The diameter of permutation groups

H. A. Helfgott and Á. Seress

July 2013

Cayley graphs

Definition

$G = \langle S \rangle$ is a group. The Cayley graph $\Gamma(G, S)$ has vertex set G with g, h connected if and only if $gs = h$ or $hs = g$ for some $s \in S$.

By definition, $\Gamma(G, S)$ is undirected.

Cayley graphs

Definition

$G = \langle S \rangle$ is a group. The Cayley graph $\Gamma(G, S)$ has vertex set G with g, h connected if and only if $gs = h$ or $hs = g$ for some $s \in S$.

By definition, $\Gamma(G, S)$ is undirected.

Definition

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

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

(Same as graph theoretic diameter.)

How large can the diameter be?

The diameter can be very small:

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

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 large abelian factor group may have Cayley graphs with diameter proportional to $|G|$. An easy argument shows that $\operatorname{diam} \Gamma(G, S) \geq \log_{2|S|} |G|$.

Rubik's cube

$$S = \{(1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19), (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35), (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11), (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24), (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27), (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)\}$$

$Rubik := \langle S \rangle$, $|Rubik| = 43252003274489856000.$

Rubik's cube

$$S = \{(1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19), (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35), (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11), (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24), (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27), (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)\}$$

$Rubik := \langle S \rangle$, $|Rubik| = 43252003274489856000.$

$20 \leq \mathrm{diam}\, \Gamma(Rubik, S) \leq 29$ (Rokicki 2009)

Rubik's cube

$$S = \{(1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19), (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35), (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11), (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24), (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27), (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)\}$$

$Rubik := \langle S \rangle$, $|Rubik| = 43252003274489856000.$

$20 \leq \mathrm{diam}\, \Gamma(Rubik, S) \leq 29$ (Rokicki 2009)
$\mathrm{diam}\, \Gamma(Rubik, S \cup \{s^2 \mid s \in S\}) = 20$ (Rokicki 2009)

The diameter of groups

Definition

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

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 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 simple, nonabelian $\Rightarrow \mathrm{diam}\,(G) = O(\log^c |G|)$.

Conjecture true for

- $\mathrm{PSL}(2, p)$, $\mathrm{PSL}(3, p)$ (Helfgott 2008, 2010)

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 simple, nonabelian $\Rightarrow \mathrm{diam}\,(G) = O(\log^c |G|)$.

Conjecture true for

- $\mathrm{PSL}(2, p)$, $\mathrm{PSL}(3, p)$ (Helfgott 2008, 2010) and, after some further generalizations by Dinai, Gill-Helfgott,...

The diameter of groups

Definition

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

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

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

Conjecture true for

- $\mathrm{PSL}(2, p)$, $\mathrm{PSL}(3, p)$ (Helfgott 2008, 2010) and, after some further generalizations by Dinai, Gill-Helfgott,...
- Lie-type groups of bounded rank (Pyber, E. Szabó 2011) and (Breuillard, Green, Tao 2011)

What about alternating groups?

Alternating groups: why are they a difficult case?

Attempt # 1: Techniques for Lie-type groups

Diameter results for Lie-type groups are 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.

Alternating groups: why are they a difficult case?

Attempt # 1: Techniques for Lie-type groups

Diameter results for Lie-type groups are 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 give all elements of G.

Tripling length $O(\log \log |G|)$ times gives diameter $3^{O(\log \log |G|)} = (\log |G|)^c$.

Product theorems are false in Alt_n.

Example

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

For example, if $m \approx \sqrt{n}$ then growth is too small.

Product theorems are false in Alt_n.

Example

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

For example, if $m \approx \sqrt{n}$ then growth is too small.

Moreover: many of the techniques developed for Lie-type groups are not applicable. No varieties in Alt_n or Sym_n, hence no “escape from subvarieties” or dimensional estimates.

Product theorems are false in Alt_n.

Example

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

For example, if $m \approx \sqrt{n}$ then growth is too small.

Moreover: many of the techniques developed for Lie-type groups are not applicable. No varieties in Alt_n or Sym_n, hence no "escape from subvarieties" or dimensional estimates.

