CS59200-PRS: Pseudorandomness Nov 5, 2025

Lecture 20: Pseudorandom States and State Design

Lecturer: Wei Zhan *Scribe: Wenbo Xie*

1 Pseudorandom Quantum State

As Haar random states are hard to prepare, we would like some quantum states that can be efficiently prepared while indistinguishable from Haar measure. This leads to the notion of pseudorandom quantum states.

Definition 1. *An n-qubit pseudorandom state (PRS) ensemble is a set of states $\{|\psi_k\rangle\}$ such that:*

- *Each $|\psi_k\rangle$ can be prepared by a P-uniform quantum circuit of size $\mathrm{poly}(n)$, where the P machine is given the key (seed) $k \in \{0,1\}^\ell$ as input with $\ell \leq \mathrm{poly}(n)$.*
- *The ensemble $\{|\psi_k\rangle\}$ is indistinguishable from Haar random states, even when multiple copies of the states are given. That is,*

$$\left| \mathop{\mathbb{E}}_{k\in\{0,1\}^\ell} \left[A\left(|\psi_k\rangle^{\otimes t}\right)\right] - \mathop{\mathbb{E}}_{|\psi\rangle\sim \mathrm{Haar}(N)} \left[A\left(|\psi\rangle^{\otimes t}\right)\right] \right| \leq \mathrm{negl}(n)$$

for every polynomial-time quantum distinguisher A, and every $t \leq \mathrm{poly}(n)$.

Notice that the definition is a direct analogy of classical pseudorandom generators, except for the t-copy part. For PRG it is unnecessary to specify the number of copies as the bit strings can be directly copied by the algorithm A when needed. However, quantum states in general cannot be copied:

Theorem 1 (No-Cloning Theorem)**.** *There is no quantum algorithm U that, given a state $|\psi\rangle$, outputs a state close to $|\psi\rangle|\psi\rangle$. That is, there is no unitary U such that*

$$\|U|\psi\rangle|0^n\rangle - |\psi\rangle|\psi\rangle\|_2 \leq 0.1$$

for every n-qubit state $|\psi\rangle$.

Proof. Let $|\psi\rangle$ and $|\phi\rangle$ be two quantum states. Suppose that there is a unitary U such that $\|U|\psi\rangle|0^n\rangle - |\psi\rangle|\psi\rangle\|_2 \leq 0.1$. Applying U to the state $|\psi\rangle$ and $|\phi\rangle$ and taking the inner product between the resulting states, we get

$$\langle\psi|\langle 0^n|U^\dagger U|\phi\rangle|0^n\rangle = \langle\psi|\phi\rangle\,.$$

On the other hand, taking the inner product between two copies of $|\psi\rangle$ and two copies of $|\phi\rangle$, we get

$$|(\langle\psi|\langle\psi|)(|\phi\rangle|\phi\rangle)| = |\langle\psi|\phi\rangle|^2.$$

Using the assumption, we can get

$$\begin{aligned}
&\left||\langle\psi|\phi\rangle| - |\langle\psi|\phi\rangle|^2\right| \\
=\ &\left|\left|\langle\psi|\langle 0^n|U^\dagger U|\phi\rangle|0^n\rangle\right| - |(\langle\psi|\langle\psi|)(|\phi\rangle|\phi\rangle)|\right| \\
\leq\ &\left|\langle\psi|\langle 0^n|U^\dagger U|\phi\rangle|0^n\rangle - (\langle\psi|\langle\psi|)(|\phi\rangle|\phi\rangle)\right| \\
=\ &\left|\langle\psi|\langle 0^n|U^\dagger U|\phi\rangle|0^n\rangle - \langle\psi|\langle 0^n|U^\dagger(|\phi\rangle|\phi\rangle)\right| + \left|\langle\psi|\langle 0^n|U^\dagger(|\phi\rangle|\phi\rangle) - (\langle\psi|\langle\psi|)(|\phi\rangle|\phi\rangle)\right| \\
\leq\ &\|U|\psi\rangle|0^a\rangle\|_2 \cdot \|U|\phi\rangle|0^n\rangle - |\phi\rangle|\phi\rangle\|_2 + \|U|\psi\rangle|0^n\rangle - |\psi\rangle|\psi\rangle\|_2 \cdot \||\phi\rangle|\phi\rangle\|_2 \\
\leq\ &0.2
\end{aligned}$$

