Pseudorandom Approximate Unitary Designs

Or one way to sample uniformly random quantum circuits

Pedro Paredes

PCMI Research Talk

July 24, 2023

Joint work with:

Ryan O'Donnell
CMU

Rocco Servedio
Columbia University

Consider $\mathrm{U}(N)$ — the group of $N \times N$ unitary matrices

Consider $\mathrm{U}(N)$ — the group of $N \times N$ unitary matrices

Question:

How to "efficiently" sample from Haar measure on $\mathrm{U}(N)$?

Consider $\mathrm{U}(N)$ — the group of $N \times N$ unitary matrices

Question:

How to "efficiently" sample from uniform measure on $\mathrm{U}(N)$?

Consider $\mathrm{U}(N)$ — the group of $N \times N$ unitary matrices

Question:

How to "efficiently" sample from uniform measure on $\mathrm{U}(N)$?

(or how to sample uniformly random quantum circuits)

Consider $\mathrm{U}(N)$ — the group of $N \times N$ unitary matrices

Question:

How to "efficiently" sample from uniform measure on $\mathrm{U}(N)$?

(or how to sample uniformly random quantum circuits)

Note that "morally" we need about $\widetilde{\Theta}(N^2)$ bits of entropy

Consider $\mathrm{Sym}(N)$ — the group of $N \times N$ permutation matrices

Question:

How to "efficiently" sample uniformly from $\mathrm{Sym}(N)$?

(or how to sample uniformly random classical circuits)

Note that "morally" we need about $\log(N!) = \widetilde{\Theta}(N)$ bits of entropy

Consider $\mathrm{Sym}(N)$ — the group of $N \times N$ permutation matrices

Question:

How to "efficiently" sample uniformly from $\mathrm{Sym}(N)$?

(or how to sample uniformly random classical circuits)

Note that "morally" we need about $\log(N!) = \widetilde{\Theta}(N)$ bits of entropy

Goal:

A distribution ν on $\mathrm{U}(N)$ "efficiently" samplable with $\ll N$ bits of entropy, such that:

$$\nu \overset{\text{first } k \text{ moments}}{\approx} \mathrm{U}(N)$$

Goal:

A distribution ν on $\mathrm{U}(N)$ "efficiently" samplable with $\ll N$ bits of entropy, such that:

$$\nu \overset{\text{first } k \text{ moments}}{\approx} \mathrm{U}(N)$$

Formally we will consider:

Definition (ε-approximate unitary k-design):

$$\left\| \mathop{\mathbf{E}}_{\boldsymbol{X} \sim \nu} \left[\boldsymbol{X}^{\otimes k} \otimes (\overline{\boldsymbol{X}})^{\otimes k} \right] - \mathop{\mathbf{E}}_{\boldsymbol{X} \sim \mathrm{U}(N)} \left[\boldsymbol{X}^{\otimes k} \otimes (\overline{\boldsymbol{X}})^{\otimes k} \right] \right\|_1 \leqslant \varepsilon$$

Goal:

A distribution ν on $\mathrm{U}(N)$ "efficiently" samplable with $\ll N$ bits of entropy, such that:

$$\nu \overset{\substack{\text{first } k \\ \text{moments}}}{\approx} \mathrm{U}(N)$$

Formally we will consider:

Definition (ε-approximate unitary k-design):

$$\left\| \mathop{\mathbf{E}}_{\boldsymbol{X} \sim \nu} \left[\boldsymbol{X}^{\otimes k} \otimes (\overline{\boldsymbol{X}})^{\otimes k} \right] - \mathop{\mathbf{E}}_{\boldsymbol{X} \sim \mathrm{U}(N)} \left[\boldsymbol{X}^{\otimes k} \otimes (\overline{\boldsymbol{X}})^{\otimes k} \right] \right\|_1 \leqslant \varepsilon$$

Intuition: $\boldsymbol{X}^{\otimes k} \otimes (\overline{\boldsymbol{X}})^{\otimes k}$ is a $N^{2k} \times N^{2k}$ matrix
entries are products of k entries of $\boldsymbol{X}$ and their conjugates

Intuition: entries are degree $2k$ monomials in entries of $\boldsymbol{X}$

Consider the notion of classical expanders

Consider the notion of classical expanders

$$\left\| \mathop{\mathbf{E}}_{\boldsymbol{\pi} \sim \nu} [B(\boldsymbol{\pi})] - \mathop{\mathbf{E}}_{\boldsymbol{\pi} \sim \mathrm{Sym}(N)} [B(\boldsymbol{\pi})] \right\|_{\mathrm{op}} \leqslant \lambda$$

Where $B(\boldsymbol{\pi}) :=$ permutation matrix defined by $\boldsymbol{\pi}$

Consider the notion of classical expanders

$$\left\| \underbrace{\mathop{\mathbf{E}}_{\boldsymbol{\pi} \sim \nu} [B(\boldsymbol{\pi})]}_{\text{Adjacency Matrix}} - \underbrace{\mathop{\mathbf{E}}_{\boldsymbol{\pi} \sim \mathrm{Sym}(N)} [B(\boldsymbol{\pi})]}_{\text{1-eigenspace}} \right\|_{\mathrm{op}} \leqslant \lambda$$

