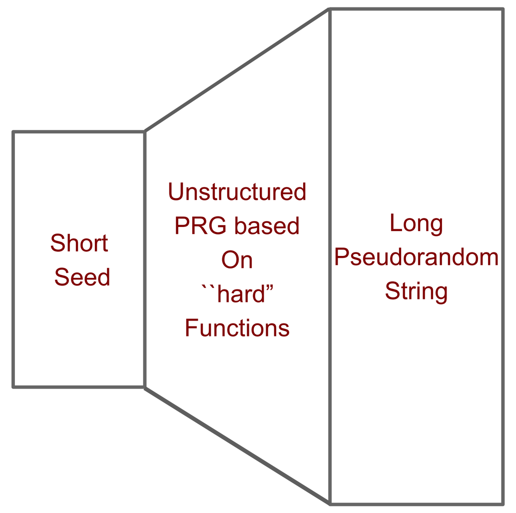
# Structured Derandomization: Pseudorandomness with Symmetries


THE UNIVERSITY OF CHICAGO

Tushant Mittal


## Central message – Pseudorandom objects with algebraic structure (symmetry) are useful!

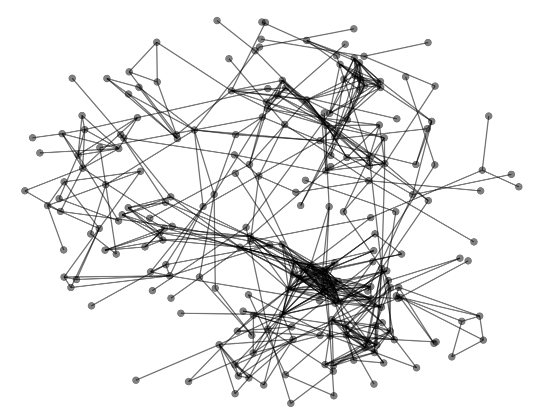
"Black-box" pseudorandom generator




Hard to use it beyond direct derandomization

Graph Structure →

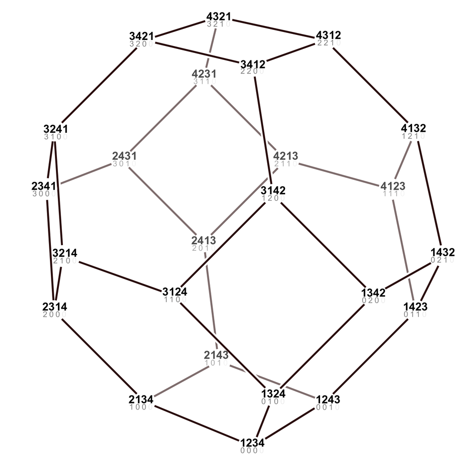
"Pseudorandom" graph ( **Expander** ) Image -[Iri15]



Added graph Structure useful to build worst-case inputs, codes, etc..

Symmetry →

Graph with group symmetry (Cayley Graph) Image -[Pie]



Algebraic structure (symmetry) is useful too!

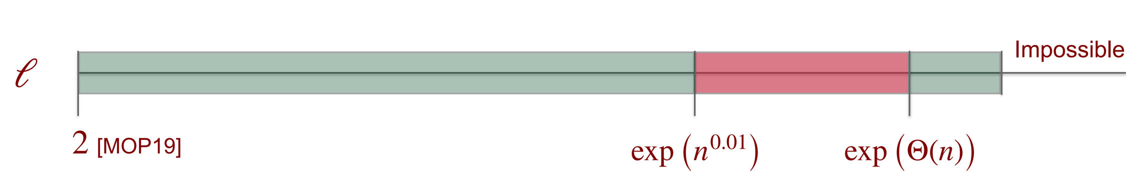
## Quantum LDPC Codes via symmetric expander graphs [Jeronimo–M–O'Donnell–Paredes–Tulsiani ITCS'22]

Motivation Recent breakthroughs show that one can construct **large distance quantum LDPC codes** using symmetric expander graphs.

