Lecture 6

Methods in Quantum Computing

Yuval Sanders, 6 September 2021

Measurement and Tomography

Computation is Classical In, Classical Out

Quantum computations are sandwiched by preparation and measurement

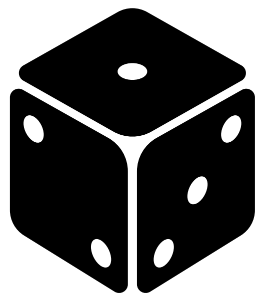
Preparation: classical information —> quantum state
(usually in the form of all-zero state)

Measurement: quantum state —> classical information
(usually in “computational basis”, i.e. zeroes and ones)

Measurement is a bit different from preparation: outcome is **random**.
Preparation can *also* be random, but usually isn’t.

Randomness = Uncertainty

Measuring a non-computational-basis state yields uncertain outcome

Uncertain outcomes are represented by probability distributions. 

Simplest example: Bernoulli trials (a.k.a. coin flips) 

The outcome of the flip depends largely, but not entirely on the physical properties of the coin. The random thing is not the *coin*, but the *flip*.

N flips: H heads, T tails, $H + T = N$.
Define $h = H/N$, $t = T/N$, $h + t = 1$.
In limit as $N \longrightarrow \infty$, a fair coin would have $h = t = 1/2$.
Unfair coin could have other distributions.

Probability Distributions

Sets of numbers assigned to a random process that summarise statistics

Coin tosses: set of outcomes = {heads, tails}.
Probability distribution: Pr(heads) and Pr(tails); Pr(heads) + Pr(tails) = 1
“Expected” number of heads = Pr(heads) × no. tosses

Die rolls: set of outcomes = {1, 2, 3, 4, 5, 6}
Probability distribution: Pr(1), Pr(2), Pr(3), Pr(4), Pr(5), Pr(6); sum = 1
“Expected” number of 6s = Pr(6) × no. throws

Quantum Measurements

Random processes that depends on quantum state and measurement instrument

Recall that we describe quantum measurements using *positive-operator-valued measure* (POVM).
i.e. set of positive operators that add up to identity operator.
The POVM represents the physics of a **measurement**.

The outcome of a measurement depends on both the measurement instrument and the **quantum state** as represented by a density matrix.
POVM $= \{M_1, M_2, \ldots, M_n\}$ & state $= \rho \implies \Pr(k) = \mathrm{Tr}(M_k \rho)$

Example

Measuring single pure qubit in computational basis = Bernoulli trial

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle;\ \rho = |\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix}$$

POVM $= \{|0\rangle\langle 0|, |1\rangle\langle 1|\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

$$\Pr(0) = \mathrm{Tr}(|0\rangle\langle 0|\rho) = \langle 0|\rho|0\rangle = |\alpha|^2;\ \Pr(1) = |\beta|^2$$

Distribution of Bernoulli trial is determined by ρ.

Observation

Cannot perfectly reconstruct state from measurement statistics

$$|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle; \ |-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Both states have $\Pr(0) = \Pr(1) = \frac{1}{2}$, meaning we can distinguish them!

Similarly, cannot distinguish between any of $\frac{1}{\sqrt{2}}|0\rangle + \frac{e^{i\theta}}{\sqrt{2}}|1\rangle$.

The measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ is “missing” information about state.
This measurement is “tomographically incomplete”.

Quantum State Tomography

Given many copies of a state, figure out its density operator

Given: black box with button. Push the button, get fixed ρ.

Goal: figure out ρ.

Procedure:

1. Choose “tomographically complete” measurement.
2. Press button, measure state, and record outcome.
3. Enough measurements recorded? YES: continue, NO: go to 2.
4. Do some statistics to figure out state.