Where $B(\boldsymbol{\pi}) :=$ permutation matrix defined by $\boldsymbol{\pi}$

Consider the notion of classical expanders

$$\left\| \underbrace{\mathop{\mathbf{E}}_{\boldsymbol{\pi}\sim\nu}[B(\boldsymbol{\pi})]}_{\text{Adjacency Matrix}} - \underbrace{\mathop{\mathbf{E}}_{\boldsymbol{\pi}\sim \mathrm{Sym}(N)}[B(\boldsymbol{\pi})]}_{\text{1-eigenspace}} \right\|_{\mathrm{op}} \leqslant \lambda$$

Where $B(\boldsymbol{\pi}) :=$ permutation matrix defined by $\boldsymbol{\pi}$

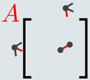
d-regular graph $\equiv$ Sum of d permutation matrices

Consider the notion of classical expanders

$$\left\| \underbrace{\mathop{\mathbf{E}}_{\boldsymbol{\pi}\sim\nu}[B(\boldsymbol{\pi})]}_{\text{Adjacency Matrix}} - \underbrace{\mathop{\mathbf{E}}_{\boldsymbol{\pi}\sim\mathrm{Sym}(N)}[B(\boldsymbol{\pi})]}_{\text{1-eigenspace}} \right\|_{\mathrm{op}} \leqslant \lambda$$

Where $B(\boldsymbol{\pi}) :=$ permutation matrix defined by $\boldsymbol{\pi}$

d-regular graph $\equiv$ Sum of d permutation matrices



Random walk step $\equiv$ Picking a permutation uniformly at random

Definition (ε-approximate unitary k-design):

$$\left\| \mathop{\mathbf{E}}_{\boldsymbol{X} \sim \nu} \left[\boldsymbol{X}^{\otimes k} \otimes (\overline{\boldsymbol{X}})^{\otimes k} \right] - \mathop{\mathbf{E}}_{\boldsymbol{X} \sim \mathrm{U}(N)} \left[\boldsymbol{X}^{\otimes k} \otimes (\overline{\boldsymbol{X}})^{\otimes k} \right] \right\|_1 \leqslant \varepsilon$$

• Definitions •

Definition (ε-approximate unitary k-design):

$$\left\| \mathop{\mathbf{E}}_{\nu}\left[\boldsymbol{X}^{\otimes k,k}\right] - \mathop{\mathbf{E}}_{\mathrm{U}(N)}\left[\boldsymbol{X}^{\otimes k,k}\right] \right\|_1 \leqslant \varepsilon$$

• Definitions •

Definition (ε-approximate unitary k-design):

$$\left\| \mathop{\mathbf{E}}_{\nu} \left[\boldsymbol{X}^{\otimes k,k} \right] - \mathop{\mathbf{E}}_{\mathrm{U}(N)} \left[\boldsymbol{X}^{\otimes k,k} \right] \right\|_1 \leqslant \varepsilon$$

Definition ((N, ε, k)-tensor-product-expander):

$$\left\| \mathop{\mathbf{E}}_{\nu} \left[\boldsymbol{X}^{\otimes k,k} \right] - \mathop{\mathbf{E}}_{\mathrm{U}(N)} \left[\boldsymbol{X}^{\otimes k,k} \right] \right\|_{\mathrm{op}} \leqslant \varepsilon$$

• Definitions •

Definition (ε-approximate unitary k-design):

$$\left\| \underset{\nu}{\mathbf{E}} \left[\boldsymbol{X}^{\otimes k,k} \right] - \underset{\mathrm{U}(N)}{\mathbf{E}} \left[\boldsymbol{X}^{\otimes k,k} \right] \right\|_1 \leqslant \varepsilon$$

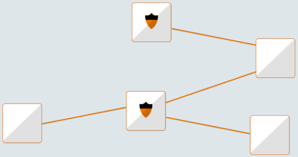
Definition ((N, ε, k)-tensor-product-expander):

$$\left\| \underset{\nu}{\mathbf{E}} \left[\boldsymbol{X}^{\otimes k,k} \right] - \underset{\mathrm{U}(N)}{\mathbf{E}} \left[\boldsymbol{X}^{\otimes k,k} \right] \right\|_{\mathrm{op}} \leqslant \varepsilon$$

Fact

A $(N, \varepsilon/N^k, k)$-TPE is an ε-approximate unitary k-design

Part I: Motivation



• What is known? •

$N = 2^n$

Method	Bits of Entropy	Efficient?
Randomized	$O(nk + \log(1/\varepsilon))$	✗

• What is known? •

$N = 2^n$

Method	Bits of Entropy	Efficient?
Randomized	$O(nk + \log(1/\varepsilon))$	✗
[BHH'19] [HHJ'20] [Haf'22]	$O(k^C n^2 \log(1/\varepsilon))$	✓

• What is known? •

$N = 2^n$

Method	Bits of Entropy	Efficient?
Randomized	$O(nk + \log(1/\varepsilon))$	✗
[BHH'19] [HHJ'20] [Haf'22]	$O(k^C n^2 \log(1/\varepsilon))$	✓
Us	$O(nk + \log(1/\varepsilon))$	✓

