Growth in groups: a tale of SL_n and Sym_n

H A Helfgott

Our problem: Let G be a finite, simple, non-abelian group
$A \subset G$ generate G

Bound $\mathrm{diam}(\underbrace{\Gamma(G,A)})$, that is, the least k s.t. $(A \cup \{e\})^k = G$

Cayley graph:
vertices G, edges (g, ag)

notation:
$|A|$ = number of elements of A

$A^k = \{a_1 a_2 \cdots a_k : a_1, \ldots, a_k \in A\}$

Babai's conj:
$\mathrm{diam}(\Gamma(G,A)) \leq (\log|G|)^C$ ← absolute constant C independent of A or G

Related problems: 1) Let $A \subset G$ generate G.
Must A^3 be much larger than A? (clearly not the case in abelian groups)

"approximate subgroups" ≈ A for which the answer is "no"

2) When is $\Gamma(G,A)$ an expander graph?

Meaning: $|AB| \geq (1+\delta)|B|$ for $\forall B \subset G$, $|B| \leq \frac{1}{2}|G|$

expander graph
small mixing time ⟸
small diameter ⟸

What are the finite, simple, non-abelian groups?

by the Classification thm of Finite Simple Groups

1. groups of Lie type (matrix groups)

2. $\mathrm{Alt}(n) < \mathrm{Sym}(n)$ permutation of n elements

3.  monsters (finitely many, so we ignore them)

Strongest results known:

for G classical (SL_n, SO_n, Sp_{2n}), group $G(\mathbb{F}_q)$

$+/-$

$q=p^\alpha$, p not too small

$$\mathrm{diam}(\Gamma(G,A)) \le c(\log|G|)^{400n^4}$$

(Bajpai-Dona-H., 202..)

For $G = \mathrm{Sym}(n)$

$$\mathrm{diam}\, G \le c(\log|G|)^{C\log^3 n \log\log n}$$

(H.-Seress, 2014)

also:
other results (H., H.-Gill, BGT, PS, BDH, ...) valid for arbitrary characteristic p

bounded rank
- other Lie groups over $\mathbb{F}_q$ (exceptional groups)
- more exotic companions (Steinberg groups, Suzuki...)

rank of $SL_n = n-1$, rank of $SO_{2n} = n$, rank of $SO_{2n+1} = n$, ...

Comparing SL_n (say) and $Sym(n)$

Some tools/approaches are valid for all groups:

e.g.

- Orbit-stabilizer theorem for sets
- growth in a subgroup $\Rightarrow$ growth in the group
- growth in # of orbits $\Rightarrow$ growth in the group

also, moral:

THINK IN TERMS OF ACTIONS $G \curvearrowright X$

Main difference:

the action of groups of Lie type such as $SL_n(\mathbb{F}_q)$ is geometrical, and linear:

$G \curvearrowright \mathbb{A}^n(\mathbb{F}_q)$: $\underset{\text{variety}}{V} \rightsquigarrow \underset{\text{variety (of the same degree)}}{gV}$.

- dimensional bounds

$$|A \cap V| \lesssim |A|^{\frac{\dim(V)}{\dim(G)}}$$

- escape from subvarieties

the actions of $Sym(n)$ on

- $\{1, \dots, n\}$
- pairs of distinct elements $\binom{[n]}{2}$

etc.

are actions $G \curvearrowright X$ on small sets X

diam(Schreier graph) $\leq |X|$ (trivially)

and so mixing time $\lesssim d|X|^2$ $\quad d$ = degree

$\rightsquigarrow$ mixing arguments (e.g., Babai splitting lemma for sets)

Parallels

Diameter bounds (over S_n, and in some sense same over $Sym(n)$) are based on

Growth of sets in groups ("key proposition") (H^2 2005-08 was already of this type)

Let G be a group of Lie type of bounded rank

$A \subset G$ generating G

Then either $|A^3| \geq |A|^{1+\delta}$ $\delta > 0$ fixed ← meaning: does not depend on: A or q

but it does depend on n

(or on rank G)

(it has to)

or A is large ($> |G|^{1-\epsilon}$) and $A^3 = G$.

Cor: $|A^{3^m}| \geq |A|^{(1+\delta)^m}$

Why does it have to?

