# Incompressibility and spectral gaps of random circuits

arXiv: 2406.07478

Chi-Fang Chen, Jeongwan Haah, Jonas Haferkamp,
Yunchao Liu, Tony Metger, and Xinyu (Norah) Tan

Jan 30, 2025

# Outline

**Incompressibility**

- “random circuits form $t$-designs with $O(t)$ gates” implies “random circuits are incompressibile”

**Spectral gaps**

- “random circuits form $t$-designs with $O(t)$ gates”

**Kassabov’s expander**

- Backbone: an efficient implementation of Kassabov’s expander on the alternating group

# Outline

**Incompressibility**

- “random circuits form $t$-designs with $O(t)$ gates” implies “random circuits are incompressibile”

**Spectral gaps**

- “random **reversible** circuits form **permutation** $t$-designs with $O(t)$ gates” implies
- “random **quantum** circuits form **unitary** $t$-designs with $O(t)$ gates”

**Kassabov’s expander**

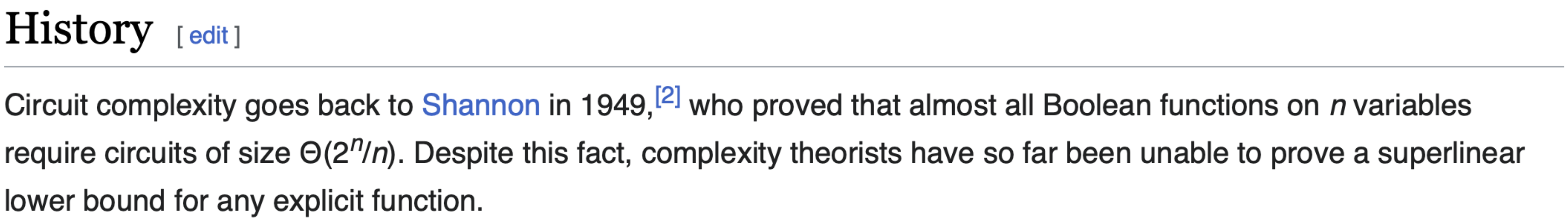
- Backbone: an efficient implementation of Kassabov’s expander on the alternating group

# What does “a circuit is incompressibile” mean?

- The **circuit complexity** of $U$, $C_\delta(U) :=$ the minimum number of “small” gates to implement $U$ approximately (in operator norm).
  - A unitary operator $U \in \mathrm{U}(2^n)$
  - A Boolean function $f\colon\{0,1\}^n \to \{0,1\}$
  - A reversible classical circuit $\pi \in \mathrm{Sym}(2^n)$ or $\mathrm{Alt}(2^n)$
- Suppose I tell you that $U$ can be constructed with gates $U_1, U_2, \cdots, U_L$.
  - i.e., $U = U_L \cdots U_2 U_1$ (a circuit description).
- Can you tell me if $U$ can be compressed?
  - i.e., does there exist another decomposition of $U$ using $< L$ gates?
  - If $U$ cannot be compressed, then $C_\delta(U) = L$.

# How hard is circuit compression?

- Proving circuit lower bounds for specific functions is an extremely hard problem!
- An easier problem: what is the circuit complexity of a uniformly random circuit?



