\mathbb{Q}_p$, for a simple Chevalley group G over F, we have $w(G)^3 = G$.

Image Size

Estimating image size

Larsen and Shalev, 2009 proved the following:

For each non-trivial word w and $\epsilon > 0$, there exists $N = N(w, \epsilon)$ such that if $n > N$ then

$$\frac{|w(Alt_n)|}{|Alt_n|} \geq \frac{1}{n^{\frac{29}{9}+\epsilon}}.$$

Estimating image size

In the same paper, Larsen and Shalev proved the following:

For all non-trivial w there exists $N = N(w)$ such that if G is a finite simple group of Lie type of rank n which is not of type A_n or ${}^2A_n$ and $|G| \geq N$ then

$$\frac{|w(G)|}{|G|} \geq \frac{c}{n}$$

where c is an absolute constant depending on w.

Shalev's conjecture

Shalev conjectured that the bound, in the last inequality, should hold for the groups of type A_n and ${}^2A_n$ too.

Theorem (Galt, Kulshrestha, Singh, Vdovin: Journal of Group Theory 2019)

We proved the Shalev's conjecture for power maps.

Let $w = X^M$ be the power word on $G = PSL_n(q)$ or $PSU_n(q)$ where q is odd. Then, there exists $N = N(M)$ such that if $|G| > N$ we have,

$$\frac{|w(G)|}{|G|} \geq \frac{\ln(n)}{2nM^2}.$$

Groups of type A_1

It is known that every element of $SL_2(\mathbb{F}_q)$ is a product of two-squares. (In fact, results for more general words are known.)

Theorem (Kulshrestha, Singh: Proc. Indian Acad. Sci. Math. Sci: 2020)

Suppose characteristic of k is not 2.

1. *Every element of $SL_2(k)$ is a product of 2 squares.*

2. *In addition, if 2 is a square in k, then every element of $SL_1(Q)$ is a product of two squares if and only if -1 is a square in $SL_1(Q)$, where Q is a quaternion division algebra.*

Lower triangular matrix groups

Notation:

- q power of a prime p,
- $T(n,q)$ lower triangular matrix group,
- $U(n,q)$ uni-triangular subgroup and
- $U_{p-1}(n,q) = \{(a_{ij}) \in U(n,q) \mid a_{ij} = 0,\ \forall\ i-j \leq p-1\}$.

Then,

1. $U(n,q)^p \subset U_{p-1}(n,q)$.

2. $U(n,q)^p = 1$ if and only if $n \leq p$, and $U(n,q)^p = U_{p-1}(n,q)$ if and only if $n = p+1, p+2$.

Theorem (Dolfi, Singh, Yadav: Journal of Algebra and its application, 2020)

1. Let $n \geq p+3$. Then, the set $U(n,q)^p$ is a proper generating subset of $U_{p-1}(n,q)$ and when $q \geq n-p-1$,

$$|U(n,q)^p| > \frac{1}{3}|U_{p-1}(n,q)|.$$

2. Suppose $q > n-p-1$. Then, for the group $T = T(n,q)$ we have,

$$\frac{|T^p|}{|T|} \geq \frac{2^{n-2}}{9(q-1)^{n-2}q^{(p-1)(n-p)}}.$$

In fact, every element of $U_{p-1}(n,q)$ is a product of two elements from $U(n,q)^p$.

Generating functions for the powers in $GL(n,q)$ (Kundu and Singh, 2020)

For the group $GL(n,q)$ and $M \geq 2$, we have computed the generating function for the number of semisimple, regular and regular semisimple classes and elements which are M^{th} powers in $GL(n,q)$.

Polya's cycle index for symmetric groups is generalised by Kung and Stong to cycle index for $GL(n,q)$ and, by Fulman for other classical groups. Our results generalise the known results for $M = 1$ due to Wall, Macdonald, Fulman, Miller etc.

Asymptotic Bounds

Finite reductive groups

- Let $\mathbb{F}_q$ be a finite field and $k = \bar{\mathbb{F}}_q$.
- Let G be a connected reductive group over k with Frobenius map F, so that $G(\mathbb{F}_q) = G^F$ is a finite group of Lie type.
- This allows us to consider $G(\mathbb{F}_q) \subset G$.

