Efficient approximate unitary designs from random Pauli rotations

Jeongwan Haah
Stanford University

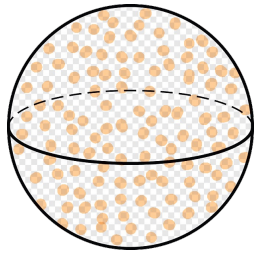
Yunchao Liu
Harvard University

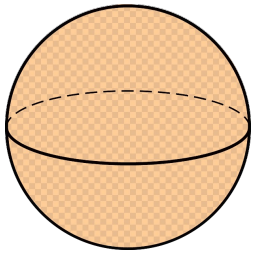
Xinyu (Norah) Tan
MIT

QIP 2025
Raleigh, NC

What is a unitary t-design?

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





- Define a mixed unitary channel on t copies of n qubits $\left(\mathbb{C}^{2^n}\right)^{\otimes t}$:

$$\mathcal{H}_{t,\nu}\colon A \mapsto \mathbb{E}_{U\sim\nu}\, U^{\otimes t} \cdot A \cdot \left(U^\dagger\right)^{\otimes t}$$

- **Definition**: ν is an <u>exact</u> unitary t-design if $\mathcal{H}_{t,\nu} = \mathcal{H}_{t,\mathrm{Haar}}$
- If $\mathcal{H}_{t,\nu} = \mathcal{H}_{t,\mathrm{Haar}}$ for all $t \geq 1$, then ν is the Haar measure on $\mathrm{SU}(2^n)$

Approximate designs

- Define a mixed unitary channel on t copies of n qubits $\left(\mathbb{C}^{2^n}\right)^{\otimes t}$:

$$\mathcal{H}_{t,\boldsymbol{\nu}}: A \mapsto \mathbb{E}_{U\sim\boldsymbol{\nu}}\, U^{\otimes t} \cdot A \cdot \left(U^{\dagger}\right)^{\otimes t}$$

- **Definition**: $\boldsymbol{\nu}$ is an ϵ **additive error** approximate unitary t-design if

$$\left\|\mathcal{H}_{t,\boldsymbol{\nu}} - \mathcal{H}_{t,\mathrm{Haar}}\right\|_{\diamond} \leq \epsilon$$

Approximate designs (multiplicative error)

- Define a mixed unitary channel on t copies of n qubits $\left(\mathbb{C}^{2^n}\right)^{\otimes t}$:

$$\mathcal{H}_{t,\boldsymbol{\nu}}: A \mapsto \mathbb{E}_{U\sim\boldsymbol{\nu}}\, U^{\otimes t} \cdot A \cdot \left(U^{\dagger}\right)^{\otimes t}$$

- **Definition**: $\boldsymbol{\nu}$ is an ϵ **multiplicative error** approximate unitary t-design if

$$(1-\epsilon)\cdot \mathcal{H}_{t,\text{Haar}} \preccurlyeq \mathcal{H}_{t,\boldsymbol{\nu}} \preccurlyeq (1+\epsilon)\cdot \mathcal{H}_{t,\text{Haar}}$$

- Multiplicative error is <u>much stronger</u> than additive error

Most common recipe to generate unitary designs

A random walk model: circuits with L i.i.d. random gates

- $U_L \cdots U_2 U_1$ where each $U_i \sim \nu$
- $\nu^{*L} = \nu * \cdots * \nu$
- How fast does it converge to a t-design?

Multiplicative error designs from spectral gaps

- Let ν be a distribution on $\mathrm{SU}(2^n)$ for one step/walk

$$Q := \mathbb{E}_{U\sim\nu}(U \otimes \bar{U})^{\otimes t}$$

- The largest singular value of Q is $\lambda_1(Q) = 1$
- The **spectral gap** for ν is $\Delta(\nu, t) = 1 - \lambda_2(Q)$

- **Lemma [BHH12]**: ν^{*L} is a unitary t-design with **multiplicative error** ϵ if

$$L = O\left(\frac{1}{\Delta(\nu, t)} \cdot \left(nt + \log(1/\epsilon)\right)\right)$$

	paper	model	spectral gap	$O(1)$ multiplicative error design depth
	BHH12	Brickwork	$\Omega(n^{-1}t^{-9.5})$	$O(nt^{10.5})$
	Haferkamp22	Brickwork	$\Omega(n^{-1}t^{-4-o(1)})$	$O(nt^{5+o(1)})$
	HLT24	Pauli rotations	$\Omega(t^{-1})$	$O(n \cdot \log(n) \cdot t^2)$
5pm	MPSY24	Permutation + Phase + Clifford	✗	$O(\text{poly}(n) \cdot t^2)$
4:30pm	CBBDHX24	Products of exponentiated sums of permutations	✗	$O(\text{poly}(n) \cdot t^2 \cdot \text{polylog}(t))$
Short plenary on Thursday	CHHLMT24	Brickwork	$\tilde{\Omega}(n^{-1})$	$\tilde{O}(nt) = O(nt \cdot (\log t)^7)$

- Explicit constants: the spectral gap is at least $1/(4t)$.
- The spectral gap holds for ALL $t \geq 1$. All other papers holds for $t \leq 2^{\Theta(n)}$.
- Simple construction and proof: the entire paper is 21 pages.

