Haar measures and unitary designs

Myeongjin Shin

QISCA Summer School 2025
Quantum Learning and Complexity Theory – **Lecture 2**

July 20, 2025

Haar measure

Definition 1 (Haar measure)

The Haar measure on the unitary group $\mathrm{U}(d)$ is the unique probability measure μ_H that is both left and right invariant over the group $\mathrm{U}(d)$, i.e., for all integrable functions f and for all $V \in \mathrm{U}(d)$, we have:

$$\int_{\mathrm{U}(d)} f(U)\, d\mu_H(U) = \int_{\mathrm{U}(d)} f(UV)\, d\mu_H(U) = \int_{\mathrm{U}(d)} f(VU)\, d\mu_H(U). \tag{1}$$

The Haar measure is a probability measure, satisfying:

- $\int_S 1\, d\mu_H(U) \geq 0$
- $\int_{\mathrm{U}(d)} 1\, d\mu_H(U) = 1$
- $\mathbb{E}_{U \sim \mu_H} [f(U)] := \int_{\mathrm{U}(d)} f(U)\, d\mu_H(U)$

Why Haar measure?

- Tool for **analyzing** randomness.
- Among the randomness, we have to find the answer. We can get the **probability** of finding the answer. ($\text{Prob}_{|\phi\rangle\sim\mu_H}[|f(\phi) - \mathbb{E}_{|\psi\rangle\sim\mu_H}[f(\psi)]| \geq \epsilon]$). The calculations of probability can lead to **complexity**.
- Applications in fidelity, channel calculations, concentration inequalities, quantum machine learning, classical shadow tomography, etc.

Haar measure properties

right

$E\left[(UV)^{\otimes k_1} \otimes (UV)^{*\otimes k_2}\right]$

$V = e^{\frac{i2\pi}{k_1 - k_2}}$

$\parallel$

Proposition 2

Let $k_1, k_2 \in \mathbb{N}$. If $k_1 \neq k_2$, then we have $\underset{U \sim \mu_H}{\mathbb{E}} \left[U^{\otimes k_1} \otimes U^{* \otimes k_2}\right] = 0$. $e^{i2\pi} E[\ \parallel\ ]$

$k = k_1 = k_2$ $\quad = -1$

Proposition 3

For all integrable functions f defined on $\mathrm{U}(d)$, we have that:

unique

$$\underset{U \sim \mu_H}{\mathbb{E}} \left[f\left(U^\dagger\right)\right] = \underset{U \sim \mu_H}{\mathbb{E}} \left[f\left(U\right)\right]. \tag{2}$$

Moment operator

Definition 4 (k-th Moment operator)

The k-th moment operator, with respect to the probability measure μ_H, is defined as $\mathcal{M}^{(k)}_{\mu_H} : \mathcal{L}\left((\mathbb{C}^d)^{\otimes k}\right) \to \mathcal{L}\left((\mathbb{C}^d)^{\otimes k}\right)$:

$$\mathcal{M}^{(k)}_{\mu_H}(O) := \mathop{\mathbb{E}}_{U \sim \mu_H}\left[U^{\otimes k} O U^{\dagger \otimes k}\right], \tag{3}$$

for all operators $O \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$.

In order to characterize the moment operator, we need to define the k**-th order commutant** of a set of matrices S.

Commutant

Definition 5 (Commutant)

Given $S \subseteq \mathcal{L}\left(\mathbb{C}^d\right)$, we define its k-th order commutant as

$[A, B] = AB - BA$

$$\mathrm{Comm}(S, k) := \{A \in \mathcal{L}\left((\mathbb{C}^d)^{\otimes k}\right) : \left[A, B^{\otimes k}\right] = 0 \ \forall B \in S\}. \quad (4)$$

It is worth noting that $\mathrm{Comm}(S, k)$ is a vector subspace.(pset)

Properties of Moment operator

Lemma 6 (Properties of the moment operator)

The moment operator $\mathcal{M}_{\mu_H}^{(k)}(\cdot) := \underset{U\sim\mu_H}{\mathbb{E}}\left[U^{\otimes k}\,(\cdot)\,U^{\dagger\otimes k}\right]$ *has the following properties:*

1. *It is linear, trace-preserving, and self-adjoint with respect to the Hilbert-Schmidt inner product.*
2. *For all* $A \in \mathcal{L}\left((\mathbb{C}^d)^{\otimes k}\right)$, $\mathcal{M}_{\mu_H}^{(k)}(A) \in \mathrm{Comm}(\mathrm{U}(d), k)$.
3. *If* $A \in \mathrm{Comm}(\mathrm{U}(d), k)$, *then* $\mathcal{M}_{\mu_H}^{(k)}(A) = A$.

