6.S895: Quantum Cryptography

Lecture: Pseudo-random Quantum States

Lecturer: Alex Poremba **Scribe:** Vinod Vaikuntanathan

1 Motivation

Why are "random quantum states" interesting?

- *Entanglement theory:* it is not hard to show that a random bipartite quantum state is highly entangled.
- *Chaotic quantum systems:* Time evolution of a chaotic quantum system mixes pretty quickly. An example is the time evolution in black holes.
- *Cryptographic applications:* What is the minimal assumption in quantum cryptography? In classical cryptography, one-way functions are minimal. PRS are interesting because the existence of PRS is weaker than the existence of one-way functions (and even $\mathcal{P} \neq \mathcal{NP}$.) This follows from a result of Kretschmer who showed that PRS can exist relative to an oracle w.r.t which $\mathcal{P} = \mathcal{NP}$.

2 Haar-Random Quantum States

How should one define a "random quantum state"? Let's compare classical randomness with quantum randomness. We have:

- The uniform distribution on n-bit strings; the quantum analog is the Haar measure.
- t-wise independence; the quantum analog is t-designs.
- Pseudorandom generator; the quantum analog is a PRS, and pseudorandom functions; the quantum analog of PRU.

Let's look at an example: compare a random bit and a random qubit. In the classical case, the sample space is $\Omega = \{0, 1\}$,

$$\mathbb{E}_{b \sim \{0,1\}}[b] = \frac{1}{2} \cdot 0 + \frac{1}{2} \cdot 1 = \frac{1}{2}$$

whereas in the quantum state, it is a random unit vector, so $\Omega = S(2)$. It turns out that

$$\mathbb{E}_{|\psi\rangle \sim S(d)}[|\psi\rangle \langle\psi|] = I/2 = \frac{1}{2} |0\rangle \langle 0| + |1\rangle \langle 1|$$

Let

- $S(d)$: set of $|\psi\rangle \in \mathbb{C}^d$ such that $\langle\psi|\psi\rangle = 1$.
- $U(d)$: set of all unitary matrices over $\mathbb{C}^d$.

Definition 1 (Haar Measure). *The Haar measure μ_H is the unique left/right invariant measure over the unitary group $U(d)$: for every "nice" f and every $V \in U(d)$,*

$$\mathbb{E}_{U\sim U(d)}[f(U)] = \mathbb{E}_{U\sim U(d)}[f(U\cdot V)] = \mathbb{E}_{U\sim U(d)}[f(V\cdot U)]$$

where

$$\mathbb{E}_{U\sim U(d)}[f(U)] = \int_{U(d)} f(U)\, d_{\mu_H}U$$

The definition of μ_H also extends to states in the following way:

$$\mathbb{E}_{|\psi\rangle\sim S(d)}[f(|\psi\rangle\langle\psi|)] \stackrel{def}{=} \mathbb{E}_{U\sim U(d)}[f(U|0\rangle\langle 0|U^\dagger)]$$

Definition 2 (State t-design). *An ensemble $\nu = \{p_i, |\psi_i\rangle\}$ over d-dimensional states is a state t-design if*

$$\mathbb{E}_{|\psi\rangle\sim\nu}[(|\psi\rangle\langle\psi|)^{\otimes t}] = \mathbb{E}_{|\psi\rangle\sim S(d)}[|\psi\rangle\langle\psi|^{\otimes t}]$$

Symmetric Subspace. Let

$$\mathsf{Sym}_t(\mathbb{C}^d) = \{|\psi\rangle \in (\mathbb{C}^d)^{\otimes t} \;:\; P_d(\sigma)|\psi\rangle = |\psi\rangle \text{ for all } \sigma \in S_t\}$$

where $P_d(\pi)$ is the permutation matrix corresponding to π. The projector onto $\mathsf{Sym}_t(\mathbb{C}^d)$ is

$$\Pi^{d,t}_{sym} = \frac{1}{t!}\sum_{\sigma\in S_t} P_d(\sigma)$$

(This needs proof!)

