Pseudorandom Unitaries and Compressed Purifications

Fermi Ma

joint work with Hsin-Yuan Huang

Can an **efficient circuit** **look random**?

Can an **efficient circuit** **look random**?

family of $\mathrm{poly}(n)$-size
n-qubit circuits $\{U_k\}$

Can an **efficient circuit** **look random**?

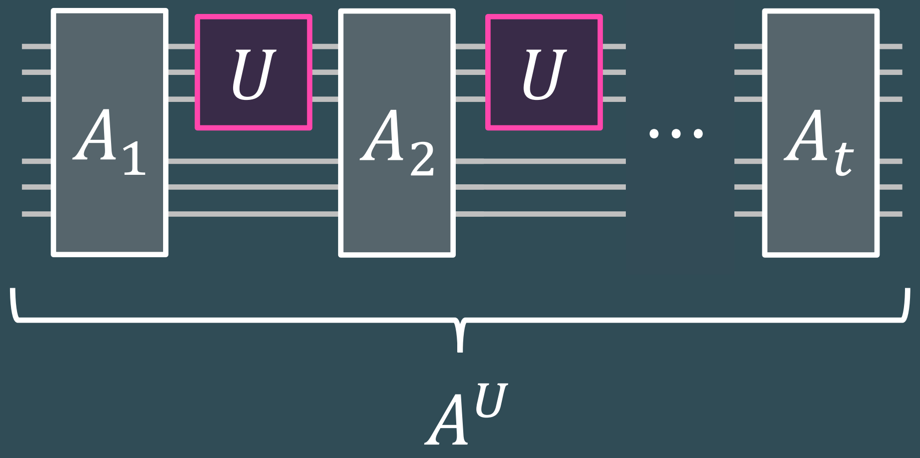
family of $\mathbf{poly}(n)$-size n-qubit circuits $\{U_k\}$

indistinguishable from a Haar-random unitary

Can an **efficient circuit look random**?

family of $\mathrm{poly}(n)$-size n-qubit circuits $\{U_k\}$

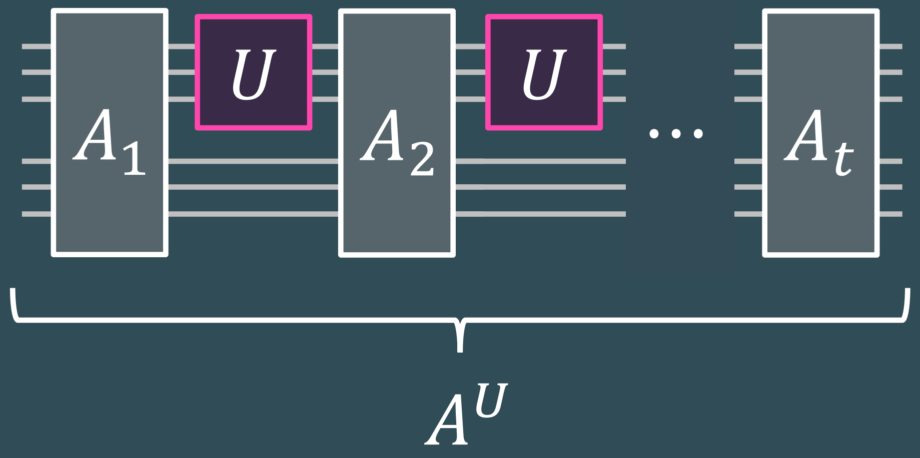
indistinguishable from a Haar-random unitary



Can an **efficient circuit look random**?

