

Unitary Designs

MATH595 RQT 2025

Mayank Bhatia, Theshani Nuradha, Shuen Wu

Overview

- Introduction to Unitary k -designs
- Unitary 2-designs and fidelity estimation
- Clifford group is unitary 3-design
- Unitary designs in nearly optimal depth

Introduction

- Generating **random states and random unitary operators** is an important resource in quantum information processing
- Generating Haar-random unitary operators is inefficient: the number of gates grows **exponentially with the number of qubits**.
- Useful to identify **subsets of the unitary group** that can adequately simulate the Haar-measure

Unitary k -designs

$$\sum_{i=1}^M p_i V_i^{\otimes k} X (V_i^\dagger)^{\otimes k} = \int_{\mathcal{U}_d} U^{\otimes k} X (U^\dagger)^{\otimes k} dU \quad \text{for all } X \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$$

$$\mathbb{E}_{V \sim p} [V^{\otimes k} X (V^\dagger)^{\otimes k}] = E_{U \sim \mu_H} [U^{\otimes k} X (U^\dagger)^{\otimes k}]$$

- $(p_i, V_i)_{i=1}^M$ is called a unitary k -design
- Unitary k -design implies unitary $k - 1$ -design
(choose $X = Y \otimes \frac{I}{d}$ and apply partial trace)

Equivalent Definitions

1. $\mathbb{E}_{V \sim p} [V^{\otimes k} X V^{\dagger \otimes k}] = \mathbb{E}_{U \sim \mu_H} [U^{\otimes k} X U^{\dagger \otimes k}]$ for all $X \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$.
2. $\mathbb{E}_{V \sim p} [V^{\otimes k} \otimes V^{*\otimes k}] = \mathbb{E}_{U \sim \mu_H} [U^{\otimes k} \otimes U^{*\otimes k}]$.
3. $\mathbb{E}_{V \sim p} [p(V)] = \mathbb{E}_{U \sim \mu_H} [p(U)]$ for all polynomials $p(U)$ homogeneous of degree k in the matrix elements of U and homogeneous of degree k in the matrix elements of U^* .

For unitary 2-designs

- For a super operator Λ (quantum channel)

$$\mathbb{E}_{U \sim \nu}(\Lambda) : \rho \mapsto \int_{\mathcal{U}(D)} d\nu(U) U^\dagger \Lambda(U \rho U^\dagger) U$$

If ν is set to the uniform probability measure on $\{U_1, \dots, U_K\}$ then, for any quantum channel Λ ,

$$\mathbb{E}_\nu(\Lambda) = \mathbb{E}_{\mu_H}(\Lambda).$$

Approximate unitary 2-design

$$\|\mathbb{E}_\nu(\Lambda) - \mathbb{E}_{\mu_H}(\Lambda)\|_\diamond \leq \varepsilon \|\Lambda\|_\diamond$$

Diamond distance of two channels:

$$\sup_{\rho_{RA}} \frac{1}{2} \|\mathcal{N}_{A \rightarrow B}(\rho_{RA}) - \mathcal{M}_{A \rightarrow B}(\rho_{RA})\|_1$$

Dankert, C., Cleve, R., Emerson, J., & Livine, E. (2009). Exact and Approximate Unitary 2-Designs and their Application to Fidelity Estimation. *Physical Review A—Atomic, Molecular, and Optical Physics*, 80(1), 012304.

Gross, D., Audenaert, K., & Eisert, J. (2007). Evenly distributed unitaries: On the structure of unitary designs. *Journal of mathematical physics*, 48(5).

Clifford Group

- Normalizer of the Pauli group under conjugation, it takes one Pauli operator to another.

The uniform distribution over the Clifford group on n qubits is a unitary 2-design with $D = 2^n$.

- Can be constructed by circuits of size $O(n^2)$

Approximate unitary 2-design

For all $\varepsilon > 0$, an ε -approximate unitary 2-design on n qubits can be implemented by in-place circuits of size $O(n \log 1/\varepsilon)$ and depth $O(\log n \log 1/\varepsilon)$.

