Frontiers of Quantum Complexity and Cryptography Spring 2022

Lecture 4 - Haar-random states and the symmetric subspace

Lecturer: Henry Yuen *Scribes: Yulong Li*

1 Overview

In the first half of Lecture 4, we introduce symmetric subspace, which ties to a pure state tomography algorithm that will be finished up in the second half of Lecture 4. Before rigorously defining symmetric subspace, we will first see several motivating scenarios considering random state in a box.

2 Random State in a Box

2.1 Scenario 1: a random state with classical randomness

Consider the following procedure:

1. Saple a random string $x \in \{0,1\}^n$
2. Prepare n qubits in the state $|x_1, x_2, \ldots, x_n\rangle$
3. Put the n qubits in a box.

If you were handed this box, but weren't allowed to open it to "take a look" at the state (i.e. measure it), how would you describe your belief about the state of the box? It wouldn't be a pure state, because the state is a probabilistic mixture. You would have to use the density matrix formalism.

Let ρ describes the density matrix of the state in the box. It is the sum of the pure density matrix $|x\rangle\langle x|$, over all $x \in \{0,1\}^n$, weighted by the probability 2^{-n}.

$$\rho = \sum_{x \in \{0,1\}^n} 2^{-n} |x\rangle\langle x| = 2^{-n} I$$

This last equality follows because $\sum_{x \in \{0,1\}^n} |x\rangle\langle x|$ is equal to the $2^n \times 2^n$ identity matrix.

The identity (up to scaling) is known as the *maximally mixed state*, because it is, in a sense, maximally random.

2.2 Scenario 2: a random state with quantum randomness

Let's now consider the following procedure:

1. Sample a classical description of a Haar random vector "$|\psi\rangle$" of dimension $d = 2^n$ (e.g. by sampling complex Gaussians are described in the previous lecture).

2. Prepare n qubits in the state $|\psi\rangle$.

3. Put the state in a box.

Note that this procedure is not something that can be carried out efficiently: this is because sampling a Haar random vector takes time 2^n, which is huge for non-small n. As discussed last time in lecture, constructing a Haar-random n-qubit state requires exponentially large quantum circuits, so that also takes a large amount of resources. However now are not concerned with efficiency; we are interested in the question of how we mathematically describe the state of the box (before we open it).

Let σ describes the density matrix of the state in the box. What is more subtle now is that we are sampling $|\psi\rangle$ from a continuous distribution, so it's not obvious how to describe it as a convex combination of a finite number of pure states. We can instead describe σ as an *integral* over $S(\mathbb{C}^d)$ (which recall denotes the set of unit vectors in $\mathbb{C}^d$):

$$\sigma = \int |\psi\rangle\langle\psi| \, \mathrm{d}\psi$$

where $\mathrm{d}\psi$ denotes Haar measure on $S(\mathbb{C}^d)$.

If you're worried about what it means to take an integral over density matrices, one can think of σ as the limit of density matrices

$$\sigma_\epsilon = \frac{1}{|N_\epsilon|} \sum_{|\psi\rangle \in N_\epsilon} |\psi\rangle\langle\psi|$$

where N_ϵ denotes a finite discretization of the sphere $S(\mathbb{C}^d)$ (e.g. every point on $S(\mathbb{C}^d)$ is within ϵ of a point in N_ϵ, and "covered" by the same number of points in N_ϵ).

Interestingly, $\sigma = \rho$ (the density matrix from Scenario 1) and we shall see this by the definition of Haar measure.

Claim 1.

$$\sigma = \int |\psi\rangle\langle\psi| \, \mathrm{d}\psi = 2^{-n} I$$

Proof. First we show that σ is unitarily invariant, i.e. for all unitaries U, $U\sigma U^\dagger = \sigma$.

$$U\sigma U^\dagger = \int U|\psi\rangle\langle\psi|U^\dagger \, \mathrm{d}\psi = \int |\psi\rangle\langle\psi| \, \mathrm{d}\psi = \sigma$$

where in the second to last equality we use the definition of a Haar random state, specifically that $|\psi\rangle \sim Haar(d) \implies U|\psi\rangle \sim Haar(d)$. Thus for all unitaries U, $U\sigma = \sigma U$. For all $A \in \mathbb{C}^{d\times d}$, A can be written as a linear combination of unitary matrices (refer to this link), $A\sigma = \sigma A$. It is left as a question in Problem Set 2 to show that σ is thus a multiple of the identity matrix I. Since $\mathrm{Tr}(\sigma) = 1$, we have $\sigma = 2^{-n} I$. $\square$

According to this calculation, a Haar-random state does not differ from a random classical bitstring. We will see that the difference between Haar-random quantum states and random classical states only become apparent when you consider more complicated scenarios.