family of $\mathrm{poly}(n)$-size n-qubit circuits $\{U_k\}$

indistinguishable from a Haar-random unitary



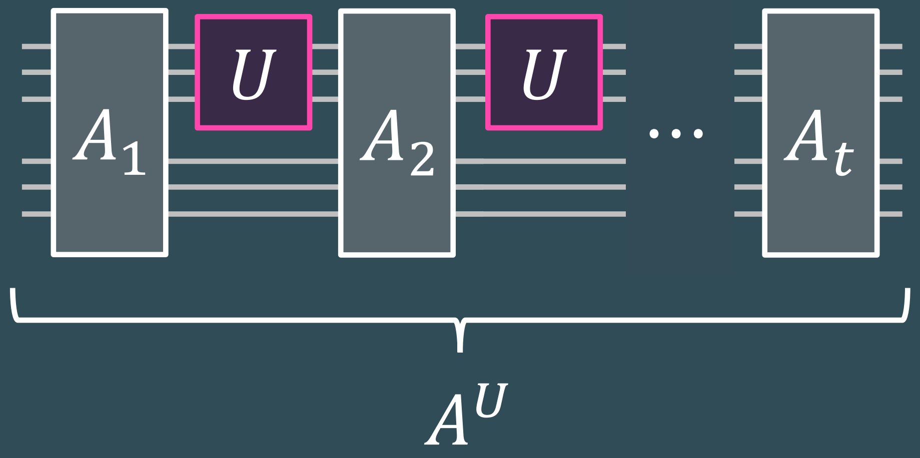
No efficient A^U can distinguish

- $U \leftarrow \{U_k\}$
- $U \leftarrow$ Haar

Can an **efficient circuit look random**?

family of $\mathrm{poly}(n)$-size n-qubit circuits $\{U_k\}$

indistinguishable from a Haar-random unitary



No efficient A^U can distinguish

- $U \leftarrow \{U_k\}$
- $U \leftarrow$ Haar

$\{U_k\}$ is a **pseudorandom unitary (PRU)**.

(as defined by JLS18)

Why study pseudorandom unitaries (PRUs)?

Why study pseudorandom unitaries (PRUs)?

- **Physics:** model highly scrambling physical processes [KP23,EFLVY24,YE24]

Why study pseudorandom unitaries (PRUs)?

- **Physics:** model highly scrambling physical processes [KP23,EFLVY24,YE24]
- **Cryptography:** quantum analog of pseudorandom functions

Why study pseudorandom unitaries (PRUs)?

- **Physics:** model highly scrambling physical processes [KP23,EFLVY24,YE24]
- **Cryptography:** quantum analog of pseudorandom functions
- Implications for quantum algorithms and learning

Why study pseudorandom unitaries (PRUs)?

- **Physics:** model highly scrambling physical processes [KP23,EFLVY24,YE24]
- **Cryptography:** quantum analog of pseudorandom functions
- Implications for quantum algorithms and learning
- New perspectives on random unitaries

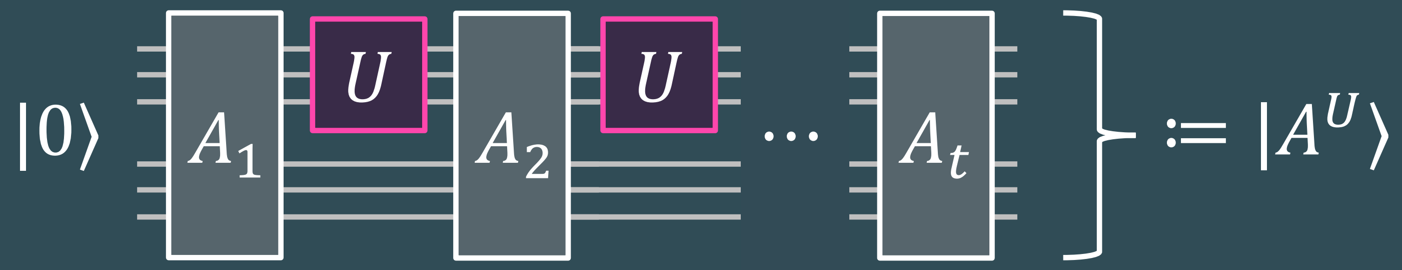
Open question: do PRUs exist? (under cryptographic assumptions)

Open question: do PRUs exist? (under cryptographic assumptions)

