Growth in permutation groups and linear algebraic groups

H. A. Helfgott

September 2018

Cayley graphs

Definition

$G = \langle S \rangle$ is a group. The (undirected) Cayley graph $\Gamma(G, S)$ has

- vertex set G and
- edge set $\{\{g, ga\} : g \in G, a \in S\}$.

Cayley graphs

Definition

$G = \langle S \rangle$ is a group. The (undirected) Cayley graph $\Gamma(G, S)$ has

- vertex set G and
- edge set $\{\{g, ga\} : g \in G, a \in S\}$.

Definition

The diameter of $\Gamma(G, S)$ is

$$\operatorname{diam} \Gamma(G, S) = \max_{g \in G} \min_{k} g = s_1 \cdots s_k, \ s_i \in S \cup S^{-1}.$$

(Same as graph theoretic diameter.)

How large can the diameter be?

The diameter can be very small:

$$\mathrm{diam}\,\Gamma(G, G) = 1$$

How large can the diameter be?

The diameter can be very small:

$$\mathrm{diam}\,\Gamma(G, G) = 1$$

The diameter also can be very big:

$G = \langle x \rangle \cong Z_n, \qquad \mathrm{diam}\,\Gamma(G, \{x\}) = \lfloor n/2 \rfloor$

More generally, G with a large abelian quotient may have Cayley graphs with diameter proportional to $|G|$.

How large can the diameter be?

The diameter can be very small:

$$\mathrm{diam}\,\Gamma(G, G) = 1$$

The diameter also can be very big:

$G = \langle x \rangle \cong Z_n, \qquad \mathrm{diam}\,\Gamma(G, \{x\}) = \lfloor n/2 \rfloor$

More generally, G with a large abelian quotient may have Cayley graphs with diameter proportional to $|G|$.

For generic G, however, diameters seem to be much smaller than $|G|$.

How large can the diameter be?

The diameter can be very small:

$$\operatorname{diam} \Gamma(G, G) = 1$$

The diameter also can be very big:

$G = \langle x \rangle \cong Z_n, \qquad \operatorname{diam} \Gamma(G, \{x\}) = \lfloor n/2 \rfloor$

More generally, G with a large abelian quotient may have Cayley graphs with diameter proportional to $|G|$.

For generic G, however, diameters seem to be much smaller than $|G|$. Example: for the group G of permutations of the Rubik cube and S the set of moves, $|G| = 43252003274489856000$, but $\operatorname{diam}(G, S) = 20$ (Davidson, Dethridge, Kociemba and Rokicki, 2010)

The diameter of groups

Definition

$$\operatorname{diam}(G) := \max_S \operatorname{diam} \Gamma(G, S)$$

The diameter of groups

Definition

$$\mathrm{diam}\,(G) := \max_{S} \mathrm{diam}\,\Gamma(G,S)$$

Conjecture (Babai, in [Babai,Seress 1992])

There exists a positive constant c: such that
G finite, simple, nonabelian $\Rightarrow \mathrm{diam}\,(G) = O(\log^c |G|)$.

The diameter of groups

Definition

$$\mathrm{diam}\,(G) := \max_S \mathrm{diam}\,\Gamma(G,S)$$

Conjecture (Babai, in [Babai,Seress 1992])

There exists a positive constant c: such that
G finite, simple, nonabelian $\Rightarrow \mathrm{diam}\,(G) = O(\log^c |G|)$.

Conjecture true for

- $\mathrm{PSL}(2,p)$, $\mathrm{PSL}(3,p)$ (Helfgott 2008, 2010)
- $\mathrm{PSL}(2,q)$ (Dinai; Varjú); work towards PSL_n, PSp_{2n} (Helfgott-Gill 2011)
- groups of Lie type of bounded rank (Pyber, E. Szabó 2011) and (Breuillard, Green, Tao 2011)

But what about permutation groups? Hardest: what about the alternating group A_n?

Alternating groups, Classification Theorem

Reminder: a permutation group is a group of permutations of n objects.

S_n = group of all permutations (S = “symmetric”)
A_n = unique subgroup of S_n of index 2 (A = “alternating”)

Alternating groups, Classification Theorem

Reminder: a permutation group is a group of permutations of n objects.