## History [ edit ]

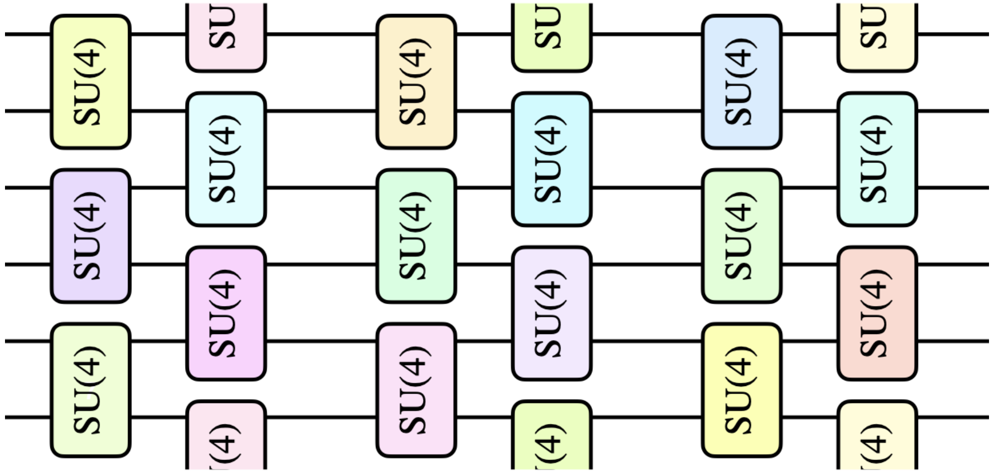
Circuit complexity goes back to Shannon in 1949,[2] who proved that almost all Boolean functions on $n$ variables require circuits of size $\Theta(2^n/n)$. Despite this fact, complexity theorists have so far been unable to prove a superlinear lower bound for any explicit function.

---- "A random function is complex."

- Similarly…
  - A uniformly random $2^n \times 2^n$ permutation is complex.
  - A Haar random $2^n \times 2^n$ unitary is complex.

# An intermediate question…

- Suppose I give you a **random** circuit $U$ generated by $L$ gates, can you compress $U$?
- Random circuit (a random walk model)
  - The qubit/bit connectivity can be arbitrary (e.g. brickwork, all-to-all connection, …)
  - At each step
    - Quantum world: apply a Haar random 2-qubit gate
    - Classical world: apply a uniformly random 3-bit permutation gate



# An intermediate question…

- Suppose I give you a **random** circuit $U$ generated by $L$ gates, can you compress $U$?
- Random circuit (a random walk model)
  - The qubit/bit connectivity can be arbitrary (e.g. brickwork, all-to-all connection, …)
  - At each step
    - Quantum world: apply a Haar random 2-qubit gate
    - Classical world: apply a uniformly random 3-bit permutation gate
- **Theorem 1**: A random quantum circuit on $n$ qubits with $\boldsymbol{L \leq O(2^{n/2})}$ gates **cannot** be implemented approximately by any quantum circuit with fewer than $\boldsymbol{L/\mathrm{poly}(n)}$ gates.

---- "Random quantum circuits are incompressibile."

# Brown-Susskind conjecture

- **Theorem 1**: A random quantum circuit on $n$ qubits with $\boldsymbol{L \leq O(2^{n/2})}$ gates **cannot** be implemented approximately by any quantum circuit with fewer than $\boldsymbol{L/\mathrm{poly}(n)}$ gates.

---- "Linear growth of robust quantum circuit complexity"

$$U(t) = e^{-iHt}$$

$H$: a generic time-independent local Hamiltonian (that models **black holes**)