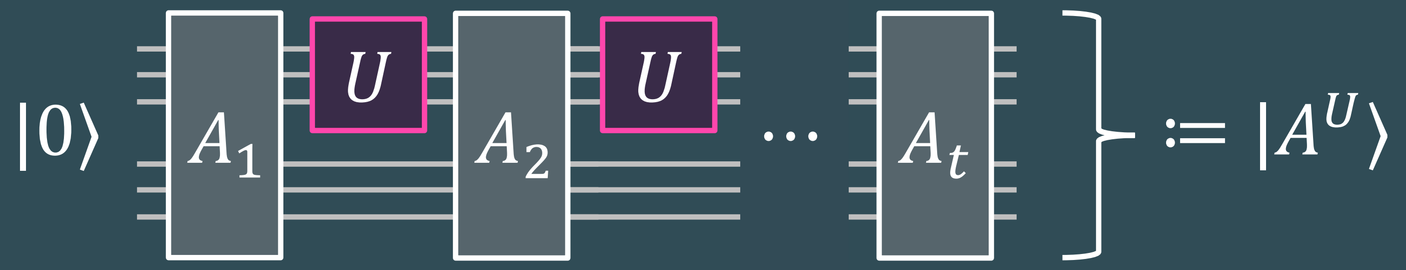
Prior work: PRUs secure against **restricted** adversaries [LQSYZ23,AGKL23,BM24,MPSY24,CBBDHX24,...]

What makes PRUs tricky?

What makes PRUs tricky?



What makes PRUs tricky?



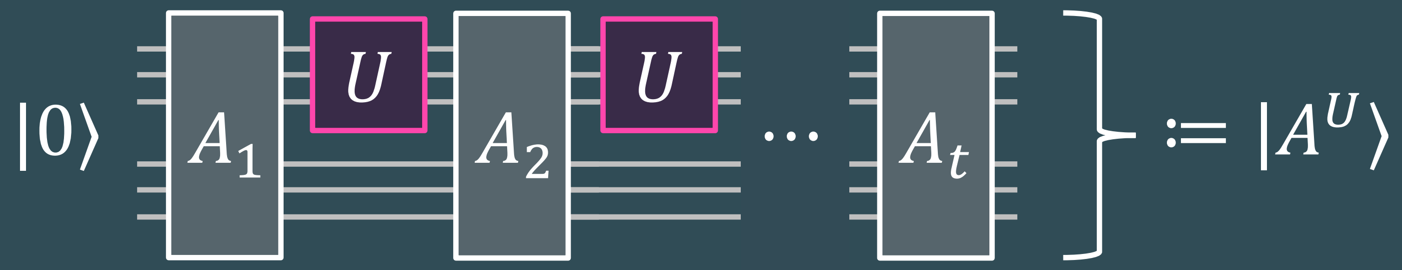
Goal: $\mathbb{E}_{U \leftarrow \mathrm{PRU}} |A^U\rangle\langle A^U| \approx \mathbb{E}_{U \leftarrow \mathrm{Haar}} |A^U\rangle\langle A^U|$

What makes PRUs tricky?

Goal: $\mathbb{E}_{U \leftarrow \mathrm{PRU}} |A^U\rangle\langle A^U| \approx \mathbb{E}_{U \leftarrow \mathrm{Haar}} |A^U\rangle\langle A^U|$

Usual approach: Weingarten calculus from representation theory

What makes PRUs tricky?



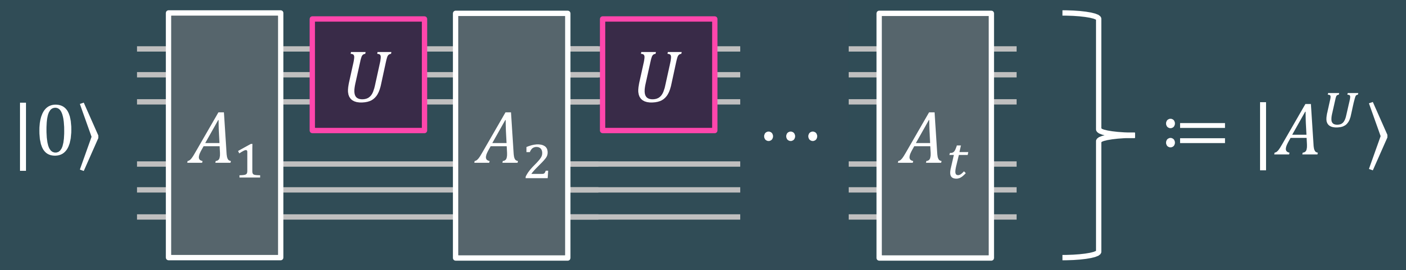
Goal: $\mathbb{E}_{U \leftarrow \mathrm{PRU}} |A^U\rangle\langle A^U| \approx \mathbb{E}_{U \leftarrow \mathrm{Haar}} |A^U\rangle\langle A^U|$

