Electronic Colloquium on Computational Complexity, Report No. 73 (2014)

Group representations that resist random sampling

Shachar Lovett
Computer Science and Engineering
University of California, San Diego
slovett@cs.ucsd.edu

Cristopher Moore
Santa Fe Institute
moore@cs.unm.edu

Alexander Russell
Computer Science and Engineering
University of Connecticut
acr@cse.uconn.edu

May 14, 2014

Abstract

We show that there exists a family of groups G_n and nontrivial irreducible representations ρ_n such that, for any constant t, the average of ρ_n over t uniformly random elements $g_1, \ldots, g_t \in G_n$ has operator norm 1 with probability approaching 1 as $n \to \infty$. More quantitatively, we show that there exist families of finite groups for which $\Omega(\log \log |G|)$ random elements are required to bound the norm of a typical representation below 1. This settles a conjecture of A. Wigderson.

1 Introduction

The Alon-Roichman theorem [1] asserts that $O(\log |G|/\epsilon^2)$ elements, chosen independently and uniformly from a finite group G, yield with high probability a Cayley graph with second eigenvalue no more than ϵ. As there are groups for which $O(\log |G|)$ elements are necessary to even generate the group, this bound is tight up to a constant when $\epsilon = \Omega(1)$. The condition that a collection of group elements $g_1, \ldots, g_t$ yield a graph with second eigenvalue ϵ is equivalent to the condition that every nontrivial irreducible representation ρ of G is approximately annihilated in the sense that

$$\left\| \frac{1}{t} \sum_{i=1}^{t} \rho(g_i) \right\|_{\mathrm{op}} \leq \epsilon \,. \tag{1}$$

where if the graph is undirected we demand that $\{g_1, \ldots, g_t\}$ is closed under inverse.

This invites a more refined analysis of the Alon-Roichman theorem popularized by a question of A. Wigderson [3, Conjecture 2.8.4]: *Are there universal constants t and $\delta > 0$ such that*

$$\mathop{\mathbb{E}}_{g_1,\ldots,g_t} \left[\left\| \frac{1}{t} \sum_{i=1}^{t} \rho(g_i) \right\|_{\mathrm{op}} \right] \leq 1 - \delta \tag{2}$$

holds for all finite groups G and all nontrivial irreducible representations ρ of G? As above, the g_i are selected independently and uniformly from G.

ISSN 1433-8092

To support this notion, we remark that there are known families of "highly nonabelian" finite groups, such as $\mathsf{SL}_2(\mathbb{F}_p)$ as $p \to \infty$, which yield expanding Cayley graphs over a constant number of uniformly random group elements $g_1, \ldots, g_t$ [2]. It follows that (2) holds for every representation. Likewise, (2) holds for all nontrivial irreducible representations of abelian groups: for example, while no constant number of elements suffice to make $\mathbb{Z}_2^n$ into an expander, or even to generate the group, just $t = 2$ uniformly random elements suffice to bound the expected norm of any one irreducible representation to $1 - \delta$, with a universal constant $\delta > 0$.

Distinct irreducible representations of a finite group possess various independence properties when viewed as random variables by selecting a uniformly random group element: for example, their entries are pairwise uncorrelated in any basis. Intuitively, Wigderson's question asks whether the dependence on $\log |G|$ in the Alon-Roichman theorem is an artifact of the requirement that every representation be annihilated—a collection of ostensibly independent events which one might imagine occur with constant probability with the selection of each new group element—or is a feature that can manifest even in a single irreducible representation. Indeed, a positive answer to the question would imply that $O(\log |\widehat{G}|)$ random elements suffice to turn any group G into an expanding Cayley graph, where $\hat{G}$ denotes the set of irreducible representations of G.

We answer this question in the negative. Our strategy will be to work in a family of finite groups of the form $G = K^n$, where K has constant size, is nonabelian, and has trivial center. Such groups simultaneously possess high-dimensional representations and the property that any collection of a bounded number of group elements generate a subgroup of bounded size. In this setting, for each constant $t > 0$, we establish two results:

- When K has a faithful irreducible representation ρ of dimension at least two, we show that the representation $\rho^n = \rho \otimes \cdots \otimes \rho$ of $G = K^n$ has the property that

$$\Pr_{g_1, \ldots, g_t} \left[\left\| \frac{1}{t} \sum_i \rho^n(g_i) \right\|_{\mathrm{op}} = 1 \right] \geq 1 - \exp(-\Omega(n)),$$

  where the g_i are elements of G chosen uniformly and independently at random. See Theorem 1 for a more precise statement.