$\langle M_{\mu_H}^{(k)}(A), B\rangle = \langle A, M_{\mu_H}^{(k)}(B)\rangle$

$\mathrm{Tr}(M_k(A), B)$

$= \mathbb{E}\,\mathrm{Tr}(U^{\otimes k} A U^{\dagger\otimes k} B)$

$= \mathbb{E}\,\mathrm{Tr}(A\, U^{\dagger\otimes k} B\, U^{\otimes k})$

$= \mathrm{Tr}(A, M_k(B))$

Projector onto the commutant

Theorem 7 (Projector onto the commutant)

The moment operator $\mathcal{M}^{(k)}_{\mu_H}(\cdot) = \mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes k}\,(\cdot)\,U^{\dagger\otimes k}\right]$ *is the orthogonal projector onto the commutant* $\mathrm{Comm} := \mathrm{Comm}(\mathrm{U}(d), k)$ *with respect to the Hilbert-Schmidt inner product. In particular, let* $P_1, \ldots, P_{\dim(\mathrm{Comm})}$ *be an orthonormal basis of* Comm *and let* $O \in \mathcal{L}((\mathbb{C}^d)^{\otimes k})$*. Then, we have:*

extended basis $P_1, P_2, \cdots, P_{\dim(U)}$

$$\mathcal{M}^{(k)}_{\mu_H}(O) = \sum_{i=1}^{\dim(\mathrm{Comm})} \langle P_i, O\rangle_{HS} P_i \,. \tag{5}$$

$$M_{\mu_H}^{(k)}(O) = \sum_{i=1}^{\dim(U)} \langle P_i, M_{\mu_H}^{(k)}(O)\rangle P_i = \sum_{i=1}^{\dim(\mathrm{Comm})} \langle P_i, \,\cdot\,\rangle P_i + \cancel{\sum_{i>1}}$$

$$= \sum_i \langle P_i, O\rangle P_i$$

$M_{\mu_H}(O)^{(k)}$

$$\langle O, M_{\mu_H}(P_i)^{(k)}\rangle = \langle O, P_i\rangle$$

Permutation operators

Definition 8 (Permutation operators)

Given $\pi \in S_k$ an element of the symmetric group S_k, we define the permutation matrix $V_d(\pi)$ to be the unitary matrix that satisfies:

$$V_d(\pi) \underline{|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle} = \underline{|\psi_{\pi^{-1}(1)}\rangle \otimes \cdots \otimes |\psi_{\pi^{-1}(k)}\rangle}, \tag{6}$$

for all $|\psi_1\rangle, \ldots, |\psi_k\rangle \in \mathbb{C}^d$.

Theorem 9 (Schur-Weyl duality)

The k-th order commutant of the unitary group is the span of the permutation operators associated to S_k:

$$\mathrm{Comm}(\mathrm{U}(d), k) = \mathrm{span}\Big(V_d(\pi) : \pi \in S_k\Big). \tag{7}$$

Easy to check that $\mathrm{span}\Big(V_d(\pi) : \pi \in S_k\Big) \subseteq \mathrm{Comm}(\mathrm{U}(d), k)$.

How about $\mathrm{Comm}(\mathrm{U}(d), k) \subseteq \mathrm{span}\Big(V_d(\pi) : \pi \in S_k\Big)$? (pset)

$\forall U \in U(d)$

$\underline{V_d(\pi) U^{\otimes k} = U^{\otimes k} V_d(\pi)}$

$V_d(\pi) U^{\otimes k} |\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle = V_d(\pi) \left(U|\psi_1\rangle \otimes \cdots \otimes U|\psi_k\rangle\right)$

$= U^{\otimes k} V_d(\pi) |\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$

Permutation operators

Proposition 10

For $\pi \in S_k$, the permutation matrices $V_d(\pi)$ are linearly independent if $k \leq d$, but linearly dependent if $k > d$.

