LECTURE 27 (April 29th)

TODAY PRS (wrap up)
Pseudorandom Unitaries & Unitary t-designs

RECAP PRS construction

$|\psi_f\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$ where $f: \{0,1\}^n \to \{0,1\}$ is a uniformly random boolean function

Replace f with t-wise independent function to get a t-design and with a pseudorandom function to get a Pseudorandom state family

Theorem $|\psi_f\rangle$ is a $O\left(\frac{t^2}{2^n}\right)$ - approximate t-design in trace distance.

i.e. $$\left\| \mathbb{E}\, |\psi_f\rangle\langle\psi_f|^{\otimes t} - \mathbb{E}_{|\psi\rangle \sim \text{Haar}} |\psi\rangle\langle\psi|^{\otimes t} \right\|_1 \lesssim \frac{t^2}{2^n}.$$

Symmetric Subspace $\quad \text{Sym}_{d,t} = \{ |\psi\rangle \in (\mathbb{C}^d)^{\otimes t} \mid R_\sigma |\psi\rangle = |\psi\rangle \text{ for all } \sigma \in S_t \}$

Fact $$\mathbb{E}_{|\psi\rangle \sim \text{Haar}} |\psi\rangle\langle\psi|^{\otimes t} = \underbrace{\frac{\Pi_{\text{sym}_{d,t}}}{\dim(\Pi_{\text{sym}_{d,t}})}}_{:= \rho_{\text{sym}}}$$ where $\Pi_{\text{sym}_{d,t}}$ is the projector on $\text{Sym}_{d,t}$

This is the maximally mixed state on the symmetric subspace

Thus, our task boils down to showing

$$\mathbb{E}_f\, |\psi_f\rangle\langle\psi_f|^{\otimes t} \approx \rho_{\text{sym}}$$

In order to do this, let us give an explicit basis for the symmetric subspace

Basis for symmetric subspace: For a computational basis state $|x_1, \dots x_t\rangle$ where each $x_i \in [d]$, define the following symmetrization operation

$$|\text{sym}(x_1, \dots x_t)\rangle = \frac{1}{\sqrt{t!}} \sum_\sigma R_\sigma |x_1, \dots x_t\rangle$$

Example $$|\text{sym}(1,2,3)\rangle = \frac{|123\rangle + |132\rangle + |213\rangle + |321\rangle + |231\rangle + |312\rangle}{\sqrt{6}}$$
$|\text{sym}(3,2,1)\rangle$

$$|\text{sym}(1,1,2)\rangle = |\text{sym}(2,1,1)\rangle = \cdots = \frac{|112\rangle + |211\rangle + |121\rangle}{\sqrt{3}}$$

The collection of all such distinct vectors give an orthonormal basis for $\text{Sym}_{d,t}$ (We won't prove it here)

How many such vectors are there ? The vectors correspond to "types"

If all $x_1, \dots x_t$ are distinct , # vectors $= \binom{d}{t}$

If some of them are 1's, some are 2's, ... & and so on

In general, a type of a vector is given by $(c_1, \dots c_d)$ where $c_i \geq 0$ are integers and $\sum c_i = t$

Total # of vectors $=$ $\dim(\mathrm{Sym}_{d,t})$ $=$ # of solutions to $\sum c_i = t$ with $c_i \geq 0$

$$= \binom{d+t-1}{t-1}$$

The "distinct" types correspond to having some t out of d c_i's being 1's and rest being 0's.

The span of these vectors will play a key role, so let us define $\mathrm{Sym} \wedge \mathrm{Dist}$ to be the subspace spanned by these vectors and $\rho_{\mathrm{Sym}\wedge\mathrm{Dist}}$ to be the maximally mixed state on this subspace

