Journal of Algebra 421 (2015) 349–368

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Random generators of the symmetric group: Diameter, mixing time and spectral gap

Harald A. Helfgott [a,*], Ákos Seress [b,c], Andrzej Zuk [d]

[a] École Normale Supérieure, Département de Mathématiques, 45 rue d'Ulm, F-75230 Paris, France
[b] Centre for the Mathematics of Symmetry and Computation, The University of Western Australia, Crawley, WA 6009, Australia
[c] Department of Mathematics, The Ohio State University, Columbus, OH 43210, USA
[d] Institut de Mathématiques, Université Paris 7, 13 rue Albert Einstein, 75013 Paris, France

ARTICLE INFO

Article history:
Received 15 March 2014
Available online 12 September 2014
Communicated by William M. Kantor and Charles Leedham-Green

Keywords:
Symmetric group
Permutation groups
Diameter
Spectral gap

ABSTRACT

Let g, h be a random pair of generators of $G = \mathrm{Sym}(n)$ or $G = \mathrm{Alt}(n)$. We show that, with probability tending to 1 as $n \to \infty$, (a) the diameter of G with respect to $S = \{g, h, g^{-1}, h^{-1}\}$ is at most $O(n^2(\log n)^c)$, and (b) the mixing time of G with respect to S is at most $O(n^3(\log n)^c)$. (Both c and the implied constants are absolute.)

These bounds are far lower than the strongest worst-case bounds known (in Helfgott–Seress, 2013); they roughly match the worst known examples. We also give an improved, though still non-constant, bound on the spectral gap.

Our results rest on a combination of the algorithm in (Babai–Beals–Seress, 2004) and the fact that the action of a pair of random permutations is almost certain to act as an expander on ℓ-tuples, where ℓ is an arbitrary constant (Friedman et al., 1998).

* Corresponding author.
E-mail addresses: harald.helfgott@ens.fr (H.A. Helfgott), zuk@math.jussieu.fr (A. Zuk).

http://dx.doi.org/10.1016/j.jalgebra.2014.08.033
0021-8693/

1. Introduction

1.1. Results

Let G be a finite group. Let S be a set of generators of G; assume $S = S^{-1}$. The (undirected) *Cayley graph* $\Gamma(G,S)$ is the graph having the elements of G as its vertices and the pairs $\{g, gs\}$ ($g \in G$, $s \in S$) as its edges. The *diameter* of G with respect to S is the diameter $\mathrm{diam}(\Gamma(G,S))$ of the Cayley graph $\Gamma(G,S)$:

$$\mathrm{diam}\big(\Gamma(G,S)\big) = \max_{g_1,g_2\in G} \min_{\substack{P \text{ a path} \\ \text{from } g_1 \text{ to } g_2}} \mathrm{length}(P),$$

where the *length* of a path is the number of edges it traverses. In other words, $\mathrm{diam}(\Gamma(G,S))$ is the maximum, for $g \in G$, of the length ℓ of the shortest expression $g = s_1 s_2 \cdots s_\ell$ with $s_i \in S$.

Theorem 1.1. *Let $S = \{g, h, g^{-1}, h^{-1}\}$, where g, h are elements of* $\mathrm{Sym}(n)$ *taken at random, uniformly and independently. Let $G = \langle S\rangle$. Then, with probability $1 - o(1)$, the diameter* $\mathrm{diam}(\Gamma(G,S))$ *of G with respect to S is at most $O(n^2(\log n)^c)$, where c and the implied constants are absolute.*

In the study of permutation groups, bounds are wanted not just for the diameter but also for two closely related quantities that give a finer description of the quality of a generating set S. The *spectral gap* is the difference $\lambda_0 - \lambda_1$ between the two largest eigenvalues λ_0, λ_1 (where $\lambda_0 = 1$ and $\lambda_0 \geq \lambda_1$) of the normalized adjacency matrix $\mathscr{A}$ on $\Gamma(G,S)$, seen as an operator on functions $f : G \to \mathbb{C}$:

$$\mathscr{A} f(g) := \frac{1}{|S|} \sum_{h\in S} f(gh). \tag{1.1}$$

The other quantity is the *mixing time*. A lazy random walk on $\Gamma(G,S)$ consists of taking $x_1, x_2, \ldots \in G$ at random and independently with distribution

$$\mu = \frac{1}{2} 1_{\{e\}} + \frac{1}{2|S|} 1_S, \tag{1.2}$$

where $1_A(x) = 1$ if $x \in A$ and $1_A(x) = 0$ if $x \notin A$; the outcome of the lazy random walk of length k is $x_1 x_2 \cdots x_k$. The (ϵ, d)-*mixing time* $t_{\mathrm{mix},\epsilon,d}$ is the least k such that the distribution $\mu^{(k)} = \mu * \mu * \cdots * \mu$ of the outcome of a lazy random walk of length k is very close to the uniform distribution $1_G/|G|$ on G:

$$d\left(\mu^{(k)}, \frac{1}{|G|} 1_G\right) \leq \epsilon,$$