D

§ 5.3 Pseudorandom unitaries relative to $(\mathcal{U}, \mathcal{C})$

Story:
- We now show that PRUs exist relative to $(\mathcal{U}, \mathcal{C})$.
- The security proof actually does not depend on $\mathcal{C}$ — the same construction is secure for any language $\mathcal{C}$ that is independent of the randomly sampled $\mathcal{U}$.
- The PRU ensemble for a given length is supplied directly by $\mathcal{U}$.

Def^: PRU ensemble: For a given length n, the PRU ensemble is uniform over the 2^n different n-qubit unitaries in $\mathbb{U}_n$.

Notation: Denote by $\{U_k\}_{k \in [N]}$ the PRU ensemble (for a fixed n).

Story: We first establish that the average advantage of a poly-time adversary is small against our PRU construction.

Lemma 31. Consider: a quantum algorithm $A^{\mathcal{O}\mathcal{U}}$ that makes T queries to $U = (U_1 \dots U_N) \in \mathbb{U}(\mathbb{C}^2)^N$ & $\mathcal{O} \in \mathbb{U}(\mathbb{C}^2)$.

For a fixed U, define

$$adv(A^U) := \Pr_{k \leftarrow [N]}[A^{U_k, U}(\cdot) = 1] - \Pr_{O \leftarrow \mu_D}[A^{O,U}(\cdot) = 1].$$

Then, $\exists$ a universal constant $C > 0$ s.t.

$$\mathop{\mathbb{E}}_{U \leftarrow \mathcal{U}_D^N}[adv(A^U)] \leq \frac{CT^2}{N}$$

Proof

Strategy: • Reduce to the quantum query lower bound for unstructured search.

• Intuitively, if A could identify whether $O \in \{U_1, \ldots, U_N\}$ or not, then A can be modified into an alg. B that finds a single marked item from a list of size N.

• Then the BBBV theorem [BBBV '97] forces T to be $\Omega(\sqrt{N})$

• The formal proof is as follows.

Construction: B^x : queries a string $x \in \{0,1\}^N$ as follows:

- B draws a unitary $V = (V_0 V_1 \ldots V_N) \in \mathbb{U}(\Delta)^{N+1}$ from μ_Δ^{N+1}.
- B runs A replacing
  - queries to O by those to V_0

For a fixed U, define:

$$adv(\mathcal{A}^U) := \Pr_{k \leftarrow [N]}\left[\mathcal{A}^{U_k, U} = 1\right] - \Pr_{O \leftarrow \mu_\Delta}\left[\mathcal{A}^{O, U} = 1\right].$$

Then, $\exists$ a universal constant $C > 0$ s.t.

$$\mathop{\mathbb{E}}_{U \leftarrow \mu_\Delta^N}\left[adv(\mathcal{A}^U)\right] \leq \frac{CT^2}{N}$$

Proof.

Strategy: • Reduce to the quantum query lower bound for unstructured search.

• Intuitively, if $\mathcal{A}$ could identify whether $O \in \{U_1 \dots U_N\}$ or not, then $\mathcal{A}$ can be modified into an alg. $\mathcal{B}$ that finds a single marked item from a list of size N.

• Then the BBBV theorem [BBBV '97] forces T to be $\Omega(\sqrt{N})$

• The formal proof is as follows.

Construction: $\mathcal{B}^x$: queries a string $x \in \{0,1\}^N$ as follows:

- $\mathcal{B}$ draws a unitary $V = (V_0\, V_1 \dots V_N) \in \mathbb{U}(\Delta)^{N+1}$ from μ_Δ^{N+1}.

- $\mathcal{B}$ runs $\mathcal{A}$ replacing
  - queries to O by those to V_0.

• queries to $U_k \in U$ by V_0 if $x_k = 1$
V_k if $x_k = 0$.

Let $e_k \in \{0,1\}^N$ be the string with 1 in the k^{th} position & 0 elsewhere.

NB: $\mathop{\mathbb{E}}_{U \leftarrow \mathcal{M}_D^N} [adv(\mathcal{A}^U)] =$

$$\mathop{\mathbb{E}}_{U \leftarrow \mathcal{M}_D^N} \left[\mathop{Pr}_{k \leftarrow [N]} \left[\mathcal{A}^{U_k, U} = 1 \right] \right] - \mathop{\mathbb{E}}_{U \leftarrow \mathcal{M}_D^N} \left[\mathop{Pr}_{0 \leftarrow \mathcal{M}_D} \left[\mathcal{A}^{0, U} = 1 \right] \right]$$

$$= \mathop{Pr}_{k \leftarrow [N]} \left[\mathcal{B}^{e_k} = 1 \right] - Pr \left[\mathcal{B}^{0^N} = 1 \right]$$

$$\leq \frac{cT^2}{N}$$

□

Story: • The next lemma, uses Lemma 31 above to show that $|adv(\mathcal{A}^U)|$ is small w/ extremely high prob. (not just the average)

• This follows from the strong concentration property of the Haar measure.

• This strengthened version of Lemma 31 will be needed to argue that the advantage remains small, even after union bounding over all classical advice.

Lemma 32. Consider a quantum alg. $A^{O,U}$ that makes T queries to $U = (U_1 \dots U_N) \in \mathbb{U}(D)^N$ & $O \in \mathbb{U}(N)$.