Note that the bulk of the symmetric subspace is made by the distinct vectors since

$$\frac{\binom{d}{t}}{\binom{d+t-1}{t-1}} \geq \frac{\binom{d}{t}}{\binom{d+t}{t}} = \frac{\frac{d!}{t!(d-t)!}}{\frac{(d+t)!}{t!\,d!}} = \frac{d(d-1)\cdots(d-t+1)}{(d+t)\cdots\cdots(d+1)}$$

$$\geq \frac{(d-t)^t}{(d+t)^t}$$

$$= \left(1-\frac{t}{d}\right)^t$$

$$\geq 1 - O\left(t^2/d\right)$$

This easily implies the following claim (whose details are left to exercises)

$\boxed{\text{Claim 1}}$ $\| \rho_{\mathrm{Sym}} - \rho_{\mathrm{Sym}\wedge\mathrm{Dist}} \|_1 \lesssim t^2/d$

To complete the proof of the theorem, we shall sketch a proof of the following

$\boxed{\text{Claim 2}}$ $\| \mathbb{E}_f |\psi_f\rangle\langle\psi_f|^{\otimes t} - \rho_{\mathrm{Sym}\wedge\mathrm{Dist}} \|_1 \lesssim t^2/d$

Together these imply that $\| \mathbb{E}_f |\psi_f\rangle\langle\psi_f|^{\otimes t} - \rho_{\mathrm{Sym}} \|_1 \lesssim t^2/d$

<u>Proof sketch for Claim 2</u> Recall that $|\psi_f\rangle = \frac{1}{\sqrt{d}} \sum_{x\in[d]} (-1)^{f(x)} |x\rangle$ where $d = 2^n$

$$|\psi_f\rangle^{\otimes t} = \frac{1}{\sqrt{d^t}} \sum_{x_1,\dots x_t \in [d]^t} (-1)^{f(x_1)} (-1)^{f(x_2)} \cdots |x_1, \dots x_t\rangle := \frac{1}{\sqrt{d^t}} \sum_{\vec{x}\in[d]^t} (-1)^{f(\vec{x})} |\vec{x}\rangle$$

Moreover, permuting the t registers does not change the ~~state~~ state, so,

$$\mathbb{E}_\sigma R_\sigma |\psi_f\rangle^{\otimes t} = |\psi_f\rangle^{\otimes t}$$

and $\mathbb{E}_f |\psi_f\rangle\langle\psi_f|^{\otimes t} = \mathbb{E}_\sigma R_\sigma \left(\mathbb{E}_f |\psi_f\rangle\langle\psi_f|^{\otimes t}\right)$ $\quad (\star)$

Thus, $\mathbb{E}_f |\psi_f\rangle\langle\psi_f|^{\otimes t} = \mathbb{E}_f \frac{1}{d^t} \sum_{\vec{x},\vec{y}\in[d]^t} (-1)^{f(\vec{x})} (-1)^{f(\vec{y})} |\vec{x}\rangle\langle\vec{y}|$

$$= \frac{1}{d^t} \sum_{\substack{\vec{x},\vec{y} \\ \text{dis}}} \mathbb{E}\left[(-1)^{f(\vec{x})}(-1)^{f(\vec{y})}\right] |\vec{x}\rangle\langle\vec{y}|$$

$$+ \frac{1}{d^t} \sum_{\substack{\vec{x},\vec{y} \\ \text{not dist.}}} \mathbb{E}\left[(-1)^{f(\vec{x})}(-1)^{f(\vec{y})}\right] |\vec{x}\rangle\langle\vec{y}|$$

In the first term, the expectation

$$\mathbb{E}\left[(-1)^{f(x_1)} \cdots (-1)^{f(x_t)} (-1)^{f(y_1)} \cdots (-1)^{f(y_t)}\right] = \begin{cases} 1 & \text{if } y_1 \dots y_t = x_{\pi(1)}, \dots x_{\pi(t)} \\ 0 & \text{o/w} \end{cases}$$

for some permuation π of t elements

So, the first term $= \frac{1}{d^t} \sum_{\vec{x}} \sum_{\pi} |\vec{x}\rangle\langle\vec{x}| R_\pi$

$$= \frac{\sqrt{t!}}{d^t} \sum_{\vec{x}} |\vec{x}\rangle\langle \mathrm{sym}(\vec{x})|$$