This result holds, for instance, if $K = S_3$, the group of permutations of three elements, and ρ is its two-dimensional representation. We also show

- When ρ is selected according to the Plancherel measure, which assigns each irreducible representation probability mass proportional to the square of its dimension, we show that with probability $1 - O(1/\sqrt[4]{n})$, ρ has the property that

$$\Pr_{g_1, \ldots, g_t} \left[\left\| \frac{1}{t} \sum_i \rho^n(g_i) \right\|_{\mathrm{op}} = 1 \right] \geq 1 - O\left(\frac{1}{\sqrt[4]{n}} \right),$$

  where the g_i are elements of G chosen uniformly and independently at random. See Theorem 2 for a more precise statement.

In fact, these estimates establish that there are infinite families of groups for which there is a representation ρ such that $\Omega(\log \log |G|)$ uniformly random elements are necessary to bound the norm

of ρ as in (2), for any constant $\delta > 0$. Recall that the Alon-Roichman theorem guarantees that $O(\log |G|)$ random elements suffice with high probability to bound the norm of *every* irrep ρ, and thus turn G into an expander. Closing this gap remains an interesting open question.

These negative results for independent and uniformly random group elements suggest the following question, which is existential rather than probabilistic: Are there constants t and $\delta > 0$ such that, for any group G and any nontrivial irreducible representation ρ, there exist t elements $g_1, \ldots, g_t \in G$ such that

$$\left\| \frac{1}{t} \sum_i \rho(g_i) \right\|_{\mathrm{op}} \leq 1 - \delta \, ?$$

Our construction cannot rule out this possibility.

Notation and actions on the group algebra

Given a finite group G, let $\widehat{G}$ denote its set of irreducible representations. We assume throughout that all representations are unitary. For a representation ρ, we let $\chi_\rho(g) = \operatorname{tr} \rho(g)$ denote its character, and let $d_\rho = \chi_\rho(1)$ denote its dimension. For two class functions, χ and ψ on G, we define

$$\langle \chi, \psi \rangle_G = \frac{1}{|G|} \sum_g \chi(g) \psi(g)^* \tag{3}$$

and remark that the characters of the irreducible representations of G form an orthonormal basis for the space of class functions with respect to the inner product (3). Thus if ρ is irreducible and σ is a representation, $\langle \rho, \sigma \rangle_G$ is the number of copies of ρ appearing in σ.

If H is a subgroup of G and χ is the character of a representation of G, we let $\operatorname{Res}_H \chi$ denote this class function restricted to the subgroup H; when we wish to emphasize the ambient group G, we write $\operatorname{Res}^G_H \chi$. If $G = K^n$ and ρ is a representation of K, we let ρ^n denote the representation of G given by the rule

$$\rho^n(g_1, \ldots, g_n) = \rho(g_1) \otimes \cdots \otimes \rho(g_n)$$

and remark that $\chi_{\rho^n}(g_1, \ldots, g_n) = \prod_{j=1}^n \chi_\rho(g_j)$. We overload this notation, defining

$$\chi_{\rho^n}(g) = \operatorname{Res}_K \chi_{\rho^n}(g, \ldots, g)$$

to be the character obtained on K by restricting χ_{ρ^n} to the "diagonal" subgroup $\{(g, \ldots, g) \mid g \in K\} \cong K$.

Let $\mathbb{C}[G]$ denote the group algebra on G. The left action of G on $\mathbb{C}[G]$ obtained by linearly extending the rule $g : g' \mapsto gg'$ induces the *(left) regular representation* R of G, with character

$$\chi_R(g) = \begin{cases} |G| & \text{if } g = 1, \\ 0 & \text{otherwise.} \end{cases}$$

