Ph 220: Quantum Learning Theory
Lecture Note 9: Pseudorandom Unitaries (PRU)

Hsin-Yuan Huang (Robert)

California Institute of Technology

1 Introduction

In previous lectures, we discussed the existence of *Pseudorandom States* (PRS), which are efficiently preparable quantum states that are indistinguishable from Haar-random states. Today, we address the dynamical analog of this question. Haar-random unitaries are fundamental to quantum information, appearing in randomized benchmarking, black-hole dynamics models, and quantum cryptography. However, implementing a truly Haar-random unitary on n qubits requires exponential circuit depth ($\mathcal{O}(2^{2n})$ gates). This motivates a central question in quantum learning theory and quantum cryptography:

Can we construct efficient polynomial-size quantum circuits that are computationally indistinguishable from Haar-random unitaries?

If such circuits exist, we call them **Pseudorandom Unitaries (PRUs)**. Their existence implies a fundamental hardness of learning: if a unitary is a PRU, no polynomial-time algorithm can learn its input-output behavior or distinguish it from a maximally random evolution.

1.1 The Main Result

Theorem 1 (Existence of PRUs)**.** Assume the existence of quantum-secure one-way functions (OWFs). Then, there exists an ensemble of efficiently implementable unitaries that is computationally indistinguishable from the Haar measure.

Specifically, for any polynomial-time quantum adversary $\mathcal{A}$ making $t = \mathrm{poly}(n)$ adaptive queries:

$$\left| \Pr_{U \sim \mathcal{U}_{\mathrm{PRU}}} [\mathcal{A}^U = 1] - \Pr_{U \sim \mathcal{U}_{\mathrm{Haar}}} [\mathcal{A}^U = 1] \right| \leq \mathrm{negl}(n). \tag{1}$$

2 The Construction

2.1 Information-Theoretic Construction

To prove security, we first analyze an information-theoretic idealization where cryptographic primitives are replaced by truly random functions.

Definition 1 (Ideal PRU Construction)**.** Let $N = 2^n$. The unitary U is defined as the composition:

$$U := P_\pi \cdot F_f \cdot C \tag{2}$$

where:

1. $C \in \mathcal{C}_n$ is a uniformly random **Clifford unitary** (provides global mixing).
2. F_f is a **random phase oracle** defined by a random Boolean function $f : \{0,1\}^n \to \{0,1\}$:
$$F_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle\,. \tag{3}$$
3. P_π is a **random permutation oracle** defined by a random permutation $\pi \in S_N$:
$$P_\pi\,|x\rangle = |\pi(x)\rangle\,. \tag{4}$$

Remark 1 (Computational Instantiation)**.** To obtain an efficient circuit, we replace:

- The random function f with a quantum-secure pseudorandom function (PRF).
- The random permutation π with a quantum-secure pseudorandom permutation (PRP).

Both primitives can be constructed efficiently assuming quantum-secure one-way functions exist. The Clifford group is a 3-design and can be sampled efficiently ($\mathcal{O}(n^2)$ gates).

3 Proof of Indistinguishability

Let $\mathcal{A}$ be a quantum adversary that makes $t = \mathrm{poly}(n)$ adaptive queries to the unknown unitary. We must bound the trace distance between the system state when interacting with the PRU versus the Haar ensemble. First, let us write down the output state from any quantum algorithm making t queries to an unknown unitary U,

$$|\psi^U\rangle_{AB} = \prod_{i=1}^{t} U_A W_{i,AB}\,|0^{n+m}\rangle_{AB}\,, \tag{5}$$

We have a system register of n qubits A and an ancillary registor of m qubits B. The n-qubit unitary U_A acts on the n-qubit system A. We will index the register each operation acts on in the following. We would like to understand how small the following is:

$$\left\|\mathbb{E}_{\pi,f,C}|\psi^{P_\pi\cdot F_f\cdot C}\rangle\langle\psi^{P_\pi\cdot F_f\cdot C}| - \mathbb{E}_{U:\mathrm{Haar}}|\psi^U\rangle\langle\psi^U|\right\|_1 \tag{6}$$