2.3 Scenario 3: another random state with classical randomness

Consider the following procedure:

1. Sample a random string $x \in \{0,1\}^n$
2. Prepare $2n$ qubits in the state $|x,x\rangle$
3. Put the $2n$ qubits in a box

Let ρ' denote the density matrix of the state in the box:

$$\rho' = \sum_{x \in \{0,1\}^n} 2^{-n} |x,x\rangle\langle x,x|$$

Note that this is different from the *maximally entangled state* $\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x,x\rangle$, which is a pure state.

Note also this is not the maximally mixed state on $2n$ qubits (i.e. dimension $2^{2n} \times 2^{2n}$); that would be written as

$$2^{-2n} \sum_{x,y \in \{0,1\}^n} |x,y\rangle\langle x,y| \ .$$

Further, there are no non-zero off-diagonal entries in ρ' (if we write the entries of ρ' in the standard basis) meaning that it represents a *classical mixture* of states.

2.4 Scenario 4: another random state with quantum randomness

Consider the following procedure:

1. Sample a classical description of a Haar random vector "$|\psi\rangle$" of dimension $d = 2^n$ (e.g. by sampling complex Gaussians are described in the previous lecture).
2. Prepare $2n$ qubits in the state $|\psi\rangle \otimes |\psi\rangle$.
3. Put the state in a box.

Let σ' describes the density matrix of the state in the box. Again, we can describe σ' with a integral over $S(\mathbb{C}^d)$:

$$\sigma' = \int |\psi\rangle\langle\psi|^{\otimes 2} \, \mathrm{d}\psi \ .$$

This is a $2n$-qubit density matrix (i.e. it has dimension $d^2 \times d^2$). What are the properties of this matrix? What are its entries? To determine σ', we now need to discuss the *symmetric subspace*.

3 The Symmetric Subspace

Definition 2. *For positive integers d, k, define the symmetric subspace, denoted as* $\mathrm{Sym}(d,k)$

$$\mathrm{Sym}(d,k) = \mathrm{span}\left\{ |\psi\rangle^{\otimes k} \mid |\psi\rangle \in \mathbb{C}^d \right\} \subseteq (\mathbb{C}^d)^{\otimes k}$$

Let $P^{\mathrm{sym}}_{d,k}$ be the projector onto $\mathrm{Sym}(d,k)$.

We shall first show that $\mathrm{Sym}(d,k)$ is in fact a proper subspace of $(\mathbb{C}^d)^{\otimes k}$ with the following claim.

Claim 3. $P^{\mathrm{sym}}_{d,k} \neq I$

Proof. It suffices to show one counter-example: $|0,1\rangle - |1,0\rangle \notin \mathrm{Sym}(d,2)$. To see this is true, consider any $|\psi\rangle \in \mathbb{C}^d$, we have

$$\langle \psi, \psi| \big(|0,1\rangle - |1,0\rangle\big) = \langle \psi|0\rangle \ \langle \psi|1\rangle \ - \langle \psi|1\rangle \ \langle \psi|0\rangle \ = 0$$

. Now consider a vector $|\theta\rangle \in \mathrm{Sym}(d,2)$; by definition this is a linear combination of states of the form

$$|\theta\rangle = \sum_i \alpha_i |\psi_i\rangle \otimes |\psi_i\rangle$$

where $\alpha_i \in \mathbb{C}$ and $|\psi_i\rangle \in \mathbb{C}^d$. Then we have

$$\langle \theta| \ \big(|0,1\rangle - |1,0\rangle\big) = \sum_i \alpha_i (\langle \psi_i| \otimes \langle \psi_i|)\,(|0,1\rangle - |1,0\rangle) = 0 \ .$$

This shows that $|0,1\rangle - |1,0\rangle$ is orthogonal to $\mathrm{Sym}(d,2)$. □

Another relatively straightforward claim is as follows.

Claim 4. $\sigma' = \int |\psi\rangle\langle\psi|^{\otimes 2}\,\mathrm{d}\psi$ *is supported on* $\mathrm{Sym}(d,2)$.