which implies $|\langle\psi|\phi\rangle|^2 \geq |\langle\psi|\phi\rangle| - 0.2$. But, it cannot hold for all $|\psi\rangle, |\phi\rangle$. □

More over, multiple copies is necessary to ensure that the ensemble actually looks random. Since A consists of quantum operations, it is linear in the density matrix of the input state, which implies

$$\mathop{\mathbb{E}}_{k\sim\{0,1\}^l}\left[A\left(|\psi_k\rangle\langle\psi_k|^{\otimes t}\right)\right] = A\left(\mathop{\mathbb{E}}_{k\sim\{0,1\}^l}\left[|\psi_k\rangle\langle\psi_k|^{\otimes t}\right]\right).$$

If there is only a single copy of each state $|\psi_k\rangle$ (i.e., $t = 1$), then the random basis states $|\psi_k\rangle = |k\rangle$ (with $\ell = n$) also satisfies the definition of PRS, as both $\mathop{\mathbb{E}}_{k\sim\{0,1\}^n}[|k\rangle\langle k|]$ and $\mathop{\mathbb{E}}_{|\psi\rangle\sim\mathrm{Haar}(N)}[|\psi\rangle\langle\psi|]$ are $\frac{1}{N}I_N$ and they cannot be distinguished by any quantum algorithm, thus making the definition trivial. In contrast, even with two copies a random basis state can be easily distinguished from a Haar random state: when measured over the computational basis, two copies of the basis state always gives the same outcome while a Haar random state will give a different outcome on each copy.

1.1 Exotic Properties of PRS

Despite the similarities in their definitions, there are many properties of PRG we list below that is not shared with PRS, mostly due to the fact that Haar random states are much more complex objects that random bit strings.

Cannot be shortened: The first $n-1$ bits of a PRG output is also pseudorandom, but given an n-qubit PRS, its first $n-1$ qubit is not an $(n-1)$-qubit PRS. Even the first single qubit is not a single-qubit PRS. This is because the partial trace of a Haar random state is highly likely close to a maximally mixed state, instead of a random pure state.

Cannot be extended: The output length of a PRG G can be doubled by considering $(G(s), G(s'))$ with two independent seeds s and s'. This does not work with PRS, as the resulting state is a product state but a Haar random state on $2n$ qubits are almost always entangled.

No trivial seed length: For PRG we require the seed length ℓ to be smaller than the output length n since otherwise it is trivial. For PRS we don't have trivial construction for any $\ell \leq \text{poly}(n)$.

No distinguisher $\Leftrightarrow$ next-qubit predictor: This crucial property for PRG does not have a PRS counterpart, mainly due to the first property that a part of the PRS is not PRS, thus breaking the hybrid argument.

These properties rends almost every trick we used for classical PRG unusable for PRS. Therefore, to reason about PRS we have to go back to the fundamentals and understand the structure of Haar random states.

2 State Design

Definition 2 (State Design)**.** *An ensemble of states $\{|\psi_k\rangle\}$ is called a* state t-design *if*

$$\mathop{\mathbb{E}}_{k}\left[(|\psi_k\rangle\langle\psi_k|)^{\otimes t}\right] = \mathop{\mathbb{E}}_{|\psi\rangle\sim\text{Haar}(N)}\left[(|\psi\rangle\langle\psi|)^{\otimes t}\right].$$

Remark 2. Notice that the notion of state design is incomparable with PRS: While state design asserts statistical indistinguishability which is stronger than the computational indistinguishability of PRS, the number of copies t here is fixed while the indistinguishability of PRS needs to hold for every polynomial t. However, when t is superpolynomial, a t-design is directly a PRS.