Exercise

Qubit Tomography

POVM: $\left\{ \frac{I+X}{6}, \frac{I-X}{6}, \frac{I+Y}{6}, \frac{I-Y}{6}, \frac{I+Z}{6}, \frac{I-Z}{6} \right\}$

State: $\rho = \begin{bmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{bmatrix}$

Show (1) that each element of the POVM is a positive operator, and (2) that ρ can be reconstructed from the measurement statistics.

Matrix Norms and State Fidelities

How “Close” are Two Quantum States?

And how do we measure “distance”?

Tomographic reconstruction of a state works perfectly
only if we have *infinite* measurement data.

In the real world, we gather a large-but-not-infinite amount of data.
The tomographic reconstruction is *approximate*.
More data yields better approximation.

Estimated state $\hat{\rho}$ is a good approximation to ρ if $\hat{\rho} - \rho$ is nearly zero.

“Closeness” of Two Vectors = “Size” of Difference

In general, we can define a “metric” in terms of a “norm”

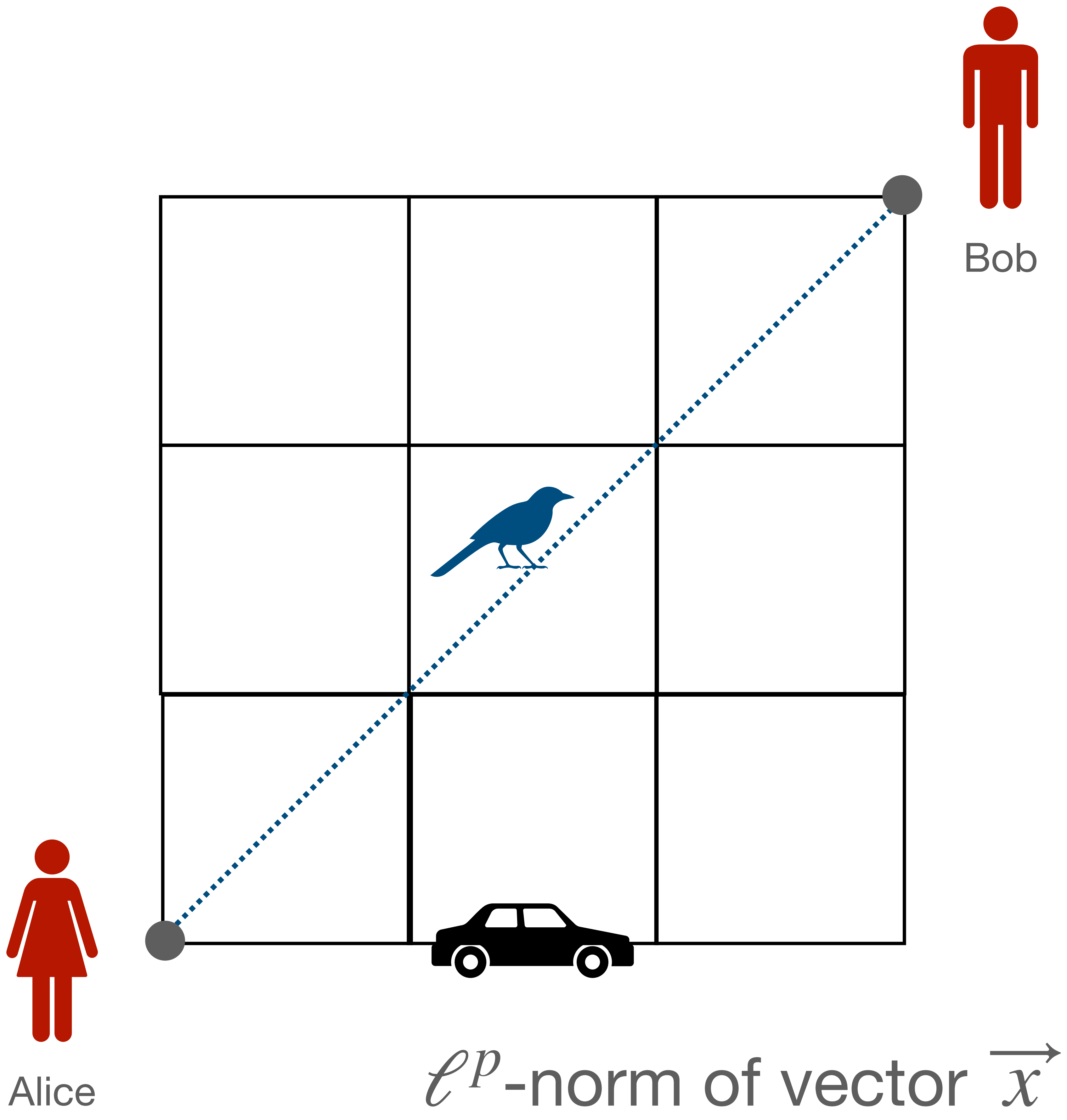
The “size” of a matrix A is written $||A||$ and is a positive real number.
Must also satisfy $||\alpha A|| = |\alpha|||A||$ for any complex number α
as well as the “triangle inequality” $||A + B|| \leq ||A|| + ||B||$.