Unitary 2-designs and fidelity estimation

- Average fidelity of a channel (Haar –average)

$$F_{\text{avg}}(\Lambda) \equiv \int_{\mathcal{U}(d)} dU \text{Tr}[U|0\rangle\langle 0|U^\dagger \Lambda(U|0\rangle\langle 0|U^\dagger)]$$

- It is a polynomial function of homogeneous degree 2
- Sampling from **unitary 2-design** is sufficient
- Can be used estimate entanglement fidelity

$$F_e(\Lambda) = \langle \Phi | (\mathcal{I} \otimes \Lambda) (|\Phi\rangle\langle \Phi|) | \Phi \rangle$$

$$F_{\text{avg}}(\Lambda) = \frac{dF_e(\Lambda) + 1}{d + 1}$$

- A proof idea for: $F_{\text{avg}}(\Lambda) = \frac{dF_e(\Lambda) + 1}{d + 1}$
 - Two channel fidelities are invariant under twirling wrt. the unitary group
 - The equality holds for the depolarizing channel
 - Twirling a channel wrt. the unitary group gives the depolarizing channel
 - So, the inequality holds for all channels

$$\begin{array}{ccc}
 \rho & \leftrightarrow & \Lambda_\rho \\
 \text{twirl} \downarrow & & \downarrow \text{twirl} \\
 \rho_p & \leftrightarrow & \Lambda_p^{\text{dep}}
 \end{array}$$

Horodecki, M., Horodecki, P., & Horodecki, R. (1999). General teleportation channel, singlet fraction, and quasidistillation. *Physical Review A*, 60(3), 1888.

Nielsen, M. A. (2002). A simple formula for the average gate fidelity of a quantum dynamical operation. *Physics Letters A*, 303(4), 249-252.

Fidelity Estimation Protocol

$$F_{\text{avg}}(\Lambda) \equiv \int_{\mathcal{U}(d)} dU \text{Tr}[U|0\rangle\langle 0|U^\dagger \Lambda(U|0\rangle\langle 0|U^\dagger)]$$

- By sampling from Clifford group
 - Apply random unitary to the input state to 0 state
 - Apply the channel
 - Apply unitary conjugate to the output state
 - Measure in the computational basis
 - Repeating this process

The average fidelity of a quantum channel Λ acting on n qubits, can be estimated to within $\delta > 0$ with error probability $\varepsilon > 0$ at a cost of $O(\log 1/\varepsilon)$ evaluations of the channel conjugated by in-place circuits of size $O(\mathbf{n} \log 1/\varepsilon)$ and depth $O(\log \mathbf{n} \log 1/\varepsilon)$

The Clifford Group is a Unitary 3-design

Theorem 2. The Clifford group is a unitary 3-design. [Webb, Z. (2015)]

- Defines Pauli invariance and Pauli mixing
- Defines Pauli 2-mixing
- Shows Clifford group is Pauli invariant and Pauli 2-mixing
- Shows Pauli invariance + Pauli 2-mixing implies an ensemble is a 3-design
- Hence, Clifford group is a 3-design

Pauli Group Notation

Some notation on the Pauli group:

- $\tilde{\mathcal{P}}_1 := \langle i\mathbb{I}_{\mathbb{C}^2}, \sigma_X, \sigma_Z \rangle$
- $\tilde{\mathcal{P}}_n := \tilde{\mathcal{P}}_1^{\otimes n}$
- $\mathcal{P}_n := \tilde{\mathcal{P}}_n / \langle i\mathbb{I}_{\mathbb{C}^{2^n}} \rangle$ where as representatives we take $p \in \mathcal{P}_n$ with $p^2 = \mathbb{I}_{\mathbb{C}^{2^n}}$
- $\hat{\mathcal{P}}_n := \mathcal{P}_n \setminus \{ \mathbb{I}_{\mathbb{C}^{2^n}} \}$
- $\bar{\mathcal{P}}_n := \{ \pm p : p \in \hat{\mathcal{P}}_n \}$
- $F(p_1, p_2) := \begin{cases} 0, & p_1 p_2 = p_2 p_1, \\ 1, & p_1 p_2 = -p_2 p_1. \end{cases}$

