GROUP REPRESENTATIONS THAT RESIST WORST-CASE SAMPLING

YUFEI ZHAO

Abstract. Motivated by expansion in Cayley graphs, we show that there exist infinitely many groups G with a nontrivial irreducible unitary representation whose average over every set of $o(\log\log|G|)$ elements of G has operator norm $1 - o(1)$. This answers a question of Lovett, Moore, and Russell, and strengthens their negative answer to a question of Wigderson.

The construction is the affine group of $\mathbb{F}_p$ and uses the fact that for every $A \subset \mathbb{F}_p \setminus \{0\}$, there is a set of size $\exp(\exp(O(|A|)))$ that is almost invariant under both additive and multiplicative translations by elements of A.

Let G be a finite group and ρ a unitary representation of G. For a subset $S \subset G$, we say that S is *ϵ-expanding* with respect to ρ if

$$\left\| \frac{1}{|S|} \sum_{g \in S} \rho(g) \right\|_{\mathrm{op}} \le 1 - \epsilon.$$

Otherwise, we say that ρ *ϵ-resists* S. We say that $S \subset G$ is *ϵ-expanding* if it is ϵ-expanding with respect to every non-trivial irreducible unitary representation of G, which is essentially the same as saying that the adjacency matrix of the Cayley graph on G generated by S has all eigenvalues, except the top one, bounded by $1 - \epsilon$ in absolute value. It is closely related to a more combinatorial notion of expansion in graphs via Cheeger's inequality.

By a theorem of Alon and Roichman [1] on eigenvalues of random Cayley graphs, for any group G, a random set of $C_\epsilon \log|G|$ group elements is ϵ-expanding with high probability. This bound is tight for abelian groups, up to constant factors. For example, when $G = (\mathbb{Z}/2\mathbb{Z})^n$, it takes $n = \log_2|G|$ elements simply to generate the group.

On the other hand, for certain families of "highly non-abelian" groups, including all non-abelian simple groups, a bounded number of generators suffices to obtain ϵ-expansion. In certain cases, such as $\mathrm{SL}_2(\mathbb{F}_p)$ [2], and more generally, any finite simple groups of Lie type of bounded rank [3], we know that $\{g, h, g^{-1}, h^{-1}\}$ is ϵ-expanding with high probability for uniformly random group elements g and h. See surveys [4, 6] for more on expansion.

Wigderson conjectured [8] in his 2010 Barbados lectures that there is some constant k so that for any finite group G and a nontrivial irreducible

The author was supported by an Esmée Fairbairn Junior Research Fellowship at New College, Oxford and a Research Fellowship at the Simons Institute, Berkeley.

unitary representation ρ, a list of k random elements of G is $(1/2)$-expanding with respect to ρ with probability at least $1/2$. Note that this is true for abelian groups, where every irreducible representation is one-dimensional, even though it takes $C \log |G|$ elements to expand with respect to every non-trivial irreducible representation simultaneously.

Wigderson's conjecture was disproved by Lovett, Moore, and Russell [5], who found an infinite family of groups such that, with high probability, a random subset of k elements does not expand at all with respect to a specific nontrivial irreducible representation. More specifically, they showed that if K is a fixed non-abelian group with trivial center (e.g., $K = S_3$), and ρ is a faithful irreducible unitary representation of ρ, then, $G = K^n$ with the irreducible representation $\rho^n = \rho \otimes \cdots \otimes \rho$ has the property that, as $n \to \infty$, provided that $k = o(\log n)$, one has

$$\mathbb{P}_{g_1,\dots,g_k \in G}\left[\left\|\frac{\rho^n(g_1) + \cdots + \rho^n(g_k)}{k}\right\|_{\mathrm{op}} = 1\right] = 1 - o(1).$$

Therefore, there are infinitely many groups G with a non-trivial irreducible unitary representation that resist a random set of size $o(\log \log |G|)$. Despite these negative results for random group elements, they asked whether there are constants k and ϵ such that for any group G and any nontrivial irreducible representation ρ, there exist some k elements of G that ϵ-expand respect to ρ. We answer this question in the negative.

Theorem 1. *For every $\epsilon > 0$, there is some $c_\epsilon > 0$ so that there exist infinitely many groups G with a nontrivial irreducible unitary representation ρ that ϵ-resists every $S \subset G$ with $|S| \le c_\epsilon \log \log |G|$, i.e.,*

$$\left\|\frac{\rho(g_1) + \cdots + \rho(g_k)}{k}\right\|_{\mathrm{op}} \ge 1 - \epsilon \tag{1}$$

for any $g_1, \dots, g_k \in G$ with $k \le c_\epsilon \log \log |G|$.

More succinctly, there exist groups G with a representation that $o(1)$-resists any set of $o(\log \log |G|)$ elements (the construction in [5] works for a random set, whereas ours works for all sets).

This gives a strong negative answer to Wigderson's question, as it shows that there no choice of a constant number of elements of G can ϵ-expand with respect to ρ, let alone a random choice.

We prove Theorem 1 by taking $G = \mathrm{Aff}(\mathbb{F}_p)$, the affine group of $\mathbb{F}_p$. Its elements are affine transformations $x \mapsto ax + b$, where $a \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$. Let ρ denote its standard representation with the trivial component removed. It is easy to check that ρ is a $(p-1)$-dimensional irreducible representation. Theorem 1 for $\mathrm{Aff}(\mathbb{F}_p)$ is an immediate consequence of the following result.