Definition 11 (Identity and Flip operators)

The identity permutation operator $\mathbb{I}$ is:

$$\mathbb{I}\left(|\psi\rangle \otimes |\phi\rangle\right) = |\psi\rangle \otimes |\phi\rangle\,, \qquad \text{for all } |\psi\rangle\,, |\phi\rangle \in \mathbb{C}^d. \tag{8}$$

The Flip operator $\mathbb{F}$ is:

"swap

$$\mathbb{F}\left(|\psi\rangle \otimes |\phi\rangle\right) = |\phi\rangle \otimes |\psi\rangle\,, \qquad \text{for all } |\psi\rangle\,, |\phi\rangle \in \mathbb{C}^d. \tag{9}$$

$\mathbf{Tr}((A \otimes B)\, F) = \mathbf{Tr}\,(AB).$

Theorem 12 (Computing moments)

Let $O \in \mathcal{L}\left((\mathbb{C}^d)^{\otimes k}\right)$. The moment operator can then be expressed as a linear combination of permutation operators:

$\in \mathrm{Comm}(U(d), k)$

$\mathrm{tr}(\mathbb{E}[\cancel{U^{\otimes k}} O \underbrace{U^{\dagger\otimes k} V_d(\sigma)^\dagger}_{V_d(\sigma) \cancel{U^{\otimes k}}}]$

$$\mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes k} O U^{\dagger\otimes k}\right] = \sum_{\pi\in S_k} c_\pi(O) V_d(\pi), \tag{10}$$

where the coefficients $c_\pi(O)$ can be determined by solving the following linear system of $k!$ equations:

$$\mathbf{Tr}\left(V_d^\dagger(\sigma) O\right) = \sum_{\pi\in S_k} c_\pi(O)\mathbf{Tr}\left(V_d^\dagger(\sigma) V_d(\pi)\right) \quad \text{for all } \sigma \in S_k. \tag{11}$$

This system always has at least one solution.

Examples on the next slides.

Computing moments examples

Example 13

$$\mathrm{Comm}(\mathrm{U}(d), k = 1) = \mathsf{span}\left(I\right), \tag{12}$$

$$\mathrm{Comm}(\mathrm{U}(d), k = 2) = \mathsf{span}\left(\mathbb{I}, \mathbb{F}\right). \tag{13}$$

Prove this.(pset)

Computing moments examples

Example 14 (First and second moment)

Given $O \in \mathcal{L}\left(\mathbb{C}^d\right)$, we have:

$$\mathop{\mathbb{E}}_{U\sim\mu_H}\left[UOU^\dagger\right] = \frac{\mathbf{Tr}(O)}{d} I. \tag{14}$$

Given $O \in \mathcal{L}((\mathbb{C}^d)^{\otimes 2})$, we have:

$$\mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes 2} O U^{\dagger\otimes 2}\right] = c_{\mathbb{I},O}\mathbb{I} + c_{\mathbb{F},O}\mathbb{F}, \tag{15}$$

Deduce $c_{\mathbb{I},O}$, $c_{\mathbb{F},O}$ with Theorem 10.(pset)

Symmetric Subspace

Definition 15 (Symmetric subspace)

$$\mathrm{Sym}_k(\mathbb{C}^d) := \left\{ |\psi\rangle \in (\mathbb{C}^d)^{\otimes k} : V_d(\pi)|\psi\rangle = |\psi\rangle \;\; \forall \pi \in S_k \right\}. \tag{16}$$

To facilitate our analysis, we also define the operator $P_{\mathrm{sym}}^{(d,k)}$ as follows:

$$P_{\mathrm{sym}}^{(d,k)} := \frac{1}{k!} \sum_{\pi \in S_k} V_d(\pi). \tag{17}$$

Theorem 16 (Projector on $\mathrm{Sym}_k(\mathbb{C}^d)$)

$P_{\mathrm{sym}}^{(d,k)}$ is the orthogonal projector on the symmetric subspace $\mathrm{Sym}_k(\mathbb{C}^d)$.
We also have $\underline{\mathrm{Sym}_k(\mathbb{C}^d) = \mathrm{Im}\left(P_{\mathrm{sym}}^{(d,k)}\right)}$.