Usual approach: Weingarten calculus from representation theory

$$\int_{U_d} dU U_{ij} \bar{U}_{k\ell} = \delta_{ik}\delta_{j\ell} \,\mathrm{Wg}(1,d) = \frac{\delta_{ik}\delta_{j\ell}}{d}.$$

$$\int_{U_d} dU U_{ij} U_{k\ell} \bar{U}_{mn} \bar{U}_{pq} = (\delta_{im}\delta_{jn}\delta_{kp}\delta_{\ell q} + \delta_{ip}\delta_{jq}\delta_{km}\delta_{\ell n}) \,\mathrm{Wg}(1^2, d) + (\delta_{im}\delta_{jq}\delta_{kp}\delta_{\ell n} + \delta_{ip}\delta_{jn}\delta_{km}\delta_{\ell q}) \,\mathrm{Wg}(2,d).$$

What makes PRUs tricky?



Goal: $\mathbb{E}_{U \leftarrow \mathrm{PRU}} |A^U\rangle\langle A^U| \approx \mathbb{E}_{U \leftarrow \mathrm{Haar}} |A^U\rangle\langle A^U|$

Usual approach: Weingarten calculus from representation theory

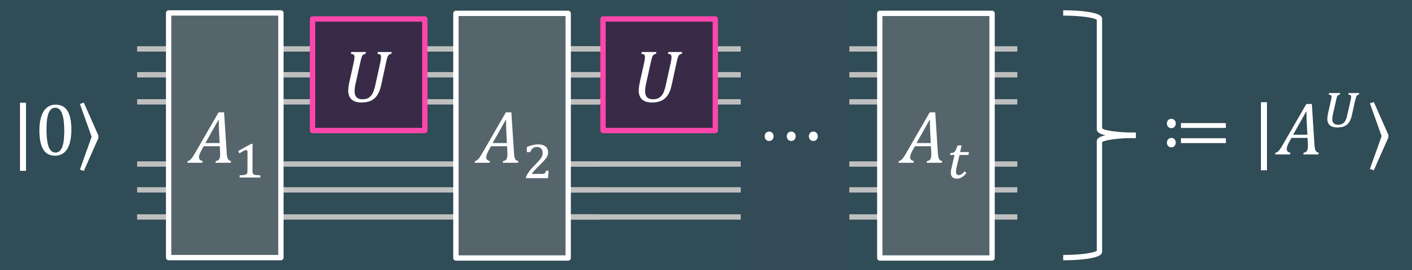
$$Wg(\sigma, d) = \frac{1}{q!^2} \sum_{\lambda} \frac{\chi^{\lambda}(1)^2 \chi^{\lambda}(\sigma)}{s_{\lambda,d}(1)}$$

where the sum is over all partitions λ of q (Collins 2003). Here χ^{λ} is the character of S_q corresponding to the partition λ and s is the Schur polynomial of λ, so that $s_{\lambda d}(1)$ is the dimension of the representation of U_d corresponding to λ.

$$\int_{U_d} dU U_{ij} \bar{U}_{k\ell} = \delta_{ik}\delta_{j\ell}\,\mathrm{Wg}(1,d) = \frac{\delta_{ik}\delta_{j\ell}}{d}.$$

$$\int_{U_d} dU U_{ij} U_{k\ell} \bar{U}_{mn} \bar{U}_{pq} = (\delta_{im}\delta_{jn}\delta_{kp}\delta_{\ell q} + \delta_{ip}\delta_{jq}\delta_{km}\delta_{\ell n})\,\mathrm{Wg}(1^2, d) + (\delta_{im}\delta_{jq}\delta_{kp}\delta_{\ell n} + \delta_{ip}\delta_{jn}\delta_{km}\delta_{\ell q})\,\mathrm{Wg}(2, d).$$

What makes PRUs tricky?