Remark 3. Another way to think about t-design is that it is a quantum analog of classical k-wise uniformity. This can be seen by think of a random vector $X \in \{0,1\}^n$. We have X is k-wise uniform, if and only if

$$\mathop{\mathbb{E}}_{X}[X^{\otimes k}] = \mathop{\mathbb{E}}_{U\sim\{0,1\}^n}[U^{\otimes k}].$$

In both state designs and PRS, the key question is to under stand what exactly is $\mathop{\mathbb{E}}_{|\psi\rangle\sim\text{Haar}(N)}\left[(|\psi\rangle\langle\psi|)^{\otimes t}\right]$. When $t = 1$ we know it is the maximally mixed state $\frac{1}{N}I_N$. When $t = 2$, what is

$$\mathop{\mathbb{E}}_{|\psi\rangle\sim\text{Haar}(N)}\left[(|\psi\rangle\langle\psi|)^{\otimes 2}\right]?$$

One might guess that it is $\left(\frac{1}{N}I_N\right)^{\otimes 2}$, but there is a simple argument showing it is *not*.

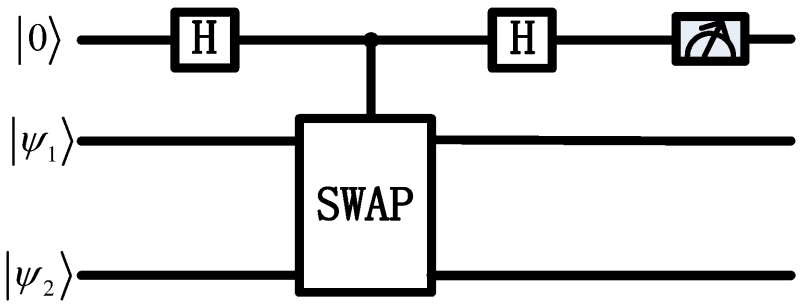

Figure 1: SWAP Test

2.1 SWAP Test

First, we define the the SWAP operator. The SWAP operator is the unitary that maps $|\psi\rangle|\phi\rangle \mapsto |\phi\rangle|\psi\rangle$ for every two n-qubit states $|\psi\rangle$ and $|\psi\rangle$. Moreover, one can define the controlled-SWAP (cSWAP) as follows:

$$\text{cSWAP} : \begin{cases} |0\rangle|\psi\rangle|\phi\rangle \mapsto |0\rangle|\psi\rangle|\phi\rangle, \\ |1\rangle|\psi\rangle|\phi\rangle \mapsto |1\rangle|\phi\rangle|\psi\rangle. \end{cases}$$

Now, let us consider the circuit in Figure 1, and valuate the quantum state before the measurement. Starting with $|0\rangle|\psi\rangle|\phi\rangle$:

$$\begin{aligned} |0\rangle|\psi\rangle|\phi\rangle &\xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|\psi\rangle|\phi\rangle \\ &\xrightarrow{\text{cSWAP}} \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle) \\ &\xrightarrow{H} \frac{1}{\sqrt{2}}(|+\rangle|\psi\rangle|\phi\rangle + |-\rangle|\phi\rangle|\psi\rangle) \\ &= \frac{1}{2}\big[|0\rangle(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) + |1\rangle(|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle)\big]. \end{aligned}$$

Measuring the first qubit, the probability that the measurement outputs 1 is

$$\begin{aligned} \Pr[\text{outputting 1}] &= \left\| \frac{1}{2}\big(|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle\big) \right\|_2^2 \\ &= \frac{1}{4}\left[1 + 1 - \langle\phi|\psi\rangle\langle\psi|\phi\rangle - \langle\psi|\phi\rangle\langle\phi|\psi\rangle\right] \\ &= \frac{1}{2} - \frac{1}{2}|\langle\psi|\phi\rangle|^2 \\ &= \begin{cases} 0 & \text{if } |\psi\rangle = |\phi\rangle, \\ \frac{1}{2} & \text{if } |\psi\rangle \text{ and } |\phi\rangle \text{ are orthogonal.} \end{cases} \end{aligned}$$