Any function $||\cdot|| : V \to \mathbb{R}_{\geq 0}$ satisfying the above axioms
is called a “norm” for the (complex) vector space V.

A vector space equipped with a norm is a “normed” vector space.

Example

Euclidean norm vs Manhattan taxicab norm



As the bird flies, Alice and Bob are $3\sqrt{2}$ units apart.
But a taxicab must drive 6 units.
Same vector space, **different norms**.

Alice at (0,0), Bob at (3,3).

Bird's distance: $\sqrt{(3-0)^2+(3-0)^2} = \sqrt{2\times 3^2} = 3\sqrt{2}$

Taxi's distance: $|3-0|+|3-0| = 3+3 = 6$

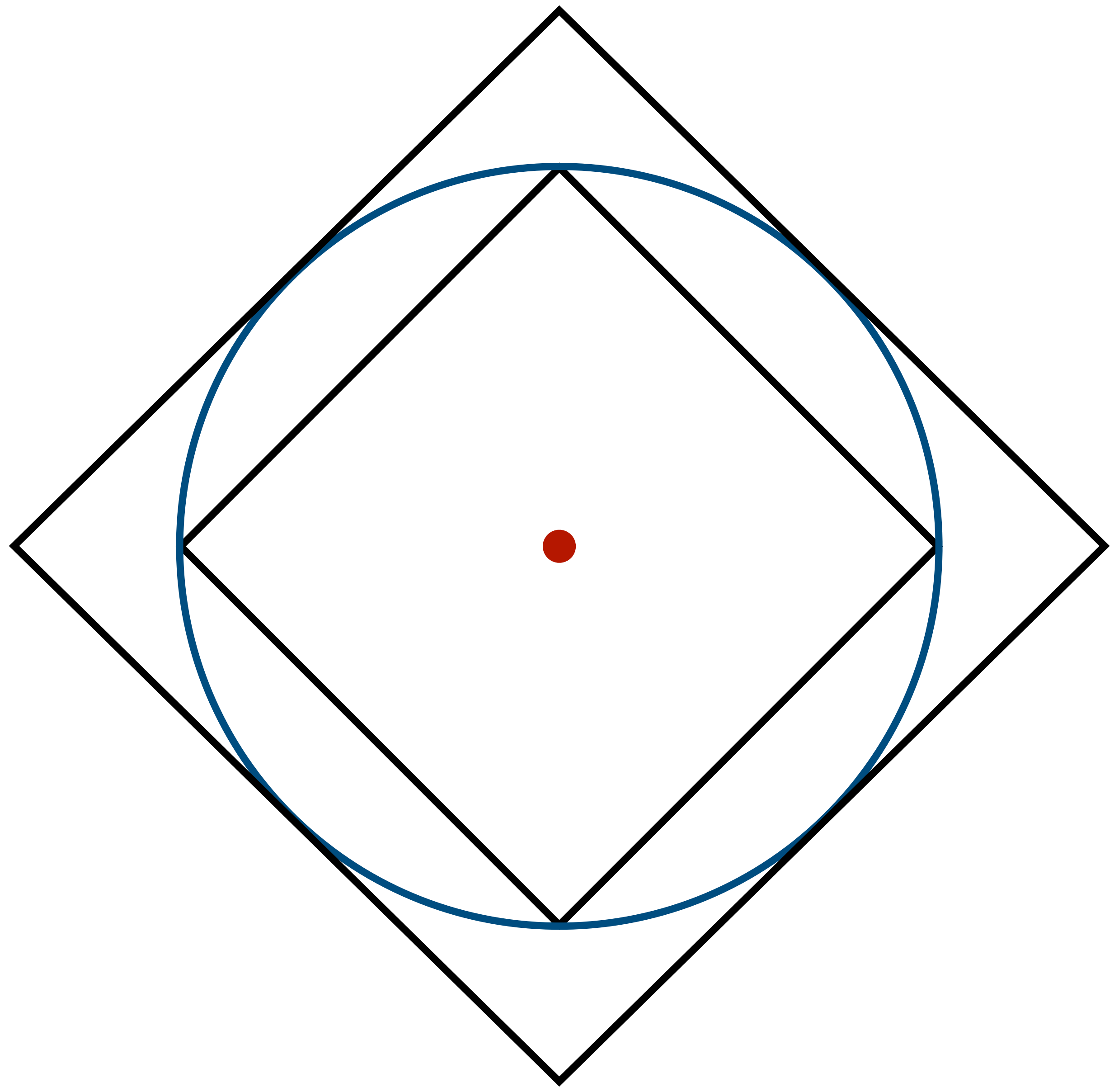
Bird's distance = ℓ^2-norm of difference vector = Euclidean norm
Taxi's distance = ℓ^1-norm of difference vector = Manhattan taxicab norm

