The width of a finite simple group

Nick Gill (OU)

September 4, 2012

Growth

Let A be a finite subset of a group G.

Growth

Let A be a finite subset of a group G.
Define

$$A^2 = A \cdot A := \{a_1 \cdot a_2 \mid a_1, a_2 \in A\}.$$

Growth

Let A be a finite subset of a group G.
Define
$$A^2 = A \cdot A := \{a_1 \cdot a_2 \mid a_1, a_2 \in A\}.$$

We are interested in studying the size of $A^2, A^3, A^4, \ldots$ we call this the study of the *growth* of A.

Doubling and tripling

Doubling and tripling

Suppose first that G is abelian (the classical setting for additive combinatorics).

Doubling and tripling

Suppose first that G is abelian (the classical setting for additive combinatorics).

- If $|AA| \leq K|A|$ then $|A^\ell| \leq K^\ell|A|$ [P-R].

Doubling and tripling

Suppose first that G is abelian (the classical setting for additive combinatorics).

- If $|AA| \leq K|A|$ then $|A^\ell| \leq K^\ell|A|$ [P-R].

Now drop the condition that G is abelian.

Doubling and tripling

Suppose first that G is abelian (the classical setting for additive combinatorics).

- If $|AA| \leq K|A|$ then $|A^\ell| \leq K^\ell|A|$ [P-R].

Now drop the condition that G is abelian.

- If $|AAA| \leq K|A|$ then $|A^\ell| \leq K^{2\ell-5}|A|$ [H-T].

Simple groups of Lie type

Let A be a subset of $G = G_r(q)$. How does the set A grow? This question is partially answered, with a strong value of K, by a theorem of Pyber-Szabo, Breuillard-Green-Tao building on work of Helfgott, Dinai, Helfgott-G.

Simple groups of Lie type

Let A be a subset of $G = G_r(q)$. How does the set A grow? This question is partially answered, with a strong value of K, by a theorem of Pyber-Szabo, Breuillard-Green-Tao building on work of Helfgott, Dinai, Helfgott-G.

Theorem

Fix $r > 0$. There exists a positive number ϵ such that for any generating set A in $G_r(q)$ either

- $|AAA| \geq |A|^{1+\varepsilon}$, *or*
- $AAA = G$.

Simple groups of Lie type

Let A be a subset of $G = G_r(q)$. How does the set A grow? This question is partially answered, with a strong value of K, by a theorem of Pyber-Szabo, Breuillard-Green-Tao building on work of Helfgott, Dinai, Helfgott-G.

Theorem

Fix $r > 0$. There exists a positive number ϵ such that for any generating set A in $G_r(q)$ either

- $|AAA| \geq |A|^{1+\varepsilon}$, *or*
- $AAA = G$.

Applications are manifold: diameter bounds, expansion, sieving...

Dependence on the rank [P-S]

Let A be a generating set of $SL_n(q)$ containing:

Dependence on the rank [P-S]

Let A be a generating set of $SL_n(q)$ containing:

1. T, the set of diagonal matrices; $|T| = (q-1)^{n-1}$;

Dependence on the rank [P-S]

Let A be a generating set of $SL_n(q)$ containing:

1. T, the set of diagonal matrices; $|T| = (q-1)^{n-1}$;
2. a, b, two elements generating this copy of $SL_2(q)$:

$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$$

Dependence on the rank [P-S]

Let A be a generating set of $SL_n(q)$ containing:

1. T, the set of diagonal matrices; $|T| = (q-1)^{n-1}$;
2. a, b, two elements generating this copy of $SL_2(q)$:

$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$$

3. The following n-cycle monomial matrix s

$$\begin{pmatrix} & a & & \\ & & \ddots & \\ & & & c \\ d & & & \end{pmatrix}$$

Dependence on the rank [P-S]

Let A be a generating set of $SL_n(q)$ containing:

1. T, the set of diagonal matrices; $|T| = (q-1)^{n-1}$;
2. a, b, two elements generating this copy of $SL_2(q)$:

$$\begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{pmatrix}$$

3. The following n-cycle monomial matrix s

$$\begin{pmatrix} & a & & \\ & & \ddots & \\ & & & c \\ d & & & \end{pmatrix}$$

Now $A^3 \neq G$ and, if $q = 3$, $|A^3| \leq 17 \cdot |A| < |A|^{1+\frac{5}{n-1}}$.