3.1 Purification

Consider any fixed n-qubit unitary C (not necessarily Clifford). We can purify the mixed state when π and f are chosen randomly to obtain the following state:

$$|\phi^C\rangle_{ABFP} = \sum_{\pi} \frac{1}{\sqrt{2^n!}} \sum_{f} \frac{1}{\sqrt{2^{2^n}}} \sum_{\substack{x_1,\ldots,x_t\in\{0,1\}^n\\ y_1,\ldots,y_t\in\{0,1\}^n}} \prod_{i=1}^{t} P_{\pi,A} F_{f,A} C_A W_{i,AB}\,|0^{n+m}\rangle_{AB}\,|f,\pi\rangle_{FP}\,. \tag{7}$$

By construction, we have

$$\mathbb{E}_{\pi,f}|\psi^{P_\pi\cdot F_f\cdot C}\rangle\langle\psi^{P_\pi\cdot F_f\cdot C}|_{AB} = \mathrm{Tr}_{FP}|\phi^C\rangle\langle\phi^C|_{ABFP}. \tag{8}$$

We can expand the definition of P_π and F_f to obtain

$$|\phi^C\rangle_{ABFP} = \sum_{\substack{x_1,\ldots,x_t\in\{0,1\}^n\\ y_1,\ldots,y_t\in\{0,1\}^n}} \prod_{i=1}^{t} |y_i\rangle\langle x_i|_A C_A W_{i,AB}\,|0^{n+m}\rangle_{AB}\,|\widetilde{\Phi}_{x,y}\rangle_{FP}\,, \tag{9}$$

$$|\widetilde{\Phi}_{x,y}\rangle_{FP} = \sum_{\pi} \frac{1}{\sqrt{2^n!}} \sum_{f} \frac{1}{\sqrt{2^{2^n}}} (-1)^{\sum_i f(x_i)} \prod_{i=1}^{t} \delta_{\pi(x_i)=y_i}\,|f,\pi\rangle_{FP}\,. \tag{10}$$

3.2 Geometry

It's a simple exercise to check that:

- $|\widetilde{\Phi}_{x,y}\rangle_{FP} = 0$ if $x_1, \ldots, x_t$ are distinct but $y_1, \ldots, y_t$ are not distinct.
- $|\widetilde{\Phi}_{x,y}\rangle_{FP} = 0$ if $x_1, \ldots, x_t$ are not distinct but $y_1, \ldots, y_t$ are distinct.
- $\langle\widetilde{\Phi}_{x,y}\,|\widetilde{\Phi}_{x,y}\rangle_{FP} = \frac{(2^n-t)!}{2^n!}$ if $x_1, \ldots, x_t$ are distinct and $y_1, \ldots, y_t$ are distinct.

It's also a simple exercise to check the following inner product relation:

- $\langle\widetilde{\Phi}_{x',y'}\,|\widetilde{\Phi}_{x,y}\rangle_{FP} = \frac{(2^n-t)!}{2^n!}\delta_{\{(x_i,y_i)\}_i=\{(x'_i,y'_i)\}_i}$ if $x_1, \ldots, x_t$ are distinct, and $y_1, \ldots, y_t$ are distinct, and $x'_1, \ldots, x'_t$ are distinct, and $y'_1, \ldots, y'_t$ are distinct.
- $\langle\widetilde{\Phi}_{x',y'}\,|\widetilde{\Phi}_{x,y}\rangle_{FP} = 0$ if $x_1, \ldots, x_t$ are distinct, and $y_1, \ldots, y_t$ are distinct, but $x'_1, \ldots, x'_t$ are not distinct, and $y'_1, \ldots, y'_t$ are not distinct.