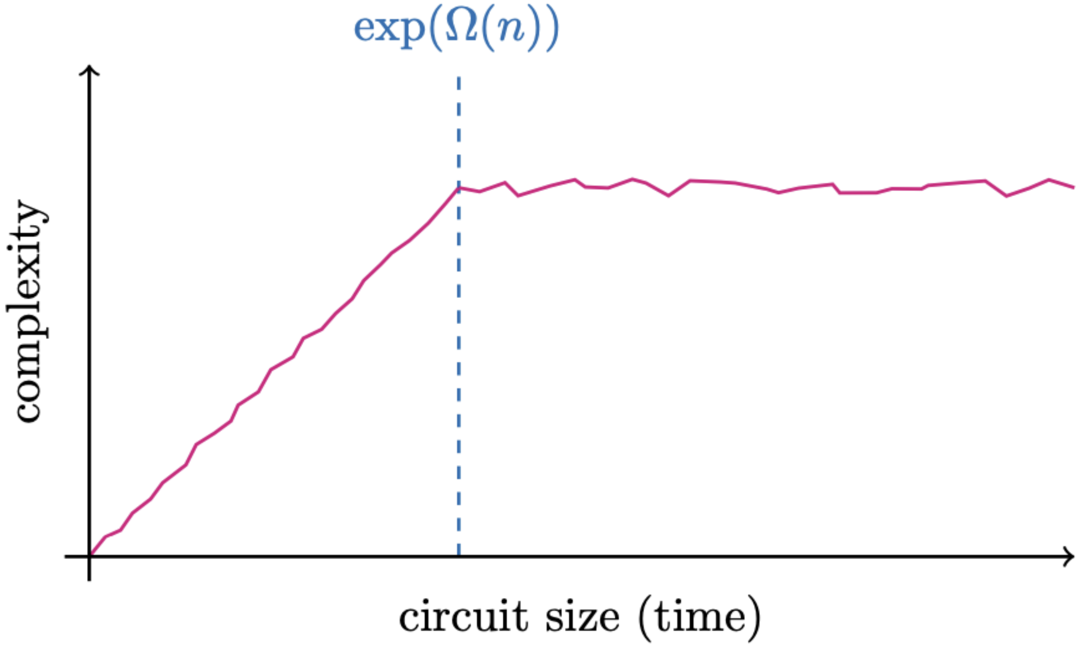
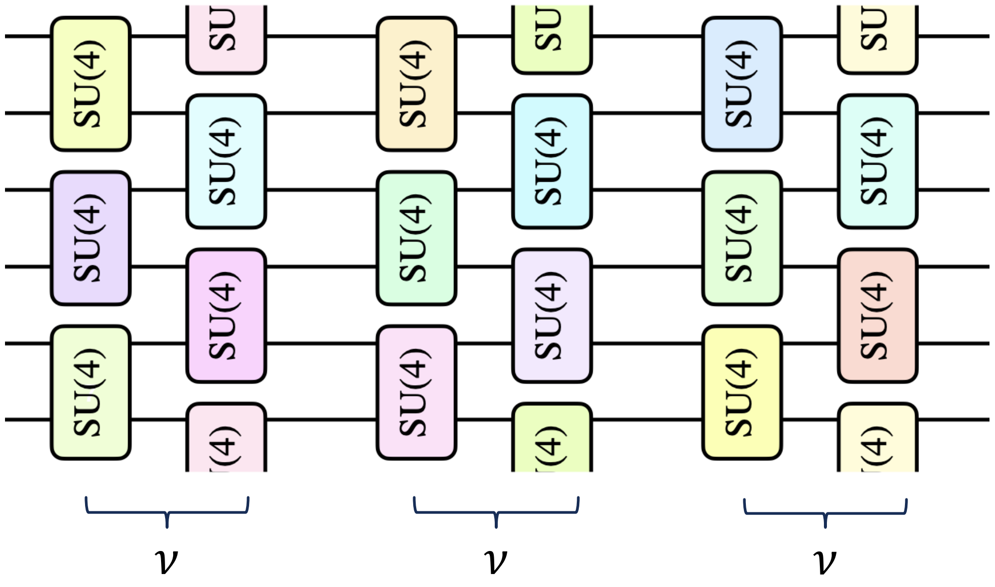


Figure: 1912.04297

# What is a unitary $t$-design?

- A $\epsilon$-approximate unitary $t$-design is a probability distribution on $\mathrm{U}(2^n)$
  - Statistically indistinguishable from the Haar measure
  - $t$-th moment of this distribution $\approx_\epsilon$ $t$-th moment of the Haar measure

- A random circuit with $L$ i.i.d. gates $U_i \sim \nu$



As $L \to \infty$, $\underbrace{\nu * \nu * \cdots * \nu}_{L \text{ times}} \to \mu_{\text{Haar}}$

A recipe to create a unitary $t$-design using the random circuit model

- Specify a generating set that is universal
- Calculate the convergence rate $L \coloneqq L(n, t)$