Proof.

$$P^{\mathrm{sym}}_{d,2}\sigma' = \int P^{\mathrm{sym}}_{d,2} |\psi\rangle\langle\psi|^{\otimes 2}\,\mathrm{d}\psi = \int |\psi\rangle\langle\psi|^{\otimes 2}\,\mathrm{d}\psi = \sigma'$$

□

In fact, σ' is a multiple of $P^{\mathrm{sym}}_{d,2}$. The following claim requires representation theory that will not be covered in this class, so it is stated without a proof.

Theorem 5.

$$\sigma' = \frac{P^{\mathrm{sym}}_{d,2}}{\mathrm{Tr}(P^{\mathrm{sym}}_{d,2})} \ .$$

Nevertheless, we will be able to specify $\mathrm{Tr}(P^{\mathrm{sym}}_{d,2})$ by specifying a set of orthogonal basis of $\mathrm{Sym}(d,k)$. Before doing so, we shall give an equivalent definition of $\mathrm{Sym}(d,k)$.

Definition 6. *For a permutation $\pi \in S_k$, define the unitary R_π acting on $(\mathbb{C}^d)^{\otimes k}$ such that $R_\pi|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle = |\psi_{\pi(1)}\rangle \otimes \cdots \otimes |\psi_{\pi(k)}\rangle$ where $|\psi_i\rangle \in \mathbb{C}^d$ for $i \in [k]$. Define*

$$\mathrm{Sym}(d,k)' = \{v \in (\mathbb{C}^d)^{\otimes k} \mid R_\pi\, v = v \ \forall \ \pi \in S_k\}$$

In other words, $\mathrm{Sym}(d,k)'$ is the set of all vectors (not necessarily unit length) on k registers, each register of dimension d, such that permuting the k registers leaves the vector invariant.

We verify that $\mathrm{Sym}(d,k)'$ forms a subspace: if $v, w \in \mathrm{Sym}(d,k)'$, then for all permutations $\pi \in S_k$

$$R_\pi(v + w) = R_\pi v + R_\pi w = v + w \ .$$

Therefore $v + w \in \mathrm{Sym}(d,k)'$.

Claim 7. $\mathrm{Sym}(d,k)' = \mathrm{Sym}(d,k)$

Proof. The direction $\mathrm{Sym}(d,k) \subseteq \mathrm{Sym}(d,k)'$ follows directly through definitions. The other direction is more involved. Interested readers can refer to [Har13]. □

With this equivalent definition, we can give a characterization of the projector $P^{\mathrm{sym}}_{d,k}$.

Claim 8. $P^{\mathrm{sym}}_{d,k} = \frac{1}{k!}\sum_{\pi \in S_k} R_\pi$

Proof. Let $\Pi = \frac{1}{k!}\sum_{\pi \in S_k} R_\pi$. Using the definition of R_π, one can directly verify that Π is Hermitian and $\Pi^2 = I$, and thus Π is a projector. For every $\pi \in S_k$, one can verify that $R_\pi \Pi = \Pi$, which implies $Im(\Pi) \subseteq \mathrm{Sym}(d,k)$. Finally, for every $|\theta\rangle \in \mathrm{Sym}(d,k)$, it is evident that $\Pi|\theta\rangle = |\theta\rangle$, which implies that $\mathrm{Sym}(d,k) \subseteq Im(\Pi)$, and thus $\mathrm{Sym}(d,k) = Im(\Pi)$. □

3.1 Examples and nonexamples of states in the symmetric subspace

The following states are examples of states in the symmetric subspace:

1. $|0,0\rangle \in \mathrm{Sym}(2,2)$
2. $\frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) \in \mathrm{Sym}(2,2)$
3. $\frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) \in \mathrm{Sym}(2,2)$
4. $\frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) \in \mathrm{Sym}(2,2)$

States that are *not* in the symmetric subspace:

1. $|0,1\rangle \notin \mathrm{Sym}(2,2)$
2. $\frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) \notin \mathrm{Sym}(2,2)$.

This second state is in what's called the *anti-symmetric subspace*, because if you swap the two registers (i.e. apply R_π for $\pi = (12)$), then you obtain a minus sign:

$$R_\pi \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) = -\frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) \ .$$

3.2 Orthogonal basis for $\mathrm{Sym}(d, k)$

Definition 9. *(Symmetrization) Fix orthogonal basis $|1\rangle, |2\rangle, \ldots, |d\rangle$ for $\mathbb{C}^d$. Consider a d-tuple $t = (t_1, \cdots, t_d) \in \mathbb{N}^d$ such that $\sum_{j=1}^d t_j = k$, and the state $|\psi\rangle = |1\rangle^{\otimes t_1}|2\rangle^{\otimes t_2} \cdots |d\rangle^{\otimes t_d}$. We can "symmetrize" $|\psi\rangle$ by the following procedure. Consider the set*

$$S_t = \{(s_1, s_2, \cdots, s_k) \in [d]^k \mid \sum_{i=1}^k \mathbb{1}[s_i = j] = t_j \ \forall\ j \in [d]\}$$