Theorem 3.

$$\mathbb{E}_{|\psi\rangle\sim S(d)}[|\psi\rangle\langle\psi|^{\otimes t}] = \frac{\Pi^{d,t}_{sym}}{\mathsf{Tr}(\Pi^{d,t}_{sym})}$$

where $\mathsf{Tr}(\Pi^{d,t}_{sym}) = \mathsf{dim}(Sym_t(\mathbb{C}^d)) = \binom{(t+d-1)}{t}$

Proof. See Harrow for proof. □

Definition 4 (Pseudorandom Quantum State). *Let $d = 2^n$. A family of states $\{|\phi_k\rangle \in S(d)\}_{k\in K}$ is pseudorandom if*

- *There is a QPT algorithm F such that*
$$G(k, |0\rangle) = |\phi_k\rangle$$
- *For every $t = \mathsf{poly}(n)$,*
$$\mathbb{E}_{k\sim K}[|\phi_k\rangle\langle\phi_k|^{\otimes t}] \approx_c \mathbb{E}_{|\psi\rangle\sim S(d)}[|\phi_k\rangle\langle\phi_k|^{\otimes t}]$$

  More formally, for every QPT A and every $t = \mathsf{poly}(n)$:

$$\left|\Pr_{k\leftarrow K}[A(|\phi_k\rangle\langle\phi_k|^{\otimes t})] - \Pr_{|\phi\rangle\sim S(d)}[A(|\phi\rangle\langle\phi|^{\otimes t})]\right| = \text{negl}(n)$$

Construction of a PRS.

Theorem 5. *One-way functions imply PRS.*

We will use post-quantum secure pseudorandom functions as a building block. The construction is a binary phase state. Pick any PRF F_k.

$$|\psi_k\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{x \in \{0,1\}^n} (-1)^{F_k(x)} |x\rangle$$

First, to construct this state, start with

$$H^{\otimes n} |0\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{x \in \{0,1\}^n} |x\rangle$$

compute the PRF in superposition to get

$$\frac{1}{\sqrt{2^n}} \cdot \sum_{x \in \{0,1\}^n} |x\rangle |F_k(x)\rangle$$

Phase kick-back: compute a Z map on the second register to get

$$\frac{1}{\sqrt{2^n}} \cdot \sum_{x \in \{0,1\}^n} (-1)^{F_k(x)} |x\rangle |F_k(x)\rangle$$

and uncompute F_k to get the PRS state

$$\frac{1}{\sqrt{2^n}} \cdot \sum_{x \in \{0,1\}^n} (-1)^{F_k(x)} |x\rangle$$

We now prove security. There are three hybrid expressions.

- **Hybrid** 1. This is
  $$\mathbb{E}_{k \sim K}[|\phi_k\rangle \langle \phi_k|^{\otimes t}]$$
  where F_k is the PRF.
- **Hybrid** 2. This is
  $$\mathbb{E}_{f \sim F}[|\phi_f\rangle \langle \phi_f|^{\otimes t}]$$
  where f is a uniformly random function from $\{0,1\}^n$ to $\{0,1\}$ and
  $$|\phi_f\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$$
- **Hybrid** 3. This is
  $$\mathbb{E}_{|\psi\rangle \sim S(d)}[|\phi\rangle \langle \phi|^{\otimes t}]$$

Hybrids 1 and 2 are computationally indistinguishable because of the post-quantum security of the PRF (where the adversary can make quantum superposition queries.) Let's write

$$\begin{aligned}\mathbb{E}_{f\sim F}[|\phi_f\rangle\langle\phi_f|^{\otimes t}] &= d^{-t}\cdot \sum_{x_1,\ldots,x_t,y_1,\ldots,y_t} \mathbb{E}_{f\sim F}[(-1)^{f(x_1)+\ldots+f(x_t)+f(y_1)+\ldots+f(y_t)}]\,|x_1,\ldots,x_t\rangle\langle y_1,\ldots,y_t| \\ &\approx_{t/\sqrt{2^n}} d^{-t}\cdot \sum_{\text{distinct } x_1,\ldots,x_t,\text{distinct } y_1,\ldots,y_t} \mathbb{E}_{f\sim F}[(-1)^{f(x_1)+\ldots+f(x_t)+f(y_1)+\ldots+f(y_t)}]\,|x_1,\ldots,x_t\rangle\langle y_1,\ldots,y_t|\end{aligned}$$

where the second inequality is by the gentle measurement lemma given below.

Now, the expectation is 0 whenever $x_1,\ldots,x_t$ is *not* a permutation of $y_1,\ldots,y_t$ and 1 otherwise. Then, this expectation is exactly

$$\frac{\Pi_{sym}^{d,t}}{\mathsf{Tr}(\Pi_{sym}^{d,t})}$$

which is precisely Hybrid 3. Done!

Lemma 6 (Gentle Measurement Lemma)**.** *Let ρ be a state and Π be a projector such that*

$$\mathsf{Tr}(\Pi\rho) \geq 1-\varepsilon$$

for $\varepsilon \geq 0$. Then,

$$\mathsf{TD}\left(\rho, \frac{\Pi\rho\Pi}{\mathsf{Tr}(\Pi\rho)}\right) \leq \sqrt{\varepsilon}$$