Next

- Our construction
  - What is a random Pauli rotation?
- The spectral gap bound
- Proof sketch

Main result

- $\exp(i\theta P/2)$ with $\theta \sim [-\pi, \pi]$ and $P \sim \{I, X, Y, Z\}^{\otimes n} \setminus \{I^{\otimes n}\}$
  - $[-\pi, \pi]$ can be discretized
- With all-to-all connection, $\exp(i\theta P/2)$ can be implemented in depth $3 + 2 \cdot \log n$

- **Theorem:** For any integers $n, t \geq 1$,

$$\Delta_t := 1 - \boldsymbol{\lambda_2}\left(\mathbb{E}_{\theta,P}\left(e^{i\theta P/2} \otimes e^{-i\theta \bar{P}/2}\right)^{\otimes t}\right) \geq \frac{1}{4t}$$

As a result, $L = O(t^2 n)$ random Pauli rotations

$$e^{i\theta_L P_L/2} \ldots e^{i\theta_2 P_2/2}\, e^{i\theta_1 P_1/2}$$

form $O(1)$ multiplicative error unitary t-designs in circuit depth $O(L \log n)$.

Proof

$$\mathbb{E}_{\theta,P}\left(e^{i\theta P/2}\otimes e^{-i\theta\bar{P}/2}\right)^{\otimes t}$$

Hermitian, $\lambda_1 = 1$
Our goal: upper bound λ_2

- Let us rewrite $\left(e^{i\theta P/2}\otimes e^{-i\theta\bar{P}/2}\right)^{\otimes t} = e^{i\theta\cdot \boldsymbol{J_P}}$
- **Note 1:** For any Hermitian matrices A and B

$$e^{iA}\otimes e^{iB} = e^{i(A\otimes I + I\otimes B)}$$

- So $\boldsymbol{J_P} = \frac{1}{2}\sum_{j=1}^{t}(I\otimes I)^{j-1}\otimes\underbrace{(P\otimes I - I\otimes\bar{P})}_{\text{eigenvalues:}-2,0,2}\otimes(I\otimes I)^{t-j}$
  - The eigenvalues of $\boldsymbol{J_P}$ are integers in $[-t,t]$
- Now average over θ: $\mathbb{E}_{\theta\sim[-\pi,\pi]}e^{i\theta\cdot \boldsymbol{J_P}} = \boldsymbol{K_P}$

the orthogonal projector onto the kernel of $\boldsymbol{J_P}$

Proof

$$\mathbb{E}_{\theta,P}\left(e^{i\theta P/2} \otimes e^{-i\theta \bar{P}/2}\right)^{\otimes t} = \mathbb{E}_{P\in \mathrm{P}_n} K_P$$

K_P is the kernel projector of J_P

$$\left(e^{i\theta P/2} \otimes e^{-i\theta \bar{P}/2}\right)^{\otimes t} = e^{i\theta \cdot J_P}$$

$$J_P = \frac{1}{2}\sum_{j=1}^{t} (I \otimes I)^{j-1} \otimes (P \otimes I - I \otimes \bar{P}) \otimes (I \otimes I)^{t-j}$$

- **Note 2:** $\rho: U \mapsto (U \otimes \bar{U})^{\otimes t}$ is a **SU(2^n) Lie group** representation.

  $\rho_*: P \mapsto J_P$ is the induced **su(2^n) Lie algebra** representation.

Both ρ and ρ_* can be decomposed into irreducible representations (**irreps**)

$$\lambda_2\left(\mathbb{E}_{\theta,P}\left(e^{i\theta P/2} \otimes e^{-i\theta \bar{P}/2}\right)^{\otimes t}\right) = \max_{\text{nontrivial } \tau\in\rho} \lambda_1\left(\mathbb{E}_{P\in \mathrm{P}_n} K(\tau_*(P))\right)$$

Proof

$$\lambda_2\left(\mathbb{E}_{\theta,P}\left(e^{i\theta P/2}\otimes e^{-i\theta \bar{P}/2}\right)^{\otimes t}\right) = \max_{\text{nontrivial } \tau\in\rho} \lambda_1\left(\mathbb{E}_{P\in \mathrm{P}_n} K\left(\tau_*(P)\right)\right)$$

- **Note 3:** For any non-zero Hermitian matrix H, the kernel projector $K(H) \preccurlyeq I - \frac{H^2}{\|H\|_\infty^2}$
- So $K(\tau_*(P)) \preccurlyeq I - \frac{(\tau_*(P))^2}{t^2}$
- **Note 4:** For each irrep τ_* of $\mathrm{su}(2^n)$,

  $\sum_{P\in \mathrm{P}_n} \tau_*(P)^2 \propto I$ is known as the **quadratic Casimir** operator.
  - We know exactly which irreps occur in ρ_*
  - Given any irrep τ_*, we know the exact scalar in the quadratic Casimir operator
- **Lemma:** For any non-trivial irrep $\tau \in \rho$, $\mathbb{E}_{P\in \mathrm{P}_n} \tau_*(P)^2 \succcurlyeq \frac{t}{4} I$ Q.E.D.

Summary

- Random circuits from $O(t^2 n)$ random Pauli rotations give a constant multiplicative error unitary t-design.
- Each $\exp(i\theta P/2)$ can be implemented in $O(\log n)$ depth.
- All constants are nice and explicit.
- Our result holds for all $t \geq 1$.
- Simple proof of the spectral gap.