$V_d(\pi) P_{sym}^{(d,k)} = P_{sym}^{(d,k)} \rightarrow P_{sym}^{(d,k)\,2} = P_{sym}^{(d,k)}, \; P_{sym}^{\dagger} = P_{sym}$

$\rightarrow$ orthogonal proj

$P_{sym} |\psi\rangle \in \mathrm{Sym}_k(\mathbb{C}^d) \Rightarrow \mathrm{Im}(P_{sym}) \subseteq \mathrm{Sym}_k(\mathbb{C}^d)$

If $|\psi\rangle \in \mathrm{Sym}_k(\mathbb{C}^d)$, $P_{sym}|\psi\rangle = \frac{1}{k!}\sum_{\pi} V_d(\pi)|\psi\rangle = \frac{1}{k!}\sum |\psi\rangle = |\psi\rangle$

$\Rightarrow \mathrm{Sym}_k(\mathbb{C}^d) \subseteq \mathrm{Im}(P_{sym})$

Dimension of symmetric subspace

Theorem 17 (Dimension of the symmetric subspace)

If $d \geq k$, we have

$$\mathbf{Tr}\left(P_{\mathrm{sym}}^{(d,k)}\right) = \dim\left(\mathrm{Sym}_k(\mathbb{C}^d)\right) = \binom{k+d-1}{k}. \tag{18}$$

otherwise $\mathbf{Tr}\left(P_{\mathrm{sym}}^{(d,k)}\right) = 0$.

$n_1 + n_2 + \cdots + n_d = K$

$|i_1\rangle \quad |i_2\rangle \quad \cdots \quad |i_d\rangle$

P set

Anti-symmetric subspace

Definition 18 (Anti-symmetric subspace)

The anti-symmetric subspace is the set:

$$\mathrm{ASym}_k(\mathbb{C}^d) := \left\{ |\psi\rangle \in (\mathbb{C}^d)^{\otimes k} : V_d(\pi)\,|\psi\rangle = \mathrm{sgn}\,(\pi)\,|\psi\rangle \;\; \forall\, \pi \in S_k \right\}, \tag{19}$$

where $\mathrm{sgn}\,(\sigma)$ denotes the sign of a permutation $\sigma \in S_k$.

$(-1)^n$

Similarly as before, we can define the operator:

$$P_{\mathrm{asym}}^{(d,k)} := \frac{1}{k!} \sum_{\pi \in S_k} \mathrm{sgn}\,(\pi)\, V_d(\pi). \tag{20}$$

Projector on anti-symmetric subspace

Theorem 19

$P_{\mathrm{asym}}^{(d,k)}$ *is the orthogonal projector on the anti-symmetric subspace* $\mathrm{ASym}_k(\mathbb{C}^d)$*.*
We also have $\underline{\mathrm{Im}\left(P_{\mathrm{asym}}^{(d,k)}\right) = \mathrm{ASym}_k(\mathbb{C}^d)}$*.*

Proposition 20 (Dimension of the anti-symmetric subspace)

If $d \geq k$, we have:

$$\mathbf{Tr}\left(P_{\mathrm{asym}}^{(d,k)}\right) = \underline{\dim\left(\mathrm{ASym}_k(\mathbb{C}^d)\right) = \binom{d}{k}}, \tag{21}$$

otherwise $\mathbf{Tr}\left(P_{\mathrm{asym}}^{(d,k)}\right) = 0$.

Proposition 21

We have $P_{\mathrm{asym}}^{(d,k)\dagger} P_{\mathrm{sym}}^{(d,k)} = 0$. In particular $P_{\mathrm{asym}}^{(d,k)}$ and $P_{\mathrm{sym}}^{(d,k)}$ are orthogonal with respect to the Hilbert-Schmidt inner product.

We can deduce $(\mathbb{C}^d)^{\otimes 2} = \mathrm{Sym}_2(\mathbb{C}^d) \oplus \mathrm{ASym}_2(\mathbb{C}^d)$.

$$P_{asym} P_{sym} = \frac{1}{k!} \sum_{\pi \in S_k} \mathrm{sgn}(\pi)\, \underbrace{V_d(\pi) P_{sym}} = \left(\frac{1}{k!} \sum \mathrm{sgn}(\pi)\right) P_{sym} = 0$$

$$\binom{d+1}{2} + \binom{d}{2} = d^2$$

Definition 22 (Haar measure on states)

Given a state $|\phi\rangle$ in $\mathbb{C}^d$, we denote

$O = |\phi\rangle\langle\phi|^{\otimes k}$

$$\mathop{\mathbb{E}}_{|\psi\rangle\sim\mu_H}\left[|\psi\rangle\langle\psi|^{\otimes k}\right] := \mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes k}\,|\phi\rangle\langle\phi|^{\otimes k}\,U^{\dagger\otimes k}\right]. \tag{22}$$