As a consequence of character orthogonality, one can express R as the sum

$$R = \bigoplus_{\rho \in \widehat{G}} d_\rho \rho \, ,$$

i.e., it contains d_ρ copies of each irreducible representation ρ. Thus its character can be written

$$\chi_R = \sum_{\rho \in \widehat{G}} d_\rho \chi_\rho \, .$$

The algebra $\mathbb{C}[G]$ can likewise be given the structure of a $G \times G$ representation B by linearly extending the rule $(g_1, g_2) : g \mapsto g_1 g g_2^{-1}$. Its character χ_B thus satisfies

$$\chi_B(g_1, g_2) = \left|\left\{g \,:\, g_1 g g_2^{-1} = g\right\}\right|.$$

Again applying character orthogonality, B can be expressed as the sum

$$B = \bigoplus_{\rho \in \widehat{G}} \rho \otimes \rho^*$$

and thus

$$\chi_B(g_1, g_2) = \sum_{\rho \in \widehat{G}} \chi_\rho(g_1) \cdot \chi_\rho^*(g_2).$$

Finally, the Plancherel measure $\mathscr{P}$ on $\widehat{G}$ assigns each representation ρ the probability mass

$$\mathscr{P}(\rho) = \frac{d_\rho^2}{|G|}.$$

If $G = K^n$, then selecting $\rho = \rho_1 \otimes \cdots \otimes \rho_n$ from the Plancherel measure on $\widehat{G}$ is the same as selecting the ρ_i independently from the Plancherel measure on $\widehat{K}$.

2 Remarks on the subgroup structure of groups of the form K^n

Anticipating the proofs, we collect a few facts about subgroups of $G = K^n$. Given $g \in G$, let $g_i \in K$ denote its ith coordinate; note that $\pi_i(g) = g_i$ is a homomorphism from G to K. We consider the subgroup H generated by a collection of t elements $h^{(1)}, \ldots, h^{(t)}$ of K^n. Given such a collection, define the function $\mathrm{S} : \{1, \ldots, n\} \to K^t$ so that $S(i)$ lists their ith coordinates:

$$\mathrm{S}(i) = (h_i^{(1)}, \ldots, h_i^{(t)}). \tag{4}$$

Let $\sim_{\mathrm{S}}$ denote the equivalence class on $\{1, \ldots, n\}$ given by the level sets of S, so that

$$i \sim_{\mathrm{S}} j \Leftrightarrow \mathrm{S}(i) = \mathrm{S}(j).$$

That is, $i \sim_{\mathrm{S}} j$ if and only if $h_i^{(m)} = h_j^{(m)}$ for all $1 \le m \le t$. As a consequence, we also have $h_i = h_j$ for any $h \in H$. Thus if we define the subgroup of elements of K^n that respect this equivalence,

$$\tilde{H} = \{(g_1, \ldots, g_n) \mid i \sim_{\mathrm{S}} j \Rightarrow g_i = g_j\} \subseteq K^n, \tag{5}$$

we have $h^{(m)} \in \tilde{H}$ for all m, and hence $H \subset \tilde{H}$. (Note that S, $\sim_S$, and $\tilde{H}$ depend implicitly on the collection $h^{(1)}, \ldots, h^{(t)}$.)

While the group H may have quite complicated structure, $\tilde{H}$ is isomorphic to K^ℓ for some $\ell \ge 1$, where $\ell \le n$ is the number of equivalence classes of $\sim_{\mathrm{S}}$. Moreover, as the function S takes no more than $|K|^t$ different values, $\ell \le |K|^t$ and $|H| \le |\tilde{H}| \le |K|^{|K|^t}$. Thus, as recorded in the following lemma, if $|K|$ and t are constant than H is of constant size.

Lemma 1. *Let H be the subgroup of K^n generated by t elements $h^{(1)}, \ldots, h^{(t)}$. Then $|H| \le |K|^{|K|^t}$.*

The size of the smallest equivalence class of $\sim_S$ plays an essential role in both proofs. To name this quantity, for a sequence of elements $h^{(1)}, \ldots, h^{(t)}$, let

$$d = d(h^{(1)}, \ldots, h^{(t)}) = \min_{i \in \{1,\ldots,n\}} \left| \{ j \mid i \sim_S j \} \right| .$$

We set down two straightforward tail bounds on $d(h^{(1)}, \ldots, h^{(t)})$, when the $h^{(m)}$ are selected independently and uniformly at random from K^n.