S_n = group of all permutations (S = "symmetric")
A_n = unique subgroup of S_n of index 2 (A = "alternating")

An asymptotic person's view of the Classification Theorem:

Alternating groups, Classification Theorem

Reminder: a permutation group is a group of permutations of n objects.

S_n = group of all permutations (S = “symmetric”)
A_n = unique subgroup of S_n of index 2 (A = “alternating”)

An asymptotic person’s view of the Classification Theorem: The finite simple groups are (a) finite groups of Lie type, (b) A_n, (c) a finite number of unpleasant things (“sporadic”).

Alternating groups, Classification Theorem

Reminder: a permutation group is a group of permutations of n objects.

S_n = group of all permutations (S = “symmetric”)
A_n = unique subgroup of S_n of index 2 (A = “alternating”)

An asymptotic person’s view of the Classification Theorem: The finite simple groups are (a) finite groups of Lie type, (b) A_n, (c) a finite number of unpleasant things (“sporadic”).

Alternating groups, Classification Theorem

Reminder: a permutation group is a group of permutations of n objects.

S_n = group of all permutations (S = “symmetric”)
A_n = unique subgroup of S_n of index 2 (A = “alternating”)

An asymptotic person’s view of the Classification Theorem: The finite simple groups are (a) finite groups of Lie type, (b) A_n, (c) a finite number of unpleasant things (“sporadic”).
Finite numbers of things do not matter asymptotically. We can thus focus on (a) and (b).

Diameter of the alternating group: results

Theorem (Helfgott, Seress 2011)

$$\mathrm{diam}\,(A_n) \leq \exp(O(\log^4 n \log\log n)).$$

Diameter of the alternating group: results

Theorem (Helfgott, Seress 2011)

$$\mathrm{diam}\,(A_n) \leq \exp(O(\log^4 n \log\log n)).$$

Corollary

$G \leq S_n$ *transitive* $\Rightarrow \mathrm{diam}\,(G) \leq \exp(O(\log^4 n \log\log n))$.

Diameter of the alternating group: results

Theorem (Helfgott, Seress 2011)

$$\mathrm{diam}\,(A_n) \leq \exp(O(\log^4 n \log\log n)).$$

Corollary

$G \leq S_n$ transitive $\Rightarrow \mathrm{diam}\,(G) \leq \exp(O(\log^4 n \log\log n))$.

The corollary follows from the main theorem and (Babai-Seress 1992), which uses the Classification. (As pointed out by Pyber, there is an error in (Babai-Seress 1992), but it has been fixed.)

Diameter of the alternating group: results

Theorem (Helfgott, Seress 2011)

$$\mathrm{diam}\,(A_n) \leq \exp(O(\log^4 n \log\log n)).$$

Corollary

$G \leq S_n$ *transitive* $\Rightarrow \mathrm{diam}\,(G) \leq \exp(O(\log^4 n \log\log n))$.

The corollary follows from the main theorem and (Babai-Seress 1992), which uses the Classification. (As pointed out by Pyber, there is an error in (Babai-Seress 1992), but it has been fixed.)

The Helfgott-Seress theorem also uses the Classification.

Product theorems

Since (Helfgott 2008), diameter results for groups of Lie type have been proven by product theorems:

Theorem

There exists a polynomial $c(x)$ such that if G is simple, Lie-type of rank r, $G = \langle A \rangle$ then $A^3 = G$ or

$$|A^3| \geq |A|^{1+1/c(r)}.$$

In particular, for bounded r, we have $|A^3| \geq |A|^{1+\varepsilon}$ for some constant ε.

Product theorems

Since (Helfgott 2008), diameter results for groups of Lie type have been proven by product theorems:

Theorem

There exists a polynomial $c(x)$ such that if G is simple, Lie-type of rank r, $G = \langle A \rangle$ then $A^3 = G$ or

$$|A^3| \geq |A|^{1+1/c(r)}.$$

In particular, for bounded r, we have $|A^3| \geq |A|^{1+\varepsilon}$ for some constant ε.