# Incompressibility follows from “linear” unitary *t*-designs

- **Lemma**: A random unitary sampled from a $t$-design has circuit complexity $\Omega(t)$.
- If your $\boldsymbol{t}$-design can be constructed using $\boldsymbol{O(n^a t)}$ random gates,
  - i.e., a random circuit $U$ with $\boldsymbol{L}$ gates is a $\boldsymbol{\Omega(L/n^a)}$-design.
  - By lemma, w.h.p., $C_\delta(U) = \Omega(L/n^a)$

- **Theorem 2** (linear unitary $t$-designs):

For any $n \geq 2$, $\boldsymbol{t \leq \Theta(2^{n/2})}$, 2-local all-to-all random quantum circuits with $\boldsymbol{L = O(tn^4)}$ random gates form approximate unitary $\boldsymbol{t}$-designs with a constant **multiplicative error**.

$O(t \cdot \mathrm{poly}(n))$ also holds for any connected architecture and any universal generating set (containing inverses and algebraic matrix entries).

# $t$-wise independent permutations (= permutation $t$-designs)

- A distribution $\nu$ on $\mathrm{Alt}(2^n)$ is $t$-wise independent permutations if
  - For any distinct bitstrings, $x_1, \cdots, x_t \in \{0,1\}^n$
  - Sample $\boldsymbol{\sigma} \sim \boldsymbol{\nu}$, the distribution of $(\sigma(x_1), \cdots, \sigma(x_t))$ is the same as if $\boldsymbol{\sigma} \sim_{\mathbf{unif}} \mathbf{Alt}(2^n)$

- For any distinct bitstrings $x_1, \cdots, x_t \in \{0,1\}^n$ and any distinct bitstrings $y_1, \cdots, y_t \in \{0,1\}^n$,
$$\Pr_{\sigma \sim \nu}[\sigma(x_1) = y_1, \cdots, \sigma(x_t) = y_t] = \Pr_{\sigma \sim \mathrm{unif}}[\sigma(x_1) = y_1, \cdots, \sigma(x_t) = y_t]$$

- $\mathbb{E}_{\sigma \sim \nu}\ \sigma^{\otimes t} = \mathbb{E}_{\sigma \sim \mathrm{unif}}\ \sigma^{\otimes t}$

# Multiplicative-error designs from spectral gaps

- Given a distribution $\nu$ on $\mathrm{Alt}(2^n)$, the **spectral gap** for $\nu$ is

$$\mathrm{gap}(\nu, t) := 1 - \underbrace{\left\| \mathbb{E}_{\sigma\sim\nu}\, \sigma^{\otimes t} - \mathbb{E}_{\sigma\sim\mathrm{unif}}\, \sigma^{\otimes t} \right\|_\infty}_{\text{The } \textbf{essential norm} \text{ of } \nu \,=\, g(\nu,t)}$$

- $g(\nu^{*L}, t) \leq g(\nu, t)^L$
- **Lemma**: $\nu^{*L}$ is a permutation $t$-design with **multiplicative error** $\epsilon$ when

$$L = O(\mathrm{gap}(\nu, t)^{-1} \cdot (nt + \log(1/\epsilon)))$$

**Independent from $t$!**

- To prove our main theorems, it suffices to show that $\mathrm{gap}(\nu, t) = 1/\mathrm{poly}(n)$.

# Multiplicative-error designs from spectral gaps

- Given a distribution $\nu$ on $\mathrm{SU}(2^n)$, the **spectral gap** for $\nu$ is

$$\mathrm{gap}(\nu, t) \coloneqq 1 - \underbrace{\left\| \mathbb{E}_{U\sim\nu}(U \otimes \overline{U})^{\otimes t} - \mathbb{E}_{U\sim\mathrm{Haar}}(U \otimes \overline{U})^{\otimes t} \right\|_\infty}_{\text{The } \textbf{essential norm} \text{ of } \nu \coloneqq g(\nu, t)}$$

