The diameter of permutation groups

Ákos Seress

February 2011, Queenstown

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.)

Computing the diameter is difficult

NP-hard even for elementary abelian 2-groups (Even, Goldreich 1981)

Computing the diameter is difficult

NP-hard even for elementary abelian 2-groups (Even, Goldreich 1981)

How large can be the diameter?

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

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

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)

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:
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:
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)
- Lie-type groups of bounded rank (Pyber, E. Szabó 2011) and (Breuillard, Green, Tao 2011)

Alternating groups ???

Alternating groups: why is it difficult?

Attempt # 1: Techniques for Lie-type groups

Diameter results for Lie-type groups are proven by product theorems:

Theorem (Pyber, Szabó)

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 is it difficult?

Attempt # 1: Techniques for Lie-type groups

Diameter results for Lie-type groups are proven by product theorems:

Theorem (Pyber, Szabó)

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

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, $|S^3| \leq 9(m+1)(m+2)|S|$.

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

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, $|S^3| \leq 9(m+1)(m+2)|S|$.

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

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

Attempt # 2: construction of a 3-cycle

Any $g \in A_n$ 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 $g \in A_n$ 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)

$G = \langle S \rangle \cong A_n$ 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 2011)

$G = \langle S \rangle \cong A_n$ 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)

$G = \langle S \rangle \cong A_n$ 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 2011)

$G = \langle S \rangle \cong A_n$ 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 $A_n = \langle S \rangle$, there exists a word of length $\exp(\sqrt{n \log n}(1 + o(1)))$, defining $h \in A_n$ with $|\mathrm{supp}(h)| \leq n/4$. Consequently

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

A quasipolynomial bound

Theorem (Helfgott, Seress 2011)

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

Babai's conjecture would require
$\mathrm{diam}\,(A_n) \le n^{O(1)} = \exp(O(\log n))$.

A quasipolynomial bound

Theorem (Helfgott, Seress 2011)

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

Babai's conjecture would require
$\mathrm{diam}\,(A_n) \le n^{O(1)} = \exp(O(\log n))$.

Corollary

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

A quasipolynomial bound

Theorem (Helfgott, Seress 2011)

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

Babai's conjecture would require
$\mathrm{diam}\,(A_n) \le n^{O(1)} = \exp(O(\log n))$.

Corollary

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

Corollary follows from

Theorem (Babai, Seress 1992)

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

A quasipolynomial bound

Theorem (Helfgott, Seress 2011)

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

Babai's conjecture would require
$\mathrm{diam}\,(A_n) \le n^{O(1)} = \exp(O(\log n))$.

Corollary

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

Corollary follows from

Theorem (Babai, Seress 1992)

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

http://www.math.osu.edu/˜seress.1/Publications.html