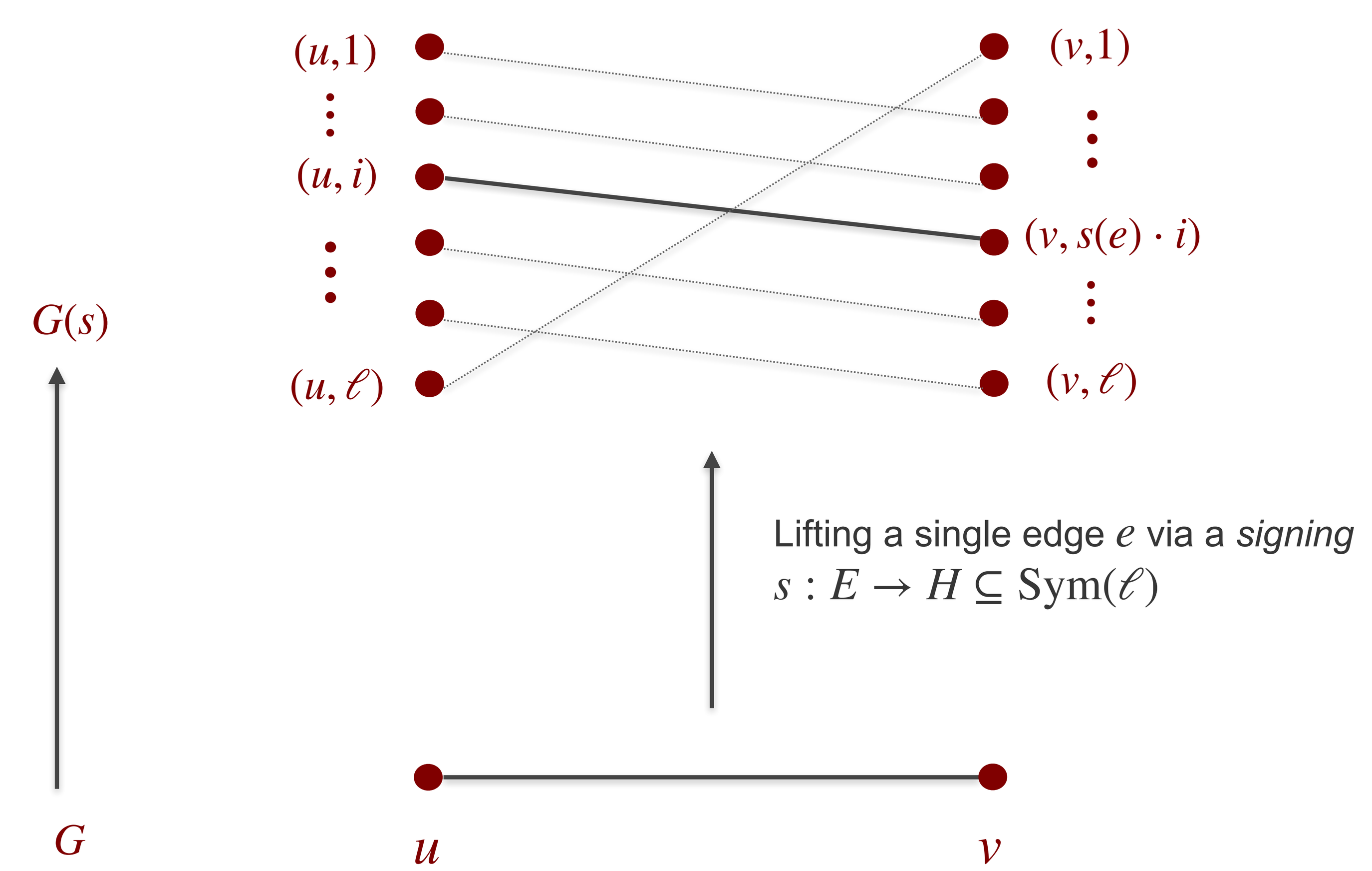
Main Result We show that for any Abelian group $G$, we can deterministically construct expanding minimal graphs having symmetries of $G$.

Techniques We use the framework of *graph lifts*, introduced by Bilu and Linial. We strengthen the techniques of [MOP19] that analyze $(Z_2, 2)$-lifts to tackle $(Z_\ell, \ell)$ lifts for exponentially large $\ell$.

Applications Via these connections, our construction yields explicit **good quasi-cyclic LDPC codes**, and quantum LDPC codes of almost-linear distance $(n/\log n)$.




Our work covers the green region.




Lift of a graph based on a group $H \subseteq \mathrm{Sym}(\ell)$.

## References


[GGOW16] Ankit Garg, Leonid Gurvits, Rafael Oliveira, and Avi Wigderson. A Deterministic Polynomial Time Algorithm for Non-commutative Rational Identity Testing. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 109–117, 2016. doi:10.1109/FOCS.2016.95.