Moreover, we have:

$C_\pi = C_{\sigma\pi}$

$M_{\mu_H}(//) = C_I\, k!\, P_{sym}$

$C_I = \dfrac{1}{k!\,\mathrm{Tr}(P_{sym})}$

$$\mathop{\mathbb{E}}_{|\psi\rangle\sim\mu_H}\left[|\psi\rangle\langle\psi|^{\otimes k}\right] = \frac{P_{\mathrm{sym}}^{(d,k)}}{\mathbf{Tr}\left(P_{\mathrm{sym}}^{(d,k)}\right)}. \tag{23}$$

$\forall \sigma \in S_k,\quad V_d(\sigma^{-1})\, M_{\mu_H}^{(k)}(|\phi\rangle\langle\phi|^{\otimes k}) = \sum_\pi C_\pi V_d(\sigma^{-1}) V_d(\pi)$

$U^{\otimes k}$ $\qquad V_d(\sigma^{-1})|\phi\rangle^{\otimes k} = |\phi\rangle^{\otimes k}$ $\qquad \| $

$V_d(\sigma^{-1})\, M_{\mu_H}^{(k)}(|\phi\rangle\langle\phi|^{\otimes k}) = M_{\mu_H}^{(k)}(\;//\;)$ $\qquad \sum C_{\sigma\pi} V_d(\pi)$

Questions?

Spherical designs

Definition 23 (Spherical t-design)

Let $P_t : S(\mathbb{R}^d) \to \mathbb{R}$ be a polynomial in d variables, with all terms homogeneous in degree most t. A set $X = \{x : x \in S(\mathbb{R})\}$ is a spherical t-design if

$$\frac{1}{|X|} \sum_{x \in X} P_t(x) = \int_{S(\mathbb{R}^d)} P_t(u) d\mu(u) \tag{24}$$

holds for possible $\forall P_t$, where $d\mu$ is the uniform, normalized spherical measure.

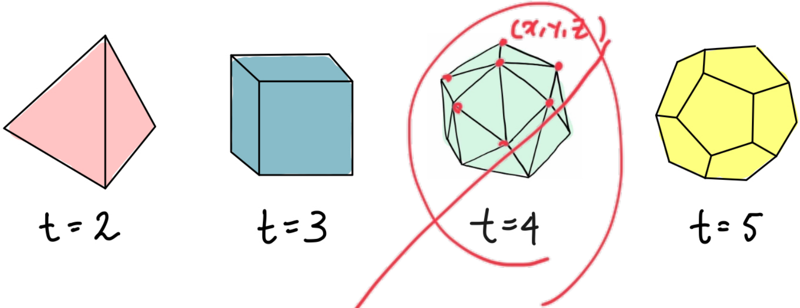


Figure: Spherical t-designs

For example, $f(x, y, z) = x^4 - 4x^3y + y^2z^2$ then compute the average value of f by using spherical 4-design on the figure.

Unitary designs

Generating Haar random unitaries on a quantum computer could be expensive. (Most unitaries require an exponential number of elemantary gates)

Definition 24 (Unitary k-design)

Let ν be a probability distribution defined over a set of unitaries $S \subseteq \mathrm{U}(d)$. The distribution ν is unitary k-design if and only if:

$$\mathop{\mathbb{E}}_{V\sim\nu}\left[V^{\otimes k} O V^{\dagger\otimes k}\right] = \mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes k} O U^{\dagger\otimes k}\right], \tag{25}$$

for all $O \in \mathcal{L}\left((\mathbb{C}^d)^{\otimes k}\right)$.