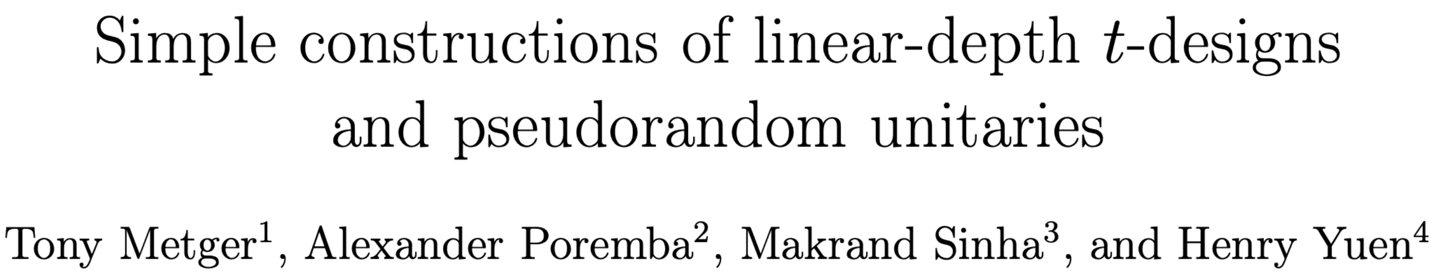
- $g(\nu^{*L}, t) \leq g(\nu, t)^L$
- **Lemma**: $\nu^{*L}$ is a unitary $t$-design with **multiplicative error** $\epsilon$ when

$$L = O\left(\mathrm{gap}(\nu, t)^{-1} \cdot (nt + \log(1/\epsilon))\right)$$

**Independent from $t$!**

- To prove our main theorems, it suffices to show that $\mathrm{gap}(\nu, t) = 1/\mathrm{poly}(n)$.

# “PFC” ensemble



Simple constructions of linear-depth $t$-designs and pseudorandom unitaries

Tony Metger[1], Alexander Poremba[2], Makrand Sinha[3], and Henry Yuen[4]

arXiv: 2404.12647

### C: A random Clifford

### F: A random phase gate

$$F = \sum_{v \in \{0,1\}^n} (-1)^{f(v)} |v\rangle\langle v|$$

where $f: \{0,1\}^n \to \{0,1\}$

### P: A random permutation

$$P = \sum_{v \in \{0,1\}^n} |\pi(v)\rangle\langle v|$$

where $\pi \in \mathrm{Sym}(2^n)$

- [MPSY24]: The “PFC” ensemble forms an **additive-error** $t$-design for any $t \leq O(2^{n/2})$.

# Let us modify “PFC”

- [MPSY24]: The “PFC” ensemble forms an **additive-error** $t$-design for any $t \leq O(2^{n/2})$.

💡 To prove ***t*-independent spectral gaps** for **2-local** random quantum circuits:

1. Show an initial spectral gap for “PFC”
2. Break “PFC” into “baby steps of local gates”
3. Analyze the spectral gap of one “baby step”
4. Relate it to the spectral gap of 2-local random quantum circuits

- **Lemma**: The spectral gap for the “**CPFPC**” ensemble is $\Omega(\frac{t}{2^{n/2}})$.

# Step 2

1. Show an initial spectral gap for “CPFPC”
2. **Break “CPFPC” into “baby steps of local gates”**
3. Analyze the spectral gap of one “baby step”
4. Relate it to the spectral gap of 2-local random quantum circuits

- C: Replace with any 2-design with a constant multiplicative error.
- P: Kassabov’s expander on the alternating group.
- F: Mixing in an abelian group is slow…
  - Let us get rid of F!
  - Simulate $F$ by $PZ_1P^{-1}$

# Step 3: The “CPZPC” ensemble

1. Show an initial spectral gap for “CPFPC”
2. Break “CPFPC” into “baby steps of local gates”
3. **Analyze the spectral gap of one “baby step”**
4. Relate it to the spectral gap of 2-local random quantum circuits