Lemma 2. *Let $h^{(1)}, \ldots, h^{(t)}$ be t independent and uniformly random elements of K^n. Then*

1. $\Pr\left[d(h^{(1)}, \ldots, h^{(t)}) \le \dfrac{n}{2|K|^t} \right] \le \dfrac{4|K|^{2t}}{n}$ *and,*
2. *for any $\ell \ge 1$,* $\Pr\left[d(h^{(1)}, \ldots, h^{(t)}) < \ell \right] \le n^\ell |K|^t \, \mathrm{e}^{-n/|K|^t}$.

Proof. For a given $s \in K^t$, let X_s be the random variable equal to the size of the corresponding set in the partition, $\{i : S(i) = s\}$. Since X_s is binomially distributed as $\mathrm{Bin}(n, 1/|K|^t)$, we have $\mathbb{E} X_s = n/|K|^t$ and $\mathrm{Var} X_s \le n/|K|^t$. By Chebyshev's inequality,

$$\Pr\left[\left| X_s - \frac{n}{|K|^t} \right| \ge \frac{n}{2|K|^t} \right] \le \frac{4|K|^t}{n} .$$

Since there are $|K|^t$ elements of K^t, the union bound implies the statement (1) of the lemma. As for statement (2), for any s the probability that $X_s < \ell$ is no more than

$$\sum_{i=0}^{\ell-1} \binom{n}{i} \left(\frac{1}{|K|^t} \right)^i \left(1 - \frac{1}{|K|^t} \right)^{n-i} \le \sum_{i=0}^{\ell-1} \binom{n}{i} \left(1 - \frac{1}{|K|^t} \right)^n \le \left[\sum_{i=0}^{\ell-1} \binom{n}{i} \right] \left(\mathrm{e}^{-1/|K|^t} \right)^n \le n^\ell \, \mathrm{e}^{-n/|K|^t} .$$

Then the union bound implies the statement (2) of the lemma. □

Note that the random variable X_s obeys the Chernoff bound, making it much more concentrated than the second moment calculation of (1) suggests, but this is not important to our results.

3 An explicit construction

Theorem 1. *Let $G = K^n$ where K is a finite nonabelian group with trivial center. Let ρ a faithful irreducible representation of K of dimension $d_\rho \ge 2$. Then there is an integer $\kappa_\rho \ge 2$ such that for every $t > 0$,*

$$\Pr_{h^{(1)},\ldots,h^{(t)}} \left[\left\| \frac{1}{t} \sum_{m=1}^{t} \rho^n(h^{(m)}) \right\|_{\mathrm{op}} = 1 \right] \ge 1 - n^{\kappa_\rho} |K|^t \exp(-n/|K|^t) ,$$

where $h^{(1)}, \ldots, h^{(t)} \in G$ are independent and uniform.

We begin by observing that a representation satisfying the conditions of the theorem above has the property that

$$\rho^{\otimes k} = \underbrace{\rho \otimes \cdots \otimes \rho}_{k \text{ times}}$$

contains a copy of the trivial representation for all sufficiently large k. For instance, if $K = S_3$ and ρ is its two-dimensional representation, then this holds for any $k \ge 2$. The following is a classic fact of representation theory, but we give a proof for completeness:

Lemma 3. *Let K be a finite group with trivial center and ρ a faithful irreducible representation of K of dimension $d_\rho \geq 2$. Then there is an integer $\kappa_\rho \geq 2$ so that for all $k \geq \kappa_\rho$, $\langle \chi_\rho^k, 1\rangle_K > 0$.*

Proof. As ρ is faithful, the only element $h \in K$ such that $\rho(k)$ is a scalar matrix is the identity:

$$\{h \mid \rho(h) = \lambda \mathbb{1} \text{ for some } \lambda \in \mathbb{C}\} = \mathscr{Z}(K) = \{1\},$$

where $\mathscr{Z}(K)$ denotes the (trivial) center of K. By unitarity, it follows that $|\chi_\rho(h)| < d_\rho$ for all $h \neq 1$. Expanding

$$\langle \chi_\rho^k, 1\rangle_K = \frac{1}{|K|}\sum_{h\in K} \chi_\rho(h)^k = \frac{d_\rho^k}{|K|}\Bigg[1 + \underbrace{\sum_{h\neq 1}\left(\frac{\chi_\rho(h)}{d_\rho}\right)^k}_{(\dagger)}\Bigg],$$

it is evident that, for sufficiently large k, each term of the sum (†) is strictly less than $1/(|K|-1)$ in absolute value. For such k, the quantity in brackets above is strictly positive, as desired. □

