COMS 6998 - Frontiers of Quantum Complexity & Crypto Spring 2022

Lecture 2: State Tomography

Lecturer: Henry Yuen *Scribes: Sandip Nair*

1 State Tomography

Quantum State Tomography refers to the following task: given k copies of a quantum state ρ (denoted by $\rho^{\otimes k}$) and a precision parameter ϵ, output a *classical description* of a quantum state ρ' such that

$$D(\rho, \rho') \leq \epsilon$$

where $D(\cdot, \cdot)$ denotes the trace distance between two quantum states.

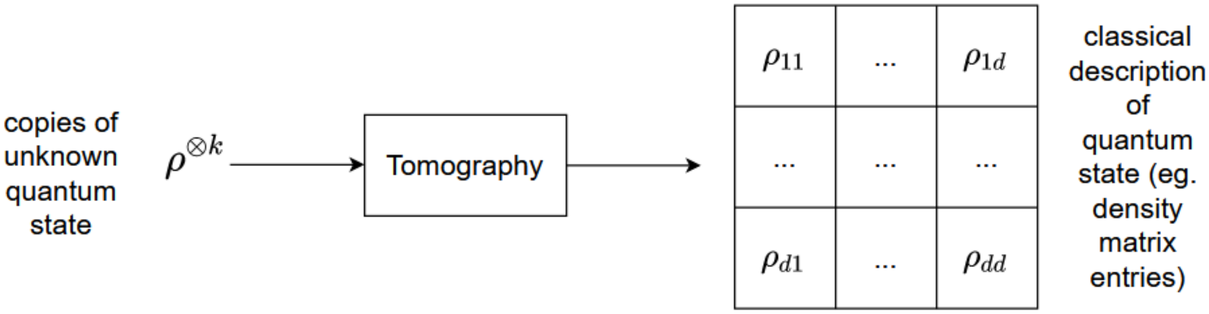
copies of unknown quantum state
$\rho^{\otimes k}$
Tomography
ρ_{11}
...
ρ_{1d}
...
...
...
ρ_{d1}
...
ρ_{dd}
classical description of quantum state (eg. density matrix entries)

Figure 1: Quantum State Tomography

This problem naturally gives rise to the following questions:

1. Is state tomography possible with *any* number of copies of the quantum state?
2. What is the minimum number of copies necessary?
3. When can the process of Tomography be made efficient?

1.1 Difficulty of state tomography

In this lecture we explore the difficulty of state tomography, and show a *lower bound* on the number of copies needed to accomplish the tomography task. To start off with, one would naturally ask about whether state tomography is possible using a single copy of a quantum state; this would be the most desirable and resource-efficient method if possible! However, intuition says that this should not be possible because quantum states are extremely fragile: measuring the given copy of a quantum state would cause it to collapse, irrevocably losing all information about the original state.

We now argue that one copy is far from sufficient for tomography. In fact, one needs a number of copies that scales with the dimension of the state, or equivalently one needs a number of copies that grows *exponentially* in the number of qubits of the state.

Theorem 1. *Any tomography algorithm for d-dimensional states that succeeds with error $\epsilon = \frac{1}{4}$ requires at least $\Omega(d/\log d)$ copies of the unknown input state.*

The argument proceeds by showing that, if there was a too-good-to-be-true tomography procedure (i.e. one that uses too few copies of a state), then one can obtain a too-good-to-be-true information compression method, violating known results in quantum information theory.

More formally: let $d = 2^n$ and suppose there exists a tomography procedure that on input k copies of an n-qubit quantum state $|\psi\rangle^{\otimes k}$ outputs a classical description of a state vector $|\theta\rangle$ such that

$$\| \, |\psi\rangle - |\theta\rangle \, \| \leq \epsilon$$

where $\epsilon = \frac{1}{4}$. This would imply a *quantum communication protocol* for a person Alice to convey a classical message to another person Bob using a "quantum codebook", which we will describe below.

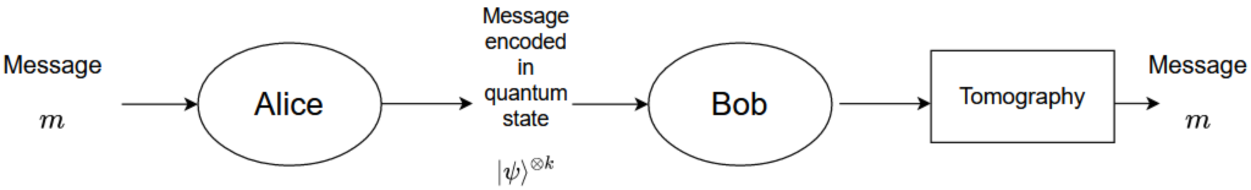

Figure 2: Hypothetical Quantum Communication Protocol using Tomography

1.1.1 Protocol description

Before the protocol begins, Alice and Bob agree on an encoding scheme (also known as a *quantum codebook*):

$$m \in \{0,1\}^r \Longleftrightarrow |\psi_m\rangle \in \mathbb{C}^d$$

on n-qubits. This encoding scheme should satisfy the following *distance property*: for all $m \neq m'$, we have that

$$\| \, |\psi_m\rangle - |\psi_{m'}\rangle \, \| \geq 2\epsilon \ .$$

We will indicate what r is shortly. But supposing that there is such a quantum codebook, Alice can convey r bits of classical information to Bob by sending kn quantum bits as follows:

1. When Alice wants to convey a classical message m to Bob, she encodes the message using the predetermined encoding scheme and then sends k copies of the n-qubit state $|\psi_m\rangle$ (so Bob receives kn qubits in total.)