Escape: guarantee that you can leave an exceptional set (a variety V of codimension > 0.
Dimensional estimates = estimates of type
$|A^k \cap V| \sim |A|^{\frac{\dim(V)}{\dim(G)}}$.

Attempt # 2: construction of a 3-cycle

Any $g \in \mathrm{Alt}_n$ is the product of at most $(n/2)$ 3-cycles:

$(1, 2, 3, 4, 5, 6, 7) = (1, 2, 3)(1, 4, 5)(1, 6, 7)$

$(1, 2, 3, 4, 5, 6) = (1, 2, 3)(1, 4, 5)(1, 6)$

$(1, 2)(3, 4) = (1, 2, 3)(3, 1, 4)$

Attempt # 2: construction of a 3-cycle

Any $g \in \mathrm{Alt}_n$ is the product of at most $(n/2)$ 3-cycles:

$(1,2,3,4,5,6,7) = (1,2,3)(1,4,5)(1,6,7)$

$(1,2,3,4,5,6) = (1,2,3)(1,4,5)(1,6)$

$(1,2)(3,4) = (1,2,3)(3,1,4)$

It is enough to construct one 3-cycle (then conjugate to all others).
Construction in stages, cutting down to smaller and smaller support.

Support of $g \in \mathrm{Sym}(\Omega)$: $\mathrm{supp}(g) = \{\alpha \in \Omega \mid \alpha^g \neq \alpha\}$.

One generator has small support

Theorem (Babai, Beals, Seress 2004)

$G = \langle S \rangle \cong \mathrm{Alt}_n$ and $|\mathrm{supp}(a)| < (\frac{1}{3} - \varepsilon)n$ for some $a \in S$. Then $\mathrm{diam}\,\Gamma(G, S) = O(n^{7+o(1)})$.

Recent improvement:

Theorem (Bamberg, Gill, Hayes, Helfgott, Seress, Spiga 2012)

$G = \langle S \rangle \cong \mathrm{Alt}_n$ and $|\mathrm{supp}(a)| < 0.63n$ for some $a \in S$. Then $\mathrm{diam}\,\Gamma(G, S) = O(n^c)$.

One generator has small support

Theorem (Babai, Beals, Seress 2004)

$G = \langle S \rangle \cong \mathrm{Alt}_n$ and $|\mathrm{supp}(a)| < (\frac{1}{3} - \varepsilon)n$ for some $a \in S$. Then $\mathrm{diam}\, \Gamma(G, S) = O(n^{7+o(1)})$.

Recent improvement:

Theorem (Bamberg, Gill, Hayes, Helfgott, Seress, Spiga 2012)

$G = \langle S \rangle \cong \mathrm{Alt}_n$ and $|\mathrm{supp}(a)| < 0.63n$ for some $a \in S$. Then $\mathrm{diam}\, \Gamma(G, S) = O(n^c)$. The proof gives $c = 78$ (with some further work, $c = 66 + o(1)$).

How to construct one element with moderate support?

Up to recently, only one result with no conditions on the generating set.

Theorem (Babai, Seress 1988)

Given $\mathrm{Alt}_n = \langle S \rangle$, *there exists a word of length* $\exp(\sqrt{n \log n}(1 + o(1)))$ *on* S, *defining* $h \in \mathrm{Alt}_n$ *with* $|\mathrm{supp}(h)| \leq n/4$. *As a consequence,*

$$\mathrm{diam}\,(\mathrm{Alt}_n) \leq \exp(\sqrt{n \log n}(1 + o(1))).$$

A quasipolynomial bound

Theorem (Helfgott, Seress 2011)

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

A quasipolynomial bound

Theorem (Helfgott, Seress 2011)

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

(Babai's conjecture states in this case that $\mathrm{diam}\,(\mathrm{Alt}_n) \leq n^{O(1)} = \exp(O(\log n))$.)

A quasipolynomial bound

Theorem (Helfgott, Seress 2011)

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

(Babai's conjecture states in this case that $\mathrm{diam}\,(\mathrm{Alt}_n) \leq n^{O(1)} = \exp(O(\log n))$.)