Given $G = \langle S \rangle$, $O(\log \log |G|)$ applications of the theorem gives all elements of G.
Tripling the length $O(\log \log |G|)$ times gives diameter $3^{O(\log \log |G|)} = (\log |G|)^c$.

(Pyber, Spiga) Product theorems are false in A_n.

Example

$G = A_n$, $H \cong A_m \leq G$, $g = (1, 2, \ldots, n)$ (n odd).
$S = H \cup \{g\}$ generates G, $|S^3| \leq 9(m+1)(m+2)|S|$.

Related phenomenon: for G of Lie type, rank unbounded, we cannot remove the dependence of the exponent $1/c(r)$ on the rank r.

(Pyber, Spiga) Product theorems are false in A_n.

Example

$G = A_n$, $H \cong A_m \leq G$, $g = (1, 2, \ldots, n)$ (n odd).
$S = H \cup \{g\}$ generates G, $|S^3| \leq 9(m+1)(m+2)|S|$.

Related phenomenon: for G of Lie type, rank unbounded, we cannot remove the dependence of the exponent $1/c(r)$ on the rank r.

Powerful techniques, developed for Lie-type groups, are not directly applicable:

- dimensional estimates (Helfgott 2008, 2010; generalized by Pyber, Szabo, 2011; prefigured in Larsen-Pink, as remarked by Breuillard-Green-Tao, 2011)
- escape from subvarieties (cf. Eskin-Mozes-Oh, 2005)

Aims

Product theorems are useful, and not just because they imply diameter bounds. They directly imply bounds on spectral gaps, mixing times, etc.

Aims

Product theorems are useful, and not just because they imply diameter bounds. They directly imply bounds on spectral gaps, mixing times, etc.

Our aims are:

1. a simpler, more natural proof of Helfgott-Seress,
2. a weak product theorem for A_n,
3. a better exponent than 4 in $\exp((\log n)^4 \log\log n)$,
4. removing the dependence on the Classification Theorem.

Aims

Product theorems are useful, and not just because they imply diameter bounds. They directly imply bounds on spectral gaps, mixing times, etc.

Our aims are:

1. a simpler, more natural proof of Helfgott-Seress,
2. a weak product theorem for A_n,
3. a better exponent than 4 in $\exp((\log n)^4 \log\log n)$,
4. removing the dependence on the Classification Theorem.

Here we fulfill aims (1) and (2).

Aims

Product theorems are useful, and not just because they imply diameter bounds. They directly imply bounds on spectral gaps, mixing times, etc.

Our aims are:

1. a simpler, more natural proof of Helfgott-Seress,
2. a weak product theorem for A_n,
3. a better exponent than 4 in $\exp((\log n)^4 \log\log n)$,
4. removing the dependence on the Classification Theorem.

Here we fulfill aims (1) and (2). L. Pyber is working on (4).

A weak product theorem for A_n (or S_n)

Theorem (Helfgott 2018)

There are $C, c > 0$ *such that the following holds. Let* $A \subset S_n$ *be such that* $A = A^{-1}$ *and* A *generates* A_n *or* S_n*. Assume* $|A| \geq n^{C(\log n)^2}$*. Then either*

$$|A^{n^C}| \geq |A|^{1+c\frac{\log \frac{\log |A|}{\log n}}{(\log n)^2 \log\log n}}$$

or

$$\mathrm{diam}\,(\Gamma(\langle A\rangle, A)) \leq n^C \max_{\substack{A' \subset G\\ G = \langle A'\rangle}} \mathrm{diam}\,(\Gamma(G, A')),$$

where G *is a transitive group on* $m \leq n$ *elements with no alternating factors of degree* $> 0.9n$*.*

A weak product theorem for A_n (or S_n)

Theorem (Helfgott 2018)

There are $C, c > 0$ such that the following holds. Let $A \subset S_n$ be such that $A = A^{-1}$ and A generates A_n or S_n. Assume $|A| \geq n^{C(\log n)^2}$. Then either

$$|A^{n^C}| \geq |A|^{1+c\frac{\log\frac{\log|A|}{\log n}}{(\log n)^2\log\log n}}$$

or

$$\operatorname{diam}(\Gamma(\langle A\rangle, A)) \leq n^C \max_{\substack{A' \subset G\\ G=\langle A'\rangle}} \operatorname{diam}(\Gamma(G, A')),$$

where G is a transitive group on $m \leq n$ elements with no alternating factors of degree $> 0.9n$.