Now, we go back to the second example above. Clearly, $|\psi\rangle|\psi\rangle$ for all quantum states passes the SWAP test and $|i\rangle|j\rangle$ won't pass for all computational basis vector $|i\rangle \neq |j\rangle$, which implies $\mathbb{E}_{|\psi\rangle}[(|\psi\rangle\langle\psi|)^{\otimes 2}]$ passes SWAP test and $\frac{1}{N^2}\sum_{i,j}|i\rangle\langle i|\otimes|j\rangle\langle j| = \left(\frac{1}{N}I_N\right)^{\otimes 2}$ does not.

3 Symmetric Subspace

In general, the state $\mathop{\mathbb{E}}_{|\psi\rangle\sim\mathrm{Haar}(N)}[(|\psi\rangle\langle\psi|)^{\otimes t}]$ can be characterized by the two properties:

- Invariance under SWAP applied on any two copies;
- Invariance under $U^{\otimes t}$ for every $U \in \mathbb{U}(N)$.

To characterize the first property, we define the symmetric subspace $\mathrm{Sym}_{N,t}$ be the subspace of $(\mathbb{C}^N)^{\otimes t}$ spanned by states invariant under SWAP operations:

$$\mathrm{Sym}_{N,t} = \left\{ |\psi\rangle \in (\mathbb{C}^N)^{\otimes t} \;\middle|\; \mathrm{SWAP}_{ij}|\psi\rangle = |\psi\rangle,\ \forall i,j \right\}.$$

Since SWAP operations generate all permutations over the copies, that is, for $\sigma \in S_t$ (the symmetric group on t elements), define the permutation operator

$$V_\sigma : |\psi_1\rangle \otimes \cdots \otimes |\psi_t\rangle \mapsto |\psi_{\sigma(1)}\rangle \otimes \cdots \otimes |\psi_{\sigma(t)}\rangle,$$

then the symmetric subspace can be equivalently defined as

$$\mathrm{Sym}_{N,t} = \left\{ |\psi\rangle \in (\mathbb{C}^N)^{\otimes t} \;\middle|\; V_\sigma|\psi\rangle = |\psi\rangle,\ \forall \sigma \in S_t \right\}.$$

Define the symmetrization operator

$$\Pi_{\mathrm{sym}} = \frac{1}{t!}\sum_{\sigma\in S_t} V_\sigma.$$

We have the following properties:

1. $\Pi_{\mathrm{sym}}^2 = \Pi_{\mathrm{sym}}$ (since $\sum_{\sigma,\tau\in S_t} V_\sigma V_\tau = \sum_{\sigma,\tau\in S_t} V_{\sigma\tau} = t!\sum_\sigma V_\sigma$).
2. $\Pi_{\mathrm{sym}}^\dagger = \Pi_{\mathrm{sym}}$ (since $\sum_\sigma V_\sigma^\dagger = \sum_\sigma V_{\sigma^{-1}} = \sum_\sigma V_\sigma$).
3. $\Pi_{\mathrm{sym}}|\psi\rangle = |\psi\rangle$ for all $|\psi\rangle \in \mathrm{Sym}_{N,t}$.
4. $\Pi_{\mathrm{sym}}|\psi\rangle \in \mathrm{Sym}_{N,t}$ for all $|\psi\rangle \in (\mathbb{C}^N)^{\otimes t}$.

This means that Π_{sym} is the orthogonal projection onto $\mathrm{Sym}_{N,t}$.