Finite reductive groups

- Let $\mathbb{F}_q$ be a finite field and $k = \bar{\mathbb{F}}_q$.
- Let G be a connected reductive group over k with Frobenius map F, so that $G(\mathbb{F}_q) = G^F$ is a finite group of Lie type.
- This allows us to consider $G(\mathbb{F}_q) \subset G$.
- We consider the power map $\omega\colon G \to G$ given by $x \mapsto x^M$. Clearly, this map is defined over $\mathbb{F}_q$.
- We consider the image of the set $G(\mathbb{F}_q)$ under this map, denoted as $G(\mathbb{F}_q)^M$.

Examples to keep in mind

- Consider the group $GL(n)$ over k.
- Define $F\colon GL(n) \to GL(n)$ by $(a_{i,j}) \mapsto (a_{i,j}^q)$. This is a Frobenius map and $GL(n)^F = GL(n)(\mathbb{F}_q) = GL(n,q)$.
- Consider the map F on $GL(n)$ given by $(a_{i,j}) \mapsto {}^t(a_{i,j}^q)^{-1}$. The fixed point set is the unitary group $GL(n)^F = U(n,q) \subset GL(n,q^2)$.

Notation

Denote the set of M-power regular semisimple elements as

$$G(\mathbb{F}_q)^M_{rs} := G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{rs},$$

the set of M-power semisimple elements as

$$G(\mathbb{F}_q)^M_{ss} := G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{ss},$$

and M-power regular elements as

$$G(\mathbb{F}_q)^M_{rg} := G(\mathbb{F}_q)^M \cap G(\mathbb{F}_q)_{rg}.$$

Question

We are interested in studying the asymptotic values of the following as $q \to \infty$:

$$\frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{rs}|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{ss}|}{|G(\mathbb{F}_q)|}, \frac{|G(\mathbb{F}_q)^M_{rg}|}{|G(\mathbb{F}_q)|}.$$

Theorem (Kulshrestha, Kundu, Singh: 2020)

- G a connected reductive group defined over $\mathbb{F}_q$
- $M \geq 2$ an integer

Theorem (Kulshrestha, Kundu, Singh: 2020)

- G a connected reductive group defined over $\mathbb{F}_q$
- $M \geq 2$ an integer
- Then,

$$\lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{rs}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{ss}|}{|G(\mathbb{F}_q)|}$$

$$= \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{rg}|}{|G(\mathbb{F}_q)|} = \sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}$$

- where the sum varies over non-conjugate maximal tori T in $G(\mathbb{F}_q)$,
- $T = T_{d_1,\cdots,d_s} \cong C_{d_1} \times \cdots \times C_{d_s}$ reflects the cyclic structure of T, and the group $W_T = N_{G(\mathbb{F}_q)}(T)/T$.

IISER PUNE

Example $GL(2,q)$

- There are two maximal tori up to conjugacy.
- The split maximal torus $T_1 \cong C_{q-1} \times C_{q-1}$ with $|W_{T_1}| = 2$, and the anisotropic torus $T_2 \cong C_{q^2-1}$ with $|W_{T_2}| = 2$.
- Thus, the probability of finding a M^{th} power in $GL(2,q)$ is

$$= \frac{1}{2.(M, q-1)(M, q-1)} + \frac{1}{2.(M, q^2-1)}.$$

Example $GL(2,q)$

- When $M=2$ the probability is $\frac{1}{2.(2,q-1)^2}+\frac{1}{2.(2,q^2-1)}=\frac{3}{8}$ if q is odd and 1 if q is even.