• What is known? •

$N = 2^n$

Method	Bits of Entropy	Efficient?
Randomized	$O(nk + \log(1/\varepsilon))$	✗
[BHH'19] [HHJ'20] [Haf'22]	$O(k^C n^2 \log(1/\varepsilon))$	✓
Us	$O(nk + \log(1/\varepsilon))$	✓

(Note: our work also achieves designs for other groups, like $\mathrm{O}(N)$)

• Some applications •

Algorithmic	Cryptographic	Lower Bounds
Efficient state tomography Fidelity estimation	Non-malleable encryption	Quantum hypothesis selection

• Some applications •

Algorithmic	Cryptographic	Lower Bounds
Efficient state tomography Fidelity estimation	Non-malleable encryption	Quantum hypothesis selection

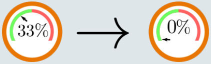
Note: our work also has some classical applications

Let's look at the motivation behind them

• Classical Detour: Why Pseudorandom? •

1 Convert random algorithms to deterministic using similar time

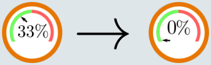
Ex: Primes in P, Undirected Reachability



• Classical Detour: Why Pseudorandom? •

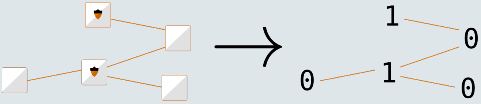
① Convert random algorithms to deterministic using similar time

Ex: Primes in P, Undirected Reachability



② Construct explicit objects whose existence is only guaranteed by the probabilistic method

Ex: Expanders, Efficient Codes



Definition: Pseudorandom Generator G

$G : \{0,1\}^t \to \{0,1\}^n$ ε-fools a family of tests $\mathcal{F}$, where $f \in \mathcal{F}$ is $f : \{0,1\}^n \to \{0,1\}$ if

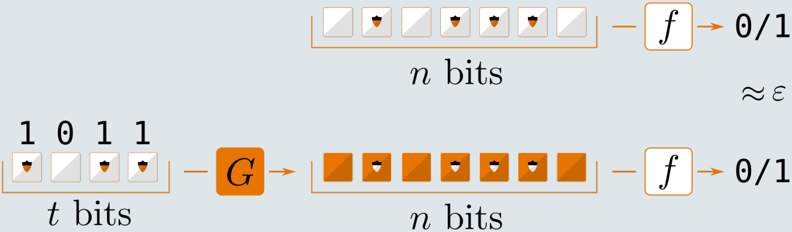
$$\forall f \in F, \qquad \left|\boldsymbol{P}_{x \sim U_n}[f(x) = 1] - \boldsymbol{P}_{z \sim U_t}[f(G(z)) = 1]\right| \leqslant \varepsilon$$

• Pseudorandom Generators •

Definition: Pseudorandom Generator G

$G : \{0,1\}^t \to \{0,1\}^n$ ε-fools a family of tests $\mathcal{F}$, where $f \in \mathcal{F}$ is $f : \{0,1\}^n \to \{0,1\}$ if

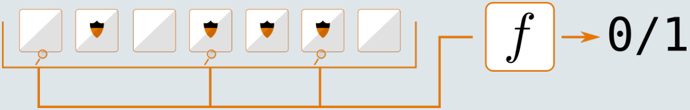
$$\forall f \in F, \qquad \left| \boldsymbol{P}_{x \sim U_n}[f(x) = 1] - \boldsymbol{P}_{z \sim U_t}[f(G(z)) = 1] \right| \leqslant \varepsilon$$



• k-wise independence •

Consider the family of k-wise independent tests:

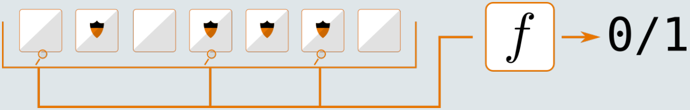
$$f \in \mathcal{F} \text{ only looks at most } k \text{ bits of the input}$$



• k-wise independence •

Consider the family of k-wise independent tests:

$f \in \mathcal{F}$ only looks at most k bits of the input



Example: k-wise uniform bits

G is k-wise independent if for $\boldsymbol{x} \sim U_N$ and all distinct $i_1, i_2, \ldots i_k$

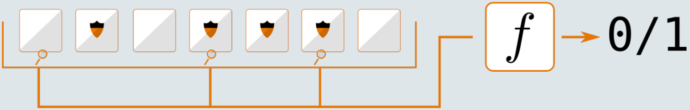
i_1th bit of $G(\boldsymbol{x})$, ..., i_kth bit of $G(\boldsymbol{x})$ are uniform

i.e. the probability of seeing any length k binary string is $1/2^k$

• k-wise independence •

Consider the family of k-wise independent tests:

$f \in \mathcal{F}$ only looks at most k bits of the input



Example: k-wise uniform bits

G is k-wise independent if for $\boldsymbol{x} \sim U_N$ and all distinct $i_1, i_2, \ldots i_k$

i_1th bit of $G(\boldsymbol{x})$, . . . , i_kth bit of $G(\boldsymbol{x})$ are uniform

i.e. the probability of seeing any length k binary string is $1/2^k$

Theorem [ABI'85]