ℓ^p-norm of vector $\overrightarrow{x} = (x_1, x_2, \ldots, x_n)$: $\left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p}$

$$\lim_{p\to\infty} \|\overrightarrow{x}\|_p = \max\{x_1, \ldots, x_n\}$$

Equivalence of metrics

Different norms disagree quantitatively but not qualitatively (i.e. topologically)



If the bird would fly one unit between two points
(from centre of circle to its circumference),
the taxi would drive between 1 and $\sqrt{2}$ units
(between smaller and larger diamonds).

Knowing the bird-distance implies *bounds* on the taxi-distance.
The taxi-distance varies around the circle,
so there is no direct conversion between the norms.

But both distances agree about whether two points are close together.
This is why they are “equivalent” metrics:
both normed vector spaces have the same *topology*.

Schatten p-Norms

A convenient set of matrix norms

Idea: calculate p-norm of the eigenvectors of a matrix.

$$\|A\|_p = \|\vec{\lambda}\|_p = \left(\sum_i |\lambda_i|^p\right)^{1/p} = \left(\mathrm{Tr}\begin{bmatrix} |\lambda_1| & 0 & \cdots & 0 \\ 0 & |\lambda_2| & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & |\lambda_n| \end{bmatrix}^p\right)^{1/p} = \left(\mathrm{Tr}\,\Lambda^p\right)^{1/p}$$

By unitary invariance, $\Lambda = \sqrt{A^\dagger A} =: |A|$. [**Exercise:** check this.]

Hence: Schatten p-norm $\|A\|_p$ of any matrix A (not necessarily diagonalisable) is $\left(\mathrm{Tr}\,|A|^p\right)^{1/p}$.

Quantum computing people like the 1-norm because $\|\rho\|_1 = 1$ for density operators.

Trace Distance

Standard distance for quantum states, induced by the Schatten 1-norm

$$\mathrm{dist}(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1$$

This number is between 0 and 1 and extends a standard distance measure on probability distributions, the *total variation distance* (TVD).