- When $M=3$, the probability would be:

$$\begin{cases} 1 & \text{if } q=0 \pmod 3 \\ \frac{2}{9} & \text{if } q=1 \pmod 3 \\ \frac{2}{3} & \text{if } q=2 \pmod 3. \end{cases}$$

Example $GL(2,q)$ and $M = 2$

From direct computation following the work in Kundu and Singh (Generating functions for the powers in $GL(n,q)$: 2020), we have the following:

q	$\lvert GL(2,q)^2 \rvert$	$\lim_{q\to\infty} \frac{\lvert GL(2,q)^2 \rvert}{\lvert GL(2,q) \rvert}$
odd	$\frac{3}{8}q^4 - \frac{5}{8}q^3 + \frac{1}{8}q^2 + \frac{5}{8}q - \frac{1}{2}$	$\frac{3}{8}$
even	$q^4 - 2q^3 + 2q - 1$	1

q	$\lvert GL(2,q)^2_{rg} \rvert$	$\lvert GL(2,q)^2_{ss} \rvert$	$\lvert GL(2,q)^2_{rs} \rvert$
odd	$\frac{3}{8}q^4 - \frac{5}{8}q^3 + \frac{1}{8}q^2 - \frac{3}{8}q - \frac{1}{2}$	$\frac{3}{8}q^4 - \frac{9}{8}q^3 + \frac{5}{8}q^2 + \frac{9}{8}q - 1$	$\frac{3}{8}q^4 - \frac{9}{8}q^3 + \frac{5}{8}q^2 + \frac{1}{8}q$
even	$q^4 - 2q^3 + q$	$q^4 - 2q^3 + 2q - 1$	$q^4 - 2q^3 + q$

$GL(2,q)$ and $M = 3$

q	$\lvert GL(2,q)^3 \rvert$	$\lim_{q\to\infty} \frac{\lvert GL(2,q)^3 \rvert}{\lvert GL(2,q) \rvert}$
0	$q^4 - 2q^3 + 2q - 1$	1
1	$\frac{2}{9}(q^4 - q^3 - q^2 + q)$	$\frac{2}{9}$
2	$\frac{2}{3}(q^4 - q^3 - q^2 + q)$	$\frac{2}{3}$

q	$\lvert GL(2,q)^3_{rg} \rvert$	$\lvert GL(2,q)^3_{ss} \rvert$	$\lvert GL(2,q)^3_{rs} \rvert$
0	$q^4 - 2q^3 + q$	$q^4 - 2q^3 + 2q - 1$	$q^4 - 2q^3 + q$
1	$\frac{2}{9}q^4 - \frac{2}{9}q^3 - \frac{2}{9}q^2 - \frac{1}{9}q + \frac{1}{3}$	$\frac{2}{9}q^4 - \frac{5}{9}q^3 + \frac{1}{9}q^2 + \frac{5}{9}q - \frac{1}{3}$	$\frac{2}{9}q^4 - \frac{5}{9}q^3 + \frac{1}{9}q^2 + \frac{2}{9}$
2	$\frac{2}{3}q^4 - \frac{2}{3}q^3 - \frac{2}{3}q^2 - \frac{1}{3}q + 1$	$\frac{2}{3}q^4 - \frac{5}{3}q^3 + \frac{1}{3}q^2 + \frac{5}{3}q - 1$	$\frac{2}{3}q^4 - \frac{5}{3}q^3 + \frac{1}{3}q^2 + \frac{2}{3}q.$

IISER PUNE

Some ideas involved in the proof of Main Theorem

Main Theorem (Kulshrestha, Kundu, Singh: 2020)

- $G/\mathbb{F}_q$ connected reductive; $M \geq 2$ be an integer.

Then,

$$\lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{rs}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{ss}|}{|G(\mathbb{F}_q)|} = \lim_{q\to\infty} \frac{|G(\mathbb{F}_q)^M_{rg}|}{|G(\mathbb{F}_q)|}$$

$$= \sum_{T=T_{d_1},\cdots,d_s} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)}$$

- sum varies over non-conjugate maximal tori T in $G(\mathbb{F}_q)$,
- $T = T_{d_1,\cdots,d_s} \cong C_{d_1} \times \cdots \times C_{d_s}$ cyclic structure of T,
- the group $W_T = N_{G(\mathbb{F}_q)}(T)/T$.

IISER PUNE

The key Lemma

- The key step to prove the Main Theorem is,

$$\frac{|G(\mathbb{F}_q)^M_{rs}|}{|G(\mathbb{F}_q)|} = \sum_{T=T_{d_1,\cdots,d_s}} \frac{1}{|W_T|(M,d_1)\cdots(M,d_s)} + \mathcal{O}(q^{-1})$$

- where the sum varies over non-conjugate maximal tori T in $G(\mathbb{F}_q)$,
- $T = T_{d_1,\cdots,d_s} \cong C_{d_1} \times \cdots \times C_{d_s}$ reflects the cyclic structure, and the group $W_T = N_{G(\mathbb{F}_q)}(T)/T$.

