On probabilistic generation of $\mathrm{PSL}_n(q)$

A. M. Mordcovich

Joint work with M. Quick, C. M. Roney-Dougal

University of St Andrews | FOUNDED 1413

12th of August, 2017

Probability of generating a group

- Let $d(G)$ be the size of the smallest set that generates G.

Probability of generating a group

- Let $d(G)$ be the size of the smallest set that generates G.
- If we pick k elements from group G where repetitions are allowed (assuming that $k \leq d(G)$), what is the probability of us generating this group?

Probability of generating a group

- Let $d(G)$ be the size of the smallest set that generates G.
- If we pick k elements from group G where repetitions are allowed (assuming that $k \leq d(G)$), what is the probability of us generating this group?
- We denote this probability by $P_G(k)$.

Probability of generating a group

- Let $d(G)$ be the size of the smallest set that generates G.
- If we pick k elements from group G where repetitions are allowed (assuming that $k \leq d(G)$), what is the probability of us generating this group?
- We denote this probability by $P_G(k)$.

Example: $P_{\mathbb{Z}_5}(2)$

- Consider $G = \mathbb{Z}_5$. We aim to calculate $P_G(2)$. If we pick an element that is not the identity element, then it generates the whole group.

Probability of generating a group

- Let $d(G)$ be the size of the smallest set that generates G.
- If we pick k elements from group G where repetitions are allowed (assuming that $k \leq d(G)$), what is the probability of us generating this group?
- We denote this probability by $P_G(k)$.

Example: $P_{\mathbb{Z}_5}(2)$

- Consider $G = \mathbb{Z}_5$. We aim to calculate $P_G(2)$. If we pick an element that is not the identity element, then it generates the whole group.
- So then the only pair that does not generate the whole group is a pair of identity elements. Since the number of possible pairs is 25 we have that $P_2(G) = 24/25$

Definition of $P_{G,N}(k)$

- Let N be a normal subgroup of a group G. Let us also suppose that $d(G), d(G/N) \leq k$.

Definition of $P_{G,N}(k)$

- Let N be a normal subgroup of a group G. Let us also suppose that $d(G), d(G/N) \leq k$.
- If we pick k elements from G (repetitions allowed), what is the probability that they generate G given that they also generates G modulo N?

Definition of $P_{G,N}(k)$

- Let N be a normal subgroup of a group G. Let us also suppose that $d(G), d(G/N) \leq k$.
- If we pick k elements from G (repetitions allowed), what is the probability that they generate G given that they also generates G modulo N?
- We denote this probability by $P_{G,N}(k)$.

The Classification of Finite Simple Groups

- We now look at the finite simple groups and the finite almost simple groups.

- We now look at the finite simple groups and the finite almost simple groups.
- A group G is almost simple if it satisfies $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S.

- We now look at the finite simple groups and the finite almost simple groups.
- A group G is almost simple if it satisfies $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S.
- Every finite simple group lies in one of the following classes:

- We now look at the finite simple groups and the finite almost simple groups.
- A group G is almost simple if it satisfies $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S.
- Every finite simple group lies in one of the following classes:

Classification of Finite Simple Groups

- We now look at the finite simple groups and the finite almost simple groups.
- A group G is almost simple if it satisfies $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S.
- Every finite simple group lies in one of the following classes:

Classification of Finite Simple Groups

- Cyclic groups $\mathbb{Z}_p$ of prime order

The Classification of Finite Simple Groups

- We now look at the finite simple groups and the finite almost simple groups.
- A group G is almost simple if it satisfies $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S.
- Every finite simple group lies in one of the following classes:

Classification of Finite Simple Groups

- Cyclic groups $\mathbb{Z}_p$ of prime order
- Alternating groups A_n of degree of at least 5

- We now look at the finite simple groups and the finite almost simple groups.
- A group G is almost simple if it satisfies $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S.
- Every finite simple group lies in one of the following classes:

Classification of Finite Simple Groups

- Cyclic groups $\mathbb{Z}_p$ of prime order
- Alternating groups A_n of degree of at least 5
- Simple groups of Lie type

- We now look at the finite simple groups and the finite almost simple groups.
- A group G is almost simple if it satisfies $S \leq G \leq \mathrm{Aut}(S)$ for some non-abelian simple group S.
- Every finite simple group lies in one of the following classes:

Classification of Finite Simple Groups

- Cyclic groups $\mathbb{Z}_p$ of prime order
- Alternating groups A_n of degree of at least 5
- Simple groups of Lie type
- One of 26 sporadic simple groups

Generation of finite simple groups.

- So given a finite simple group what can we say about the probability of us picking two elements (repetition allowed) that generate the group?

Generation of finite simple groups.

- So given a finite simple group what can we say about the probability of us picking two elements (repetition allowed) that generate the group?

Theorem

For all finite simple groups G, $P_G(2) > 0$.

- So given a finite simple group what can we say about the probability of us picking two elements (repetition allowed) that generate the group?

Theorem

For all finite simple groups G, $P_G(2) > 0$.

Theorem [Dixon, 1969; Kantor-Lubotzky, 1990; Liebeck-Shalev, 1995]

Generation of finite simple groups.

- So given a finite simple group what can we say about the probability of us picking two elements (repetition allowed) that generate the group?

Theorem

For all finite simple groups G, $P_G(2) > 0$.

Theorem [Dixon, 1969; Kantor-Lubotzky, 1990; Liebeck-Shalev, 1995]

For finite simple groups G we have $P_G(2) \to 1$ as $|G| \to \infty$.

Generation of finite simple groups.

- So given a finite simple group what can we say about the probability of us picking two elements (repetition allowed) that generate the group?

Theorem

For all finite simple groups G, $P_G(2) > 0$.

Theorem [Dixon, 1969; Kantor-Lubotzky, 1990; Liebeck-Shalev, 1995]

For finite simple groups G we have $P_G(2) \to 1$ as $|G| \to \infty$.

Theorem [Menezes, Quick & Roney-Dougal, 2013]

Generation of finite simple groups.

- So given a finite simple group what can we say about the probability of us picking two elements (repetition allowed) that generate the group?

Theorem

For all finite simple groups G, $P_G(2) > 0$.

Theorem [Dixon, 1969; Kantor-Lubotzky, 1990; Liebeck-Shalev, 1995]

For finite simple groups G we have $P_G(2) \to 1$ as $|G| \to \infty$.

Theorem [Menezes, Quick & Roney-Dougal, 2013]

$P_G(2) \geq 53/90 = 0.58\overline{8}$.

Bounding $P_G(2)$

- Let us start from the definition of $P_G(2)$ and see what we can derive from there. First let us assume that $d(G) \leq 2$, then

.

Bounding $P_G(2)$

- Let us start from the definition of $P_G(2)$ and see what we can derive from there. First let us assume that $d(G) \leq 2$, then

$$P_G(2) = \mathbb{P}(\langle x, y \rangle = G | \ (x, y) \in G \times G)$$

.

Bounding $P_G(2)$

- Let us start from the definition of $P_G(2)$ and see what we can derive from there. First let us assume that $d(G) \leq 2$, then

$$\begin{aligned} P_G(2) &= \mathbb{P}(\langle x, y\rangle = G|\ (x,y) \in G \times G) \\ &= 1 - \mathbb{P}(\langle x, y\rangle \neq G|\ (x,y) \in G \times G) \end{aligned}$$

.