Using $(\star)$,

$$= \frac{\sqrt{t!}}{d^t} \frac{1}{t!} \sum_\sigma R_\sigma |\vec{x}\rangle\langle \mathrm{sym}(\vec{x})|$$

$$= \frac{1}{d^t} \sum_{\vec{x}} |\mathrm{sym}(\vec{x})\rangle\langle \mathrm{sym}(\vec{x})| = \frac{t!}{d^t} \Pi_{\mathrm{sym}\wedge\mathrm{dist}}$$

$$= \frac{t!\binom{d}{t}}{d^t} \rho_{\mathrm{sym}\wedge\mathrm{Dist}} \approx \rho_{\mathrm{sym}\wedge\mathrm{Dist}} \quad \text{since } \frac{t!\binom{d}{t}}{d^t} \approx 1 \text{ if } t^2 \ll d$$

The contribution of all the non-distinct terms can be bounded by the fraction of such terms among all d^t tuples. This is the probability of seeing a collision when drawing t elements uniformly from $[d]$ & is at most t^2/d

$$\text{Thus,} \quad \mathbb{E}_f |\psi_f\rangle\langle\psi_f|^{\otimes t} = \rho_{\text{Symm Dist}} + \text{err} \qquad \text{where } \|\text{err}\|_1 \leq t^2/d$$

Pseudorandom Unitaries & Unitary t-designs

A Haar random unitary on n-qubits is a "uniformly random" $2^n \times 2^n$ unitary matrix

The notion of unitary t-designs and pseudorandom unitaries are two different ways of derandomizing a Haar random unitary

Unitary t-design: A distribution over $d \times d$ unitary matrices, where $d = 2^n$, is called a unitary t-design if for all $|\psi\rangle$,

$$\mathop{\mathbb{E}}_{U \sim t\text{-design}} \langle\psi| \left\{ U_I^{\dagger \otimes t} \; U_I^{\otimes t} \right\} |\psi\rangle \approx \mathop{\mathbb{E}}_{U \sim \text{Haar}} \langle\psi| \left\{ U_I^{\dagger \otimes t} \; U_I^{\otimes t} \right\} |\psi\rangle$$

In other words, given t parallel applications of U on the first register I (on nt-qubits), denoted by $U_I^{\otimes t}$, no procedure even efficient can distinguish the two. Here, t is fixed beforehand

Note: A state t-design is just a weaker case of this, just take any unitary that maps $|0^n\rangle^{\otimes t} \longrightarrow |\phi\rangle^{\otimes t}$ where $|\phi\rangle$ is a state t-design

Then, taking $|\psi\rangle^{\otimes t} = |0^n\rangle^{\otimes t}$ above, we also get a state t-design from the above

The guarantee above is for all states $|\psi\rangle$ which make this a lot more challenging task

There are two notions of approximations that are usually considered

Additive Error: This measures the error in the trace norm: $\forall\, |\psi\rangle$ we have

$$\left\| \mathop{\mathbb{E}}_{U \sim t\text{-design}} \langle\psi| \left\{ U_I^{\dagger \otimes t} \; U_I^{\otimes t} \right\} |\psi\rangle - \mathop{\mathbb{E}}_{U \sim \text{Haar}} \langle\psi| \left\{ U_I^{\dagger \otimes t} \; U_I^{\otimes t} \right\} |\psi\rangle \right\|_1 \leq \varepsilon$$

Multiplicative Error $\forall |\psi\rangle$, we have

$$1-\varepsilon \leq \frac{\mathbb{E}_{U\sim \text{Haar}} \langle\psi| \left\{ \left(U^{\dagger \otimes t} \otimes I\right)\left(U^{\otimes t} \otimes I\right) \right\} |\psi\rangle}{\mathbb{E}_{U\sim t\text{-design}} \langle\psi| \left\{ \left(U^{\dagger \otimes t} \otimes I\right)\left(U^{\otimes t} \otimes I\right) \right\} |\psi\rangle} \leq 1+\varepsilon$$