Goal: $\mathbb{E}_{U \leftarrow \mathrm{PRU}} |A^U\rangle\langle A^U| \approx \mathbb{E}_{U \leftarrow \mathrm{Haar}} |A^U\rangle\langle A^U|$

Usual approach: Weingarten calculus from representation theory

$$Wg(\sigma, d) = \frac{1}{q!^2} \sum_{\lambda} \frac{\chi^\lambda(1)^2 \chi^\lambda(\sigma)}{s_{\lambda,d}(1)}$$

where the sum is over all partitions λ of q (Collins 2003). Here χ^λ is the character of S_q corresponding to the partition λ and s is the Schur polynomial of λ, so that $s_{\lambda d}(1)$ is the dimension of the representation of U_d corresponding to λ.

$$\int_{U_d} dU U_{ij} \bar{U}_{k\ell} = \delta_{ik}\delta_{j\ell} \operatorname{Wg}(1, d) = \frac{\delta_{ik}\delta_{j\ell}}{d}.$$

$$\int_{U_d} dU U_{ij} U_{k\ell} \bar{U}_{mn} \bar{U}_{pq} = (\delta_{im}\delta_{jn}\delta_{kp}\delta_{\ell q} + \delta_{ip}\delta_{jq}\delta_{km}\delta_{\ell n}) \operatorname{Wg}(1^2, d) + (\delta_{im}\delta_{jq}\delta_{kp}\delta_{\ell n} + \delta_{ip}\delta_{jn}\delta_{km}\delta_{\ell q}) \operatorname{Wg}(2, d).$$

... but even this only gives you *entries* of the RHS!

[Ma-Huang24]: first provably-secure PRUs

[Ma-Huang24]: first provably-secure PRUs

We achieve two different notions:

[Ma-Huang24]: first provably-secure PRUs

We achieve two different notions:

"standard" PRUs: adversary queries U adaptively

[Ma-Huang24]: first provably-secure PRUs

We achieve two different notions:

"standard" PRUs: adversary queries U adaptively

$$\underset{\text{permutation}}{U = P} \cdot \underset{\text{function}}{F} \cdot \underset{\text{Clifford}}{C}$$ [MPSY24]

[Ma-Huang24]: first provably-secure PRUs

We achieve two different notions:

“standard” PRUs: adversary queries U adaptively

$$U = P \cdot F \cdot C$$ [MPSY24]

permutation function Clifford

“strong” PRUs: adversary queries U and $U^\dagger$ adaptively

[Ma-Huang24]: first provably-secure PRUs

We achieve two different notions:

"standard" PRUs: adversary queries U adaptively

$$U = P \cdot F \cdot C$$

[MPSY24]

permutation function Clifford

"strong" PRUs: adversary queries U and $U^\dagger$ adaptively

$$U = C^\dagger \cdot P \cdot F \cdot C$$

[Ma-Huang24]: first provably-secure PRUs

We achieve two different notions:

(this talk)

“standard” PRUs: adversary queries U adaptively

$$U = \underset{\text{permutation}}{P} \cdot \underset{\text{function}}{F} \cdot \underset{\text{Clifford}}{C}$$

[MPSY24]

“strong” PRUs: adversary queries U and $U^\dagger$ adaptively

$$U = C^\dagger \cdot P \cdot F \cdot C$$

Main idea: compressed purifications, an elementary method to analyze random unitaries

Main idea: compressed purifications, an elementary method to analyze random unitaries

This has many other applications:

Main idea: compressed purifications, an elementary method to analyze random unitaries

This has many other applications:

random matrices: under mild conditions, matrices with i.i.d. entries look Haar-random

Main idea: compressed purifications, an elementary method to analyze random unitaries

This has many other applications:

random matrices: under mild conditions, matrices with i.i.d. entries look Haar-random

Main idea: compressed purifications, an elementary method to analyze random unitaries

This has many other applications:

random matrices: under mild conditions, matrices with i.i.d. entries look Haar-random

low-depth random circuits: simplify proof of [SHH24] “gluing” lemma

Main idea: compressed purifications, an elementary method to analyze random unitaries

This has many other applications:

random matrices: under mild conditions, matrices with i.i.d. entries look Haar-random

low-depth random circuits: simplify proof of [SHH24] "gluing" lemma

Overview: compressed purifications

[M24, MH24] + [Z18]

Overview: compressed purifications

[M24, MH24] + [Z18]

- Any mixed state ρ_H has a *purification* $|\Phi\rangle_{HE}$, i.e., $\mathbf{Tr}_E\,|\Phi\rangle\langle\Phi| = \rho_H$

Overview: compressed purifications

[M24, MH24] + [Z18]

- Any mixed state ρ_H has a *purification* $|\Phi\rangle_{HE}$, i.e., $\mathbf{Tr}_E\, |\Phi\rangle\langle\Phi| = \rho_H$
- $|\Phi\rangle_{HE}$ is not unique! Can always apply an isometry on E

Overview: compressed purifications

[M24, MH24] + [Z18]

- Any mixed state ρ_H has a *purification* $|\Phi\rangle_{HE}$, i.e., $\mathbf{Tr}_E\, |\Phi\rangle\langle\Phi| = \rho_H$
- $|\Phi\rangle_{HE}$ is not unique! Can always apply an isometry on E

The plan: prove that mixed states ρ_H, σ_H are close using purification.