Corollary

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

A quasipolynomial bound

Theorem (Helfgott, Seress 2011)

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

(Babai's conjecture states in this case that $\mathrm{diam}\,(\mathrm{Alt}_n) \leq n^{O(1)} = \exp(O(\log n))$.)

Corollary

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

The corollary follows with help from

Theorem (Babai, Seress 1992)

$G \leq \mathrm{Sym}_n$ *transitive*
$\Rightarrow \mathrm{diam}\,(G) \leq \exp(O(\log^3 n)) \cdot \mathrm{diam}\,(A_k)$ *where A_k is the largest alternating composition factor of G.*

The main idea of (Babai, Seress 1988)

Given $\mathrm{Alt}(\Omega) \cong \mathrm{Alt}_n = \langle S \rangle$, construct $h \in \mathrm{Alt}_n$ with $|\mathrm{supp}(h)| \leq n/4$ as a short word on S.

The main idea of (Babai, Seress 1988)

Given $\mathrm{Alt}(\Omega) \cong \mathrm{Alt}_n = \langle S \rangle$, construct $h \in \mathrm{Alt}_n$ with $|\mathrm{supp}(h)| \leq n/4$ as a short word on S.

$p_1 = 2, p_2 = 3, \ldots, p_k$ primes: $\prod_{i=1}^k p_i > n^4$

Construct $g \in G$ containing cycles of length $p_1, p_1, p_2, \ldots, p_k$. (In general: can always construct (as a word of length $\leq n^r$) a g containing a given pattern of length r.)

For $\alpha \in \Omega$, let ℓ_α :=length of g-cycle containing α.

For $1 \leq i \leq k$, let $\Omega_i := \{\alpha \in \Omega : p_i \mid \ell_\alpha\}$.

Claim

There exists $i \leq k$ with $|\Omega_i| \leq n/4$.

Prove claim by double-counting.
After claim is proven: take $h := g^{\mathrm{order}(g)/p_i}$. Then $\mathrm{supp}(h) \subseteq \Omega_i$ and so $|\mathrm{supp}(h)| \leq n/4$. Landau:

$$\mathrm{order}(g) = e^{\sqrt{n \log n}(1+o(1))}.$$

Ideas of (Helfgott, Seress 2011): from subgroups to subsets

In common with groups of Lie type:

Some group-theoretical statements are robust – they work for all sets rather than just for subgroups.

Important basic example: orbit-stabilizer theorem for sets.

Ideas of (Helfgott, Seress 2011): from subgroups to subsets

In common with groups of Lie type:

Some group-theoretical statements are robust – they work for all sets rather than just for subgroups.
Important basic example: orbit-stabilizer theorem for sets.

Lemma (Orbit-stabilizer, generalized to sets)

Let G be a group acing on a set X. Let $x \in X$, and let $A \subset G$ be non-empty. Then

$$|(A^{-1}A) \cap Stab(x)| \geq \frac{|A|}{|Ax|}.$$

Moreover,

$$|A \cap Stab(x)| \leq \frac{|AA|}{|Ax|}.$$

Ideas of (Helfgott, Seress 2011): from subgroups to subsets

In common with groups of Lie type:

Some group-theoretical statements are robust – they work for all sets rather than just for subgroups.
Important basic example: orbit-stabilizer theorem for sets.

Lemma (Orbit-stabilizer, generalized to sets)

Let G be a group acing on a set X. Let $x \in X$, and let $A \subset G$ be non-empty. Then

$$|(A^{-1}A) \cap Stab(x)| \geq \frac{|A|}{|Ax|}.$$

Moreover,

$$|A \cap Stab(x)| \leq \frac{|AA|}{|Ax|}.$$

Classical case: A a subgroup.

Which actions?

Action of a group G on itself by conjugation
Action of a group G on G/H (by multiplication)
Action of a setwise stabilizer $\mathrm{Sym}(n)_\Sigma$ on a pointwise stabilizer $\mathrm{Sym}(n)_{\Sigma}$, by conjugation.

Which actions?