Here is an example showing it is false in $Sym(n)$ with δ independent of n

It adapts readily to show the same for SL_n

Example (Pyber, Spiga, etc.) $A = \overbrace{\mathrm{Sym}(n)}^{H} \cup \overbrace{\{1,2,\dots,n\}}^{\sigma}$

Then $H\sigma H \subset \mathrm{Sym}(n+1)$ and so $|A^3| \ll_n |A|$

Hence δ in $|A^3| \geq |A|^{1+\delta}$ must satisfy $\delta \ll 1/n$, in general

Escape and its limitations

Recall the meaning of escape: $G \curvearrowright \mathbb{A}^n$ $A \subset G$

$V \subset \mathbb{A}^n$

$x \in V$ $\langle A \rangle x \not\subset V$

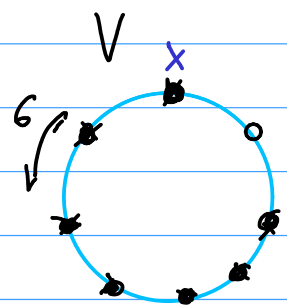
Then there is a k (depending only on $\deg(V)$, $\dim(V)$) s.t. $A^k x \not\subset V$

How large can k be forced to be?

In $\mathrm{Sym}(n)$: $A = \{\sigma\}$, $\sigma = (1\ 2 \cdots n)$ "$V=$" $\{1,\dots,n-1\}$

Then $x=1$ takes $k=n-1$ steps to escape

Can easily construct examples with $k=n-1$ based on this, not just in $\mathbb{A}^n$, but in $\mathbb{A}^2$:



At the same time: for A typical (random) $\{g_1, g_2\} \subset Sym(n)$, escape is much faster

Does this mean anything for SL_n?

OK, what about using these parallels for more than diagnosis?

· One possibility: BUILDINGS

connecting $SL_n(\mathbb{F}_q)$ with $Sym(n)$

spherical buildings: chambers = complete flags $0 < V_1 < V_2 < \cdots < V_{n-1} < \mathbb{A}^n(K)$

The distance $\delta(C_1, C_2)$ between two chambers C_1, C_2 is an element of $Sym(n)$

Promising! But: one value is generic, the others are special

Also: Buildings $\rightarrow$ Bruhat decomposition (partition of G into few cells)

Does this lead to mixing arguments? Unclear.

There may be a closer relation to energy

Worth exploring further.

And now for something (~~completely?~~ not so) different: $\mathbb{F}_{un}$

$\mathrm{Sym}(n)$ is said to equal SL_n over the field $\mathbb{F}_{un}$ with one element

(starts with some numerology by Tits in the 50s)

What does that mean?

one school: $\mathbb{F}_{un} = \mathbb{K}$, the Krasner hyperfield

(Connes-Consani 2011, Bowler, Jun, Baker-Lorscheid)

$\mathbb{K} = \{0,1\}$, $0+x = x$, $0 \cdot x = 0$, $1 \cdot x = x$, $1+1 = \{0,1\}$

Define varieties, and algebraic groups over $\mathbb{F}_{un}$

schemes

$\mathrm{Sym}(n)$ ~ closed points of $SL_n(\mathbb{K})$

What topology instead of Zariski topology?

Baker-Lorscheid:

- strong topology: defined like Zariski topology (by polynomials)
- weak topology

Closed subbasis of the weak topology:

for $x, y \in \{1, \dots, n\}$, closed parts of $V_{x,y} = \{g \in G : g(x) \neq y\}$ [sic!]

How does this work out?

(Dimensional estimates? imperfect) Some known arguments already used for $Sym(n)$ can be cast naturally in this language

Say $\operatorname{codim}(V) \geq \rho n^2$ (i.e. there are $\geq \rho n^2$ forbidden pairs (x,y))

Then, by mixing, the intersection of $C \log n$ random conjugates gVg^{-1} ($g \in A^k$, $k = O(n^3)$) is likely to be empty.

So: recover Babai's splitting lemma

but also: $\exists g \in A^k$ s.t. $|(A \cap V) g (A \cap V)^{-1} g^{-1}| \geq |A|^{1 + \frac{1}{C \log n}}$.

(lemma crucial in newer versions of HS-Seress)

with proof similar to that of dimensional estimates