Such a G exists with $t = O(kn)$

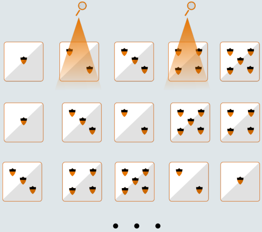
• k-wise independent permutations •

$[N]_k \to k$ distinct from $1 \dots N$

Definition: k-wise independent permutations

$\Pi \subseteq S_N$ is k-independent if for $\pi \in \Pi$

for all distinct $i_1, \dots, i_k$, $\pi(i_1), \dots, \pi(i_k)$ is uniform on $[N]_k$



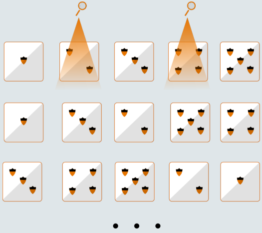
• (δ, k)-wise independent permutations •

$[N]_k \to k$ distinct from $1 \ldots N$

Definition: (δ, k)-wise independent permutations

$\Pi \subseteq S_N$ is (δ, k)-independent if for $\pi \in \Pi$

for all distinct $i_1, \ldots, i_k$, $\pi(i_1), \ldots, \pi(i_k)$ is δ-close to uniform on $[N]_k$



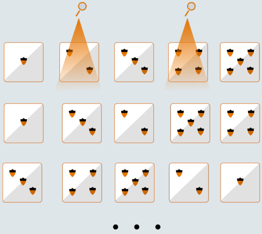
• (δ, k)-wise independent permutations •

$[N]_k \to k$ distinct from $1 \ldots N$

Definition: (δ, k)-wise independent permutations

$\Pi \subseteq S_N$ is (δ, k)-independent if for $\pi \in \Pi$

for all distinct $i_1, \ldots, i_k$, $\pi(i_1), \ldots, \pi(i_k)$ is δ-close to uniform on $[N]_k$



Theorem [KNR'05] [K'08]

Such a G exists with seed length $O(kn + \log(1/\delta))$

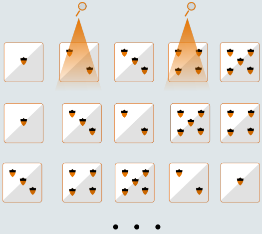
• (δ, k)-wise independent permutations •

$[N]_k \to k$ distinct from $1 \dots N$

Definition: (δ, k)-wise independent permutations

$\Pi \subseteq S_N$ is (δ, k)-independent if for $\pi \in \Pi$

for all distinct $i_1, \dots, i_k$, $\pi(i_1), \dots, \pi(i_k)$ is δ-close to uniform on $[N]_k$

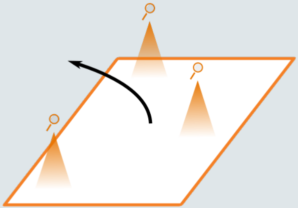


Theorem [KNR'05] [K'08]

Such a G exists with seed length $O(kn + \log(1/\delta))$

Many applications, e.g. cryptography, coding theory, expanders ...

Part II: General Framework



• Our framework •

A Baby Distribution

1. Construct $\mathcal{M}$, a set of matrices in $\mathrm{U}(N)$, such that:

- $$\left\| \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \mathop{\mathbf{E}}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right] \right\|_{\mathrm{op}} \leqslant 1 - \frac{1}{\mathrm{poly}(k) n}$$
- $|\mathcal{M}|$ really small $\rightarrow O(\log n)$ bits of entropy

• Our framework •

A Baby Distribution

1. Construct $\mathcal{M}$, a set of matrices in $\mathrm{U}(N)$, such that:

- $$\left\| \mathop{\mathbf{E}}_{\mathcal{M}} \left[M^{\otimes k,k} \right] - \mathop{\mathbf{E}}_{\mathrm{U}(N)} \left[M^{\otimes k,k} \right] \right\|_{\mathrm{op}} \leqslant 1 - \frac{1}{\mathrm{poly}(k)n}$$
- $|\mathcal{M}|$ really small $\to O(\log n)$ bits of entropy

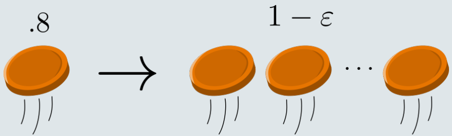
Error Reduction

2. Use $\mathcal{M}$ to obtain $\hat{\mathcal{M}}$, such that:

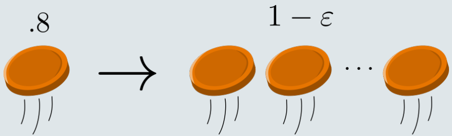
- $$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}} \left[M^{\otimes k,k} \right] - \mathop{\mathbf{E}}_{\mathrm{O}(N)} \left[M^{\otimes k,k} \right] \right\|_{\mathrm{op}} \leqslant \delta$$
- $|\hat{\mathcal{M}}|$ small $\to O(kn + \log(1/\delta))$ bits of entropy

Part III: Error Reduction

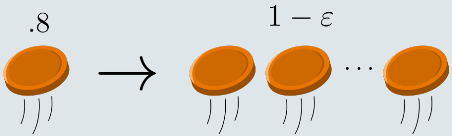
• Intuition •



• Intuition •



Intuition



$$\hat{\mathcal{M}} = \mathcal{M}^t, \text{ where } \mathcal{M}^t = \{M_1 \cdot M_2 \cdot \ldots \cdot M_t | M_i \in \mathcal{M}\}$$