Overview: compressed purifications

[M24, MH24] + [Z18]

- Any mixed state ρ_H has a *purification* $|\Phi\rangle_{HE}$, i.e., $\mathbf{Tr}_E\, |\Phi\rangle\langle\Phi| = \rho_H$
- $|\Phi\rangle_{HE}$ is not unique! Can always apply an isometry on E

The plan: prove that mixed states ρ_H, σ_H are close using purification.

1) Construct purifications $|\Phi_0\rangle_{HE}, |\Phi_1\rangle_{HE}$ of ρ, σ.

Overview: compressed purifications

[M24, MH24] + [Z18]

- Any mixed state ρ_H has a *purification* $|\Phi\rangle_{HE}$, i.e., $\mathrm{Tr}_E\,|\Phi\rangle\langle\Phi| = \rho_H$
- $|\Phi\rangle_{HE}$ is not unique! Can always apply an isometry on E

The plan: prove that mixed states ρ_H, σ_H are close using purification.

1) Construct purifications $|\Phi_0\rangle_{HE}, |\Phi_1\rangle_{HE}$ of ρ, σ.

2) Find an isometry V such that $V_E \cdot |\Phi_0\rangle_{HE} \approx |\Phi_1\rangle_{HE}$.

Overview: compressed purifications

[M24, MH24] + [Z18]

- Any mixed state ρ_H has a *purification* $|\Phi\rangle_{HE}$, i.e., $\mathrm{Tr}_E\, |\Phi\rangle\langle\Phi| = \rho_H$
- $|\Phi\rangle_{HE}$ is not unique! Can always apply an isometry on E

The plan: prove that mixed states ρ_H, σ_H are close using purification.

1) Construct purifications $|\Phi_0\rangle_{HE}, |\Phi_1\rangle_{HE}$ of ρ, σ.

2) Find an isometry V such that $V_E \cdot |\Phi_0\rangle_{HE} \approx |\Phi_1\rangle_{HE}$.

But how do we find V?

Overview: compressed purifications

[M24, MH24] + [Z18]

- Any mixed state ρ_H has a *purification* $|\Phi\rangle_{HE}$, i.e., $\mathrm{Tr}_E\,|\Phi\rangle\langle\Phi| = \rho_H$
- $|\Phi\rangle_{HE}$ is not unique! Can always apply an isometry on E

The plan: prove that mixed states ρ_H, σ_H are close using purification.

1) Construct purifications $|\Phi_0\rangle_{HE}, |\Phi_1\rangle_{HE}$ of ρ, σ.

2) Find an isometry V such that $V_E \cdot |\Phi_0\rangle_{HE} \approx |\Phi_1\rangle_{HE}$.

But how do we find V?

Philosophy: try to ***compress*** the purification.

Let’s do a simple example.

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle$$

Expand $|\Phi\rangle$ as

$$\sum_{f\in\{0,1\}^N}\left(\sum_{x\in[N]}(-1)^{f_x}|x\rangle\right)|f\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle$$

Expand $|\Phi\rangle$ as

$$\sum_{f\in\{0,1\}^N}\left(\sum_{x\in[N]}(-1)^{f_x}|x\rangle\right)|f\rangle = \sum_{x\in[N]}|x\rangle \sum_{f\in\{0,1\}^N}(-1)^{f_x}|f\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]} (-1)^{f_x} |x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N} |\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]} |x\rangle \sum_{f\in\{0,1\}^N} (-1)^{f_x} |f\rangle$$