Generalized Pauli Group

We can define

$$\tilde{\mathcal{P}}_1^d := \langle \tilde{\omega} \mathbb{I}_{\mathbb{C}^d}, \sigma_X^d, \sigma_Z^d \rangle$$

where $\sigma_X^d |j\rangle := |j+1 \pmod{d}\rangle$, $\sigma_Z^d |j\rangle := \omega^j |j\rangle$, $\omega := e^{2\pi i/d}$, $\tilde{\omega} := \begin{cases} \omega, & d \text{ odd,} \\ e^{\pi i/d}, & d \text{ even.} \end{cases}$

This gives us

- $\tilde{\mathcal{P}}_1^d := \langle \tilde{\omega} \mathbb{I}_{\mathbb{C}^d}, \sigma_X^d, \sigma_Z^d \rangle$ The Pauli group on one qudit
- $\tilde{\mathcal{P}}_n^d := (\tilde{\mathcal{P}}_1^d)^{\otimes n}$ The Pauli group on n qudits
- $\mathcal{P}_n^d := \tilde{\mathcal{P}}_n^d / \langle \tilde{\omega} \mathbb{I}_{\mathbb{C}^{d^n}} \rangle$ The Pauli group modulo phases
- $\hat{\mathcal{P}}_n^d := \mathcal{P}_n^d \setminus \{ \mathbb{I}_{\mathbb{C}^{d^n}} \}$ The Pauli group w/o phases or the identity element
- $\bar{\mathcal{P}}_n^d := \{ \omega^\ell p : p \in \hat{\mathcal{P}}_n^d, \ell \in [d] \}$ Non-identity Pauli elements with order dividing d

Clifford Group Notation

Some notation on the Clifford group:

- $\tilde{\mathcal{C}}_n := \{ c \in \mathcal{U}(\mathbb{C}^{2^n}) : \forall p \in \mathcal{P}_n, cpc^\dagger \in \tilde{\mathcal{P}}_n \}$
- $\mathcal{C}_n := \tilde{\mathcal{C}}_n / \{ e^{i\theta} \mathbb{I}_{\mathbb{C}^{2^n}} : \theta \in \mathbb{R} \}$

There also exists a generalized Clifford group with associated notation:

- $\tilde{\mathcal{C}}_n^d := \{ c \in \mathcal{U}(\mathbb{C}^{d^n}) : \forall p \in \mathcal{P}_n^d, cpc^\dagger \in \tilde{\mathcal{P}}_n^d \}$
- $\mathcal{C}_n^d := \tilde{\mathcal{C}}_n^d / \{ e^{i\theta} \mathbb{I}_{\mathbb{C}^{d^n}} : \theta \in \mathbb{R} \}$

Clifford Group Notation

We will consider subsets of the \mathcal{C}_n^d in which a particular element of \mathcal{P}_n^d gets mapped to another. For $p \in \widehat{\mathcal{P}}_n^d$ and $q \in \overline{\mathcal{P}}_n^d$, we define

$$\mathcal{C}_{p \rightarrow q} := \{ c \in \mathcal{C}_n^d : cpc^\dagger = q \}$$

We can also consider a vectorized version where $\mathbf{p} \in (\widehat{\mathcal{P}}_n^d)^m$, $\mathbf{q} \in (\overline{\mathcal{P}}_n^d)^m$:

$$\mathcal{C}_{\mathbf{p} \rightarrow \mathbf{q}} := \{ c \in \mathcal{C}_n^d : \forall i \in [m], cp_i c^\dagger = q_i \}$$

Ensembles

Definition. A (finite) ensemble of unitaries over \mathcal{X} is denoted by $\mathcal{E} = \{(\alpha_i, U_i)\}_{i \in [m]}$, where each U_i is a unitary over \mathcal{X} , $\alpha \in \mathbb{R}^m$ is a probability vector, and we think of α_i as the probability that U_i is chosen from the ensemble.