This means there exists an isometry $\mathsf{Compress}$ from FP registers to XY registers such that for any $x = (x_1, \ldots, x_t), y = (y_1, \ldots, y_t)$ that consist of distinct bitstrings,

$$\mathsf{Compress}\,|\widetilde{\Phi}_{x,y}\rangle_{FP} = \sqrt{\frac{(2^n-t)!}{2^n!}}\,|\{(x_i,y_i)\}_i\rangle_{XY}\,, \tag{11}$$

$$\text{where}\quad |\{(x_i,y_i)\}_i\rangle = \frac{1}{\sqrt{t!}}\sum_{\sigma}\sigma\,|x_1,\ldots,x_t\rangle\otimes\sigma\,|y_1,\ldots,y_t\rangle\,. \tag{12}$$

We give this isometry this name because it compresses an $\tilde{\mathcal{O}}(2^n)$-qubit register to just $\mathcal{O}(nt)$ qubits. We can now define the projector:

$$\Pi_{FP} = \sum_{\substack{x_1<\ldots<x_t\\ y_1,\ldots,y_t:\text{distinct}}}\frac{2^n!}{(2^n-t)!}|\widetilde{\Phi}_{x,y}\rangle\langle\widetilde{\Phi}_{x,y}|_{FP} = \sum_{\substack{S=\{(x_i,y_i)\}_{i=1}^t\\ x_1,\ldots,x_t:\text{distinct}\\ y_1,\ldots,y_t:\text{distinct}}}\mathsf{Compress}^\dagger|S\rangle\langle S|_{XY}\mathsf{Compress}. \tag{13}$$

Using this geometric characterization, we have:

$$|\phi^C\rangle_{ABFP} = \sum_{\substack{x_1,\ldots,x_t:\text{distinct}\\ y_1,\ldots,y_t:\text{distinct}}}\prod_{i=1}^{t}|y_i\rangle\langle x_i|_A C_A W_{i,AB}\,|0^{n+m}\rangle_{AB}\,|\widetilde{\Phi}_{x,y}\rangle_{FP}\,, \tag{14}$$

$$+\sum_{\substack{x_1,\ldots,x_t:\text{not distinct}\\ y_1,\ldots,y_t:\text{not distinct}}}\prod_{i=1}^{t}|y_i\rangle\langle x_i|_A C_A W_{i,AB}\,|0^{n+m}\rangle_{AB}\,|\widetilde{\Phi}_{x,y}\rangle_{FP}\,. \tag{15}$$

Furthermore, we have:

$$\mathsf{Compress}\cdot\Pi_{FP}\cdot|\phi^C\rangle_{ABFP} = \tag{16}$$

$$\sqrt{\frac{(2^n-t)!}{2^n!}}\sum_{\substack{x_1,\ldots,x_t:\text{distinct}\\ y_1,\ldots,y_t:\text{distinct}}}\prod_{i=1}^{t}|y_i\rangle\langle x_i|_A C_A W_{i,AB}\,|0^{n+m}\rangle_{AB}\,|\{(x_i,y_i)\}_i\rangle_{XY}\,. \tag{17}$$

3.3 Invariant State and Path-Recording Oracle

Inspired by the final expression, we define the invariant state

$$|\eta^C\rangle_{ABXY} = \sqrt{\frac{(2^n-t)!}{2^n!}} \sum_{\substack{x_1,\dots,x_t\in\{0,1\}^n \\ y_1,\dots,y_t:\text{distinct}}} \prod_{i=1}^{t} |y_i\rangle\langle x_i|_A C_A W_{i,AB} |0^{n+m}\rangle_{AB} |\{(x_i,y_i)\}_i\rangle_{XY} . \tag{18}$$

Using $\sum_{x\in\{0,1\}^n} |x\rangle \otimes \langle x| C = \sum_{y\in\{0,1\}^n} C|y\rangle \otimes \langle y|$, we have

Lemma 1 (Invariance)**.** For any n-qubit unitary C, $|\eta^C\rangle_{ABXY} = (C^{\otimes t})_X |\eta^I\rangle_{ABXY}$.