[IQS18] Gábor Ivanyos, Youming Qiao, and K. V. Subrahmanyam. Constructive non-commutative rank computation is in deterministic polynomial time. *Comput. Complex.*, 27(4):561–593, 2018. doi:10.1007/s00037-018-0165-7.

[Iri15] Alexander Iriza. Enumeration and random generation of unlabeled classes of graphs: A practical study of cycle pointing and the dissymmetry theorem. *CoRR*, abs/1511.06037, 2015. URL: http://arxiv.org/abs/1511.06037, arXiv:1511.06037.

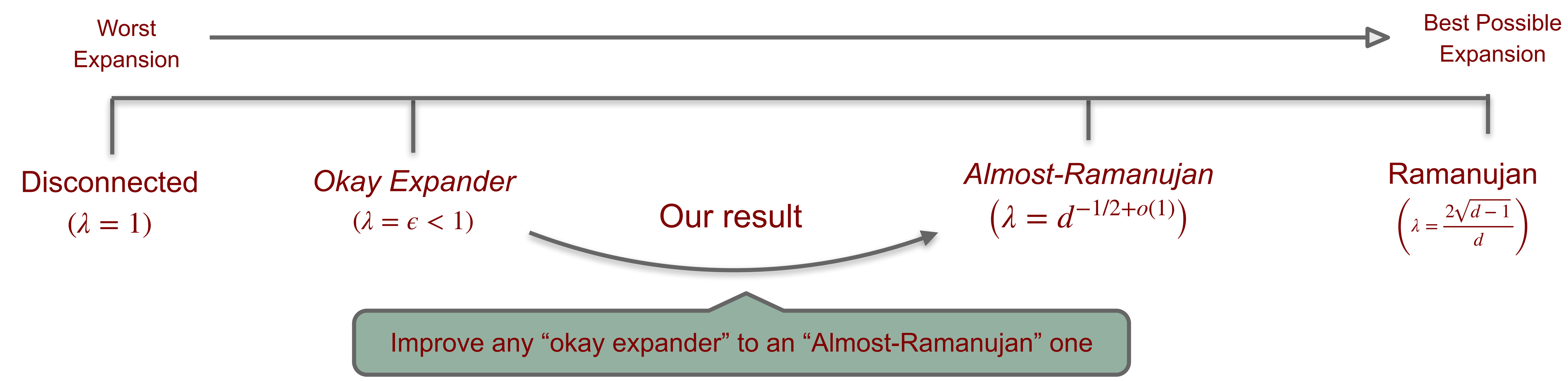
[MOP19] Sidhanth Mohanty, Ryan O'Donnell, and Pedro Paredes. Explicit near-Ramanujan graphs of every degree. *arXiv:1909.06988 [cs, math]*, October 2019. arXiv:1909.06988.


## Amplifying general expanders via algebraic ones [Jeronimo–M–Roy–Wigderson FOCS'22]

Main Result Given any family of $d$-regular expanders, we can deterministically convert it into an almost-Ramanujan one while preserving locality.

Techniques The general result is obtained by proving the seemingly special case of Cayley graphs over the symmetric group! We build upon, and vastly generalize, the breakthrough work of [Ta-Shma STOC'17] which can be seen as the special case when the group is $\mathbb{Z}_2^n$. We extend their techniques to handle **all finitely generated groups** and as a corollary, make progress on a question posed by Breuillard and Lubotzky.

Applications The first construction of explicit **almost-Ramanujan quantum expanders**, improved constructions of **dimension expanders** and **monotone expanders**. Our results generalize to finitely generated groups and arbitrary large representations yielding improved Kazhdan constants.




## Algorithm Design via Lie algebraic structure [Ivanyos–M–Qiao ITCS'22]

Setup **Symbolic Determinant Identity Testing** (SDIT) is the following decision problem – Given matrices $\{A_1, \cdots, A_n\}$,

Does the linear space $\mathcal{A} = \mathrm{span}\,(A_1, \cdots, A_n)$ contain a full-rank matrix?

The goal is to derandomize the natural randomized algorithm. It is a special case of the Polynomial Identity Testing (PIT) problem which is connected to various complexity theory conjectures.