We are interested in ensembles of Clifford elements. If \mathcal{E} is an ensemble of unitaries over \mathbb{C}^{d^n} consisting only of generalized Clifford elements, and if $p \in \widehat{\mathcal{P}}_n^d$ and $q \in \overline{\mathcal{P}}_n^d$, then $\mathcal{E}_{p \rightarrow q}$ is the sub-ensemble that only contains the generalized Clifford elements that take p to q under conjugation:

$$\mathcal{E}_{p \rightarrow q} := \{(\alpha, U) \in \mathcal{E} : U \in \mathcal{C}_{p \rightarrow q}\}.$$

We can extend this to sets of generalized Pauli elements: if $\mathbf{p} \in (\widehat{\mathcal{P}}_n^d)^m$ and $\mathbf{q} \in (\overline{\mathcal{P}}_n^d)^m$, we define

$$\mathcal{E}_{\mathbf{p} \rightarrow \mathbf{q}} := \{(\alpha, U) \in \mathcal{E} : U \in \mathcal{C}_{\mathbf{p} \rightarrow \mathbf{q}}\}.$$

Pauli Invariance

Definition 2 (Pauli-invariant). If $\mathcal{X} = \mathbb{C}^{d^n}$, then an ensemble \mathcal{E} is (right) Pauli-invariant if for every $p \in \mathcal{P}_n^d$,

$$(\alpha, U) \in \mathcal{E} \implies (\alpha, e^{i\theta_U} U p) \in \mathcal{E},$$

for some $\theta_U \in \mathbb{R}$.

- The ensemble does not "care" if you right-multiply everything by a Pauli matrix
- Right multiplication keeps the ensemble's action compatible with how Paulis transform under conjugation

Pauli Mixing

Definition 3 (Pauli Mixing). Let \mathcal{E} be a Pauli-invariant \mathcal{C}_n^d -ensemble. We say that \mathcal{E} is Pauli Mixing if for all $p \in \widehat{\mathcal{P}}_n^d$ the action of \mathcal{E} on p maps it to a uniform distribution over $\overline{\mathcal{P}}_n^d$. Explicitly, \mathcal{E} is Pauli mixing if for all $p \in \widehat{\mathcal{P}}_n^d$ and $q \in \overline{\mathcal{P}}_n^d$,

$$\sum_{(\alpha, U) \in \mathcal{E}_{p \rightarrow q}} \alpha = \frac{1}{|\overline{\mathcal{P}}_n^d|} = \frac{1}{d |\widehat{\mathcal{P}}_n^d|} = \frac{1}{d(d^{2n} - 1)}.$$

(Note that it can be proven that if an ensemble is Pauli invariant and Pauli Mixing, it can be shown that it must be a 2-design. We can show that the Clifford group is a 2-design via this method as well.)

Pauli 2-Mixing

Definition 4 (Pauli 2-mixing). Let \mathcal{E} be a \mathcal{C}_n^d -ensemble. We say that \mathcal{E} is Pauli 2-mixing if for all $p_1, p_2 \in \widehat{\mathcal{P}}_n^d$ and $p_1 \neq p_2$, the action of \mathcal{E} is to map (p_1, p_2) to a uniform distribution over $H_{F(p_1, p_2)}$. Explicitly, \mathcal{E} is Pauli 2-mixing if for all $\mathbf{p} = (p_1, p_2) \in (\widehat{\mathcal{P}}_n^d)^2$ with $p_1 \neq p_2$, and all $\mathbf{q} \in H_{F(p_1, p_2)}$,

$$\sum_{(\alpha, U) \in \mathcal{E}_{\mathbf{p} \rightarrow \mathbf{q}}} \alpha = \frac{1}{|H_{F(p_1, p_2)}|} = \begin{cases} \frac{1}{d|\widehat{\mathcal{P}}_n^d|(|\widehat{\mathcal{P}}_n^d| + 1 - 2d)} = \frac{1}{d(d^{2n} - 1)(d^{2n} - 2d)}, & F(p_1, p_2) = 0, \\ \frac{1}{d|\widehat{\mathcal{P}}_n^d|(|\widehat{\mathcal{P}}_n^d| + 1)} = \frac{1}{d^{2n+1}(d^{2n} - 1)}, & F(p_1, p_2) \neq 0. \end{cases}$$

where

$$H_\ell := \{ (q_1, q_2) \in (\overline{\mathcal{P}}_n^d)^2 : q_1 \not\sim q_2 \text{ and } F(q_1, q_2) = \ell \}.$$

(Note that if an ensemble is Pauli 2-mixing, then it is Pauli mixing.)