Immediate corollary (via Babai-Seress): Helfgott-Seress bound on the diameter of $G = A_n$ (or $G = S_n$), or rather $\operatorname{diam} G \ll \exp(O(\log^4 n(\log\log n)^2))$.

Dimensional estimates and their analogues, I

The following is an example of a dimensional estimate.

Lemma

Let $G = \mathrm{SL}_2(K)$, K finite. Let $A \subset G$ generate G; assume $A = A^{-1}$. Let V be a one-dimensional subvariety of SL_2. Then either $|A^3| \geq |A|^{1+\delta}$ or

$$|A \cap V(K)| \leq |A|^{\frac{\dim V}{\dim \mathrm{SL}_2} + O(\delta)} = |A|^{1/3+O(\delta)}.$$

Dimensional estimates and their analogues, I

The following is an example of a dimensional estimate.

Lemma

Let $G = \mathrm{SL}_2(K)$, K finite. Let $A \subset G$ generate G; assume $A = A^{-1}$. Let V be a one-dimensional subvariety of SL_2. Then either $|A^3| \geq |A|^{1+\delta}$ or

$$|A \cap V(K)| \leq |A|^{\frac{\dim V}{\dim \mathrm{SL}_2} + O(\delta)} = |A|^{1/3+O(\delta)}.$$

A more abstract statement:

Lemma

Let G be a group. Let $R, B \subset G$, $R = R^{-1}$. Let $k = |B|$. Then

$$\left| \left(\cup_{g \in B} g R g^{-1} \right)^2 \right| \geq \frac{|R|^{1+\frac{1}{k}}}{\left| \cap_{g \in B \cup \{e\}} g R^{-1} R g^{-1} \right|}.$$

Dimensional estimates and their analogues, I

The following is an example of a dimensional estimate.

Lemma

Let $G = \mathrm{SL}_2(K)$, K finite. Let $A \subset G$ generate G; assume $A = A^{-1}$. Let V be a one-dimensional subvariety of SL_2. Then either $|A^3| \geq |A|^{1+\delta}$ or

$$|A \cap V(K)| \leq |A|^{\frac{\dim V}{\dim \mathrm{SL}_2} + O(\delta)} = |A|^{1/3+O(\delta)}.$$

A more abstract statement:

Lemma

Let G be a group. Let $R, B \subset G$, $R = R^{-1}$. Let $k = |B|$. Then

$$\left| \left(\cup_{g \in B} g R g^{-1} \right)^2 \right| \geq \frac{|R|^{1+\frac{1}{k}}}{\left| \cap_{g \in B \cup \{e\}} g R^{-1} R g^{-1} \right|}.$$

If R is special, try to make the denominator trivial.

Dimensional estimates and their analogues, II

In linear groups, “special” just means “on a subvariety”.

Dimensional estimates and their analogues, II

In linear groups, “special” just means “on a subvariety”.

What could it mean in a permutation group?

Dimensional estimates and their analogues, II

In linear groups, “special” just means “on a subvariety”. What could it mean in a permutation group?

Lemma (Special-set lemma)

Let G be a permutation group. Let $R, B \subset G$, $R = R^{-1}$, $B = B^{-1}$, $\langle B \rangle$ 2-transitive. If R^2 has no orbits of length $> \rho n$, $0 < \rho < 1$, then

$$\left| \left(\cup_{g \in B^r} g R g^{-1} \right)^2 \right| \geq |R|^{1 + \frac{c_\rho}{\log n}},$$

where $r = O(n^6)$ and $c_\rho > 0$ depends only on ρ.

Dimensional estimates and their analogues, II

In linear groups, “special” just means “on a subvariety”. What could it mean in a permutation group?