Babai's conjecture

Let G be a finite simple group and A a generating set in G. Note that

Babai's conjecture

Let G be a finite simple group and A a generating set in G. Note that

1. $A^\ell = G$ for some integer ℓ (take it as small as possible).

Babai's conjecture

Let G be a finite simple group and A a generating set in G. Note that

1. $A^\ell = G$ for some integer ℓ (take it as small as possible).
2. $\ell \geq \frac{\log |G|}{\log |A|}$

Babai's conjecture

Let G be a finite simple group and A a generating set in G. Note that

1. $A^\ell = G$ for some integer ℓ (take it as small as possible).
2. $\ell \geq \frac{\log |G|}{\log |A|}$
3. $\ell \geq \log |G|$ if $|A| = 2$.

Babai's conjecture

Let G be a finite simple group and A a generating set in G. Note that

1. $A^\ell = G$ for some integer ℓ (take it as small as possible).
2. $\ell \geq \frac{\log |G|}{\log |A|}$
3. $\ell \geq \log |G|$ if $|A| = 2$.

Conjecture (Babai)

There exists $c > 0$ such that, for any finite simple group G and any generating set $A \subset G$, $A^\ell = G$ for some $\ell \leq (\log |G|)^c$.

Babai's conjecture

Let G be a finite simple group and A a generating set in G. Note that

1. $A^\ell = G$ for some integer ℓ (take it as small as possible).
2. $\ell \geq \frac{\log |G|}{\log |A|}$
3. $\ell \geq \log |G|$ if $|A| = 2$.

Conjecture (Babai)

There exists $c > 0$ such that, for any finite simple group G and any generating set $A \subset G$, $A^\ell = G$ for some $\ell \leq (\log |G|)^c$.

Babai's conjecture is often stated in terms of the diameter of the Cayley graph.

A partial proof of Babai's conjecture

Corollary

Fix $r > 0$. There exists $c > 0$ such that for any generating set A in $G = G_r(q)$ we have $A^\ell = G$ for some $\ell \leq (\log |G|)^c$.

Proof.

□

A partial proof of Babai's conjecture

Corollary

Fix $r > 0$. There exists $c > 0$ such that for any generating set A in $G = G_r(q)$ we have $A^\ell = G$ for some $\ell \leq (\log|G|)^c$.

Proof.

1. The product theorem implies that either $|A^3| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.

□

A partial proof of Babai's conjecture

Corollary

Fix $r > 0$. There exists $c > 0$ such that for any generating set A in $G = G_r(q)$ we have $A^\ell = G$ for some $\ell \leq (\log|G|)^c$.

Proof.

1. The product theorem implies that either $|A^3| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.
2. Iterating we obtain that either $|A^{3^k}| \geq |A|^{(1+\varepsilon)^k}$ or $A^{3^k} = G$.

□

A partial proof of Babai's conjecture

Corollary

Fix $r > 0$. There exists $c > 0$ such that for any generating set A in $G = G_r(q)$ we have $A^\ell = G$ for some $\ell \leq (\log |G|)^c$.

Proof.

1. The product theorem implies that either $|A^3| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.
2. Iterating we obtain that either $|A^{3^k}| \geq |A|^{(1+\varepsilon)^k}$ or $A^{3^k} = G$.
3. If $|A|^{(1+\varepsilon)^k} \geq |G|$ we must have $A^{3^k} = G$.

□

A partial proof of Babai's conjecture

Corollary

Fix $r > 0$. There exists $c > 0$ such that for any generating set A in $G = G_r(q)$ we have $A^\ell = G$ for some $\ell \leq (\log |G|)^c$.