• Some Facts About Tensors •

Fact

$X^{\otimes k,k}$ is a representation of $\mathrm{U}(N)$: $(XY)^{\otimes k,k} = X^{\otimes k,k} Y^{\otimes k,k}$

• Some Facts About Tensors •

Fact

$X^{\otimes k,k}$ is a representation of $\mathrm{U}(N)$: $(XY)^{\otimes k,k} = X^{\otimes k,k} Y^{\otimes k,k}$

Fact

For $X_0 \in \mathrm{U}(N)$ and $\boldsymbol{X} \sim \mathrm{U}(N)$, we have $X_0 \boldsymbol{X} \sim \boldsymbol{X} X_0 \sim \mathrm{U}(N)$

• Some Facts About Tensors •

Fact

$X^{\otimes k,k}$ is a representation of $\mathrm{U}(N)$: $(XY)^{\otimes k,k} = X^{\otimes k,k} Y^{\otimes k,k}$

Fact

For $X_0 \in \mathrm{U}(N)$ and $\boldsymbol{X} \sim \mathrm{U}(N)$, we have $X_0 \boldsymbol{X} \sim \boldsymbol{X} X_0 \sim \mathrm{U}(N)$

Fact

$$X_0^{\otimes k,k}\, \mathbf{E}_{\mathrm{U}(N)}\left[\boldsymbol{M}^{\otimes k,k}\right] = \mathbf{E}_{\mathrm{U}(N)}\left[\boldsymbol{M}^{\otimes k,k}\right]$$

• Some Facts About Tensors •

Fact

$X^{\otimes k,k}$ is a representation of $\mathrm{U}(N)$: $(XY)^{\otimes k,k} = X^{\otimes k,k} Y^{\otimes k,k}$

Fact

For $X_0 \in \mathrm{U}(N)$ and $\boldsymbol{X} \sim \mathrm{U}(N)$, we have $X_0 \boldsymbol{X} \sim \boldsymbol{X} X_0 \sim \mathrm{U}(N)$

Fact

$$X_0^{\otimes k,k}\, \mathbf{E}_{\mathrm{U}(N)}\left[\boldsymbol{M}^{\otimes k,k}\right] = \mathbf{E}_{\mathrm{U}(N)}\left[\boldsymbol{M}^{\otimes k,k}\right]$$

Fact

$$\mathbf{E}_{\nu}\left[\boldsymbol{M}^{\otimes k,k}\right] \mathbf{E}_{\mathrm{U}(N)}\left[\boldsymbol{M}^{\otimes k,k}\right] = \mathbf{E}_{\mathrm{U}(N)}\left[\boldsymbol{M}^{\otimes k,k}\right]$$

• Some Facts About Tensors •

Fact

$X^{\otimes k,k}$ is a representation of $\mathrm{U}(N)$: $(XY)^{\otimes k,k} = X^{\otimes k,k} Y^{\otimes k,k}$

Fact

For $X_0 \in \mathrm{U}(N)$ and $\boldsymbol{X} \sim \mathrm{U}(N)$, we have $X_0 \boldsymbol{X} \sim \boldsymbol{X} X_0 \sim \mathrm{U}(N)$

Fact

$$X_0^{\otimes k,k} \, \mathbf{E}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right] = \mathbf{E}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right]$$

Fact

$$\mathbf{E}_{\nu} \left[\boldsymbol{M}^{\otimes k,k} \right] \mathbf{E}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right] = \mathbf{E}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right]$$

Fact

$$\mathbf{E}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right]^2 = \mathbf{E}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right],$$

so it's a projector matrix and $\Pi_{\mathrm{U}(N)} := \mathbf{E}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right]$

Lemma: Error reduction

If $\hat{\mathcal{M}} = \mathcal{M}^t$ then:

$$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \mathop{\mathbf{E}}_{\mathrm{U}(N)} \left[\boldsymbol{M}^{\otimes k,k} \right] \right\|_{\mathrm{op}} \leqslant \varepsilon^t$$

Lemma: Error reduction

If $\hat{\mathcal{M}} = \mathcal{M}^t$ then:

$$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \varepsilon^t$$

Lemma: Error reduction

If $\hat{\mathcal{M}} = \mathcal{M}^t$ then:

$$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \varepsilon^t$$

Proof. Assume $t = 2$ (general case follows from this).

Lemma: Error reduction

If $\hat{\mathcal{M}} = \mathcal{M}^t$ then:

$$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \varepsilon^t$$

Proof. Assume $t = 2$ (general case follows from this).

Note:

$$\left(\mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right)^2 = \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right]^2 - 2 \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] \Pi_{\mathrm{U}(N)} + \Pi_{\mathrm{U}(N)}^2$$

Lemma: Error reduction

If $\hat{\mathcal{M}} = \mathcal{M}^t$ then:

$$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \varepsilon^t$$

Proof. Assume $t = 2$ (general case follows from this).

Note:

$$\begin{aligned} \left(\mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right)^2 &= \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right]^2 - 2 \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] \Pi_{\mathrm{U}(N)} + \Pi_{\mathrm{U}(N)}^2 \\ &= \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right]^2 - \Pi_{\mathrm{U}(N)} \end{aligned}$$

Proof. Assume $t = 2$ (general case follows from this).