Lemma (Special-set lemma)

Let G be a permutation group. Let $R, B \subset G$, $R = R^{-1}$, $B = B^{-1}$, $\langle B\rangle$ 2-transitive. If R^2 has no orbits of length $> \rho n$, $0 < \rho < 1$, then

$$\left|\left(\cup_{g\in B^r} gRg^{-1}\right)^2\right| \geq |R|^{1+\frac{c_\rho}{\log n}},$$

where $r = O(n^6)$ and $c_\rho > 0$ depends only on ρ.

This can again be put in the form: for $R = A \cap$ special, either A grows (since $(\cup_{g\in A^r} gRg^{-1})^2 \subset A^{2r+4}$), or R is small compared to A.

Dimensional estimates and their analogues, II

In linear groups, "special" just means "on a subvariety". What could it mean in a permutation group?

Lemma (Special-set lemma)

Let G be a permutation group. Let $R, B \subset G$, $R = R^{-1}$, $B = B^{-1}$, $\langle B \rangle$ 2-transitive. If R^2 has no orbits of length $> \rho n$, $0 < \rho < 1$, then

$$\left| \left(\cup_{g \in B^r} g R g^{-1} \right)^2 \right| \geq |R|^{1 + \frac{c_\rho}{\log n}},$$

where $r = O(n^6)$ and $c_\rho > 0$ depends only on ρ.

This can again be put in the form: for $R = A \cap$ special, either A grows (since $(\cup_{g \in A^r} g R g^{-1})^2 \subset A^{2r+4}$), or R is small compared to A. Idea of proof: produce a small subset D of B^r by random walks of length r. Then $\cap_{g \in D} g R^2 g^{-1}$ is probably trivial (much as in: Babai's CFSG-free bound on the size of doubly transitive groups).

Building a prefix, I

Use basic data structures for computations with permutation groups (Sims, 1970)
Given G, write $G_{(\alpha_1,\ldots,\alpha_k)}$ for the group

$$\{g \in G : g(\alpha_i) = \alpha_i \quad \forall 1 \leq i \leq k\}$$

(the pointwise stabilizer).

Building a prefix, I

Use basic data structures for computations with permutation groups (Sims, 1970)
Given G, write $G_{(\alpha_1,\dots,\alpha_k)}$ for the group

$$\{g \in G : g(\alpha_i) = \alpha_i \quad \forall 1 \leq i \leq k\}$$

(the pointwise stabilizer).

Definition

A base for $G \leq \mathrm{Sym}(\Omega)$ is a sequence of points $(\alpha_1, \dots, \alpha_k)$ such that $G_{(\alpha_1,\dots,\alpha_k)} = 1$.
A base defines a point stabilizer chain

$$G^{[1]} \geq G^{[2]} \geq G^{[3]} \dots \geq$$

with $G^{[i]} = G_{(\alpha_1,\dots,\alpha_{i-1})}$.

Building a prefix, II

Choose $\alpha_1, \dots, \alpha_j$ greedily so that, at each step, the orbit

$$\left|\alpha_i^{(A^{-1}A)_{(\alpha_1,\dots,\alpha_{i-1})}}\right|$$

is maximal.

Building a prefix, II

Choose $\alpha_1, \ldots, \alpha_j$ greedily so that, at each step, the orbit

$$\left|\alpha_i^{(A^{-1}A)_{(\alpha_1,\ldots,\alpha_{i-1})}}\right|$$

is maximal. Stop when it is of size $< \rho n$.

Building a prefix, II

Choose $\alpha_1, \ldots, \alpha_j$ greedily so that, at each step, the orbit

$$\left|\alpha_i^{(A^{-1}A)_{(\alpha_1,\ldots,\alpha_{i-1})}}\right|$$

is maximal. Stop when it is of size $< \rho n$.

By the special set lemma, $(A^{-1}A)_{(\alpha_1,\ldots,\alpha_j)}$ must be smallish (or else A grows).

Building a prefix, II

Choose $\alpha_1, \dots, \alpha_j$ greedily so that, at each step, the orbit

$$\left|\alpha_i^{(A^{-1}A)_{(\alpha_1,\dots,\alpha_{i-1})}}\right|$$

is maximal. Stop when it is of size $< \rho n$.

By the special set lemma, $(A^{-1}A)_{(\alpha_1,\dots,\alpha_j)}$ must be smallish (or else A grows). This implies $j \gg (\log |A|)/(\log n)^2$.