To characterize the second property, we use the following result from representation theory that we are not going to prove:

Theorem 4 (Schur-Weyl Duality)**.**

$$\left\{M \in \mathbb{C}^{N^t \times N^t} \;\middle|\; U^{\otimes t} M (U^\dagger)^{\otimes t} = M, \forall U \in \mathbb{U}(N)\right\} = \operatorname{span}\left\{V_\sigma \mid \sigma \in S_t\right\}.$$

Now we can figure out $\mathop{\mathbb{E}}_{|\psi\rangle \sim \text{Haar}(N)} [(|\psi\rangle\langle\psi|)^{\otimes t}]$ exactly. By Theorem 4 we can write

$$\mathop{\mathbb{E}}_{|\psi\rangle \sim \text{Haar}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] = \sum_{\sigma \in S_t} c_\sigma V_\sigma$$

Let us consider any $\pi \in S_t$. Then,

$$\sum_{\sigma \in S_t} c_\sigma V_\sigma = V_\pi \mathop{\mathbb{E}}_{|\psi\rangle \sim \text{Haar}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] V_\pi^\dagger = \sum_{\sigma \in S_t} c_{\pi\sigma\pi^{-1}} V_\sigma$$

which implies c_σ must be the same for all σ. Since the density matrix has trace 1, using the definition of Π_{sym}, we get

$$\mathop{\mathbb{E}}_{|\psi\rangle \sim \text{Haar}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] = c \sum_{\sigma \in S_t} V_\sigma = c \cdot t! \Pi_{sym} = \frac{1}{\operatorname{Tr}[\Pi_{\text{sym}}]} \Pi_{\text{sym}}$$

The trace of the orthogonal projection Π_{sym} is exactly the dimension of the subspace it projects onto, which is $\operatorname{Sym}_{N,t}$.

Claim 5. $\dim \operatorname{Sym}_{N,t} = \#$ *ways to partition* t *into* N *parts* $= \binom{N+t-1}{t}$

Proof. Note that $\operatorname{Sym}_{N,t}$ is spanned by $\Pi_{\text{sym}}|i_1\rangle \otimes \cdots \otimes |i_t\rangle$ for $i_1, \cdots, i_t \in [N]$. These vectors in fact form a orthogonal basis, since

$$\langle i_1, \cdots, i_t | \Pi_{\text{sym}}^\dagger \Pi_{\text{sym}} | i_1', \cdots, i_t' \rangle \neq 0 \iff (i_1, \cdots, i_t) \text{ is a permutation of } (i_1', \cdots, i_t').$$

Thus the dimension of $\operatorname{Sym}_{N,t}$ is the number of distinct t-tuples in $[N]^t$ under permutations, or equivalently, the number of ways to put t identical balls into N distinct bins. □

Applying the claim above, we get

$$\begin{aligned}\mathop{\mathbb{E}}_{|\psi\rangle \sim \text{Haar}} \left[|\psi\rangle\langle\psi|^{\otimes t}\right] =& \frac{1}{\binom{N+t-1}{t}} \Pi_{\text{sym}} \\ =& \frac{1}{\binom{N+t-1}{t}} \sum_{\text{multiset } X \text{ on } [N], |X|=t} |\text{sym}_X\rangle\langle\text{sym}_X|\end{aligned}$$

where

$$|\text{sym}_X\rangle = \sqrt{\frac{m_1 \cdots m_N}{t!}} \sum_{\{i_1, \cdots, i_t\} = X} |i_1, \cdots, i_t\rangle\langle i_1, \cdots, i_t|$$

and m_i is the multiplicity of i in X. For instance, when $t = 2$ we have

$$\mathop{\mathbb{E}}_{|\psi\rangle \sim \text{Haar}} \left[|\psi\rangle\langle\psi|^{\otimes 2}\right] = \frac{2}{N(N+1)} \left[\sum_{x \in [N]} |xx\rangle\langle xx| + \frac{1}{2} \sum_{x<y} (|xy\rangle + |yx\rangle)(\langle xy| + \langle yx|)\right].$$