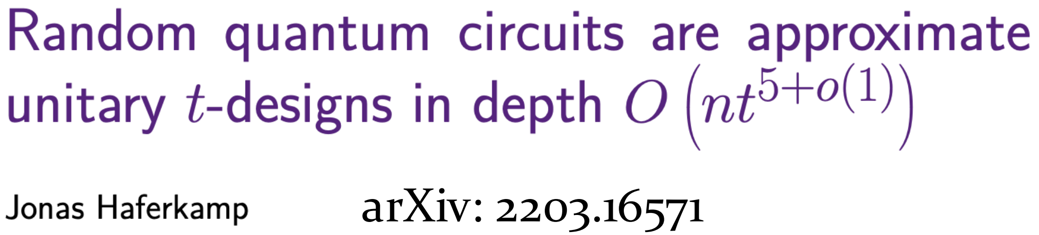
A baby step

- C: $O(n)$ layers of brickwork random 2-qubit gates
- P: $O(n^3)$ random 3-qubit gates due to Kassabov (roughly)
- Z: one fixed 1-qubit Pauli Z
- P: $O(n^3)$ random 3-qubit gates due to Kassabov (roughly)
- C: $O(n)$ layers of brickwork random 2-qubit gates

**Lemma**: For $t \leq O(2^{n/2})$, the spectral gap of “a baby step” is constant.

# Step 4

1. Show an initial spectral gap for “CPFPC”
2. Break “CPFPC” into “baby steps of local gates”
3. Analyze the spectral gap of one “baby step”
4. **Relate it to the spectral gap of 2-local random quantum circuits**



Random quantum circuits are approximate unitary $t$-designs in depth $O\left(nt^{5+o(1)}\right)$

Jonas Haferkamp

arXiv: 2203.16571

Detectability lemma

Quantum union bound

# Step 4

1. Show an initial spectral gap for “CPFPC”
2. Break “CPFPC” into “baby steps of local gates”
3. Analyze the spectral gap of one “baby step”
4. **Relate it to the spectral gap of 2-local random quantum circuits**

**Lemma**: Let $G_1, G_2, \cdots, G_m$ be subgroups of $U(2^n)$, each of which acts on only constantly many qubits. Then,

$$\mathrm{gap}(\mathrm{unif}(G_1) * \mathrm{unif}(G_2) * \cdots * \mathrm{unif}(G_m), t) \geq \delta$$

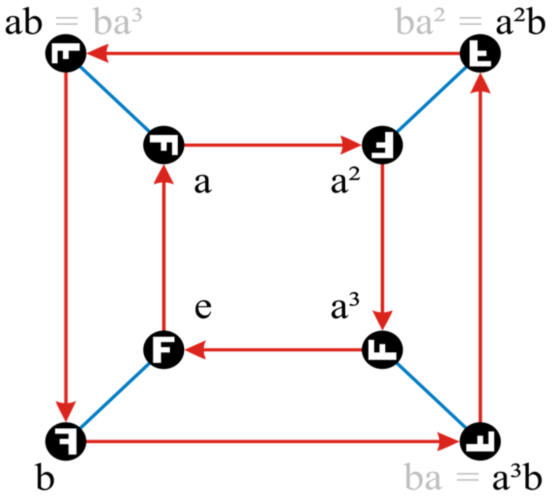
$$\Downarrow$$

$$\mathrm{gap}(\text{“2−local all−to−all”}, t) \geq \Omega(\delta/m)$$

**Theorem**: For $t \leq O(2^{n/2})$, the spectral gap of 2-local all-to-all random quantum circuits is $\Omega(n^{-3})$.

# An expander on the alternating group

- An infinite family of $\{\, (\mathrm{Alt}(N),\ S_N = \text{a generating set for } \mathrm{Alt}(N)) \,\}_N$
- The family of the associated *Cayley graphs* is "expanding".