Proof of Theorem 1. In light of Lemma 3, let K be a finite group with trivial center and ρ a faithful, irreducible representation of K of dimension $d_\rho > 2$. Consider now the representation ρ^n of the group K^n. For a sequence of elements $h^{(1)}, \ldots, h^{(t)} \in K^n$, recall that the subgroup $\tilde{H}$, defined in (5) above, contains all $h^{(m)}$ and that

$$\mathrm{Res}_{\tilde{H}}\, \rho^n = \bigotimes_{\substack{C\text{: equivalence} \\ \text{class of } \sim_S}} \mathrm{Res}_K^{K^{|C|}}\, \rho^{|C|}.$$

If each equivalence class C of $\sim_S$ has size at least κ_ρ, each factor in the tensor product above has a copy of the trivial representation, and thus $\mathrm{Res}_{\tilde{H}}\, \rho^n$ has a copy of the trivial representation. In that case,

$$\left\| \frac{1}{t}\sum_{m=1}^{t} \rho^n(h^{(m)}) \right\|_{\mathrm{op}} = 1.$$

As each equivalence class of $\sim_S$ has size at least $d(h^{(1)}, \ldots, h^{(t)})$, we conclude that

$$\Pr\left[\left\| \frac{1}{t}\sum_{m=1}^{t} \rho^n(h^{(m)}) \right\|_{\mathrm{op}} = 1\right] \geq 1 - \Pr\left[d(h^{(1)}, \ldots, h^{(t)}) < \kappa_\rho\right] \geq 1 - n^{\kappa_\rho}|K|^t\, \mathrm{e}^{-n/|K|^t},$$

by statement 2 of Lemma 2. □

4 The behavior of random representations

Focusing on the same family of groups $G = K^n$ where K is nonabelian with a trivial center, we establish that a representation ρ selected according to the Plancherel measure has the property, with high probability, that

$$\Pr_{h^{(1)},\ldots,h^{(t)}}\left[\left\| \frac{1}{t}\sum_{m=1}^{t} \rho^n(h^{(m)}) \right\|_{\mathrm{op}} = 1\right] \geq 1 - O\left(\frac{1}{\sqrt[4]{n}}\right),$$

where $h^{(1)}, \ldots, h^{(t)} \in G$ are independent and uniform.

Our proof focuses on the random variable

$$X_H = \frac{\langle \mathrm{Res}_H \chi_\rho, 1\rangle_H}{d_\rho}, \tag{6}$$

where H is a fixed subgroup of a group G and ρ is selected according to the Plancherel measure. Since X_H is the dimensionwise fraction of ρ that restricts to the trivial representation under H, whenever $X_H > 0$ we have

$$\left\| \mathop{\mathbb{E}}_{h\in H} \rho(h) \right\|_{\mathrm{op}} = 1\,.$$

The proof will show that for groups of the form K^n, if $H = \langle h^{(1)}, \ldots, h^{(t)}\rangle$ then $X_H > 0$ with high probability. We do this by computing the first two moments of X_H, first for general group-subgroup pairs, and then specializing to the groups K^n.

The expectation For the first moment, observe that if $\rho \in \widehat{G}$ is distributed according to the Plancherel measure, then

$$\begin{aligned}\mathop{\mathbb{E}}_{\rho} X_H &= \mathop{\mathbb{E}}_{\rho} \frac{\langle \mathrm{Res}_H \chi_\rho, 1\rangle_H}{d_\rho} = \sum_\rho \frac{d_\rho^2}{|G|} \frac{\langle \mathrm{Res}_H \chi_\rho, 1\rangle_H}{d_\rho} = \frac{1}{|G|}\sum_\rho d_\rho \langle \mathrm{Res}_H \chi_\rho, 1\rangle_H \\ &= \frac{1}{|G|}\left\langle \mathrm{Res}_H \sum_\rho d_\rho \chi_\rho, 1 \right\rangle_H = \frac{1}{|G|}\langle \mathrm{Res}_H \chi_R, 1\rangle_H = \frac{1}{|H|}\,.\end{aligned}$$

