Random unitaries

Uniform distribution $\leftrightarrow$ Haar measure

μ_{Haar} on $U(d)$

Defining properties: $\mu_{Haar}(U(d)) = 1$

$\mu_{Haar}(S) = \mu_{Haar}(US) = \mu_{Haar}(SU)$ for $S \subseteq U(d)$, $U \in U(d)$

Like the uniform distr. over finite groups

$$\int d\mu_{Haar}(g)\, R(g) = V^G$$

However, we need $\gtrsim 4^n$ gates to sample from μ_{Haar} on $U(2^n)$

Instead use (unitary) k-designs

$$U^{\otimes k,k} := U^{\otimes k} \otimes U^{*\otimes k}$$

why? $f(X) = U^{\otimes k} X U^{\dagger \otimes k}$ is a linear map on X

$$f \cong U^{\otimes k,k} \qquad \mathrm{vec}(f(X)) = U^{\otimes k,k}\,\mathrm{vec}(X)$$

ν is a k-design if $\mathop{\mathbb{E}}_{U\sim\nu} U^{\otimes k,k} = \mathop{\mathbb{E}}_{U\sim Haar} U^{\otimes k,k}$

For any state $|\alpha\rangle$

If ν is a unitary k-design then $U|\alpha\rangle$ is a state k-design if $U \sim \nu$.

Classical analogue: k-wise indep. [hash] function

$h: U \to [m]$ $\qquad \Pr_{h \in H}[h(x_1)=y_1 \wedge \cdots \wedge h(x_k)=y_k] = \frac{1}{m^k}$

$\forall\ x_1 \cdots x_k$ distinct $\quad \forall\ y_1 \cdots y_k \in [m]$

$k=1$

$\mathop{\mathbb{E}}_U U X U^\dagger = \mathrm{tr}(X)\frac{I}{d} \iff \mathop{\mathbb{E}}_U U \otimes U^* = \Phi$

$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \otimes |i\rangle$

examples Paulis $\{I, X, Y, Z\}$ or generalized Paulis $\sum_x \omega^{xy} |x+z\rangle\langle x|$

any $U_1, \ldots, U_{d^2}$ s.t. $\mathrm{tr}\, U_i^\dagger U_j = \delta_{ij} I$

$|\mathrm{supp}\ \nu| \geq d^2$ since ν is a 1-design

$\iff \mathcal{N}(\rho) = \int d\nu(U)\, U \rho U^\dagger = I_d/d$

$\iff (id \otimes \mathcal{N})(\Phi) = \frac{I_{d^2}}{d^2}$

$\mathcal{N} = \sum_{k=1}^{m} E_k \cdot E_k^\dagger \Rightarrow \mathrm{rank}\,(id \otimes \mathcal{N}(\text{pure state})) \leq m$

But approximately randomizing maps exist

$\mathcal{N}(\rho) = \frac{1}{m}\sum_{i=1}^{m} U_i \rho U_i^\dagger$ satisfies $\| \mathcal{N}(\rho) - \frac{I}{d} \|_\infty \leq \epsilon/d \quad \forall \rho$

whp if $m \gtrsim \frac{d}{\epsilon^2}$ and $U_1, \ldots, U_m \sim$ Haar

Pf omitted but similar to the proof last time that random states are very entangled.

Data hiding

$(I \otimes \mathcal{N})(\Phi_d)$ has rank $\frac{d}{\epsilon^2}$ but is ϵ-indistinguishable from $\frac{I_{d^2}}{d^2}$ by LOCC.

$k=2$

$\mathbb{E}_{U} U\otimes U\otimes U^*\otimes U^*$ same for $\mathbb{E}_{U\sim\mathcal{V}}$ and $\mathbb{E}_{\text{Unitary}}$

$\mathbb{E}_{\text{Unitary}} (U\otimes U) X (U\otimes U)^\dagger =: T(X)$ $\quad T(I)=I$, $T(F)=F$

T is a projector onto $U^{\otimes 2,2}$-invariant subspace of $M^d\otimes M^d$

I, F not orthogonal w.r.t. Hilbert-Schmidt inner product $\langle A,B\rangle = \operatorname{tr} A^\dagger B$

Instead use $\Pi_\pm = \frac{I\pm F}{2}$ (anti-)symmetric subspace

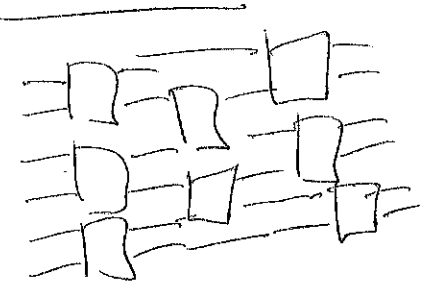
$$T(X) = \frac{\operatorname{tr}(X\Pi_+)}{\operatorname{tr}\Pi_+}\Pi_+ + \frac{\operatorname{tr}(X\Pi_-)}{\operatorname{tr}\Pi_-}\Pi_-$$

example Clifford group

$$\mathbb{E}_{U\sim\text{Cliffords}} (U\otimes U)(\sigma_p\otimes\sigma_q)(U\otimes U)^\dagger = \begin{cases} 0 & \text{if } p\neq q \\ I & \text{if } p=q=0^n \\ \sum_{r\neq 0^n} \frac{\sigma_r\otimes\sigma_r}{4^n-1} & \text{if } p=q \end{cases}$$

$$\sum_{r\neq 0^n}\sigma_r\otimes\sigma_r = 2^n F - I$$

random circuits



$\cdots$ yields ϵ-approx k-design with depth $\sim n k^{O(1)}\log(1/\epsilon)$