Building a prefix, II

Choose $\alpha_1, \ldots, \alpha_j$ greedily so that, at each step, the orbit

$$\left|\alpha_i^{(A^{-1}A)_{(\alpha_1,\ldots,\alpha_{i-1})}}\right|$$

is maximal. Stop when it is of size $< \rho n$.

By the special set lemma, $(A^{-1}A)_{(\alpha_1,\ldots,\alpha_j)}$ must be smallish (or else A grows). This implies $j \gg (\log |A|)/(\log n)^2$.

Let $\Sigma = \{\alpha_1, \ldots \alpha_{j-1}\}$. Because the orbits in all but the last link in the chain are long, the setwise stabilizer $(A^{2n})_\Sigma$, projected to S_Σ, is large, and generates A_Δ or S_Δ for $\Delta \subset \Sigma$ large.

Building a prefix, II

Choose $\alpha_1, \ldots, \alpha_j$ greedily so that, at each step, the orbit

$$\left|\alpha_i^{(A^{-1}A)_{(\alpha_1,\ldots,\alpha_{i-1})}}\right|$$

is maximal. Stop when it is of size $< \rho n$.

By the special set lemma, $(A^{-1}A)_{(\alpha_1,\ldots,\alpha_j)}$ must be smallish (or else A grows). This implies $j \gg (\log|A|)/(\log n)^2$.

Let $\Sigma = \{\alpha_1, \ldots \alpha_{j-1}\}$. Because the orbits in all but the last link in the chain are long, the setwise stabilizer $(A^{2n})_\Sigma$, projected to S_Σ, is large, and generates A_Δ or S_Δ for $\Delta \subset \Sigma$ large. We call this the *prefix*.

Building a prefix, II

Choose $\alpha_1, \dots, \alpha_j$ greedily so that, at each step, the orbit

$$\left| \alpha_i^{(A^{-1}A)_{(\alpha_1, \dots, \alpha_{i-1})}} \right|$$

is maximal. Stop when it is of size $< \rho n$.

By the special set lemma, $(A^{-1}A)_{(\alpha_1, \dots, \alpha_j)}$ must be smallish (or else A grows). This implies $j \gg (\log |A|)/(\log n)^2$.

Let $\Sigma = \{\alpha_1, \dots \alpha_{j-1}\}$. Because the orbits in all but the last link in the chain are long, the setwise stabilizer $(A^{2n})_\Sigma$, projected to S_Σ, is large, and generates A_Δ or S_Δ for $\Delta \subset \Sigma$ large. We call this the *prefix*.

The pointwise stabilizer $(A^{2n})_{(\Sigma')}$ restricted to the complement of $\Sigma' = \Sigma \cup \{\alpha_j\}$ is the *suffix*.

Building a prefix, II

Choose $\alpha_1, \dots, \alpha_j$ greedily so that, at each step, the orbit

$$\left|\alpha_i^{(A^{-1}A)_{(\alpha_1,\dots,\alpha_{i-1})}}\right|$$

is maximal. Stop when it is of size $< \rho n$.

By the special set lemma, $(A^{-1}A)_{(\alpha_1,\dots,\alpha_j)}$ must be smallish (or else A grows). This implies $j \gg (\log |A|)/(\log n)^2$.

Let $\Sigma = \{\alpha_1, \dots \alpha_{j-1}\}$. Because the orbits in all but the last link in the chain are long, the setwise stabilizer $(A^{2n})_\Sigma$, projected to S_Σ, is large, and generates A_Δ or S_Δ for $\Delta \subset \Sigma$ large. We call this the *prefix*.

The pointwise stabilizer $(A^{2n})_{(\Sigma')}$ restricted to the complement of $\Sigma' = \Sigma \cup \{\alpha_j\}$ is the *suffix*.

The setwise stabilizer $(A^{2n})_{\Sigma'}$ acts on the suffix by conjugation.

Induction (warning for vegans: Babai-Seress uses Classification)

The suffix has no orbits of size $\geq \rho n$.

What about the group H generated by the setwise stabilizer $(A^{2n})_\Sigma$?