Note:

$$\left(\mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right] - \Pi_{\mathrm{U}(N)}\right)^2 = \mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 - 2\mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right]\Pi_{\mathrm{U}(N)} + \Pi_{\mathrm{U}(N)}^2$$

$$= \mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 - \Pi_{\mathrm{U}(N)}$$

Proof. Assume $t = 2$ (general case follows from this).

Note:

$$\left(\mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right] - \Pi_{\mathrm{U}(N)}\right)^2 = \mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 - 2\mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right]\Pi_{\mathrm{U}(N)} + \Pi_{\mathrm{U}(N)}^2$$

$$= \mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 - \Pi_{\mathrm{U}(N)}$$

Also:

$$\mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 = \mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}_1^{\otimes k,k}\right]\mathop{\mathbf{E}}_{\mathcal{M}}\left[\boldsymbol{M}_2^{\otimes k,k}\right]$$

Proof. Assume $t = 2$ (general case follows from this).

Note:

$$\left(\mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right)^2 = \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right]^2 - 2 \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] \Pi_{\mathrm{U}(N)} + \Pi_{\mathrm{U}(N)}^2$$

$$= \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right]^2 - \Pi_{\mathrm{U}(N)}$$

Also:

$$\mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right]^2 = \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}_1^{\otimes k,k} \right] \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}_2^{\otimes k,k} \right]$$

$$= \mathbf{E} \left[(\boldsymbol{M}_1 \boldsymbol{M}_2)^{\otimes k,k} \right] = \mathop{\mathbf{E}}_{\mathcal{M}^2} \left[(\boldsymbol{M})^{\otimes k,k} \right]$$

Proof. Assume $t = 2$ (general case follows from this).

Note:

$$\left(\underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right] - \Pi_{\mathrm{U}(N)}\right)^2 = \underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 - 2\underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right]\Pi_{\mathrm{U}(N)} + \Pi_{\mathrm{U}(N)}^2$$
$$= \underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 - \Pi_{\mathrm{U}(N)}$$

Also:

$$\underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 = \underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}_1^{\otimes k,k}\right]\underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}_2^{\otimes k,k}\right]$$
$$= \mathbf{E}\left[(\boldsymbol{M}_1\boldsymbol{M}_2)^{\otimes k,k}\right] = \underset{\mathcal{M}^2}{\mathbf{E}}\left[(\boldsymbol{M})^{\otimes k,k}\right]$$

Putting it all together:

$$\left(\mathbf{E}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right] - \Pi_{\mathrm{U}(N)}\right)^2 = \mathbf{E}_{\mathcal{M}^2}\left[\boldsymbol{M}^{\otimes k,k}\right] - \Pi_{\mathrm{U}(N)}$$

Proof. Assume $t = 2$ (general case follows from this).

Note:

$$\left(\underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right] - \Pi_{\mathrm{U}(N)}\right)^2 = \underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 - 2\underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right]\Pi_{\mathrm{U}(N)} + \Pi_{\mathrm{U}(N)}^2$$
$$= \underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 - \Pi_{\mathrm{U}(N)}$$

Also:

$$\underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}^{\otimes k,k}\right]^2 = \underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}_1^{\otimes k,k}\right]\underset{\mathcal{M}}{\mathbf{E}}\left[\boldsymbol{M}_2^{\otimes k,k}\right]$$
$$= \mathbf{E}\left[(\boldsymbol{M}_1\boldsymbol{M}_2)^{\otimes k,k}\right] = \underset{\mathcal{M}^2}{\mathbf{E}}\left[(\boldsymbol{M})^{\otimes k,k}\right]$$

Putting it all together:

$$\left(\mathbf{E}_{\mathcal{M}}\left[\boldsymbol{M}^{\otimes k,k}\right] - \Pi_{\mathrm{U}(N)}\right)^2 = \mathbf{E}_{\mathcal{M}^2}\left[\boldsymbol{M}^{\otimes k,k}\right] - \Pi_{\mathrm{U}(N)}$$

The given operator norm bound now gives the result $\square$

• A Decent Reduction... •

Using error reduction, pick $t = \mathrm{poly}(\log N, k)\log(1/\delta)$, we conclude:

- $$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}}\left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \delta$$

• A Decent Reduction... •

Using error reduction, pick $t = \mathrm{poly}(\log N, k) \log(1/\delta)$, we conclude:

- $$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \delta$$
- But... $|\hat{\mathcal{M}}| = |\mathcal{M}|^t \to O(\mathrm{poly}(n,k) \log(1/\delta))$ bits of entropy

• Intuition for a Better Reduction •

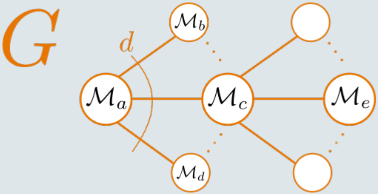
Let G be a expander d-regular graph with $|\mathcal{M}|$ vertices

Label the vertices with matrices from $\mathcal{M}$, so $v \in V$ and $M_v \in \mathcal{M}$