Intuitively, TVD calculates how frequently two distributions “disagree” with one another. (Many subtleties being avoided here.)

Trace distance is TVD maximised over all possible measurements.

State Fidelity

Very common figure-of-merit for quantum states

$$F(\rho, \sigma) := \mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$$

If $\rho = \sigma$ we have fidelity = 1, not 0 as with metric.

Sometimes people refer to the “infidelity”: $1 - F(\rho, \sigma)$, which is a metric.

If both states are pure, i.e. $\rho = |\psi\rangle\langle\psi|$, $\sigma = |\phi\rangle\langle\phi|$, we have $F(\rho, \sigma) = |\langle\phi|\psi\rangle|$.

Relationship Between Fidelity and Trace Distance

Fuchs and van de Graaf, arXiv:quant-ph/9712042

$$1 - F(\rho, \sigma) \leq \frac{1}{2}\|\rho - \sigma\|_1 \leq \sqrt{1 - F(\rho, \sigma)^2}$$

That is to say, the trace distance and the infidelity are equivalent metrics on the space of quantum states.

Hence they agree in a *qualitative* sense even when they disagree quantitatively.

Note that two pairs of states can have the same fidelity but different trace distances, and vice-versa. Just as with the Euclidean and taxicab norms.

Distinguishing Quantum States

The Quantum State Discrimination Problem

A foundational quantum information processing task

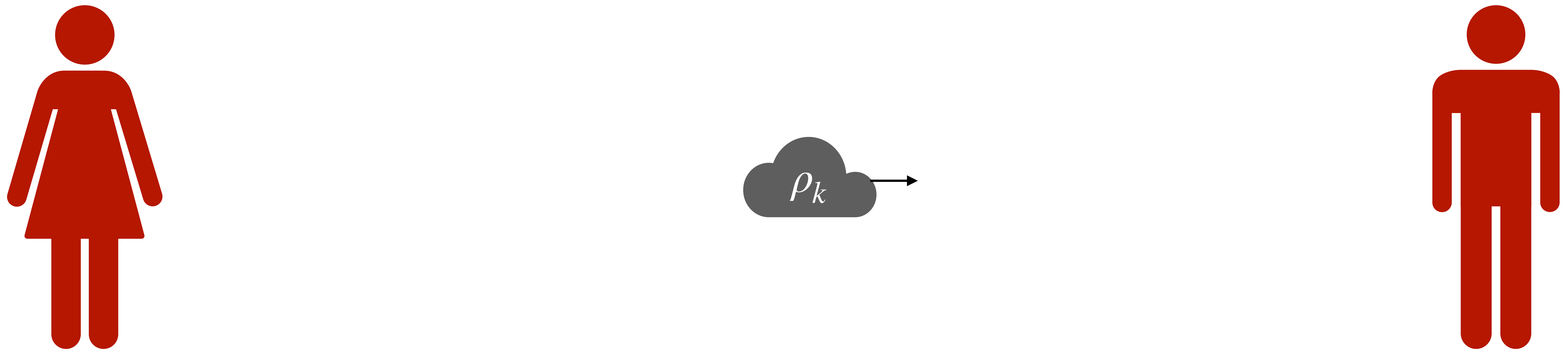
As a way of putting together the concepts we have encountered so far, we now consider the following task. I'll use some language I haven't carefully defined.

Suppose Alice generates a random variable $X = x_1, \ldots, x_n$ according to the probability distribution $\Pr(X = x_k) = p_k$. Bob knows that if she obtains outcome x_k, she will prepare state ρ_k. After preparing the state, Alice sends it to Bob.

Bob's job is to figure out Alice's state label k with maximum success probability.


x_k


ρ_k


ρ_k


$k = ?$
ρ_k

Bob's Strategy

(one possible strategy, anyway)

Bob will select a POVM $\Pi = \{\Pi_1, \ldots, \Pi_n\}$ containing the same number n of elements as Alice's "ensemble" $\{(p_1, \rho_1), \ldots, (p_n, \rho_n)\}$.