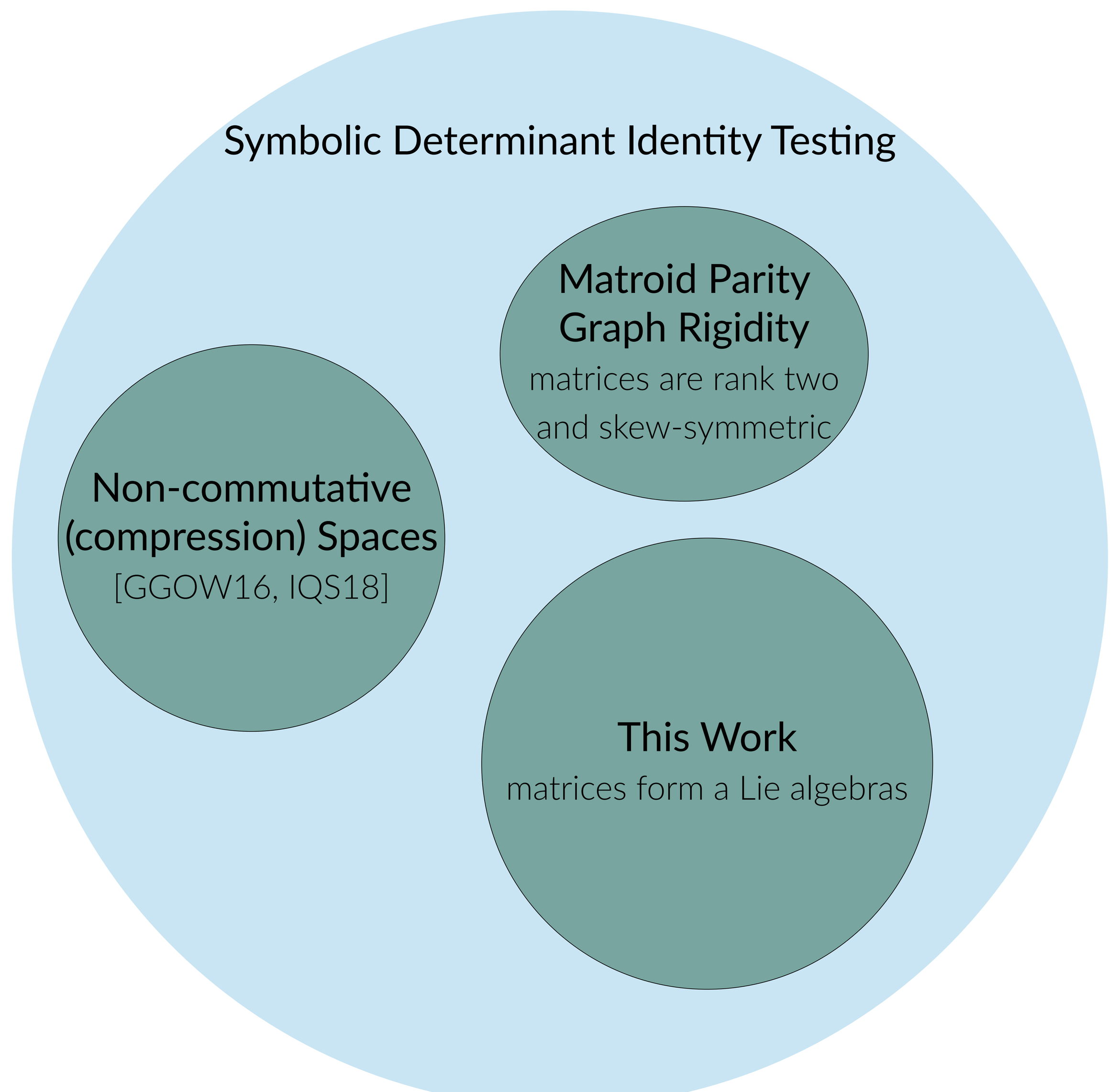
Prior Work Polynomial time algorithms exist in special cases when the matrices have

(i) Combinatorial structure – graph rigidity and matroid parity,

(ii) Geometric structure –matrices form a compression space.

Main Result We give a polynomial-time deterministic algorithm when the input $\mathcal{A}$ has additional algebraic structure (Lie algebra).

Techniques The key idea behind the null-cone result is the correspondence between Lie-groups and Lie algebras. To design the algorithm, we utilize the fact that every Lie algebra has a very special sub-algebra, called the *Cartan algebra*.




Current landscape of (infinite) families for which the problem has been derandomized.


http://mittaltushant.github.io

tushant@uchicago.edu