Intuitively, given $t = (t_1, \cdots, t_d)$, t_j specifies the number of copies of $|j\rangle$ in $|\psi\rangle$, and each $(s_1, s_2, \cdots, s_k) \in S_{(t_1,\cdots,t_d)}$ will assign t_j registers out of all k possible registers for $|j\rangle$, i.e. $s_i \in [d]$ specifies that the i-th register is $|s_i\rangle$. Then the symmetrization of $|\psi\rangle$ is

$$\sum_{(s_1,s_2,\cdots,s_k)\in S_t} |s_1\rangle \otimes |s_2\rangle \otimes \cdots \otimes |s_k\rangle$$

Denote $||t_1, \cdots, t_d\rangle\rangle$ as the symmetrization of $|1\rangle^{\otimes t_1}|2\rangle^{\otimes t_2} \cdots |d\rangle^{\otimes t_d}$.

Theorem 10. *$\{||t_1, \cdots, t_d\rangle\rangle \mid (t_1, \cdots, t_d) \in \mathbb{N}^d, \sum_{j=1}^d t_j = k\}$ forms an orthogonal basis for $\mathrm{Sym}(d, k)$.*

Proof. It's straighforward to verify that the elements in the set are in $\mathrm{Sym}(d, k)$. By noting that two elements $||t_1, \cdots, t_d\rangle\rangle$ and $||t'_1, \cdots, t'_d\rangle\rangle$ must differ at some j such that $t_j \neq t'_j$, it follows that the elements pairwise orthogonal.

To show that the set spans $\mathrm{Sym}(d, k)$, consider any k-tuple $a = (a_1, a_2, \cdots, a_k) \in [d]^k$ and the state $|\psi_a\rangle = |a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_k\rangle$. We have that $\{|\psi_a\rangle \mid a = (a_1, a_2, \cdots, a_k) \in [d]^k\}$ spans $(\mathbb{C}^d)^{\otimes k}$. It requires a bit reasoning to verify that

$$P^{\mathrm{sym}}_{d,k}|\psi_a\rangle = \frac{1}{k!}\sum_{\pi\in S_k} R_\pi|\psi_a\rangle = C||t_1, \cdots, t_d\rangle\rangle$$

where $t_j = \sum_{i=1}^n \mathbb{1}[a_i = j]$ and C is a normalization factor. This observation completes the proof. $\square$

Example 11. *Consider $d = 2, k = 3$ and the basis states $|1\rangle, |2\rangle$. The following states form a orthogonal (not normalized) basis for Sym$(2, 3)$.*

$$\begin{aligned}
||3,0\rangle\rangle &= |1\rangle \otimes |1\rangle \otimes |1\rangle \\
||2,1\rangle\rangle &= |1\rangle \otimes |1\rangle \otimes |2\rangle + |2\rangle \otimes |1\rangle \otimes |1\rangle + |1\rangle \otimes |2\rangle \otimes |1\rangle \\
||1,2\rangle\rangle &= |1\rangle \otimes |2\rangle \otimes |2\rangle + |2\rangle \otimes |1\rangle \otimes |2\rangle + |2\rangle \otimes |2\rangle \otimes |1\rangle \\
||0,3\rangle\rangle &= |0\rangle \otimes |0\rangle \otimes |0\rangle
\end{aligned}$$

With a combinatorics argument considering the number of ways to put k indistinguishable balls into d distinguishable boxes, one can arrive at the following corollary.

Corollary 12. $\dim(\mathrm{Sym}(d, k)) = \binom{k+d-1}{k}$

Finally, we can answer the initial question about σ'.

Corollary 13.

$$\int |\psi\rangle\langle\psi|^{\otimes 2}\,\mathrm{d}\psi = \binom{k+d-1}{k}^{-1} P^{\mathrm{sym}}_{d,k} = \frac{1}{(k+1)(k+2)\cdots(k+d-1)} \sum_{\pi\in S_k} R_\pi$$

A proof of this can be found in [Wat18].

References

[Har13] Aram W Harrow. The church of the symmetric subspace. *arXiv preprint arXiv:1308.6595*, 2013.

[Wat18] John Watrous. *The theory of quantum information.* Cambridge university press, 2018.