The second moment For the second moment, observe that

$$\begin{aligned}\mathop{\mathbb{E}}_{\rho} X_H^2 &= \sum_\rho \frac{d_\rho^2}{|G|} \frac{\langle \mathrm{Res}_H \chi_\rho, 1\rangle_H^2}{d_\rho^2} = \frac{1}{|G|}\sum_\rho \langle \mathrm{Res}_{H\times H} \chi_{\rho\otimes\rho^*}, 1\rangle_{H\times H} \\ &= \frac{1}{|G|}\langle \mathrm{Res}_{H\times H} \chi_B, 1\rangle_{H\times H} = \frac{1}{|G|}\frac{1}{|H|^2}\sum_{h_1,h_2\in H} |\{g : h_1^{-1} g h_2 = g\}|\,.\end{aligned}$$

Thus

$$\begin{aligned}\mathop{\mathrm{Var}}_{\rho}[X_H] &= \mathop{\mathbb{E}}_{\rho} X_H^2 - \frac{1}{|H|^2} = \frac{1}{|H|^2}\left(\sum_{(h_1,h_2)\in H\times H} \Pr_g[h_1 = g^{-1}h_2 g] - 1\right) \\ &= \frac{1}{|H|^2}\sum_{\substack{(h_1,h_2)\in H\times H \\ (h_1,h_2)\neq(1,1)}} \Pr_g[h_1 = g^{-1}h_2 g] = \frac{1}{|H|^2}\sum_{\substack{h\in H \\ h\neq 1}} \frac{|h^G \cap H|}{|h^G|} \le \frac{1}{|H|}\sum_{\substack{h\in H \\ h\neq 1}} \frac{1}{|h^G|}\,,\end{aligned}$$

where $h^G = \{g^{-1}hg : g \in G\}$ is the conjugacy class of h in G.

Applying Chebyshev's inequality, we conclude that

$$\Pr_\rho[X_H = 0] \le \Pr\left[\left|X_H - \frac{1}{|H|}\right| \ge \frac{1}{|H|}\right] \le |H| \sum_{\substack{h\in H \\ h\neq 1}} \frac{1}{|h^G|}\,. \tag{7}$$

Returning to the statement of the theorem, we will show the following.

Theorem 2. *Let K be a finite nonabelian group with trivial center and let $G = K^n$. Let t be such that $2|K|^t \le \alpha\sqrt{n}$, let $h^{(1)}, \dots, h^{(t)}$ be independent elements selected uniformly from G, and let $\rho = \rho_1 \otimes \cdots \otimes \rho_n$ be chosen according to the Plancherel measure on $\widehat{G}$. Then*

$$\Pr_{\rho, \{h^{(m)}\}}[X_H = 0] \le \frac{2\alpha}{\sqrt{n}} + \left(2^{-1/\alpha}|K|^{\alpha}\right)^{\sqrt{n}},$$

where H is the subgroup generated by the elements $h^{(1)}, \dots, h^{(t)}$ and X_H is defined as in (6). When $4|K|^t\sqrt{\log|K|} \le \sqrt{n}$, it follows that with probability at least

$$1 - \frac{\sqrt{2}}{\sqrt[4]{n \log |K|}} \tag{8}$$

a representation ρ selected according to the Plancherel measure has the property that

$$\Pr_{\{h^{(m)}\}}\left[\left\|\frac{1}{t}\sum_{m=1}^{t}\rho(h^{(m)})\right\|_{\mathrm{op}} = 1\right] \ge 1 - \frac{\sqrt{2}}{\sqrt[4]{n\log|K|}}. \tag{9}$$

Note that when $|K|^t\sqrt{\log|K|} = o(\sqrt{n})$ we may choose $\alpha = o(1/\sqrt{\log|K|})$ in the theorem above, which guarantees that $\Pr[X_H = 0] = o(1)$. Thus, in order to bring the expected norm of ρ down to $1-\epsilon$ for any constant $\epsilon > 0$, we need $t = \Omega(\log n) = \Omega(\log\log|G|)$ random elements.