• Intuition for a Better Reduction •

Let G be a expander d-regular graph with $|\mathcal{M}|$ vertices

Label the vertices with matrices from $\mathcal{M}$, so $v \in V$ and $M_v \in \mathcal{M}$



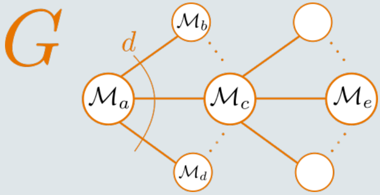
$$\hat{\mathcal{M}} = \mathcal{M}^{G,t} = \{M_{v_1} \cdot M_{v_2} \cdot \ldots \cdot M_{v_t} | v_i \sim v_{i+1}\}$$

Note: $|\hat{\mathcal{M}}| = |\mathcal{M}| d^t$

• Intuition for a Better Reduction •

Let G be a expander d-regular graph with $|\mathcal{M}|$ vertices

Label the vertices with matrices from $\mathcal{M}$, so $v \in V$ and $M_v \in \mathcal{M}$



$$\hat{\mathcal{M}} = \mathcal{M}^{G,t} = \{M_{v_1} \cdot M_{v_2} \cdot \ldots \cdot M_{v_t} | v_i \sim v_{i+1}\}$$

Note: $|\hat{\mathcal{M}}| = |\mathcal{M}| d^t$

Challenge 1: Prove that this reduces the error, like the previous reduction

Challenge 2: Pick appropriate expander graphs
(derandomized squaring [RTV'05] [RV'05])

• Technical Result •

Theorem: Operator Reduction

Let $\mathcal{M} = (M_1, \ldots, M_c)$ be a matrices in $\mathbb{R}^{r \times r}$ satisfying $\|M_i\|_{\mathrm{op}} \leqslant 1$ for all i and $\left\| \mathbf{E}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi \right\|_{\mathrm{op}} \leqslant 1 - \varepsilon$

There is a strongly explicit, space-minimal algorithm that outputs a sequence Q of $N' = O(c/(\varepsilon^{11.25}\delta^{10}))$ monomials over $M_1, \ldots, M_c$, each of length $L = 8\log_2(1/\delta)/\varepsilon^{1.25}$, such that:

$$\left\| \mathbf{E}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi \right\|_{\mathrm{op}} \leqslant \delta, \text{ for } \hat{\mathcal{M}} = \mathcal{M}^Q$$

• Technical Result •

Theorem: Operator Reduction

Let $\mathcal{M} = (M_1, \ldots, M_c)$ be a matrices in $\mathbb{R}^{r \times r}$ satisfying $\|M_i\|_{\mathrm{op}} \leqslant 1$ for all i and $\left\| \mathbf{E}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi \right\|_{\mathrm{op}} \leqslant 1 - \varepsilon$

There is a strongly explicit, space-minimal algorithm that outputs a sequence Q of $N' = O(c/(\varepsilon^{11.25}\delta^{10}))$ monomials over $M_1, \ldots, M_c$, each of length $L = 8\log_2(1/\delta)/\varepsilon^{1.25}$, such that:

$$\left\| \mathbf{E}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi \right\|_{\mathrm{op}} \leqslant \delta, \text{ for } \hat{\mathcal{M}} = \mathcal{M}^Q$$

Translation:

- $$\left\| \mathop{\mathbf{E}}_{\hat{\mathcal{M}}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \delta$$
- $|\hat{\mathcal{M}}| \leqslant \mathrm{poly}(2^{nk}/\delta) \to O(kn + \log(1/\delta))$ bits of entropy

Part IV: A Baby Distribution

$$M_1 \otimes \mathbb{I} \otimes \mathbb{I} \otimes M_2$$

$$|1\rangle \quad |2\rangle \quad |3\rangle \quad |4\rangle$$

• Recall our Goal •

1. Construct $\mathcal{M}$, a set of matrices in $\mathrm{U}(N)$, such that:

- $$\left\| \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant 1 - \frac{1}{\mathrm{poly}(k)n}$$
- $|\mathcal{M}| \leqslant \mathrm{poly}(n)$

• Recall our Goal •

1. Construct $\mathcal{M}$, a set of matrices in $\mathrm{U}(N)$, such that:

- $$\left\| \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant 1 - \frac{1}{\mathrm{poly}(k)n}$$
- $|\mathcal{M}| \leqslant \mathrm{poly}(n)$

Actually, this is given in [BHH'19], [HHJ'20], [Haf'22]!

• A Baby Distribution •

$N = 2^n$

Let $P \subset \mathrm{U}(2^\ell)$ be a finite set and $E \subseteq [n]_\ell$

• A Baby Distribution •

$N = 2^n$

Let $P \subset \mathrm{U}(2^\ell)$ be a finite set and $E \subseteq [n]_\ell$

Define $\boldsymbol{M_e} \sim P \times E$: choose $\boldsymbol{e} \sim E$, $\boldsymbol{M} \sim P$ and apply $\boldsymbol{M}$ to $\boldsymbol{e}$ substates

$$M \in \mathbf{U}(4) \qquad e = \{1, 4\}$$

$$M = M_1 \otimes M_2$$

$$M_e = M_1 \otimes \mathbb{I} \otimes \mathbb{I} \otimes M_2$$

$$|1\rangle \quad |2\rangle \quad |3\rangle \quad |4\rangle$$

• A Baby Distribution •

$N = 2^n$

Let $P \subset \mathrm{U}(2^\ell)$ be a finite set and $E \subseteq [n]_\ell$

Define $\boldsymbol{M_e} \sim P \times E$: choose $\boldsymbol{e} \sim E$, $\boldsymbol{M} \sim P$ and apply $\boldsymbol{M}$ to $\boldsymbol{e}$ substates

$$M \in \mathbf{U}(4) \qquad e = \{1, 4\}$$
$$M = M_1 \otimes M_2$$

$$M_e = M_1 \otimes \mathbb{I} \otimes \mathbb{I} \otimes M_2$$
$$|1\rangle \quad |2\rangle \quad |3\rangle \quad |4\rangle$$