If Bob obtains outcome k, he will guess that Alice sent ρ_k and hence Alice obtained $X = x_k$.

Bob's probability of success is $\sum_{i=1}^{n} p_i \operatorname{Tr}(\Pi_i \rho_i)$.

Holevo-Helstrom Theorem

Maximum success probability for $n = 2$ relates to trace distance

Suppose Alice chooses the ensemble $\{(p_1, \rho_1), (p_2, \rho_2)\}$ and
Bob tries to determine if $k = 1{,}2$ using the procedure from the previous slide.

(It turns out to be the best possible procedure.)

Then Bob can correctly determine k with probability $\Gamma = \frac{1}{2} + \frac{1}{2}||p_1\rho_1 - p_2\rho_2||$
and can do no better than this.

In particular, if $p_1 = p_2 = \frac{1}{2}$ and d is the trace distance between ρ_1 and ρ_2,
then Bob's success probability is at best $\frac{1}{2} + \frac{d}{2}$.

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$p_1 \operatorname{Tr} \Pi_1 \rho_1 + p_2 \operatorname{Tr} \Pi_2 \rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\left(\frac{1}{2} + \frac{1}{2}\right) p_1 \operatorname{Tr} \Pi_1 \rho_1 + \left(\frac{1}{2} + \frac{1}{2}\right) p_2 \operatorname{Tr} \Pi_2 \rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2}p_1 \operatorname{Tr} \Pi_1\rho_1 + \frac{1}{2}p_1 \operatorname{Tr} \Pi_1\rho_1 + \frac{1}{2}p_2 \operatorname{Tr} \Pi_2\rho_2 + \frac{1}{2}p_2 \operatorname{Tr} \Pi_2\rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2}p_1 \operatorname{Tr} \Pi_1 \rho_1 + \frac{1}{2}p_1 \operatorname{Tr}(I - \Pi_2)\rho_1 + \frac{1}{2}p_2 \operatorname{Tr} \Pi_2 \rho_2 + \frac{1}{2}p_2 \operatorname{Tr}(I - \Pi_1)\rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2}p_1 \operatorname{Tr} \Pi_1 \rho_1 + \frac{1}{2}p_1 \operatorname{Tr} \rho_1 - \frac{1}{2}p_1 \operatorname{Tr} \Pi_2 \rho_1 + \frac{1}{2}p_2 \operatorname{Tr} \Pi_2 \rho_2 + \frac{1}{2}p_2 \operatorname{Tr} \rho_2 - \frac{1}{2}p_2 \operatorname{Tr} \Pi_1 \rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2}p_1 \operatorname{Tr}\Pi_1\rho_1 + \frac{1}{2}p_1 \underbrace{\operatorname{Tr}\rho_1}_{1} - \frac{1}{2}p_1 \operatorname{Tr}\Pi_2\rho_1 + \frac{1}{2}p_2 \operatorname{Tr}\Pi_2\rho_2 + \frac{1}{2}p_2 \underbrace{\operatorname{Tr}\rho_2}_{1} - \frac{1}{2}p_2 \operatorname{Tr}\Pi_1\rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2}p_1 \operatorname{Tr}\Pi_1\rho_1 + \frac{1}{2}p_1 - \frac{1}{2}p_1 \operatorname{Tr}\Pi_2\rho_1 + \frac{1}{2}p_2 \operatorname{Tr}\Pi_2\rho_2 + \frac{1}{2}p_2 - \frac{1}{2}p_2 \operatorname{Tr}\Pi_1\rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2}\left(p_1 + p_2\right) + \frac{1}{2}p_1 \operatorname{Tr}\Pi_1\rho_1 - \frac{1}{2}p_1 \operatorname{Tr}\Pi_2\rho_1 + \frac{1}{2}p_2 \operatorname{Tr}\Pi_2\rho_2 - \frac{1}{2}p_2 \operatorname{Tr}\Pi_1\rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2}\underbrace{(p_1 + p_2)}_{1} + \frac{1}{2}p_1 \operatorname{Tr} \Pi_1 \rho_1 - \frac{1}{2}p_1 \operatorname{Tr} \Pi_2 \rho_1 + \frac{1}{2}p_2 \operatorname{Tr} \Pi_2 \rho_2 - \frac{1}{2}p_2 \operatorname{Tr} \Pi_1 \rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2} + \frac{1}{2}p_1 \operatorname{Tr} \Pi_1\rho_1 - \frac{1}{2}p_1 \operatorname{Tr} \Pi_2\rho_1 + \frac{1}{2}p_2 \operatorname{Tr} \Pi_2\rho_2 - \frac{1}{2}p_2 \operatorname{Tr} \Pi_1\rho_2$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2} + \frac{1}{2}p_1 \operatorname{Tr} \Pi_1\rho_1 - \frac{1}{2}p_2 \operatorname{Tr} \Pi_1\rho_2 + \frac{1}{2}p_2 \operatorname{Tr} \Pi_2\rho_2 - \frac{1}{2}p_1 \operatorname{Tr} \Pi_2\rho_1$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2} + \frac{1}{2}\operatorname{Tr}\Pi_1(p_1\rho_1) - \frac{1}{2}\operatorname{Tr}\Pi_1(p_2\rho_2) + \frac{1}{2}\operatorname{Tr}\Pi_2(p_2\rho_2) - \frac{1}{2}\operatorname{Tr}\Pi_2(p_1\rho_1)$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2} + \frac{1}{2}\operatorname{Tr}\Pi_1(p_1\rho_1 - p_2\rho_2) + \frac{1}{2}\operatorname{Tr}\Pi_2(p_2\rho_2 - p_1\rho_1)$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2} + \frac{1}{2}\operatorname{Tr}\Pi_1(p_1\rho_1 - p_2\rho_2) - \frac{1}{2}\operatorname{Tr}\Pi_2(p_1\rho_1 - p_2\rho_2)$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2} + \frac{1}{2}\,\mathrm{Tr}(\Pi_1 - \Pi_2)(p_1\rho_1 - p_2\rho_2)$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