Proof.

1. The product theorem implies that either $|A^3| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.
2. Iterating we obtain that either $|A^{3^k}| \geq |A|^{(1+\varepsilon)^k}$ or $A^{3^k} = G$.
3. If $|A|^{(1+\varepsilon)^k} \geq |G|$ we must have $A^{3^k} = G$.
4. Thus $A^\ell = G$ where $\ell = (\log |G|)^{\lceil \log_{1+\varepsilon} 3 \rceil + 1}$.

□

Normal subsets

Normal subsets

We say that A is a *normal subset* of G if, for all $g \in G$,

$$gAg^{-1} := \{gag^{-1} \mid a \in A\} = A.$$

Normal subsets

We say that A is a *normal subset* of G if, for all $g \in G$,

$$gAg^{-1} := \{gag^{-1} \mid a \in A\} = A.$$

Note that A is normal if and only if A is a union of conjugacy classes of G.

Normal subsets

We say that A is a *normal subset* of G if, for all $g \in G$,

$$gAg^{-1} := \{gag^{-1} \mid a \in A\} = A.$$

Note that A is normal if and only if A is a union of conjugacy classes of G.
Liebeck and Shalev proved a (much) stronger version of Babai's conjecture for normal subsets of simple groups:

Normal subsets

We say that A is a *normal subset* of G if, for all $g \in G$,

$$gAg^{-1} := \{gag^{-1} \mid a \in A\} = A.$$

Note that A is normal if and only if A is a union of conjugacy classes of G.
Liebeck and Shalev proved a (much) stronger version of Babai's conjecture for normal subsets of simple groups:

Theorem

There exists a constant $c > 0$ such that, for A a non-trivial normal subset of a simple group G, we have $G = A^\ell$ where $\ell \leq c \log |G| / \log |A|$.

Width

We define the *width* of G with respect to A to be the minimum number ℓ such that

$$G = A_1 A_2 \cdots A_\ell$$

and $A_1, \ldots, A_\ell$ are all conjugates of A in G. Write $w(G, A)$.

Width

We define the *width* of G with respect to A to be the minimum number ℓ such that

$$G = A_1 A_2 \cdots A_\ell$$

and $A_1, \ldots, A_\ell$ are all conjugates of A in G. Write $w(G, A)$.
Examples for a simple group G.

1. If G is of Lie type, A is a Sylow p-subgroup then $w(G, A) \leq 25$ [LP01].
   In fact $w(G, A) \leq 5$ [BNP08].

Width

We define the *width* of G with respect to A to be the minimum number ℓ such that

$$G = A_1 A_2 \cdots A_\ell$$

and $A_1, \ldots, A_\ell$ are all conjugates of A in G. Write $w(G, A)$.
Examples for a simple group G.

1. If G is of Lie type, A is a Sylow p-subgroup then $w(G, A) \leq 25$ [LP01].
   In fact $w(G, A) \leq 5$ [BNP08].
2. If $G = G_r(q)$, an untwisted simple group of Lie type of rank $r > 1$, and A is a particular subgroup isomorphic to $SL_2(q)$, then $w(G, A) \leq 5|\Phi^+|$ [LNS11].

Width

We define the *width* of G with respect to A to be the minimum number ℓ such that

$$G = A_1 A_2 \cdots A_\ell$$

and $A_1, \ldots, A_\ell$ are all conjugates of A in G. Write $w(G, A)$. Examples for a simple group G.

1. If G is of Lie type, A is a Sylow p-subgroup then $w(G, A) \leq 25$ [LP01].
   In fact $w(G, A) \leq 5$ [BNP08].
2. If $G = G_r(q)$, an untwisted simple group of Lie type of rank $r > 1$, and A is a particular subgroup isomorphic to $SL_2(q)$, then $w(G, A) \leq 5|\Phi^+|$ [LNS11].
   In particular, if $G = PSL_n(q)$ and A as above then $w(G, A) \leq \frac{5}{2} n(n+1)$.