Action of a group G on itself by conjugation
Action of a group G on G/H (by multiplication)
Action of a setwise stabilizer $\mathrm{Sym}(n)_\Sigma$ on a pointwise stabilizer $\mathrm{Sym}(n)_{\Sigma}$, by conjugation.
Consider also (in other ways) the natural actions:
$\mathrm{SL}_n(K)$ acts on K^n
$\mathrm{Sym}(n)$ acts on $X = \{1, 2, \ldots, n\}$
(and $X = \{1, 2, \ldots, n\}^k$, etc.)

Which actions?

Action of a group G on itself by conjugation
Action of a group G on G/H (by multiplication)
Action of a setwise stabilizer $\mathrm{Sym}(n)_\Sigma$ on a pointwise stabilizer $\mathrm{Sym}(n)_\Sigma$, by conjugation.
Consider also (in other ways) the natural actions:
$\mathrm{SL}_n(K)$ acts on K^n
$\mathrm{Sym}(n)$ acts on $X = \{1, 2, \ldots, n\}$
(and $X = \{1, 2, \ldots, n\}^k$, etc.)
The first action is useful because it is geometric.
The second action is useful because X is small.

From subgroups to subsets, II

Other results on subgroups that can be adapted.

From subgroups to subsets, II

Other results on subgroups that can be adapted.

In common with groups of Lie type:

From subgroups to subsets, II

Other results on subgroups that can be adapted.

In common with groups of Lie type:

Results with algorithmic proofs: Bochert (1889) showed that Alt_n has no large primitive subgroups; the same proof gives that, for $A \subset \mathrm{Alt}_n$ large with $\langle A \rangle$ primitive, $A^{n^4} = \mathrm{Alt}_n$. Also, e.g., Schreier.

From subgroups to subsets, II

Other results on subgroups that can be adapted.

In common with groups of Lie type:

Results with algorithmic proofs: Bochert (1889) showed that Alt_n has no large primitive subgroups; the same proof gives that, for $A \subset \mathrm{Alt}_n$ large with $\langle A \rangle$ primitive, $A^{n^4} = \mathrm{Alt}_n$. Also, e.g., Schreier.

Elementary proofs of parts of the Classification: work by Babai, Pyber.

From subgroups to subsets, II

Other results on subgroups that can be adapted.

In common with groups of Lie type:

Results with algorithmic proofs: Bochert (1889) showed that Alt_n has no large primitive subgroups; the same proof gives that, for $A \subset \mathrm{Alt}_n$ large with $\langle A \rangle$ primitive, $A^{n^4} = \mathrm{Alt}_n$. Also, e.g., Schreier.

Elementary proofs of parts of the Classification: work by Babai, Pyber.
(In Breuillard-Green-Tao, for groups of Lie type: adapt Larsen-Pink; a classification of subgroups becomes a classification of "approximate subgroups", i.e., subsets $A \subset \mathrm{Alt}_n$ such that $|AAA| \leq |A|^{1+\delta}$.)

From subgroups to subsets, II

Other results on subgroups that can be adapted.

In common with groups of Lie type:

Results with algorithmic proofs: Bochert (1889) showed that Alt_n has no large primitive subgroups; the same proof gives that, for $A \subset \mathrm{Alt}_n$ large with $\langle A \rangle$ primitive, $A^{n^4} = \mathrm{Alt}_n$. Also, e.g., Schreier.

Elementary proofs of parts of the Classification: work by Babai, Pyber.
(In Breuillard-Green-Tao, for groups of Lie type: adapt Larsen-Pink; a classification of subgroups becomes a classification of "approximate subgroups", i.e., subsets $A \subset \mathrm{Alt}_n$ such that $|AAA| \leq |A|^{1+\delta}$.) Here: a combinatorial-probabilistic proof becomes a stochastic proof. The uniform distribution gets replaced by the outcome of a random walk.

From subgroups to subsets, II

Other results on subgroups that can be adapted.

In common with groups of Lie type:

Results with algorithmic proofs: Bochert (1889) showed that Alt_n has no large primitive subgroups; the same proof gives that, for $A \subset \mathrm{Alt}_n$ large with $\langle A \rangle$ primitive, $A^{n^4} = \mathrm{Alt}_n$. Also, e.g., Schreier.