$$\frac{1}{2} + \frac{1}{2}\,\mathrm{Tr}(\Pi_1 - \Pi_2)(p_1\rho_1 - p_2\rho_2) \leq \frac{1}{2} + \frac{1}{2}\,\mathrm{Tr}\,|\,p_1\rho_1 - p_2\rho_2\,| \equiv \Gamma$$

Holevo-Helstrom Theorem – Proof

Cannot do better than Γ chance of success

Assume Bob chooses the POVM $\{\Pi_1, \Pi_2\}$.

Remember that $\Pi_1 + \Pi_2 = I$.

Bob's success probability is

Prove this!

$$\frac{1}{2} + \frac{1}{2}\mathrm{Tr}(\Pi_1 - \Pi_2)(p_1\rho_1 - p_2\rho_2) \leq \frac{1}{2} + \frac{1}{2}\mathrm{Tr}\,|\,p_1\rho_1 - p_2\rho_2\,| \equiv \Gamma$$

Kraus Decompositions and Gate Fidelities

From States to Channels

Mixed states generalise pure states, quantum channels generalise unitary operators

A *quantum channel* is a completely positive, trace preserving map.
Function: operators —> operators.
Trace preserving: output has same trace as input.

Positive map: positive operators —> positive operators
Completely positive map: density operator —> density operator
even when acting on a piece of the system instead of the whole system

(Some positive maps will not return density matrix if acting on part of an entangled state.)