The Product Decomposition Conjecture

Liebeck, Nikolov and Shalev conjectured the following:

The Product Decomposition Conjecture

Liebeck, Nikolov and Shalev conjectured the following:

Conjecture

There exists a constant $c > 0$ such that, for A any subset of a finite simple group G of size at least 2, we have $G = A_1 \cdots A_\ell$ where $A_1, \ldots, A_\ell$ are conjugates of A and $\ell \leq c \log|G| / \log|A|$.

The Product Decomposition Conjecture

Liebeck, Nikolov and Shalev conjectured the following:

Conjecture

There exists a constant $c > 0$ such that, for A any subset of a finite simple group G of size at least 2, we have $G = A_1 \cdots A_\ell$ where $A_1, \dots, A_\ell$ are conjugates of A and $\ell \leq c \log |G| / \log |A|$.

Note the similarity to Babai's conjecture - but both the assumptions and the conclusion are much stronger.

Some results

We start with a result of Gill, Pyber, Short, Szabó:

Theorem

Fix $r > 0$. There exists $c > 0$ such that, for A any subset of $G = G_r(q)$ of size at least 2, we have $G = A_1 A_2 \cdots A_\ell$ where $\ell \leq c \log |G| / \log |A|$.

A product theorem for conjugates

On the way to proving this result we came across something like a product theorem for conjugates:

Theorem

Fix $r > 0$. There exists $\varepsilon > 0$ such that, for A any subset of $G = G_r(q)$, there exists $g \in G$ such that $|A \cdot A^g| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.

A product theorem for conjugates

On the way to proving this result we came across something like a product theorem for conjugates:

Theorem

Fix $r > 0$. There exists $\varepsilon > 0$ such that, for A any subset of $G = G_r(q)$, there exists $g \in G$ such that $|A \cdot A^g| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.

We conjecture that the constant ε should be independent of r, indeed it should be uniform **across all simple groups**.

A product theorem for conjugates

On the way to proving this result we came across something like a product theorem for conjugates:

Theorem

Fix $r > 0$. There exists $\varepsilon > 0$ such that, for A any subset of $G = G_r(q)$, there exists $g \in G$ such that $|A \cdot A^g| \geq |A|^{1+\varepsilon}$ or $A^3 = G$.

We conjecture that the constant ε should be independent of r, indeed it should be uniform **across all simple groups**.

Note too that, when we're allowed to take conjugates, we achieve growth in two steps, not three.

The Skew Doubling Lemma

An explanation for the two step growth is found in the following result:

Theorem

Let A be a non-empty finite set of a group G such that, for some $K > 0$, $|AA'| \leq K|A|$ for every conjugate A' of A. Then

$$|A_1 \cdots A_\ell| \leq K^{14(\ell-1)}|A|$$

where $A_1, \ldots, A_\ell$ are conjugates of A or A^{-1}.

The Skew Doubling Lemma

An explanation for the two step growth is found in the following result:

Theorem

Let A be a non-empty finite set of a group G such that, for some $K > 0$, $|AA'| \leq K|A|$ for every conjugate A' of A. Then

$$|A_1 \cdots A_\ell| \leq K^{14(\ell-1)}|A|$$

where $A_1, \ldots, A_\ell$ are conjugates of A or A^{-1}.

Note that, if A is *normal*, we effectively regain the doubling lemma for abelian groups.

The Skew Doubling Lemma

An explanation for the two step growth is found in the following result:

Theorem

Let A be a non-empty finite set of a group G such that, for some $K > 0$, $|AA'| \leq K|A|$ for every conjugate A' of A. Then

$$|A_1 \cdots A_\ell| \leq K^{14(\ell-1)}|A|$$

where $A_1, \ldots, A_\ell$ are conjugates of A or A^{-1}.

Note that, if A is *normal*, we effectively regain the doubling lemma for abelian groups.

Could it be that classical additive combinatorics for sets in abelian groups is **really** about normal subsets of arbitrary groups?

Thanks for coming!