Theorem: Non-trivial gap construction

For a fixed small positive n_0, suppose P_{n_0} is a universal set in $\mathrm{U}(N)$

Then $\mathcal{M} = P_{n_0} \times \binom{[n]}{n_0}$ satisfies:

$$\left\| \mathop{\mathbf{E}}_{\mathcal{M}} \left[\boldsymbol{M}^{\otimes k, k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant 1 - \frac{1}{\mathrm{poly}(k) n}$$

• Proof Outline •

Abuse notation: let $P_1 \lesssim \alpha P_2$ be

$$\left\| \mathop{\mathbf{E}}_{P_1} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \alpha \left\| \mathop{\mathbf{E}}_{P_2} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}}$$

• Proof Outline •

P_{n_0} universal

Abuse notation: let $P_1 \lesssim \alpha P_2$ be

$$\left\| \mathop{\mathbf{E}}_{P_1}\left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \alpha \left\| \mathop{\mathbf{E}}_{P_2}\left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}}$$

Then:

$$P_{n_0} \times \binom{[n]}{n_0} \lesssim \kappa_{n_0} \mathrm{U}(2^{n_0}) \times \binom{[n]}{n_0}$$

From [BdS16] and [BG12]

• Proof Outline •

P_{n_0} universal

Abuse notation: let $P_1 \lesssim \alpha P_2$ be

$$\left\| \mathop{\mathbf{E}}_{P_1}\left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \alpha \left\| \mathop{\mathbf{E}}_{P_2}\left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}}$$

Then:

$$P_{n_0} \times \binom{[n]}{n_0} \lesssim \kappa_{n_0} \mathrm{U}(2^{n_0}) \times \binom{[n]}{n_0}$$

From [BdS16] and [BG12]

$$\lesssim \kappa_{n_0} \tau_{k,n_0+1} \mathrm{U}(2^{n_0+1}) \times \binom{[n]}{n_0+1}$$

• Proof Outline •

P_{n_0} universal

Abuse notation: let $P_1 \lesssim \alpha P_2$ be

$$\left\| \mathop{\mathbf{E}}_{P_1} \left[M^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \alpha \left\| \mathop{\mathbf{E}}_{P_2} \left[M^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}}$$

Then:

$$\begin{aligned} P_{n_0} \times \binom{[n]}{n_0} &\lesssim \kappa_{n_0} \mathrm{U}(2^{n_0}) \times \binom{[n]}{n_0} \\ &\lesssim \kappa_{n_0} \tau_{k,n_0+1} \mathrm{U}(2^{n_0+1}) \times \binom{[n]}{n_0+1} \\ &\lesssim \kappa_{n_0} \tau_{k,n_0+1} \dots \tau_{k,n} \mathrm{U}(N) \end{aligned}$$

From [BdS16] and [BG12]

• Proof Outline •

P_{n_0} universal

Abuse notation: let $P_1 \lesssim \alpha P_2$ be

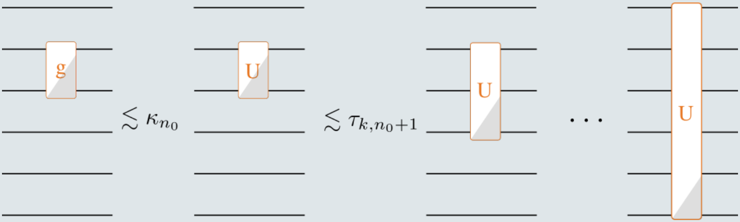
$$\left\| \mathop{\mathbf{E}}_{P_1} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}} \leqslant \alpha \left\| \mathop{\mathbf{E}}_{P_2} \left[\boldsymbol{M}^{\otimes k,k} \right] - \Pi_{\mathrm{U}(N)} \right\|_{\mathrm{op}}$$

Then:

$$\begin{aligned} P_{n_0} \times \binom{[n]}{n_0} &\lesssim \kappa_{n_0} \mathrm{U}(2^{n_0}) \times \binom{[n]}{n_0} \\ &\lesssim \kappa_{n_0} \tau_{k,n_0+1} \mathrm{U}(2^{n_0+1}) \times \binom{[n]}{n_0+1} \\ &\lesssim \kappa_{n_0} \tau_{k,n_0+1} \ldots \tau_{k,n} \mathrm{U}(N) \\ &\lesssim \left(1 - \frac{1}{\mathrm{poly}(k)n}\right) \mathrm{U}(N) \end{aligned}$$

From [BdS16] and [BG12]

• Proof Visualization •



Thanks!