Induction (warning for vegans: Babai-Seress uses Classification)

The suffix has no orbits of size $\geq \rho n$.

What about the group H generated by the setwise stabilizer $(A^{2n})_\Sigma$? If it has no orbits of size $\geq 0.9n$, then its diameter is not much larger than that of $A_{\lfloor 0.9n \rfloor}$, by (Babai-Seress 1992). This is relatively small, by induction.

Induction (warning for vegans: Babai-Seress uses Classification)

The suffix has no orbits of size $\geq \rho n$.

What about the group H generated by the setwise stabilizer $(A^{2n})_\Sigma$? If it has no orbits of size $\geq 0.9n$, then its diameter is not much larger than that of $A_{\lfloor 0.9n \rfloor}$, by (Babai-Seress 1992). This is relatively small, by induction.

The prefix, a projection of the setwise stabilizer, contains a copy of A_Δ or S_Δ, Δ not tiny. By Wielandt, this means that H contains an element $g \neq e$ of small support.

Induction (warning for vegans: Babai-Seress uses Classification)

The suffix has no orbits of size $\geq \rho n$.

What about the group H generated by the setwise stabilizer $(A^{2n})_\Sigma$? If it has no orbits of size $\geq 0.9n$, then its diameter is not much larger than that of $A_{\lfloor 0.9n \rfloor}$, by (Babai-Seress 1992). This is relatively small, by induction.

The prefix, a projection of the setwise stabilizer, contains a copy of A_Δ or S_Δ, Δ not tiny. By Wielandt, this means that H contains an element $g \neq e$ of small support. By (Babai-Beals-Seress 2004), this means that $\mathrm{diam}\,(A_n, A \cup \{g\})$ is $\ll n^{O(1)}$. Since g lies in a subgroup of relatively small diameter, we are done.

Induction (warning for vegans: Babai-Seress uses Classification)

The suffix has no orbits of size $\geq \rho n$.

What about the group H generated by the setwise stabilizer $(A^{2n})_\Sigma$? If it has no orbits of size $\geq 0.9n$, then its diameter is not much larger than that of $A_{\lfloor 0.9n \rfloor}$, by (Babai-Seress 1992). This is relatively small, by induction.

The prefix, a projection of the setwise stabilizer, contains a copy of A_Δ or S_Δ, Δ not tiny. By Wielandt, this means that H contains an element $g \neq e$ of small support. By (Babai-Beals-Seress 2004), this means that $\mathrm{diam}\,(A_n, A \cup \{g\})$ is $\ll n^{O(1)}$. Since g lies in a subgroup of relatively small diameter, we are done.

So, H has a long orbit, and in fact acts like A_m or S_m on it ($m \geq 0.9n$).

Use of special lemma, action

Set $\rho = 0.8$. Since H acts like A_m or S_m, $m \geq 0.9n$, and the suffix S has no orbits of size $\geq 0.8n$, we can use the special-set lemma.

Use of special lemma, action

Set $\rho = 0.8$. Since H acts like A_m or S_m, $m \geq 0.9n$, and the suffix S has no orbits of size $\geq 0.8n$, we can use the special-set lemma. This shows that $|S^{n^{O(1)}}| \geq |S|^{1+1/\log n}$.

Use of special lemma, action

Set $\rho = 0.8$. Since H acts like A_m or S_m, $m \geq 0.9n$, and the suffix S has no orbits of size $\geq 0.8n$, we can use the special-set lemma. This shows that $|S^{n^{O(1)}}| \geq |S|^{1+1/\log n}$.

This ensures that $|A^{n^{O(1)}}| \geq |A||S|^{1/\log n}$. But how large is S?

Use of special lemma, action

Set $\rho = 0.8$. Since H acts like A_m or S_m, $m \geq 0.9n$, and the suffix S has no orbits of size $\geq 0.8n$, we can use the special-set lemma. This shows that $|S^{n^{O(1)}}| \geq |S|^{1+1/\log n}$.

This ensures that $|A^{n^{O(1)}}| \geq |A||S|^{1/\log n}$. But how large is S?

We can find $\ll \log\log n$ elements in $A^{n^{O(1)}}$ of the pointwise stabilizer of Σ generating a group with a large orbit.