Clifford Group is Pauli Invariant + 2-Mixing

Lemma 3. The uniform ensemble \mathcal{E} over the generalized Clifford group on n qudits is Pauli-invariant and Pauli 2-Mixing.

- The generalized Pauli group is a subgroup of the Clifford group, hence we get Pauli-invariance for free.
- Clifford unitaries map any Pauli pair to any other pair with the same commutation relation.
- This action is transitive: all valid target pairs are equally reachable.
- Sets of Cliffords sending one pair to another all have the same size.
- Therefore the Clifford group spreads each Pauli pair uniformly over its orbit.
- This uniformity is exactly the Pauli 2-mixing property.

Clifford Group is a 3-design

Lemma 4. If \mathcal{E} is a Pauli-invariant and Pauli 2-mixing \mathcal{C}_n -ensemble, then \mathcal{E} is a unitary 3-design.

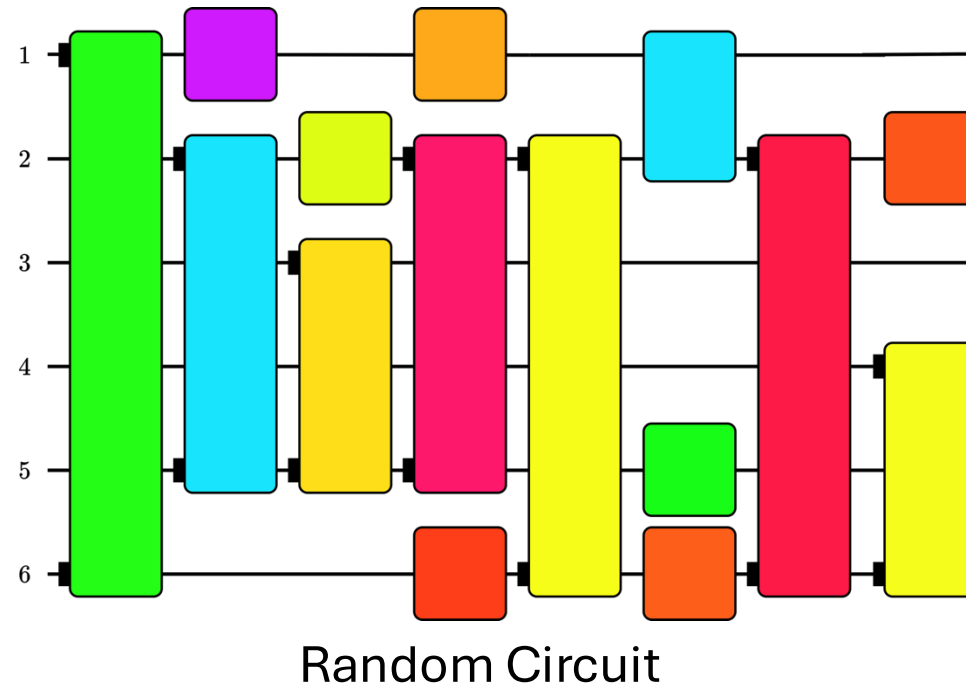
- To show the Clifford ensemble is a 3-design, it suffices to compare the 3-fold twirl on Pauli basis elements $p_1 \otimes p_2 \otimes p_3$.
- The proof splits into three cases depending on relations among the three Paulis.
- **Case 1:** One Pauli is \mathbb{I} . The 3-fold twirl reduces to the 2-design case.
- **Case 2:** $p_1 p_2 = p_3$. Use Pauli 2-mixing to average uniformly over Pauli pairs, expand in permutation operators W_π , and obtain the Haar expression.
- **Case 3:** Product $p_1 p_2 p_3$ anticommutes with some Pauli. Pauli-invariance symmetrizes the sum, giving cancellation as in Haar.
- All Pauli triples fall into one of these cases, so the Clifford twirl matches the Haar twirl; hence the ensemble is a 3-design.