Regular semisimple elements

Regular semisimple elements $\equiv$ connected component of centralizers of these elements is a maximal torus.

Regular semisimple elements are dense in $G(\mathbb{F}_q)$, thus we work with them. In fact,

$$|G(\mathbb{F}_q)_{rs}| = |G(\mathbb{F}_q)|(1 + \mathcal{O}(q^{-1})).$$

For example, when $G = GL(n, k)$ these are the ones which are conjugate to a diagonal matrix with distinct entries over algebraic closure.

Where do we find rs?

A semisimple element belongs to a maximal torus.

A regular semisimple element belongs to a unique maximal torus.

For example, maximal tori, up to conjugacy, in $GL(n, q)$ are in one-one correspondence with partitions of n.

When $n = 3$, $(1, 1, 1) \leftrightarrow \mathbb{F}_q^* \times \mathbb{F}_q^* \times \mathbb{F}_q^*$ (the split torus), $(1, 2) \leftrightarrow \mathbb{F}_q^* \times \mathbb{F}_{q^2}^*$ and $(3) \leftrightarrow \mathbb{F}_{q^3}^*$ (anisotropic torus).

Estimate over a maximal torus

- Let $T = \bar{T}(\mathbb{F}_q)$ be a maximal torus in $G(\mathbb{F}_q)$ where $\bar{T}$ is a F-stable maximal torus of G.
- $|T \cap G(\mathbb{F}_q)_{rs}| = q^r + \mathcal{O}(q^{r-1})$.
- $|T^M \cap G(\mathbb{F}_q)_{rs}| = |T^M| + \mathcal{O}(q^{r-1}) = \frac{1}{(M,d_1)\cdots(M,d_s)}|T| + \mathcal{O}(q^{r-1})$.
- For the last one, $T(\mathbb{F}_q) \cong C_{d_1} \times \cdots \times C_{d_s}$ is Abelian and the power map is a group homomorpism.

Final estimate

Hence,

$$\begin{aligned}
& \frac{|G(\mathbb{F}_q)^M_{rs}|}{|G(\mathbb{F}_q)|} \\
= \quad & \frac{1}{|G(\mathbb{F}_q)|} \sum_{\bar{T}\in\tau, T=\bar{T}(\mathbb{F}_q)} |T^M \cap G(\mathbb{F}_q)_{rs}| \\
= \quad & \frac{1}{|G(\mathbb{F}_q)|} \sum_{\bar{T}\in\tau, T=\bar{T}(\mathbb{F}_q)} \left(\frac{1}{(M,d_1)\cdots(M,d_s)} |T| + \mathcal{O}(q^{r-1}) \right)
\end{aligned}$$

Now, we take $T = T_{d_1,\ldots,d_s}$ up to conjugacy.

Final estimate

$$
\begin{aligned}
&= \frac{1}{|G(\mathbb{F}_q)|}\cdot\frac{|G(\mathbb{F}_q)|}{|N_{G(\mathbb{F}_q)}(T)|}\left(\sum_{T=T_{d_1,\ldots,d_s}}\frac{1}{(M,d_1)\cdots(M,d_s)}|T|+\mathcal{O}(q^{r-1})\right)\\
&= \left(\sum_{T=T_{d_1,\ldots,d_s}}\frac{1}{(M,d_1)\cdots(M,d_s)}\frac{1}{|W_T|}\right)+\frac{1}{|W_T||T|}\mathcal{O}(q^{r-1})\\
&= \sum_{T=T_{d_1,\ldots,d_s}}\frac{1}{(M,d_1)\cdots(M,d_s)}\frac{1}{|W_T|}+\mathcal{O}(q^{-1}).
\end{aligned}
$$

IISER PUNE

Thank You.

email : anupamk18@gmail.com

https://sites.google.com/site/anupamk182/

IISER PUNE