Definition 2 (Path-Recording Oracle)**.** Consider the isometry PRO that takes in any $x \in \{0,1\}^n$ and any set $S = \{(x_i,y_i)\}_{i=1}^{|S|}$ such that $|S| < 2^n$ and $y_1,\dots,y_{|S|}$ are distinct, and maps to

$$\mathsf{PRO}\,|x\rangle_A |S\rangle_{XY} = \frac{1}{\sqrt{N-|S|}} \sum_{y\notin y_1,\dots,y_{|S|}} |y\rangle_A |S\rangle_{XY} . \tag{19}$$

It is another simple exercise to check that this is an isometry.

We can rewrite the invariant state using the path-recording oracle:

$$|\eta^C\rangle_{ABXY} = \left(\prod_{i=1}^{t} \mathsf{PRO}_{AXY} \cdot C_A \cdot W_{i,AB}\right) |0^{n+m}\rangle_{AB} |\{\}\rangle_{XY} . \tag{20}$$

This immediately implies that the invariant state has unit norm:

Lemma 2 (Unit Norm)**.** $\langle\eta^C|\eta^C\rangle_{ABXY} = 1$.

We also define the distinct subspace projector:

$$\Pi_X = \sum_{x_1,\dots,x_t:\text{ distinct}} |x_1,\dots,x_t\rangle\langle x_1,\dots,x_t|_X . \tag{21}$$

By construction of $|\eta^C\rangle_{ABXY}$, we have the following bridge between the FP purification and the XY purification:

Lemma 3 (Bridge)**.** $\Pi_X |\eta^C\rangle_{ABXY} = \mathsf{Compress} \cdot \Pi_{FP} \cdot |\phi^C\rangle_{ABFP}$. Hence,

$$\mathrm{Tr}_{XY}\left(\Pi_X |\eta^C\rangle\langle\eta^C|_{ABXY} \Pi_X\right) = \mathrm{Tr}_{FP}\left(\Pi_{FP} |\phi^C\rangle\langle\phi^C|_{ABFP} \Pi_{FP}\right) . \tag{22}$$

3.4 Almost Distinct

By the Bridge lemma, we have

$$\mathrm{Tr}(|\eta^C\rangle\langle\eta^C|_{ABXY}) - \mathrm{Tr}(\Pi_{XY}|\eta^C\rangle\langle\eta^C|_{ABXY}\Pi_{XY}) \tag{23}$$

$$= \mathrm{Tr}(|\phi^C\rangle\langle\phi^C|_{ABFP}) - \mathrm{Tr}(\Pi_{FP}|\phi^C\rangle\langle\phi^C|_{ABFP}\Pi_{FP}). \tag{24}$$

From the Gentle Measurement Lemma in Lecture Note 8, we have

$$\left\|\mathrm{Tr}_{FP}\left(|\phi^C\rangle\langle\phi^C|_{ABFP}\right) - \mathrm{Tr}_{FP}\left(\Pi_{FP}|\phi^C\rangle\langle\phi^C|_{ABFP}\Pi_{FP}\right)\right\|_1 \tag{25}$$

$$= \mathrm{Tr}(|\phi^C\rangle\langle\phi^C|_{ABFP}) - \mathrm{Tr}(\Pi_{FP}|\phi^C\rangle\langle\phi^C|_{ABFP}\Pi_{FP}) \tag{26}$$

$$= 1 - \langle\eta^C|\,\Pi_{XY}\,|\eta^C\rangle_{ABXY} \tag{27}$$

$$= \mathrm{Tr}(|\eta^C\rangle\langle\eta^C|_{ABXY}) - \mathrm{Tr}(\Pi_{XY}|\eta^C\rangle\langle\eta^C|_{ABXY}\Pi_{XY}) \tag{28}$$

$$= \left\|\mathrm{Tr}_{XY}\left(|\eta^C\rangle\langle\eta^C|_{ABXY}\right) - \mathrm{Tr}_{XY}\left(\Pi_{XY}|\eta^C\rangle\langle\eta^C|_{ABXY}\Pi_{XY}\right)\right\|_1 . \tag{29}$$