Bounding $P_G(2)$

- Let us start from the definition of $P_G(2)$ and see what we can derive from there. First let us assume that $d(G) \leq 2$, then

$$\begin{aligned} P_G(2) &= \mathbb{P}(\langle x, y\rangle = G |\ (x,y) \in G \times G) \\ &= 1 - \mathbb{P}(\langle x, y\rangle \neq G |\ (x,y) \in G \times G) \\ &= 1 - \frac{|\{(x,y) \in G \times G |\ \langle x, y\rangle \neq G\}|}{|G \times G|}. \end{aligned}$$

Bounding $P_G(2)$

- Let us start from the definition of $P_G(2)$ and see what we can derive from there. First let us assume that $d(G) \leq 2$, then

$$\begin{aligned} P_G(2) &= \mathbb{P}(\langle x, y \rangle = G \mid (x, y) \in G \times G) \\ &= 1 - \mathbb{P}(\langle x, y \rangle \neq G \mid (x, y) \in G \times G) \\ &= 1 - \frac{|\{(x, y) \in G \times G \mid \langle x, y \rangle \neq G\}|}{|G \times G|}. \end{aligned}$$

- We notice that if x and y do not generate G if and only if they both lie in some maximal subgroup of G.

Bounding $P_G(2)$

- Let us start from the definition of $P_G(2)$ and see what we can derive from there. First let us assume that $d(G) \leq 2$, then

$$\begin{aligned} P_G(2) &= \mathbb{P}(\langle x, y\rangle = G \mid (x, y) \in G \times G) \\ &= 1 - \mathbb{P}(\langle x, y\rangle \neq G \mid (x, y) \in G \times G) \\ &= 1 - \frac{|\{(x, y) \in G \times G \mid \langle x, y\rangle \neq G\}|}{|G \times G|}. \end{aligned}$$

- We notice that if x and y do not generate G if and only if they both lie in some maximal subgroup of G.

$$\{(x, y) \in G \times G \mid \langle x, y\rangle \neq G\} = \bigcup_{M \ \max\ G} \{(x, y) \in M \times M\}.$$

Bounding $P_G(2)$ *cont.*

- So to bound $P_G(2)$ we need to bound

$$\Big| \bigcup_{M \text{ max } G} \{(x, y) \in M \times M\} \Big|.$$

Bounding $P_G(2)$ *cont*.

- So to bound $P_G(2)$ we need to bound
$$\left| \bigcup_{M \max G} \{(x,y) \in M \times M\} \right|.$$
- We can use the Inclusion-Exclusion Principle to obtain both an upper bound and lower bound.

Bounding $P_G(2)$ *cont.*

- So to bound $P_G(2)$ we need to bound
$$\left| \bigcup_{M \text{ max } G} \{(x,y) \in M \times M\} \right|.$$
- We can use the Inclusion-Exclusion Principle to obtain both an upper bound and lower bound.
$$\left| \bigcup_{M \text{ max } G} \{(x,y) \in M \times M\} \right| \leq \sum_{M \text{ max } G} |M|^2$$

Bounding $P_G(2)$ *cont.*

- So to bound $P_G(2)$ we need to bound
$$\left|\bigcup_{M \text{ max } G} \{(x,y) \in M \times M\}\right|.$$
- We can use the Inclusion-Exclusion Principle to obtain both an upper bound and lower bound.
$$\left|\bigcup_{M \text{ max } G} \{(x,y) \in M \times M\}\right| \leq \sum_{M \text{ max } G} |M|^2$$
$$\sum_{M \text{ max } G} |M|^2 - \sum_{\substack{M,N \text{ max } G \\ M \neq N}} |M \cap N|^2 \leq \left|\bigcup_{M \text{ max } G} \{(x,y) \in M \times M\}\right|$$

Bounds for $P_G(k)$

- By considering the previous and generalizing we can get the following result.

Bounds for $P_G(k)$

- By considering the previous and generalizing we can get the following result.

Theorem

Let G be a group where $d(G) \leq k$, then

- By considering the previous and generalizing we can get the following result.

Theorem

Let G be a group where $d(G) \leq k$, then

$$1 - \sum_{M \,\max\, G} |G:M|^{-k} + \sum_{\substack{M \,\max\, G \\ M \neq N}} |G : M \cap N|^{-k} \geq P_G(k) \geq 1 - \sum_{M \,\max\, G} |G:M|^{-k}.$$

Analogues for $P_{G,N}(k)$

- We can also derive an analogous result for $P_{G,N}(k)$ with a bit more effort.