$O = I \otimes O_1 \otimes \cdots \otimes O_{k-1} + \cdots$

Unitary designs

For instance, consider a distribution ν where the set of unitaries S is discrete and each unitary has an equal probability of being chosen. In this case, we have:

$$\mathop{\mathbb{E}}_{V\sim\nu}\left[V^{\otimes k} O V^{\dagger\otimes k}\right] = \frac{1}{|S|}\sum_{V\in S} V^{\otimes k} O V^{\dagger\otimes k}. \tag{26}$$

Observation 25

A probability distribution ν is a unitary k-design if and only if:

$$\mathop{\mathbb{E}}_{V\sim\nu}\left[V^{\otimes k}\otimes V^{*\otimes k}\right] = \mathop{\mathbb{E}}_{U\sim\mu_H}\left[U^{\otimes k}\otimes U^{*\otimes k}\right]. \tag{27}$$

Approximate unitary designs

To simplify the notation, we use $U^{\otimes k,k} := U^{\otimes k} \otimes U^{*\otimes k}$.

diamond norm

Definition 26 (Tensor Product Expander (TPE)-ε-approximate k-design)

Let $\varepsilon > 0$. We say that ν is a TPE ε-approximate k-design if and only if:

$$\left\| \mathop{\mathbb{E}}_{V \sim \nu} \left[V^{\otimes k,k} \right] - \mathop{\mathbb{E}}_{U \sim \mu_H} \left[U^{\otimes k,k} \right] \right\|_{\infty} \leq \varepsilon. \tag{28}$$

(Approx)

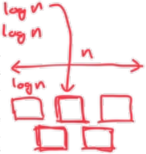
Unitary designs in nearly optimal depth

Laura Cui,[1,*] Thomas Schuster,[2,1,3,*] Fernando Brandão,[4,1] and Hsin-Yuan Huang[1,3]

[1] *Institute for Quantum Information and Matter and Department of Physics, California Institute of Technology, Pasadena, California 91125, USA*
[2] *Walter Burke Institute for Theoretical Physics, California Institute of Technology, Pasadena, California 91125, USA*
[3] *Google Quantum AI, Venice, California 90291, USA*
[4] *AWS Center for Quantum Computing, Pasadena, California 91125, USA*

We construct ε-approximate unitary k-designs on n qubits in circuit depth $\mathcal{O}(\log k \log \log nk/\varepsilon)$. The depth is exponentially improved over all known results in all three parameters n, k, ε. We further show that each dependence is optimal up to exponentially smaller factors. Our construction uses $\tilde{\mathcal{O}}(nk)$ ancilla qubits and $\mathcal{O}(nk)$ bits of randomness, which are also optimal up to $\log(nk)$ factors. An alternative construction achieves a smaller ancilla count $\tilde{\mathcal{O}}(n)$ with circuit depth $\mathcal{O}(k \log \log nk/\varepsilon)$. To achieve these efficient unitary designs, we introduce a highly-structured random unitary ensemble that leverages long-range two-qubit gates and low-depth implementations of random classical hash functions. We also develop a new analytical framework for bounding errors in quantum experiments involving many queries to random unitaries. As an illustration of this framework's versatility, we provide a succinct alternative proof of the existence of pseudorandom unitaries.

K x log n
k + log n



glue
log n - qubit

Random unitaries are ubiquitous across quantum science, serving both as fundamental theoretical tools and practical building blocks for quantum technologies. They provide useful models for understanding chaotic many-body dynamics [1–3], quantum gravity phenomena [4–6], and thermalization in isolated quantum systems [7–9]. Beyond their theoretical significance, random unitaries have been essential for device benchmarking [10–12], state tomography [13–15], quantum advantage demonstrations [16–18], and quantum cryptography [19–21]. From an analytical perspective, the uniform Haar measure over unitaries enables tractable mathematical investigations through its elegant structure and a wealth of

(a) (b)

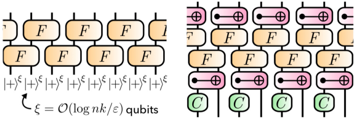


FIG. 1. Schematic of our low-depth constructions of state and unitary designs. Black vertical lines denote local patches of $\xi = \mathcal{O}(\log nk/\varepsilon)$ qubits. **(a)** Our random state designs apply a two-layer circuit of random phase gates F to the plus state. The random phases are drawn from k-wise independent

Frame potential

Definition 27 (Frame potential)

Let ν be a probability distribution defined over the set of unitaries $S \subseteq \mathrm{U}(d)$. For a given $k \in \mathbb{N}$, we define the k-frame potential, denoted as $\mathcal{F}_\nu^{(k)}$, as follows:

$$\mathcal{F}_\nu^{(k)} := \mathop{\mathbb{E}}_{U,V \sim \nu}\left[\left|\mathbf{Tr}\left(UV^\dagger\right)\right|^{2k}\right]. \tag{29}$$

Definition 28 (k-invariant measure)

Let ν be a probability distribution defined over a set of unitaries $S \subseteq \mathrm{U}(d)$. ν is k-invariant if and only if, for any polynomial $p(U)$ of degree $\leq k$ in the matrix elements of U and U^*, it holds

$$\mathop{\mathbb{E}}_{U\sim\nu}[p(U)] = \mathop{\mathbb{E}}_{U\sim\nu}[p(UV)] = \mathop{\mathbb{E}}_{U\sim\nu}[p(VU)], \tag{30}$$

for all $V \in S$.