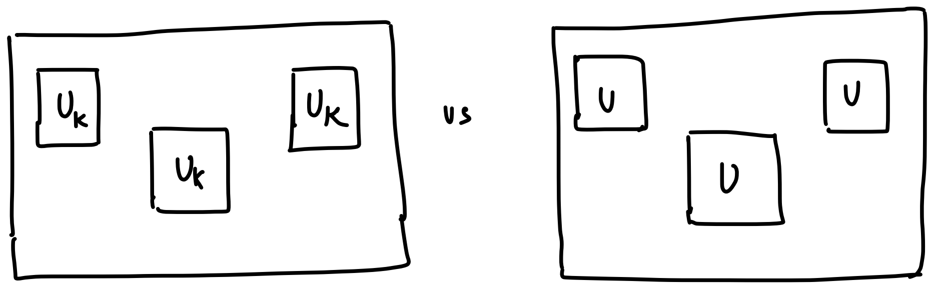
Note: Multiplicative error t-design also implies additive error t-design with the same ε parameter, but the other way could increase the error paameter by $d^{O(t)}$ factor

Pseudorandom Unitary A family of n-qubit unitaries $\{U_k\}_{k\in\{0,1\}^n}$ is called a pseudorandom unitary if

(1) Given $k\in\{0,1\}^n$, U_k can be implemented in poly(n) time

(2) No poly-time distinguisher A can query the unitary and distinguish a random U_k from a Haar random unitary,

$$\left| \mathbb{P}_{k\in\{0,1\}^n}\left[A^{U_k}(1^n)=1\right] - \mathbb{P}_{U\sim \text{Haar}}\left[A^{U}(1^n)=1\right] \right| \leq \text{negl}(n)$$



If the distinguisher A is only allowed to make parallel queries to the unitary, we say its a non-adaptive PRU. Such an algorithm A is given by

$$A^{\text{Unitary}} = \left(\text{Unitary}^{\otimes t} \otimes I\right) |\psi\rangle$$ followed by a measurement

Note that the corresponding mixed states before measurement are

$$\mathbb{E}_{U\sim\{U_k\}} \langle\psi| \left\{ \left(U^{\dagger \otimes t} \otimes I\right)\left(U^{\otimes t} \otimes I\right) \right\} |\psi\rangle \quad \text{vs} \quad \mathbb{E}_{U\sim \text{Haar}} \langle\psi| \left\{ \left(U^{\dagger \otimes t} \otimes I\right)\left(U^{\otimes t} \otimes I\right) \right\} |\psi\rangle$$

This is almost the same as a t-design but here $t=\text{poly}(n)$ is not known in advance

Note: PRUs imply PRS similar to what we discussed before for t-design

Applications & Constructions

A random quantum circuit of large enough depth gives a t-design and there are interesting applications in random circuit sampling. One of the focus of t-design construction is to get a very efficient construction of t-designs with small size and depth

One can also conjecture that a random quantum circuit of poly(n) depth is a PRU but if we could prove this without any assumption, we would show that BQP $\neq$ PSPACE

Up until recently, there was no known construction for a PRU but in a recent paper of mine with Metger, Poremba and Yuen, we showed* that the following simple construction gives a PRU as well as a Unitary t-design (*Caveat: in the current version, we have an isometry that maps n to $n + \log^2 n$ qubits instead of a unitary mapping n to n qubits)

Construction

Let C be any unitary 2-design (exact constructions are known for $t=2$)

Let $P = \sum_{x \in \{0,1\}^n} |x\rangle\langle\pi(x)|$ be a random permutation matrix (π is a random permutation of $\{0,1\}^n$)

Let $F = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle\langle x|$ be a random ± 1 diagonal matrix (f is uniformly random boolean function)

Then, $U = PFC$

- is a pseudorandom unitary if we replace F & P with pseudorandom functions & permutations
  (additive error)
- is a t-design if we replace them with their t-wise independent versions. This gives a simple and more efficient t-design construction.

Open problem: Find interesting applications of PRUs

Currently the biggest motivation comes from studying black holes where PRUs are used to model black hole dynamics so that the black hole can efficiently do it but the output looks Haar random to every feasible experiment that can be done