- We can also derive an analogous result for $P_{G,N}(k)$ with a bit more effort.

Theorem

$$1 - \sum_{\substack{M \max G \\ N \not\leq M}} |G:M|^{-k} + \sum_{\substack{M_1, M_2 \max G \\ N \not\leq M_1, M_2 \\ M_1 \neq M_2}} |G : M_1 \cap M_2|^{-k} \geq P_{G,N}(k) \geq 1 - \sum_{\substack{M \max G \\ N \not\leq M}} |G:M|^{-k}.$$

Case where G is simple

- If G is simple, and M is a maximal subgroup of G then $|G : M| = |G : N_G(M)|$.

Case where G is simple

- If G is simple, and M is a maximal subgroup of G then $|G : M| = |G : N_G(M)|$.
- Let $\mathcal{M}$ be a set of representatives for the conjugacy classes of maximal subgroups.

Case where G is simple

- If G is simple, and M is a maximal subgroup of G then $|G : M| = |G : N_G(M)|$.
- Let $\mathcal{M}$ be a set of representatives for the conjugacy classes of maximal subgroups.
- So grouping together the conjugate maximal subgroups we can see that

$$\sum_{M \text{ max } G} |G : M|^{-k} = \sum_{M \in \mathcal{M}} |G : M|^{-k} \times |G : N_G(M)| = \sum_{M \in \mathcal{M}} |G : M|^{-(k-1)}.$$

Case where G is simple cont.

Theorem

Let G be a simple group where $d(G) \leq 2$, and $\mathcal{M}$ be a set of representatives of the conjugacy classes of the maximal subgroups of G then

Case where G is simple cont.

Theorem

Let G be a simple group where $d(G) \leq 2$, and $\mathcal{M}$ be a set of representatives of the conjugacy classes of the maximal subgroups of G then

$$1 - \sum_{M \in \mathcal{M}} |G : M|^{-1} + \sum_{\substack{M \max G \\ M \neq N}} |G : M \cap N|^{-2} \geq P_G(2) \geq 1 - \sum_{M \in \mathcal{M}} |G : M|^{-1}.$$

Maximal subgroups

- From here we realise that questions asking about the probabilities $P_G(k)$ and $P_{G,N}(k)$ are actually questions regarding maximal subgroups.

Maximal subgroups

- From here we realise that questions asking about the probabilities $P_G(k)$ and $P_{G,N}(k)$ are actually questions regarding maximal subgroups.
- We have information on the maximal subgroups of simple groups.

Maximal subgroups

- From here we realise that questions asking about the probabilities $P_G(k)$ and $P_{G,N}(k)$ are actually questions regarding maximal subgroups.
- We have information on the maximal subgroups of simple groups.
- In particular, the possible maximal subgroups of Classical Simple Groups are classified into 9 Classes under Aschbacher's Theorem.

Maximal subgroups

- From here we realise that questions asking about the probabilities $P_G(k)$ and $P_{G,N}(k)$ are actually questions regarding maximal subgroups.
- We have information on the maximal subgroups of simple groups.
- In particular, the possible maximal subgroups of Classical Simple Groups are classified into 9 Classes under Aschbacher's Theorem.
- For small dimensions we know all the the maximal subgroups for the Classical Simple Groups and their related almost-simple groups [Bray, Holt & Roney-Dougal, 2013]. Therefore we can work out bounds for the probability for these cases with relative ease.

A theorem of Liebeck & Shalev

Theorem [Liebeck & Shalev]

A theorem of Liebeck & Shalev

Theorem [Liebeck & Shalev]

There exist constants $\alpha, \beta > 0$ such that

$$1 - \frac{\alpha}{m(G)} \leq P_G(2) \leq 1 - \frac{\beta}{m(G)}$$

for all finite simple groups G. Where $m(G)$ is the index of the largest (maximal) subgroup of G in G.