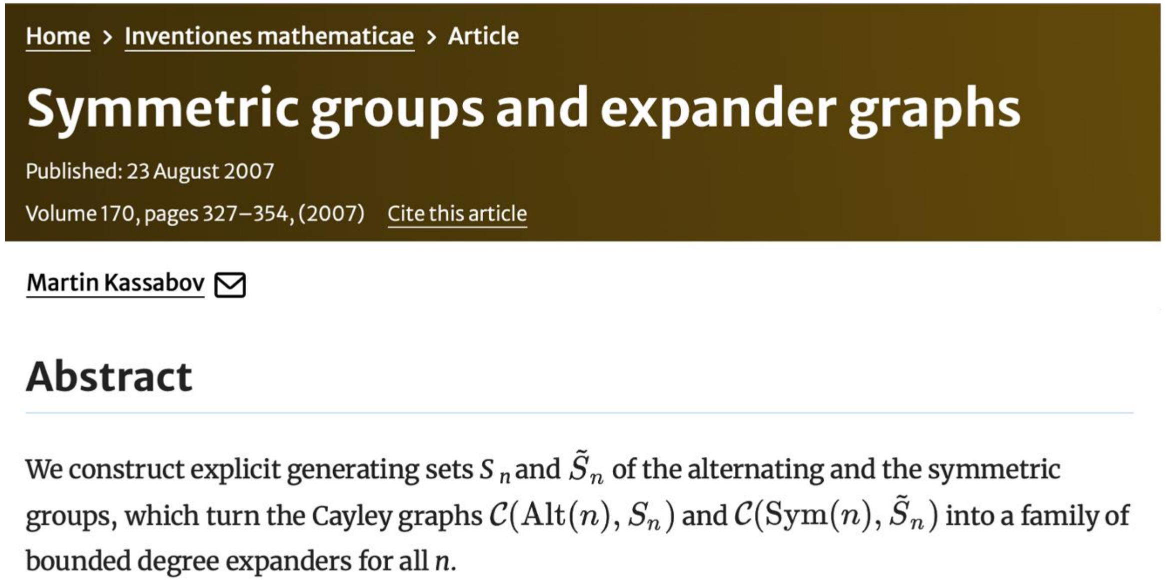


Cayley graph of the dihedral group $D_4$ generated by $a$ and $b$

Figure: Wikipedia

- The spectral gaps of the associated *adjacency matrices* are "nicely" bounded.
- $1 - \left\| \mathbb{E}_{P\sim S_N} P^{\otimes t} - \mathbb{E}_{P\sim \mathrm{Alt}(N)} P^{\otimes t} \right\|_\infty \geq \Omega(|S_N|^{-1})$