Let $\mathrm{adv}(A^U)$ be as defined in Lemma 31 above.

Then, $\exists$ a universal const $c > 0$ s.t.

for any $p \geq \frac{cT^2}{N}$, it holds that

$$\Pr_{U \leftarrow \mu_D^N}\left[\,|\mathrm{adv}(A^U)| \geq p\right] \leq 2\exp\left(-\frac{(D-2)\left(p-\frac{cT^2}{N}\right)^2}{96T^2}\right).$$

Proof NB1: $\mathrm{adv}(A^U)$ is $2T$-Lipschitz as a fn of U
(i.e. $\mathrm{adv}(A^U)$ can be expressed as the diff. of two alg. that each make T queries to U & using Lemma 28)

↓

if A^U makes T calls to U, then $f(U) := \Pr[A^U = 1]$ is T-Lipschitz in Frob. norm

NB2: Combining Lemma 31 above (that says the avg $\mathrm{adv}(A^U)$ is cT^2/N) & Theorem 10, one gets

$$\Pr_{U \leftarrow \mu_D^N}\left[\mathrm{adv}(A^U) \geq p\right] \leq \exp\left[-\frac{(D-2)\left(p-\frac{cT^2}{N}\right)^2}{96\,T^2}\right]$$

NB3: Similar reasoning yields an (upper) bound on

$$\Pr_{U \leftarrow \mu_D^N}\left[\mathrm{adv}(A^U) \leq -p\right]$$

Thus we get the final bound w/ a factor of 2 ∵ union bound.

□

Story: completes the security proof,
amounts to combining Lemma 3.2 w/
the aforementioned union bound.

Theorem 33. Let $\mathcal{C}$ be any fixed language.
Then, w/ prob 1 over $\mathcal{U} \leftarrow \mathcal{D}$ (§5.1, that then widefines $\mathcal{U}$, i.e. for each n, $\mathcal{U}_n \leftarrow H_{2^n}^{2^n}$)
$\exists$ a family of PRUs relative to $(\mathcal{U}, \mathcal{C})$
with $n(k) = k$.

[Proof. Fix an input length $n \in \mathbb{N}$.
Def^n: Key set $:= \{0,1\}^k = \{0,1\}^n =: [2^n]$
PRU family $:= \{U_k\}_{k \in \{0,1\}^n}$ where
$\mathcal{U}_n = (U_1 \cdots U_{2^n}) \in \mathbb{U}(2^n)^{2^n}$.

(in words, the family consists of the 2^n different Haar-random n-qubit unitaries supplied by $\mathcal{U}_n$)

NB1: This family has an efficient implementation relative to the oracle
— Can simulate an application of U_k to some n-qubit $|\psi\rangle$
using one query to $\mathcal{U}_n$ via
$\mathcal{U}_n |k\rangle|\psi\rangle = (|k\rangle\langle k| \otimes U_k)|k\rangle|\psi\rangle$.

Story: So, it remains to show the computational indistinguishability criterion of Def^n 16.

Setup: Assume, w.l.o.g., that the adversary is a uniform poly-time quantum algorithm $\mathcal{A}^{O,\mathcal{U},\mathcal{C}}(1^n, x)$ where $x \in \{0,1\}^{poly(n)}$ is the advice & $O \in \mathbb{U}(2^n)$ is the oracle that the adversary seeks to distinguish as pseudorandom or Haar-random.

NB1: By Lemma 32 with $N = D = 2^n$ & $T = poly(n)$, for any fixed $x \in \{0,1\}^{poly(n)}$,

$\mathcal{A}^{O,\mathcal{U},\mathcal{C}}(1^n, x)$ achieves non-negligible adv w.l. "extremely low prob." over $\mathcal{U}$

(The addition of oracle $\mathcal{C}$ has no effect on the query complexity result $\because \mathcal{C}$ is fixed & independent of $\mathcal{U}$.)

More precisely, we have that for any $p = \frac{1}{poly(n)}$,

$$\Pr_{\mathcal{U}_n \leftarrow \mathbb{M}_{2^n}}\left[\left|\Pr_{k \leftarrow [2^n]}\left[\mathcal{A}^{U_k,\mathcal{U},\mathcal{C}}(1^n, x) = 1\right] - \Pr_{O \leftarrow \mathbb{M}_{2^n}}\left[\mathcal{A}^{O,\mathcal{U},\mathcal{C}}(1^n, x) = 1\right]\right| \geq p\right] \leq \exp\left(\frac{-2^n}{poly(n)}\right).$$

NB2: By a union bound over all $x \in \{0,1\}^{poly(n)}$,

$\mathcal{A}^{O,\mathcal{U},\mathcal{C}}(1^n, x)$ achieves advantage larger than p (for any $x \in \{0,1\}^{poly(n)}$) w.p. at most $2^{poly(n)} \cdot \exp\left(\frac{-2^n}{poly(n)}\right) \leq negl(n)$.

NB3: Hence, by the Borel-Cantelli Lemma (Lemma 6),
A achieves negligible advantage for all
but finitely many input lengths $n \in \mathbb{N}$
w.p. 1 over $\mathcal{U}$
(since $\sum_n \text{negl}(n) < \infty$).

X_i: distinguishes correctly

Conclusion: $\{U_k\}_{k \in \{0,1\}^*}$ defines a PRU ensemble.