Theorem 2. *For every $\epsilon > 0$, there is some $C_\epsilon > 0$ so that for every prime p and every $A \subset \mathbb{F}_p \setminus \{0\}$, there exists some $X \subset \mathbb{F}_p$ with $|X| \le \exp(\exp(C_\epsilon |A|))$*

such that

$$|a \cdot X \setminus X| \le \epsilon |X| \quad \textit{and} \quad |(a+X) \setminus X| \le \epsilon |X| \quad \textit{for all } a \in A. \tag{2}$$

Here $a \cdot X := \{ax : x \in X\}$ and $a + X := \{a + x : x \in X\}$. Theorem 1 for $G = \mathrm{Aff}(\mathbb{F}_p)$ follows as a corollary of Theorem 2. Indeed, if S consists of affine maps $x \mapsto a_i x + b_i$, then take A to be the set of all nonzero elements that appears as a_i or b_i for some i. The claim (1) follows by considering the characteristic vector of X, appropriately normalized (noting $|X| \le p/2$ if $|S| \le c_\epsilon \log \log p$; we may need to rescale ϵ by a constant factor).

A proof of Theorem 2 was given by Terry Tao in a MathOverflow post [7].[1] We include the proof here for completeness.

Proof. Let $A = \{a_1, \dots, a_k\}$. Let $L = \lceil 1/\epsilon \rceil$. Consider the generalized arithmetic and geometric progressions

$$P = \{n_1 a_1 + \cdots + n_k a_k : 0 \le n_1, \dots, n_k < L\}, \text{ and}$$
$$Q = \{a_1^{n_1} \cdots a_k^{n_k} : 0 \le n_1, \dots, n_k < L\}.$$

Let

$$X = Q^{-1} \Bigg(\sum_{y \in Q} y \cdot P \Bigg),$$

i.e., the set of all elements that can be written as

$$y_0^{-1} \Bigg(\sum_{y \in Q} y x_y \Bigg)$$

for some choices of $y_0 \in Q$ and $x_y \in P$ for each $y \in Q$. It is easy to check (2), as $|(a+P) \setminus P| \le \epsilon |P|$ and $|(a \cdot Q) \setminus Q| \le \epsilon |Q|$ for any $a \in A$. We have $|X| \le |Q| |P|^{|Q|} \le L^k L^{k L^k} \le e^{(1/\epsilon)^{O(k)}}$. □

It remains an open question whether the bounds in Theorems 1 and 2 can be improved. We conjecture that they cannot.

Conjecture 3. *For every $\epsilon > 0$, there is some C_ϵ such that for any group G and a nontrivial irreducible unitary representation ρ, there is some $S \subset G$ with $|S| \le C_\epsilon \log \log |G|$ that is ϵ-expanding with respect to ρ.*

Conjecture 4. *For every $\epsilon > 0$, there is some $c_\epsilon > 0$ so that for every positive integer $k \le c_\epsilon \log \log p$ and prime p, there is some $A \subset \mathbb{F}_p \setminus \{0\}$ with $|A| = k$ such that every nonempty $X \subset \mathbb{F}_p$ satisfying (2) has $|X| \ge \exp(\exp(c_\epsilon k))$.*

Conjecture 5. *In the above conjectures, choosing S and A uniformly at random works with high probability.*

Note that Alon–Roichman theorem implies that Conjecture 3 is true if we replace $\log \log |G|$ by $\log |G|$ (by taking a random S). We do not know any further improvements.

[1] The author thanks Ben Green for pointing out [7] to him.

Acknowledgment. The author thanks Ben Green for discussion and Shachar Lovett for encouraging him to write up this result.

References

[1] N. Alon and Y. Roichman, *Random Cayley graphs and expanders*, Random Structures Algorithms **5** (1994), 271–284.

[2] J. Bourgain and A. Gamburd, *Uniform expansion bounds for Cayley graphs of* $\mathrm{SL}_2(\mathbb{F}_p)$, Ann. of Math. (2) **167** (2008), 625–642.

[3] E. Breuillard, B. Green, R. Guralnick, and T. Tao, *Expansion in finite simple groups of Lie type*, J. Eur. Math. Soc. (JEMS) **17** (2015), 1367–1434.

[4] S. Hoory, N. Linial, and A. Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. (N.S.) **43** (2006), 439–561 (electronic).

[5] S. Lovett, C. Moore, and A. Russell, *Group representations that resist random sampling*, Random Structures Algorithms **47** (2015), 605–614.

[6] A. Lubotzky, *Expander graphs in pure and applied mathematics*, Bull. Amer. Math. Soc. (N.S.) **49** (2012), 113–162.

[7] T. Tao, MathOverflow post at `https://mathoverflow.net/a/91675`.

[8] A. Wigderson, *Representation theory of finite groups, and applications*, Lecture notes for the 22nd McGill Invitational Workshop on Computational Complexity, 2010, available at `http://www.math.ias.edu/~avi/TALKS/Green_Wigderson_lecture.pdf` (last accessed May 11, 2017).

Mathematical Institute, Oxford OX2 6GG, United Kingdom
E-mail address: `yufei.zhao@maths.ox.ac.uk`