For any C sampled from a 2-design, we have

$$\begin{aligned}
&\mathbb{E}_C \left[1 - \langle \eta^C | \, \Pi_{XY} \, | \eta^C \rangle_{ABXY}\right] && (30)\\
&\leq \sum_{i<j\in\{1,\ldots,t\}} \sum_{z\in\{0,1\}^n} \mathbb{E}_C \, \langle \eta^C | \left(|z\rangle\!\langle z|_{X_i} \otimes |z\rangle\!\langle z|_{X_i} \otimes \mathbb{I}_{\neq X_i, \neq X_j} \right) | \eta^C \rangle_{ABXY} && (31)\\
&= \sum_{i<j\in\{1,\ldots,t\}} \sum_{z\in\{0,1\}^n} \langle \eta^I | \, \mathbb{E}_C (C^\dagger |z\rangle\!\langle z|_{X_i} C \otimes C^\dagger |z\rangle\!\langle z|_{X_i} C \otimes \mathbb{I}_{\neq X_i, \neq X_j}) \, | \eta^I \rangle_{ABXY} && (32)\\
&= \sum_{i<j\in\{1,\ldots,t\}} \sum_{z\in\{0,1\}^n} \frac{1}{2^n(2^n+1)} \langle \eta^I | \left(I + \mathrm{SWAP}_{X_i, X_j} \right) | \eta^I \rangle_{ABXY} && (33)\\
&\leq \sum_{i<j\in\{1,\ldots,t\}} \frac{2}{(2^n+1)} = \frac{t(t-1)}{2^n+1} \leq \frac{t^2}{2^n}. && (34)
\end{aligned}$$

This implies that applying the distinct subspace projector changes the state by an exponentially small amount for any polynomial t.

3.5 Roadmap

Consider any C sampled from 2-design (either Clifford or Haar).

$$\begin{aligned}
\mathbb{E}_{\pi,f,C} |\psi^{P_\pi \cdot F_f \cdot C}\rangle\!\langle \psi^{P_\pi \cdot F_f \cdot C}|_{AB} &= \mathbb{E}_C \mathrm{Tr}_{FP} \left(|\phi^C\rangle\!\langle \phi^C|_{ABFP} \right) && \text{(Purification)}\\
&\approx \mathbb{E}_C \mathrm{Tr}_{FP} \left(\Pi_{FP} |\phi^C\rangle\!\langle \phi^C|_{ABFP} \Pi_{FP} \right) && \text{(Almost Distinct)}\\
&= \mathbb{E}_C \mathrm{Tr}_{XY} \left(\Pi_X |\eta^C\rangle\!\langle \eta^C|_{ABXY} \Pi_X \right) && \text{(Bridge)}\\
&\approx \mathbb{E}_C \mathrm{Tr}_{XY} \left(|\eta^C\rangle\!\langle \eta^C|_{ABXY} \right) && \text{(Almost Distinct)}\\
&= \mathrm{Tr}_{XY} \left(|\eta^I\rangle\!\langle \eta^I|_{ABXY} \right) && \text{(Invariance)}
\end{aligned}$$

The two approximation incurs trace distance error of $t^2/2^n$. Hence,

$$\left\| \mathbb{E}_{\pi,f,C} |\psi^{P_\pi \cdot F_f \cdot C}\rangle\!\langle \psi^{P_\pi \cdot F_f \cdot C}|_{AB} - \mathrm{Tr}_{XY} \left(|\eta^I\rangle\!\langle \eta^I|_{ABXY} \right) \right\|_1 \leq 2(t^2/2^n). \quad (35)$$

By considering C to be either Haar-random or Clifford, we have

$$\left\| \mathbb{E}_{\pi,f,C} |\psi^{P_\pi \cdot F_f \cdot C}\rangle\!\langle \psi^{P_\pi \cdot F_f \cdot C}| - \mathbb{E}_{U:\mathrm{Haar}} |\psi^U\rangle\!\langle \psi^U| \right\|_1 \leq 4(t^2/2^n). \quad (36)$$

This completes the proof of the existence of PRUs. In PSET 5, you will derive how to construct PRUs in extremely low depth, which will then lead to a wide range of hardness of learning results (time, causality, topological order, phases of matter, spacetime geometry, etc.).