Simple Examples of Quantum Channels

You will see these frequently in practice

Unitary channel: $\rho \mapsto U\rho U^\dagger$

Dephasing channel: $\rho \mapsto (1-p)\rho + pZ\rho Z;\ \ 0 \leq p \leq 1$

Depolarising channel: $\rho \mapsto (1-p)\rho + p\pi;\ \ 0 \leq p \leq 1,\ \pi$ max. mixed

Kraus Representation

All quantum channels can be written in a similar way

Every quantum channel can be written in the form

$$\mathscr{E}(\rho) = \sum_i K_i \rho K_i^\dagger, \text{ where } \sum_i K_i^\dagger K_i = I.$$

The set $\{K_i\}$ are called the *Kraus operators* of the quantum channel $\mathscr{E}$.

Relevance for Practical Quantum Computing

Can't actually do unitary operators in real life!

We expect imperfections in our implementations of quantum gates.

That is to say, we may wish to implement a gate $\rho \mapsto U\rho U^\dagger$
but instead we implement some non-unitary quantum channel.

Can try to compare our implemented channel with desired gate much as we compared two density matrices with quality metrics like trace distance or state fidelity.

How to compare ideal gates to real gates?

Depends what state you feed in!

Compare two very different single-qubit gates: I vs X.

i.e. $\rho \mapsto \rho$ vs $\rho \mapsto X\rho X$.

On the one hand, can easily distinguish these two gates with input $\rho = |0\rangle\langle 0|$.

Whereas I sends this to $|0\rangle\langle 0|$, X sends this to $|1\rangle\langle 1|$.

This pair of states is perfectly distinguishable.

On the other hand, cannot distinguish these two gates with input $\rho = |+\rangle\langle +|$.

Output is $|+\rangle\langle +|$ for both I and X.

Average Gate Fidelity

Common figure-of-merit for experimental quantum computing

Idea is to calculate the average of all state fidelities.

Definition: (fidelity of channel $\mathscr{E}$ with respect to the identity channel)

$$\overline{F}(\mathscr{E}) := \int \mathrm{d}\psi \, \langle\psi| \, \mathscr{E}(\psi) \, |\psi\rangle$$

E.g. Average fidelity of depolarising channel $\mathscr{E}(\rho) = (1-p)\rho + p \cdot I/d$ is

$$\overline{F}(\mathscr{E}) = \int \mathrm{d}\psi \, \langle\psi| \, \mathscr{E}(\,|\psi\rangle\langle\psi|\,) \, |\psi\rangle = (1-p) + p/d = 1 - \frac{d-1}{d} \cdot p$$

Nielsen's Formula

A powerful tool for calculating average fidelities

[arXiv:quant-ph/0205035] — see eq. (17)

Given an orthogonal unitary basis $\{U_j\}$ for the space of operators, the average fidelity of a channel $\mathscr{E}$ is $\dfrac{d^2 + \sum_j \mathrm{Tr}(U_j^\dagger \mathscr{E}(U_j))}{d^2(d+1)}$.

In particular, if the channel is unitary (i.e. $\mathscr{E}(\rho) = V\rho V^\dagger$), then $\overline{F} = \dfrac{d^2 + \sum_j \mathrm{Tr}\left(U_j^\dagger V U_j V^\dagger\right)}{d^2(d+1)} = \dfrac{d^2 + \sum_j |\mathrm{Tr}(U_j V)|^2}{d^2(d+1)} = \dfrac{d + |\mathrm{Tr}(V)|^2}{d + d^2}$

Exercise

Fidelity of Toffoli w.r.t. Identity

The hottest quantum startup promises to do quantum computing by implementing Hadamard and Toffoli gates.

However, they have a minor issue: their Toffoli gates are not working and they are simply doing nothing (i.e. identity gates).

What is the fidelity of their “Toffoli” gate?

What if they replace all m-controlled-NOT gates with the identity?

Exercise

Fidelity of Toffoli w.r.t. Identity

Toffoli: $T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$; $\mathrm{Tr}(T) = 6$; $\overline{F} = \frac{8 + 6^2}{8 + 8^2} = \frac{44}{72} \approx 61\,\%$