The diameter of permutation groups

Ákos Seress

May 2012

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)

Definition (informal)

A decision problem is in the complexity class NP if the yes answer can be checked in polynomial time.

A decision problem is NP-complete if it is in NP and all problems in NP can be reduced to it in polynomial time.

A decision problem is NP-hard if all problems in NP can be reduced to it in polynomial time.

How large can be the diameter?

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 $|G|$.

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

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

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.

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.

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:

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

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

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

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 2012)

$G = \langle S \rangle \cong A_n$ *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 $|\mathrm{supp}(h)| \le n/4$. Consequently

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

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
$\mathrm{diam}\,(A_n) \le n^{O(1)} = \exp(O(\log n))$.

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.*

The main idea of (Babai, Seress 1988)

Given $\mathrm{Alt}(\Omega) \cong A_n = \langle S \rangle$, construct $h \in A_n$ with $|\mathrm{supp}(h)| \leq n/4$ as a short word in 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 $p_1, p_1, p_2, \ldots, p_k$.

For $\alpha \in \Omega$, let $\ell_\alpha :=$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 $|\Omega_i| \leq n/4$.

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

Proof of the claim

Claim

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

Proof: On one hand,

$$\sum_{\alpha \in \Omega} \sum_{p_i | \ell_\alpha} \log p_i \leq n \log n.$$

On the other hand,

$$\sum_{\alpha \in \Omega} \sum_{p_i | \ell_\alpha} \log p_i = \sum_{i=1}^{k} |\Omega_i| \log p_i.$$

If all $|\Omega_i| > n/4$ then

$$\sum_{i=1}^{k} |\Omega_i| \log p_i > \frac{n}{4} \log \left(\prod_{i=1}^{k} p_i \right) > n \log n,$$

a contradiction.

Cost analysis

We considered $p_1, \ldots, p_k$ so that $\prod_{i=1}^{k} p_i > n^4$. How large is k?

$\prod_{p<x} p \approx e^x = n^4$ so we have to take primes up to $x = \Theta(\log n)$, implying

$$\sum_{p<x} p = \Theta\left(\frac{\log^2 n}{\log\log n}\right).$$

(Order of magnitude can also be proven by elementary estimates on prime distribution.)

$$\mathrm{length}_S(g) = O\left(n^{\frac{\log^2 n}{\log\log n}}\right).$$

Theorem (Landau 1907)

$$\max\{|g| : g \in S_n\} = e^{\sqrt{n \log n}(1+o(1))}.$$

Hence $\mathrm{length}_S(h) = e^{\sqrt{n \log n}(1+o(1))}$.

In the original proof, same procedure is iterated $O(\log n)$ times; faster finish by Babai, Beals, Seress (2004).

The main idea of (Helfgott, Seress 2011)

Use basic data structures for computations with permutation groups (Sims, 1970)

Definition

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

$$G^{[1]} \geq G^{[2]} \geq \cdots \geq G^{[k+1]} = 1$$

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

Fixing (right) transversals T_i for $G^{[i]}$ mod $G^{[i+1]}$, every $g \in G$ can be written uniquely as $g = t_k \cdots t_2 t_1$, $t_i \in T_i$.

(H,S 2011) works with partial transversals: Suppose $G = \mathrm{Alt}(\Omega) = \langle A \rangle \cong A_n$ and there are $\alpha_1, \ldots, \alpha_m \in \Omega$:

$$|\alpha_i^{A_{(\alpha_1, \ldots, \alpha_{i-1})}}| > 0.9n.$$

Key proposition of (H,S 2011), substitution for product theorems:

Theorem

In $A^{\exp(O(\log^2 n))}$ there is a significantly longer partial transversal system or $A^{\exp(O(\log^4 n))}$ contains some permutation g with small support.

Proof techniques in (Helfgott,Seress 2011)

Subset versions of theorems of Babai, Pyber about 2-transitive groups and Bochert, Liebeck about large cardinality subgroups of A_n.

Combinatorial arguments, using random walks of quasipolynomial length on various domains to generate permutations that approximate properties of truly random elements of A_n.

Previous results on $\mathrm{diam}\,(A_n)$: main idea of (BS 1988), results of (BS1992), (BBS 2004).

Arguments are mostly combinatorial: the full symmetric group is a combinatorial rather than a group theoretic object.