Frame potential

Lemma 29

Let ν be a probability distribution defined over a set of unitaries $S \subseteq \mathrm{U}(d)$. If ν is k-invariant, then we have:

$$\mathcal{F}_{\nu}^{(k)} = \dim\left(\mathrm{Comm}(S,k)\right), \tag{31}$$

where $\mathrm{Comm}(S,k)$ is the commutant subspace.

$$F_V^{(k)} = \mathop{E}_{U,V\sim\nu}\left[|\mathrm{Tr}(UV^\dagger)|^{2k}\right] = \mathop{E}_{U\sim\nu}\left[|\mathrm{Tr}(U)|\right]^{2k} = E\left[\mathrm{Tr}(U)^k\,\mathrm{Tr}(U^*)^k\right]$$

$$= \mathrm{Tr}\left(\underbrace{E\left[U^{\otimes k}\otimes U^{*\otimes k}\right]}\right) = \dim(\mathrm{Comm}(S,k))$$

Frame potential differecne

Lemma 30 (Frame potential difference)

Let $\mathcal{F}_{\nu}^{(k)}$ and $\mathcal{F}_{\mu_H}^{(k)}$ be the frame potentials of the probability distribution ν and the Haar measure μ_H, respectively. Then, we have:

$$\mathcal{F}_{\nu}^{(k)} - \mathcal{F}_{\mu_H}^{(k)} = \left\| \mathop{\mathbb{E}}_{V\sim\nu} \left[V^{\otimes k} \otimes V^{*\otimes k} \right] - \mathop{\mathbb{E}}_{U\sim\mu_H} \left[U^{\otimes k} \otimes U^{*\otimes k} \right] \right\|_2^2 . \tag{32}$$

It follows from the Lemma that **showing that a distribution ν is a k-design** can be achieved by computing its **frame potential** and comparing it with that of the Haar measure μ_H.

Frame potential k-desgin condition

Proposition 31 (Frame potential k-design condition)

We have:

(pset)

$$\mathcal{F}_{\nu}^{(k)} \geq \mathcal{F}_{\mu_H}^{(k)} = \dim(\mathrm{span}(V_d(\pi) : \pi \in S_k)). \tag{33}$$

Moreover, the equality holds if and only if ν is a k-unitary design.
In particular, if $k \leq d$, then $\dim(\mathrm{span}(V_d(\pi) : \pi \in S_k)) = k!$.

By utilizing this result, we can derive a straightforward lower bound on the cardinality of a discrete set S of unitaries necessary to form a k-design. We can deduce that:

$$k! = \mathcal{F}_\nu^{(k)} = \underline{\frac{1}{|S|^2} \sum_{i,j=1}^{|S|} \left| \mathbf{Tr}\left(U_i U_j^\dagger \right) \right|^{2k}} \geq \underline{\frac{1}{|S|^2} \sum_{i=1}^{|S|} \left| \mathbf{Tr}\left(\overset{d}{U_i U_i^\dagger} \right) \right|^{2k}} = \frac{1}{|S|} d^{2k}. \tag{34}$$

Furthermore, considering the fact that ν constitutes a k-design (with $k \leq d$), by the previous proposition, we have that $\mathcal{F}_\nu^{(k)} = k!$. This implies that the cardinality of the set S must satisfy $|S| \geq \frac{d^{2k}}{k!}$. So, the cardinality of S must grow at least exponentially with the number of qubits.

$|S| \geq \frac{d^{2k}}{k!}$ $\quad d = 2^n$

Unitary k-design alternate definition

The following proposition provides equivalent definitions of unitary k-design:

Proposition 32 (Equivalent definitions of unitary k-design.)