# Two papers by Martin Kassabov



Home > Inventiones mathematicae > Article

## Symmetric groups and expander graphs

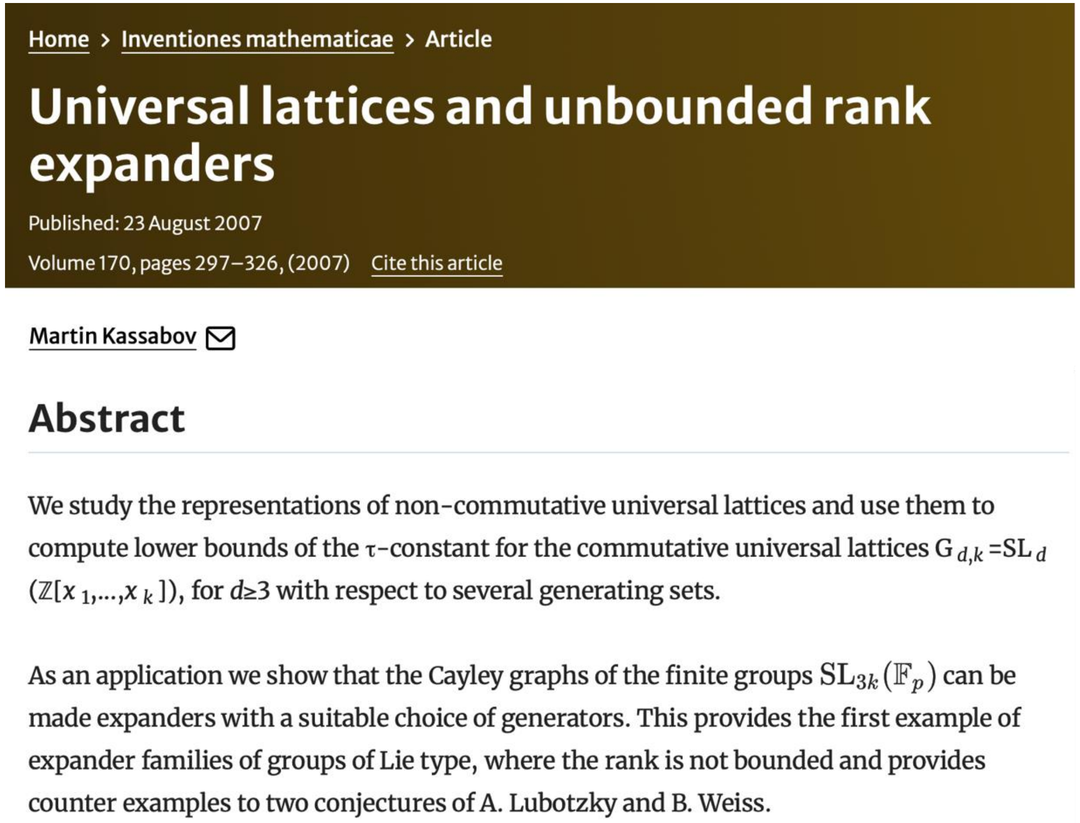
Published: 23 August 2007

Volume 170, pages 327–354, (2007) Cite this article

Martin Kassabov

### Abstract

We construct explicit generating sets $S_n$ and $\tilde{S}_n$ of the alternating and the symmetric groups, which turn the Cayley graphs $\mathcal{C}(\mathrm{Alt}(n), S_n)$ and $\mathcal{C}(\mathrm{Sym}(n), \tilde{S}_n)$ into a family of bounded degree expanders for all $n$.



Home > Inventiones mathematicae > Article

## Universal lattices and unbounded rank expanders

Published: 23 August 2007

Volume 170, pages 297–326, (2007) Cite this article

Martin Kassabov

### Abstract

We study the representations of non-commutative universal lattices and use them to compute lower bounds of the τ-constant for the commutative universal lattices $G_{d,k}=SL_d(\mathbb{Z}[x_1,\dots,x_k])$, for $d\geq 3$ with respect to several generating sets.

As an application we show that the Cayley graphs of the finite groups $\mathrm{SL}_{3k}(\mathbb{F}_p)$ can be made expanders with a suitable choice of generators. This provides the first example of expander families of groups of Lie type, where the rank is not bounded and provides counter examples to two conjectures of A. Lubotzky and B. Weiss.

But can the generating set be “efficiently implemented”?

So, the spectral gaps are constant.

An explicit generating set of constant size that is rapidly mixing, of $\mathrm{Alt}(N)$ for each $N$.

# Efficient implementation of the generators

- An infinite family of $\left\{ \left(\mathrm{Alt}(N),\ S_N = \text{a generating set for } \mathrm{Alt}(N)\right) \right\}_N$
- For each $N = 2^n$, can each generator in $S_N$ be implemented with $\mathrm{poly}(n)$ "simple" gates?

- **Theorem** (Kassabov's generators are short reversible circuit):

For any $n \geq 1$, each generator in $S_{2^n}$ can be implemented on $n$ bits using $O(n)$ NOT, controlled-NOT, and Toffoli gates without any ancilla bit.

# Summary

- We prove that random quantum circuits form multiplicative-error unitary $t$-designs with $O(t \cdot \mathrm{poly}(n))$ gates
  - Convert the "PFC" ensemble into "baby steps of local gates"
  - Prove a $t$-independent spectral gap for a baby step
  - "P" is based on an efficient implementation of Kassabov's expander on the alternating group
- Linear unitary $t$-designs → linear growth of robust quantum circuit complexity (aka. random circuits are incompressible)