Expand $|\Phi\rangle$ as

$$\sum_{f\in\{0,1\}^N} \left(\sum_{x\in[N]} (-1)^{f_x} |x\rangle \right) |f\rangle = \sum_{x\in[N]} |x\rangle \sum_{f\in\{0,1\}^N} (-1)^{f_x} |f\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho \coloneqq \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]} |x\rangle \underbrace{\sum_{f\in\{0,1\}^N} (-1)^{f_x}|f\rangle}_{|\phi_x\rangle}$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N}|\psi_f\rangle|f\rangle = \sum_{x\in[N]}|x\rangle \underbrace{\sum_{f\in\{0,1\}^N}(-1)^{f_x}|f\rangle}_{|\phi_x\rangle} = \sum_{x\in[N]}|x\rangle|\phi_x\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]} |x\rangle \sum_{f\in\{0,1\}^N} (-1)^{f_x}|f\rangle = \sum_{x\in[N]} |x\rangle|\phi_x\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]}|x\rangle \sum_{f\in\{0,1\}^N}(-1)^{f_x}|f\rangle = \sum_{x\in[N]}|x\rangle|\phi_x\rangle$$

Next, let's try to compress the N-qubit state $|\phi_x\rangle$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]} |x\rangle \sum_{f\in\{0,1\}^N} (-1)^{f_x}|f\rangle = \sum_{x\in[N]} |x\rangle|\phi_x\rangle$$

Next, let's try to compress the N-qubit state $|\phi_x\rangle$

$$|\phi_x\rangle = \sum_{f\in\{0,1\}^N} (-1)^{f\cdot e_x}|f\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]}|x\rangle \sum_{f\in\{0,1\}^N}(-1)^{f_x}|f\rangle = \sum_{x\in[N]}|x\rangle|\phi_x\rangle$$

Next, let's try to compress the N-qubit state $|\phi_x\rangle$

$$|\phi_x\rangle = \sum_{f\in\{0,1\}^N}(-1)^{f\cdot e_x}|f\rangle = H^{\otimes N}|e_x\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]} |x\rangle \sum_{f\in\{0,1\}^N} (-1)^{f_x}|f\rangle = \sum_{x\in[N]} |x\rangle|\phi_x\rangle$$

Next, let's try to compress the N-qubit state $|\phi_x\rangle$

$$|\phi_x\rangle = \sum_{f\in\{0,1\}^N} (-1)^{f\cdot e_x}|f\rangle = H^{\otimes N}|e_x\rangle$$

So $|\phi_x\rangle$'s are **orthogonal** and we can map $|\phi_x\rangle \mapsto |x\rangle$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]} |x\rangle \sum_{f\in\{0,1\}^N} (-1)^{f_x}|f\rangle = \sum_{x\in[N]} |x\rangle|\phi_x\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N}|\psi_f\rangle|f\rangle = \sum_{x\in[N]}|x\rangle\sum_{f\in\{0,1\}^N}(-1)^{f_x}|f\rangle = \sum_{x\in[N]}|x\rangle|\phi_x\rangle$$

Step 2: Apply the isometry that maps $|\phi_x\rangle \mapsto |x\rangle$.

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]} |x\rangle \sum_{f\in\{0,1\}^N} (-1)^{f_x}|f\rangle = \sum_{x\in[N]} |x\rangle|\phi_x\rangle$$

Step 2: Apply the isometry that maps $|\phi_x\rangle \mapsto |x\rangle$. We get

$$\sum_{x\in[N]} |x\rangle|x\rangle$$

Define the phase state $|\psi_f\rangle = \sum_{x\in[N]}(-1)^{f_x}|x\rangle$.

Goal: show that $\rho := \mathbb{E}_{f\leftarrow\{0,1\}^N}|\psi_f\rangle\langle\psi_f|$ is maximally mixed.

Step 1: Write down an "obvious" purification of ρ:

$$|\Phi\rangle \propto \sum_{f\in\{0,1\}^N} |\psi_f\rangle|f\rangle = \sum_{x\in[N]}|x\rangle \sum_{f\in\{0,1\}^N}(-1)^{f_x}|f\rangle = \sum_{x\in[N]}|x\rangle|\phi_x\rangle$$

Step 2: Apply the isometry that maps $|\phi_x\rangle \mapsto |x\rangle$. We get

$$\sum_{x\in[N]}|x\rangle|x\rangle$$

Since this is a purification of ρ, this means ρ is maximally mixed!

Rest of today: [MH24] PRU proof on the blackboard

Preliminary draft of the paper:

fermima.com/pru.pdf