Let ν be a probability distribution over a set of unitaries $S \subseteq \mathrm{U}$. Then, ν is a unitary k-design if and only if:

1. $\underset{U \sim \nu}{\mathbb{E}}\left[U^{\otimes k} O U^{\dagger \otimes k}\right] = \underset{U \sim \mu_H}{\mathbb{E}}\left[U^{\otimes k} O U^{\dagger \otimes k}\right]$ for all $O \in \mathcal{L}\left((\mathbb{C}^d)^{\otimes k}\right)$.
2. $\underset{V \sim \nu}{\mathbb{E}}\left[V^{\otimes k} \otimes V^{* \otimes k}\right] = \underset{U \sim \mu_H}{\mathbb{E}}\left[U^{\otimes k} \otimes U^{* \otimes k}\right]$.
3. $\mathcal{F}_\nu^{(k)} = \dim\left(\mathrm{Comm}(\mathrm{U}(d), k)\right)$.
4. $\underset{V \sim \nu}{\mathbb{E}}\left[p(V)\right] = \underset{U \sim \mu_H}{\mathbb{E}}\left[p(U)\right]$ 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^*.

Unitary 1-design

It is worth noting that any uniform distribution ν defined over a set of unitaries $S = \{U_i\}_{i=1}^{d^2}$ that forms a basis for $\mathcal{L}(\mathbb{C}^d)$ and satisfies $\mathbf{Tr}(U_i^\dagger U_j) = d\delta_{i,j}$ constitutes a 1-design. This can be easily proven by computing the frame potential as follows:

$$\mathcal{F}_\nu^{(k=1)} = \frac{1}{|S|^2} \sum_{i,j=1}^{d^2} \left| \mathbf{Tr}(U_i U_j^\dagger) \right|^2 = \frac{1}{d^4} \sum_{i,j=1}^{d^2} d^2 \delta_{i,j} = 1 = \dim(\mathrm{span}(V_d(\pi) : \pi \in S_1)) \quad (35)$$

Therefore, the uniform distribution defined over the Pauli basis $\tilde{\mathcal{P}} := \{I, X, Y, Z\}^{\otimes n}$ is a 1-design, where n is the number of qubits and $d = 2^n$.

3-design

I, X, Y, Z

$U = I \otimes X \otimes Z \otimes Y \otimes \cdots \otimes X$

$U^{\otimes k} O U^{\dagger \otimes k}$

$U^\dagger$

$Z O_{3,i} Z^\dagger$

X, Y, Z, I

$O \rightarrow \sum_i O_{1,i} \otimes O_{2,i} \otimes \cdots \otimes O_{k,i}$

The Flip operator can be elegantly represented in terms of the Pauli basis using the following expression:

$$\mathbb{F} = \sum_{P,Q\in\tilde{\mathcal{P}}} \frac{1}{d^2}\mathbf{Tr}((P\otimes Q)\,\mathbb{F})P\otimes Q = \sum_{P,Q\in\tilde{\mathcal{P}}} \frac{1}{d^2}\mathbf{Tr}(PQ)P\otimes Q = \sum_{P\in\tilde{\mathcal{P}}} \frac{1}{d}P\otimes P, \qquad (36)$$

where we wrote the Flip operator in the Pauli basis and used the *swap-trick*. Also using this, we can prove that the Pauli group forms a 1-design.(pset)

Unitary 3-design

An important set of unitaries is the Clifford group $\mathrm{Cl}(n)$ i.e. the set of unitaries which sends the Pauli group $\mathcal{P}_n$ in itself under the adjoint operation:

$$\mathrm{Cl}(n) := \{U \in \mathrm{U}(2^n) \colon UPU^\dagger \in \mathcal{P}_n \text{ for all } P \in \mathcal{P}_n\}, \tag{37}$$

where $\mathcal{P}_n := \{i^k\}_{k=0}^3 \times \{I, X, Y, Z\}^{\otimes n}$. It can be proven that the uniform distribution over the Clifford group, forms a 3-design for all $d = 2^n$, but it fails to be a 4-design.

$O(n^2/\log n)$

Clifford group

Moreover, it can be shown that any Clifford circuit can be implemented with $O(n^2/\log(n))$ gates from the set $\{H, CNOT, S\}$ where H, CNOT and S are the Hadamard, Controlled-NOT and Phase gate, respectively.

Clifford gates $\{\mathrm{H}, \mathrm{CNOT}, \mathrm{S}\}$ + non clifford T gate form universal quantum gates.

↓

classical

Thanks a lot!