Unitary designs in nearly optimal depth

Cui–Schuster–Brandão–Huang (2025)

Main result

- What is the minimum circuit depth required to generate a unitary that is indistinguishable from a Haar-random unitary?



- This work constructs unitary k -designs with depth $O(\log \log n)$.

Preliminaries

- K-th moment channel of an ensemble

$$\Phi_{\mathcal{E}}(X) := \mathbb{E}_{U \sim \mathcal{E}} \left[U^{\otimes k} X (U^\dagger)^{\otimes k} \right]$$

- Additive error condition

$$\left\| \Phi_{\mathcal{E}} - \Phi_{\mathbf{H}} \right\|_{\diamond} \leq \varepsilon.$$

- Relative error condition

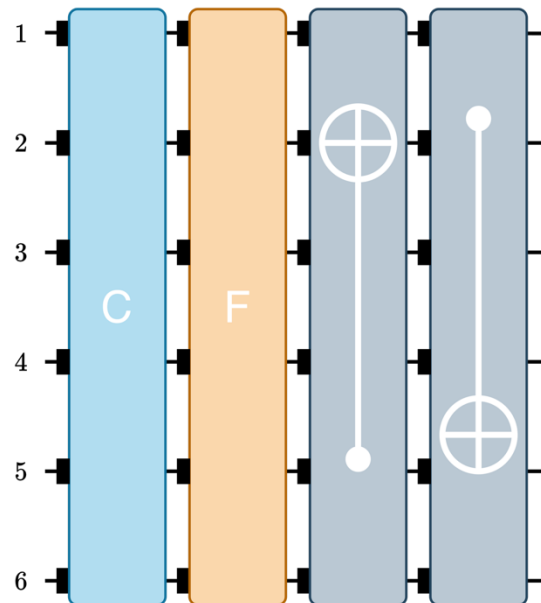
$$(1 - \varepsilon) \Phi_{\mathbf{H}} \preceq \Phi_{\mathcal{E}} \preceq (1 + \varepsilon) \Phi_{\mathbf{H}}$$

LRFC unitary

- LRFC circuits are highly structured:

$$U = S_L S_R F C \equiv \left[\sum_{x \in \{0,1\}^n} |x_L \oplus h_L(x_R) \parallel x_R\rangle \langle x_L \parallel x_R| \right] \left[\sum_{x' \in \{0,1\}^n} |x'_L \parallel x'_R \oplus h_R(x'_L)\rangle \langle x'_L \parallel x'_R| \right] \left[\sum_{z \in \{0,1\}^n} (-1)^{f(z)} |z\rangle \langle z| \right] C$$

- Each function is uniformly random.



Error decays

- Lemma techniques:
 - Decompose the k-th moment channel into Haar/error parts
 - Write $\Phi_\varepsilon = \Phi_H + \delta\Phi$
 - Φ_H is the k-th moment channel for Haar
 - $\delta\Phi$ is the error channel, orthogonal to Haar
 - Spectral decomposition of a Hermitian operator to positive/negative parts
 - Triangle inequality for the trace norm
- Lemma statement:
 - If Φ_ε has additive error ε , then $\Phi_\varepsilon \circ \Phi_\varepsilon$ has additive error at most ε^2 .