Elementary proofs of parts of the Classification: work by Babai, Pyber.
(In Breuillard-Green-Tao, for groups of Lie type: adapt Larsen-Pink; a classification of subgroups becomes a classification of "approximate subgroups", i.e., subsets $A \subset \mathrm{Alt}_n$ such that $|AAA| \leq |A|^{1+\delta}$.) Here: a combinatorial-probabilistic proof becomes a stochastic proof. The uniform distribution gets replaced by the outcome of a random walk. Possible for actions $G \to X$ with X small.

The splitting lemma

Example: Babai's splitting lemma.

Lemma (Babai)

Let $H < \mathrm{Sym}(n)$ be 2-transitive.
Let $\Sigma \subset [n] = \{1, 2, \ldots, n\}$. Assume that there are at least ρn^2 ordered pairs in $[n] \times [n]$ such that there is no $g \in H_{([\Sigma])}$ with $\alpha^g = \beta$.
Then $|H| \leq n^{O(|\Sigma|(\log n)/\rho)}$.

The splitting lemma

Example: Babai's splitting lemma.

Lemma (Babai-H-S)

Let $A \subset \mathrm{Sym}_n$ with $A = A^{-1}$, $e \in A$ and $\langle A \rangle$ 2-transitive. Let $\Sigma \subset [n] = \{1, 2, \dots, n\}$. Assume that there are at least ρn^2 ordered pairs in $[n] \times [n]$ such that there is no $g \in (A^k)_{([\Sigma])}$ with $\alpha^g = \beta$ and $k = n^{O(1)}$. Then $|H| \leq n^{O(|\Sigma|(\log n)/\rho)}$.

The splitting lemma

Example: Babai's splitting lemma.

Lemma (Babai-H-S)

Let $A \subset \mathrm{Sym}_n$ with $A = A^{-1}$, $e \in A$ and $\langle A \rangle$ 2-transitive. Let $\Sigma \subset [n] = \{1, 2, \ldots, n\}$. Assume that there are at least ρn^2 ordered pairs in $[n] \times [n]$ such that there is no $g \in (A^k)_{([\Sigma])}$ with $\alpha^g = \beta$ and $k = n^{O(1)}$. Then $|H| \leq n^{O(|\Sigma|(\log n)/\rho)}$.

Useful: it guarantees the existence of long stabilizer chains

$$A \supset A_{\alpha_1} \supset A_{(\alpha_1,\alpha_2)} \supset A_{(\alpha_1,\alpha_2,\ldots)} \supset \ldots \supset A_{(\alpha_1,\alpha_2,\ldots,\alpha_r)},$$

where $r \gg (\log |A|)/(\log n)^2$ and $|\alpha_j^{A_{\alpha_1,\ldots,\alpha_{j-1}}}| \geq 0.9n$ for every $j \leq r$.

Outline of proof of main theorem

Given: long stabilizer chain for $A \subset \mathrm{Sym}_n$ with $\Sigma = \{\alpha_1, \alpha_2, \ldots \alpha_r\}$.
Goal: increase length r of long stabilizer chain by factor > 1. (Can then recur.)

Outline of proof of main theorem

Given: long stabilizer chain for $A \subset \mathrm{Sym}_n$ with $\Sigma = \{\alpha_1, \alpha_2, \dots \alpha_r\}$.
Goal: increase length r of long stabilizer chain by factor > 1. (Can then recur.)

By Bochert and pigeonhole, $A' = (A^m)_\Sigma$, $m = n^{O(1)}$, acts like $\mathrm{Sym}(\Sigma')$ ($\Sigma' \subset \Sigma$ large) on Σ.

Outline of proof of main theorem

Given: long stabilizer chain for $A \subset \mathrm{Sym}_n$ with $\Sigma = \{\alpha_1, \alpha_2, \ldots \alpha_r\}$.
Goal: increase length r of long stabilizer chain by factor > 1. (Can then recur.)