2. Bob performs tomography on these kn qubits to obtain a classical description of a state $|\theta\rangle$ such that

$$|| \ |\theta\rangle - |\psi_m\rangle \ || \leq \epsilon$$

3. Referring the "codebook" defined by the decided encoding scheme, Bob outputs

$$m^* = \operatorname*{argmin}_m \| \ |\psi_m\rangle - |\theta\rangle \ \|$$

and outputs m^* as the message from Alice.

Due to the distance property, it must be that Bob can umambiguously recover m from $|\psi_m\rangle^{\otimes k}$, because no other state in the codebook is within ϵ of $|\theta\rangle$.

All that remains is for us to determine how large r can be. This problem can be stated as a *packing problem* as follows:

1.1.2 Packing of quantum states

What is the largest number of quantum states that we can pack into d-dimensional space such that all states are pairwise at least 2ϵ distance from each other? Consider the space of n-qubit pure states, denoted by $\mathbb{S}\left((\mathbb{C}^2)^{\otimes n}\right)$, which can be thought of as a unit ball in $d = 2^n$-dimensional complex space.

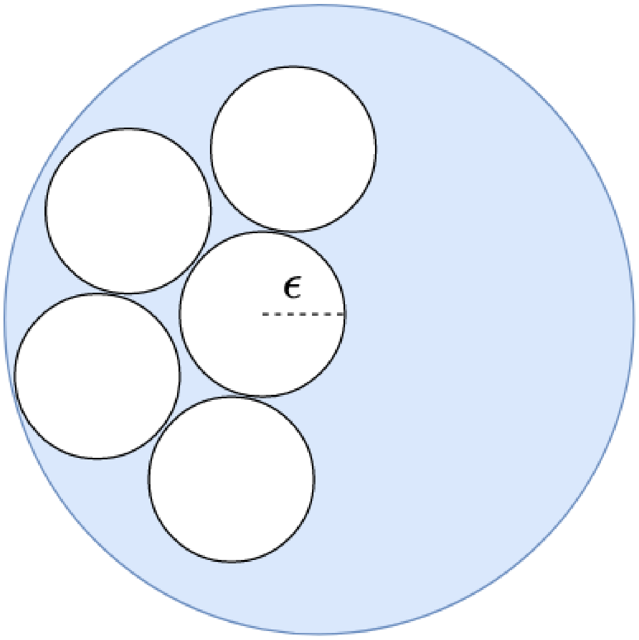

Figure 3: Unit sphere of dimension $d-1$ (since one degree of freedom is lost due to the unit vector constraint)

On this sphere, consider a "disc" of radius ϵ around each point/state such that only one point must exist within such a disc.

First, we give an upper bound on the maximum number of such discs that can be packed on the surface of the sphere. For simplicity, we consider the calculations in real space. The surface area of a sphere of radius R in $d-1$ dimensions is given by

$$S_{d-1}(R) = \frac{2\pi^{\frac{d}{2}}}{\Gamma(\frac{d}{2}-1)} R^{d-1}$$

where $\Gamma(n) = n!$ for integer n. Since the discs are sections of the unit sphere's surface, their surface area is at most the surface area of a sphere with the disc radius ϵ. In other words

$$\text{Surface area of disc of radius } \epsilon \leq S_{d-1}(\epsilon) = \frac{2\pi^{\frac{d}{2}}}{\Gamma\left(\frac{d}{2}-1\right)} \epsilon^{d-1}$$

Thus the number of discs of radius ϵ that can be packed on the surface of the unit sphere is at most

$$\frac{S_{d-1}(1)}{S_{d-1}(\epsilon)} = \frac{1}{\epsilon^{d-1}} \ .$$

It turns out that this upper bound is tight up to a constant in the exponent.

Theorem 2. *There exists at least* $\left(\frac{1}{\epsilon}\right)^{\Omega(d)}$ *states in* $\mathbb{S}(\mathbb{C}^d)$ *that are pairwise* 2ϵ *distance from each other.*

This is a mind-bogglingly huge number; if we fix $\epsilon = \frac{1}{4}$, then this number is going to be on the order of $2^{2^{\Omega(d)}}$, which is *doubly-exponential* in n. You will prove a version of this bound on your problem set.

1.1.3 Conclusion

Given this packing, this means that Alice can convey one of $(1/\epsilon)^{\Omega(d)}$ messages, or equivalently communicate

$$r = \log(1/\epsilon)^{\Omega(d)} = \Omega(d \log \frac{1}{\epsilon}) = \Omega(d)$$

bits of information. Here, we used that ϵ is a constant.

That means that Alice is able to convey $\Omega(d)$ classical bits of information to Bob by sending over kn qubits. However, there is a physical limit placed on this, which is enforced by *Holevo's theorem*:

Theorem 3 (Informal statement of Holevo's theorem)**.** *At most n bits of classical information can be reliably encoded into n qubits.*

Applying Holevo's theorem to our hypothetical quantum communication using tomography, where kn qubits are used to transfer $\Omega(d) = \Omega(2^n)$ bits of classical information, we have

$$kn \geq \Omega(d) \implies k \geq \Omega(d/n) = \Omega(d/\log d) \ .$$

Hence, we see that an exponential number of copies of the encoded quantum state is necessary for the communication, which is very expensive in terms of the physical resources required to realize it.