Comparing additive and relative error

- This relationship comes from applying the results of [cite]

$$\varepsilon_{\text{rel}} = \underbrace{2^{nk}}_{\text{normalization}} \underbrace{\binom{2^n + k - 1}{k}}_{\dim(\text{Sym}^k(\mathbb{C}^{2^n}))} \varepsilon_{\text{add}} \stackrel{\text{combinatorics}}{\leq} \left(\frac{4^{nk}}{k!}\right) \left(1 + \frac{k^2}{2^n}\right) \varepsilon_{\text{add}}$$

Tiny additive error implies small relative error

- 1) If Φ_{ε} has additive error ε , then $\Phi_{\varepsilon} \circ \Phi_{\varepsilon}$ has additive error at most ε^2
 - Therefore, the $(\text{LRFC})^P$ ensemble is a unitary k -design with additive error
$$\varepsilon_{\text{add}} = O\left(\frac{k^2}{2^{n/2}}\right)^p = O\left(\left(\frac{k^2}{2^{n/2}}\right)^p\right)$$
- 2) $\varepsilon_{\text{rel}} \leq \left(\frac{4^{nk}}{k!}\right) \left(1 + \frac{k^2}{2^n}\right) \varepsilon_{\text{add}}$
 - Therefore, the $(\text{LRFC})^P$ ensemble is a unitary k -design with relative error
$$\varepsilon_{\text{rel}} = f(n, k) \varepsilon_{\text{add}}$$

Relative error gluing theorem

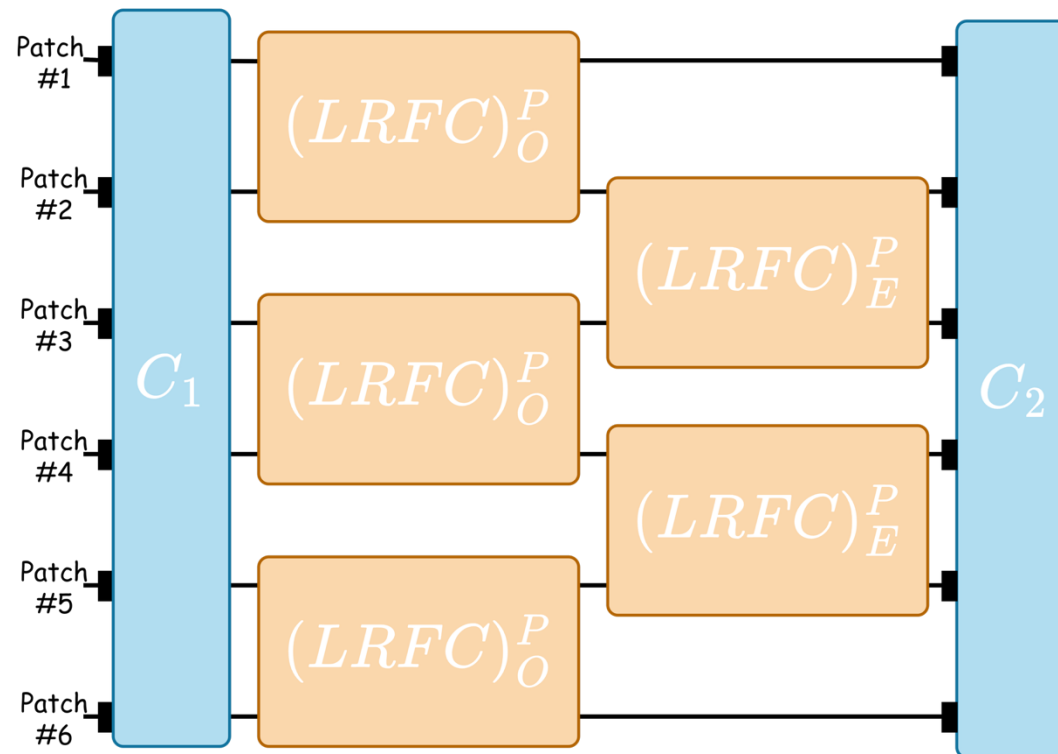
- This theorem is from Schuster, Haferkamp & Huang (2025)

Theorem 1 (Gluing small random unitary designs). *Given any approximation error $\varepsilon \leq 1$. Suppose each small random unitary in the two-layer brickwork ensemble \mathcal{E} is drawn from an $\frac{\varepsilon}{n}$ -approximate unitary k -design on 2ξ qubits with circuit depth d . Then \mathcal{E} forms an ε -approximate unitary k -design on n qubits with depth $2d$, whenever the local patch size is at least $\xi \geq \log_2(nk^2/\varepsilon)$.*

- Fact: block amplified LFRC circuit can be implemented in depth $O(p \log(k) \log(\xi))$
- Hence, taking $p = 8k + 1$ and the required local patch size, we can achieve approximate unitary k -designs in depth $O(k \log(k) \log \log(nk/\varepsilon))$. Note, this closely matches lower bounds.