A theorem of Liebeck & Shalev

Theorem [Liebeck & Shalev]

There exist constants $\alpha, \beta > 0$ such that

$$1 - \frac{\alpha}{m(G)} \leq P_G(2) \leq 1 - \frac{\beta}{m(G)}$$

for all finite simple groups G. Where $m(G)$ is the index of the largest (maximal) subgroup of G in G.

- Remember that

$$1 - \sum_{M \in \mathcal{M}} |G : M|^{-1} \leq P_G(2).$$

A theorem of Liebeck & Shalev

Theorem [Liebeck & Shalev]

There exist constants $\alpha, \beta > 0$ such that

$$1 - \frac{\alpha}{m(G)} \leq P_G(2) \leq 1 - \frac{\beta}{m(G)}$$

for all finite simple groups G. Where $m(G)$ is the index of the largest (maximal) subgroup of G in G.

- Remember that

$$1 - \sum_{M \in \mathcal{M}} |G : M|^{-1} \leq P_G(2).$$

- The theorem is more a statement that as $|G|$ gets large we may get more maximal subgroups but they are dwarfed in size by the largest ones.

Results

- Consider the inequality of Liebeck and Shalev;

$$1-\frac{\alpha}{m(G)} \leq P_G(2) \leq 1-\frac{\beta}{m(G)}$$

.

Results

- Consider the inequality of Liebeck and Shalev;

$$1 - \frac{\alpha}{m(G)} \leq P_G(2) \leq 1 - \frac{\beta}{m(G)}$$

.

- Our aim is to provide absolute values for α and β for specific families of groups, more specifically the Classical Simple Groups.

Results

- Consider the inequality of Liebeck and Shalev;

$$1 - \frac{\alpha}{m(G)} \leq P_G(2) \leq 1 - \frac{\beta}{m(G)}$$

.

- Our aim is to provide absolute values for α and β for specific families of groups, more specifically the Classical Simple Groups.
- The results we have obtained so far involve $\mathrm{PSL}_n(q)$ and the related almost simple groups.

Theorem

Results

Theorem

- If $G = \mathrm{PSL}_2(q)$ then

$$1 - \frac{\alpha}{m(G)} \leq P_G(2) \leq 1 - \frac{\beta}{m(G)}$$

where $\alpha = 38/15$ and $\beta = 1$. The left hand side becomes an equality for $q = 11$.

Results

Theorem

- If $G = \mathrm{PSL}_2(q)$ then
$$1 - \frac{\alpha}{m(G)} \leq P_G(2) \leq 1 - \frac{\beta}{m(G)}$$
where $\alpha = 38/15$ and $\beta = 1$. The left hand side becomes an equality for $q = 11$.
- If $G = \mathrm{PSL}_n(q)$ where $n > 2$ then
$$1 - \frac{\alpha}{m(G)} \leq P_G(2) \leq 1 - \frac{\beta}{m(G)}$$
where $\alpha = 57/20$ and $\beta = 16/9$.The left hand side is an equality for $n = 3$ and $q = 4$. The right hand side is an equality for $n = 3$ and $q = 3$.

Results cont.

- We also have lower bounds for $P_{G,N}(2)$ for the case of $N = PSL_n(q)$.

- We also have lower bounds for $P_{G,N}(2)$ for the case of $N = PSL_n(q)$.

Theorem

Results cont.

- We also have lower bounds for $P_{G,N}(2)$ for the case of $N = PSL_n(q)$.

Theorem

If G is almost simple with socle $N = \mathrm{PSL}_n(q)$ then

$$1 - \frac{\alpha}{m(G)} \leq P_{G,N}(2)$$

where $\alpha = 3983/1296 = 3.07$ (2 d.p.). With equality occurring when $n = 4$ and $q = 3$, and G is the extension of $\mathrm{PSL}_n(q)$ by the graph automorphism γ.