For an element $g = (g_1, \dots, g_n) \in K^n$, let $\mathrm{supp}(g) = |\{i : g_i \ne 1\}|$ denote the size of the support of g. We extend the definition to subgroups: for a subgroup $L < K^n$, define

$$\mathrm{supp}(L) = \min_{\substack{g \in L \\ g \ne 1}} \mathrm{supp}(g).$$

An essential parameter of the proof below is $\mathrm{supp}(H)$, where H is generated by the collection $h^{(1)}, \dots, h^{(t)}$. We may estimate this quantity by observing that $\mathrm{supp}(H) \ge \mathrm{supp}(\tilde{H})$ and that $\mathrm{supp}(\tilde{H})$ is the size of the smallest equivalence class of $\sim_S$. Then we have the bound

$$\mathrm{supp}(H) \ge d(h^{(1)}, \dots, h^{(t)}).$$

We finally return to the proof of Theorem 2.

Proof of Theorem 2. Let $h^{(1)}, \dots, h^{(t)}$ be t elements chosen independently and uniformly at random from K^n, and let H denote the subgroup they generate. Additionally, let $\rho = \rho_1 \otimes \cdots \otimes \rho_n$ be a representation of K^n selected according to the Plancherel measure. Then with $d = d(h^{(1)}, \dots, h^{(t)})$ as above,

$$\begin{aligned}\Pr_{\rho, \{h^{(m)}\}}[X_H = 0] &\le \Pr_{\{h^{(m)}\}}\left[d < \frac{n}{2|K|^t}\right] + \Pr_{\rho, \{h^{(m)}\}}\left[X_H = 0 \;\middle|\; d \ge \frac{n}{2|K|^t}\right] \\ &\le \frac{4|K|^{2t}}{n} + \max_{\substack{\{h^{(m)}\} \text{ such that} \\ d \ge n/2|K|^t}} \Pr_{\rho}[X_H = 0],\end{aligned} \tag{10}$$

the second line following from Lemma 2.

As K has trivial center, all nontrivial conjugacy classes of K have size at least two. In particular, the centralizer $Z_g = \{h \mid g = h^{-1}gh\}$ is a proper subgroup of K. It follows that for an element $h \neq 1$ of K^n the conjugacy class h^{K^n} has cardinality $|h^{K^n}| \geq 2^{\mathrm{supp}(h)}$. If $d \geq n/2|K|^t$, then $\mathrm{supp}(H) \geq n/2|K|^t$ and

$$|H| \sum_{h \neq 1} \frac{1}{|h^{K^n}|} \leq |H|^2 \, 2^{-\mathrm{supp}(H)} \leq |K|^{2|K|^t} 2^{-n/2|K|^t},$$

by Lemma 1. Writing $2|K|^t \leq \alpha\sqrt{n}$, we have

$$|H| \sum_{h \neq 1} \frac{1}{|h^{K^n}|} \leq \left(2^{-1/\alpha}|K|^{\alpha}\right)^{\sqrt{n}}.$$

Combining equations (7) and (10) gives

$$\Pr_{\rho,\{h^{(m)}\}}[X_H = 0] \leq \frac{2\alpha}{\sqrt{n}} + \left(2^{-1/\alpha}|K|^{\alpha}\right)^{\sqrt{n}},$$

completing the proof. The bounds of (8) and (9) are achieved by setting $\alpha = 1/(2\sqrt{\log|K|})$, in which case

$$\frac{2\alpha}{\sqrt{n}} + \left(2^{-1/\alpha}|K|^{\alpha}\right)^{\sqrt{n}} \leq \frac{1}{\sqrt{n\log|K|}} + \left(\frac{1}{2\sqrt{2}}\right)^{\sqrt{n\log|K|}} \leq \frac{2}{\sqrt{n\log|K|}}. \qquad \square$$

Acknowledgments S.L. is supported by NSF CAREER award 1350481, and C.M. and A.R. are supported by NSF grant CCF-1247081.

References

[1] Noga Alon and Yuval Roichman. Random Cayley graphs and expanders. *Random Struct. Algorithms*, 5(2):271–285, 1994.

[2] Jean Bourgain and Alexander Gamburd. On the spectral gap for finitely-generated subgroups of SU(2). *Inventiones Mathematicae*, 171:83–121, 2008.

[3] Lecture notes for the 22nd McGill Invitational Workshop on Computational Complexity. 2010. http://www.cs.mcgill.ca/~denis/barbados.html

ECCC ISSN 1433-8092

http://eccc.hpi-web.de