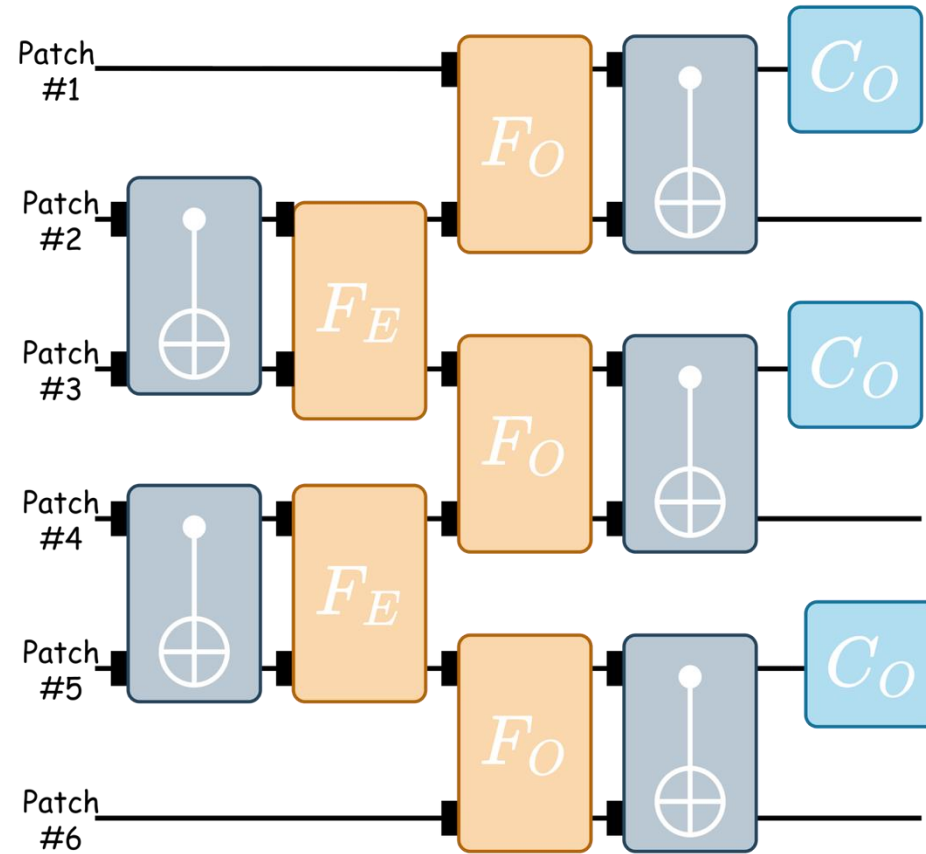
Block amplified LRFC circuit

- Hence, the following highly structured and nearly optimally shallow circuit approximately simulates a random unitary up to the k -th moment.



Other main result: blocked LRFC circuit

$$U = S_o \cdot F_e \cdot F_o \cdot S_e \cdot C_o$$



Citations

- Dankert, Cleve, Emerson & Livine (2009). *Exact and approximate unitary 2-designs and their application to fidelity estimation*. Phys. Rev. A 80, 012304.
- Webb (2016). *The Clifford group forms a unitary 3-design*. arXiv:1510.02769.
- Cui, Schuster, Brandão & Huang (2025). *Unitary designs in nearly optimal depth*. arXiv:2507.06216.
- Schuster, Haferkamp & Huang (2025). *Random unitaries in extremely low depth*. arXiv:2407.07754.