By Bochert and pigeonhole, $A' = (A^m)_\Sigma$, $m = n^{O(1)}$, acts like $\mathrm{Sym}(\Sigma')$ ($\Sigma' \subset \Sigma$ large) on Σ.
We let A' act on $A'' = A_{(\Sigma)} \subset \mathrm{Sym}_n|_{(\Sigma)}$ by conjugation.

Outline of proof of main theorem

Given: long stabilizer chain for $A \subset \mathrm{Sym}_n$ with $\Sigma = \{\alpha_1, \alpha_2, \dots \alpha_r\}$.
Goal: increase length r of long stabilizer chain by factor > 1. (Can then recur.)

By Bochert and pigeonhole, $A' = (A^m)_\Sigma$, $m = n^{O(1)}$, acts like $\mathrm{Sym}(\Sigma')$ ($\Sigma' \subset \Sigma$ large) on Σ.
We let A' act on $A'' = A_{(\Sigma)} \subset \mathrm{Sym}_n|_{(\Sigma)}$ by conjugation.

$\langle A'' \rangle$ 2-transitive on $[n] - \Sigma$ (or almost?)

Outline of proof of main theorem

Given: long stabilizer chain for $A \subset \mathrm{Sym}_n$ with $\Sigma = \{\alpha_1, \alpha_2, \dots \alpha_r\}$.
Goal: increase length r of long stabilizer chain by factor > 1. (Can then recur.)

By Bochert and pigeonhole, $A' = (A^m)_\Sigma$, $m = n^{O(1)}$, acts like $\mathrm{Sym}(\Sigma')$ ($\Sigma' \subset \Sigma$ large) on Σ.
We let A' act on $A'' = A_{(\Sigma)} \subset \mathrm{Sym}_n|_{(\Sigma)}$ by conjugation.

$\langle A'' \rangle$ 2-transitive on $[n] - \Sigma$ (or almost?)
Then there is a small subset $A''' \subset (A'')^{n^{O(\log n)}}$ with $\langle A''' \rangle$ 2-transitive. (Proof by random walks again!) By orbit-stabilizer, this makes $A'''' = (A^{m'})_{(\Sigma)}$ large (for $m' = n^{O(\log n)}$).

Outline of proof of main theorem

Given: long stabilizer chain for $A \subset \mathrm{Sym}_n$ with $\Sigma = \{\alpha_1, \alpha_2, \dots \alpha_r\}$.
Goal: increase length r of long stabilizer chain by factor > 1. (Can then recur.)

By Bochert and pigeonhole, $A' = (A^m)_\Sigma$, $m = n^{O(1)}$, acts like $\mathrm{Sym}(\Sigma')$ ($\Sigma' \subset \Sigma$ large) on Σ.
We let A' act on $A'' = A_{(\Sigma)} \subset \mathrm{Sym}_n|_{(\Sigma)}$ by conjugation.

$\langle A'' \rangle$ 2-transitive on $[n] - \Sigma$ (or almost?)
Then there is a small subset $A''' \subset (A'')^{n^{O(\log n)}}$ with $\langle A''' \rangle$ 2-transitive. (Proof by random walks again!) By orbit-stabilizer, this makes $A'''' = (A^{m'})_{(\Sigma)}$ large (for $m' = n^{O(\log n)}$).
Apply splitting lemma to prolong $\alpha_1, \alpha_2, \dots, \alpha_r$; done.

Outline of proof, continued: the other induction

$\langle A'' \rangle$ not 2-transitive on $[n] - \Sigma$ (or almost?)

Outline of proof, continued: the other induction

$\langle A'' \rangle$ not 2-transitive on $[n] - \Sigma$ (or almost?)
Then $\langle A'' \rangle$ decomposes into permutation groups on $n' \leq 0.9n$ elements; by induction, the diameter is small.

Outline of proof, continued: the other induction

$\langle A'' \rangle$ not 2-transitive on $[n] - \Sigma$ (or almost?)
Then $\langle A'' \rangle$ decomposes into permutation groups on $n' \leq 0.9n$ elements; by induction, the diameter is small.
By (Babai, Seress 1988), there is an element g of small support – use that as an existence statement; can reach g by small diameter. Done.