Use of special lemma, action

Set $\rho = 0.8$. Since H acts like A_m or S_m, $m \geq 0.9n$, and the suffix S has no orbits of size $\geq 0.8n$, we can use the special-set lemma. This shows that $|S^{n^{O(1)}}| \geq |S|^{1+1/\log n}$.

This ensures that $|A^{n^{O(1)}}| \geq |A||S|^{1/\log n}$. But how large is S?

We can find $\ll \log \log n$ elements in $A^{n^{O(1)}}$ of the pointwise stabilizer of Σ generating a group with a large orbit. This means that no element of the prefix can act trivially on them all. This guarantees that $|S| \gg |\text{prefix}|^{\delta/\log \log n}$.

Use of special lemma, action

Set $\rho = 0.8$. Since H acts like A_m or S_m, $m \geq 0.9n$, and the suffix S has no orbits of size $\geq 0.8n$, we can use the special-set lemma. This shows that $|S^{n^{O(1)}}| \geq |S|^{1+1/\log n}$.

This ensures that $|A^{n^{O(1)}}| \geq |A||S|^{1/\log n}$. But how large is S?

We can find $\ll \log \log n$ elements in $A^{n^{O(1)}}$ of the pointwise stabilizer of Σ generating a group with a large orbit. This means that no element of the prefix can act trivially on them all. This guarantees that $|S| \gg |\text{prefix}|^{\delta/\log\log n}$.

We obtain growth.

Summary of proof techniques

Subset analogues of statements in group theory, in particular:

- Orbit-stabilizer for sets; lifting and reduction statements for approximate subgroups (following Helfgott, 2010); basic object: action $G \to X$, $A \subset G$.
- Subset versions of results by Bochert, Liebeck about large subgroups of A_n.

Summary of proof techniques

Subset analogues of statements in group theory, in particular:

- Orbit-stabilizer for sets; lifting and reduction statements for approximate subgroups (following Helfgott, 2010); basic object: action $G \to X$, $A \subset G$.
- Subset versions of results by Bochert, Liebeck about large subgroups of A_n.

Random-walk analogues of the probabilistic method in combinatorics: uniform probability distribution (can't do) replaced by outcomes of short random walks (can do). Thus: subset versions of results by Babai (splitting lemma), Pyber about 2-transitive groups.

Summary of proof techniques

Subset analogues of statements in group theory, in particular:

- Orbit-stabilizer for sets; lifting and reduction statements for approximate subgroups (following Helfgott, 2010); basic object: action $G \to X$, $A \subset G$.
- Subset versions of results by Bochert, Liebeck about large subgroups of A_n.

Random-walk analogues of the probabilistic method in combinatorics: uniform probability distribution (can't do) replaced by outcomes of short random walks (can do). Thus: subset versions of results by Babai (splitting lemma), Pyber about 2-transitive groups.

Previous results on $\mathrm{diam}\,(A_n)$: (BS1992), (BBS 2004).

Moral

Moral

Worth studying for every group:
action by multiplication $G \to G/H$
($\Rightarrow$ lifting and reduction lemmas);
action by conjugation $G \to G$
($\Rightarrow$ conjugates and centralizers (tori)).

Moral

Worth studying for every group:
action by multiplication $G \to G/H$
($\Rightarrow$ lifting and reduction lemmas);
action by conjugation $G \to G$
($\Rightarrow$ conjugates and centralizers (tori)).

Also, for linear algebraic groups:
natural geometric actions $\mathrm{PSL}_n \to \mathbb{P}^n$
($\to$ dimensional analysis, escape from subvarieties)

Moral

Worth studying for every group:
action by multiplication $G \to G/H$
($\Rightarrow$ lifting and reduction lemmas);
action by conjugation $G \to G$
($\Rightarrow$ conjugates and centralizers (tori)).

Also, for linear algebraic groups:
natural geometric actions $\mathrm{PSL}_n \to \mathbb{P}^n$
($\to$ dimensional analysis, escape from subvarieties)

Also, for permutation groups:
natural actions by permutation $A_n \to \{1, 2, \ldots, n\}^k$
($\to$ stabilizer chains, random walks, effective splitting lemmas)