Methods in quantum computing

Mária Kieferová

August 22, 2023

University of Technology Sydney

Announcements

- Please email me your solutions to the bonus problems if you'd like to.
- Feel free to reserve a topic for the final presentation/report. Let me know if you're interested in a different topic or if the one you'd like is already taken.

Today

- measurements
- norm and distance
- noise channels

Quantum measurement

Obtain classical information from a quantum state. It can destroy the superposition property of a quantum state. $|b\rangle = \alpha|0\rangle + \beta|1\rangle$

Observe this qubit in state $|0\rangle$ with probability $|\alpha|^2$ and in state $|1\rangle$ with probability $|\beta|^2$. Furthermore, after the measurement, the qubit state $|b\rangle$ will disappear and collapse to the observed state $|0\rangle$ or $|1\rangle$.

General quantum measurement

A collection of $\Upsilon := \{M_i\}$, where each measurement operator $M_i \in \mathcal{L}(\mathcal{H})$ satisfies

probabilities are positive real numbers

$$\sum_i M_i = I \qquad (1)$$

always get an outcome

and each M_i is positive semi-definite operator. We call this measurements positive operator-valued measure (POVM). The probability of obtaining an outcome i on a quantum state ρ is

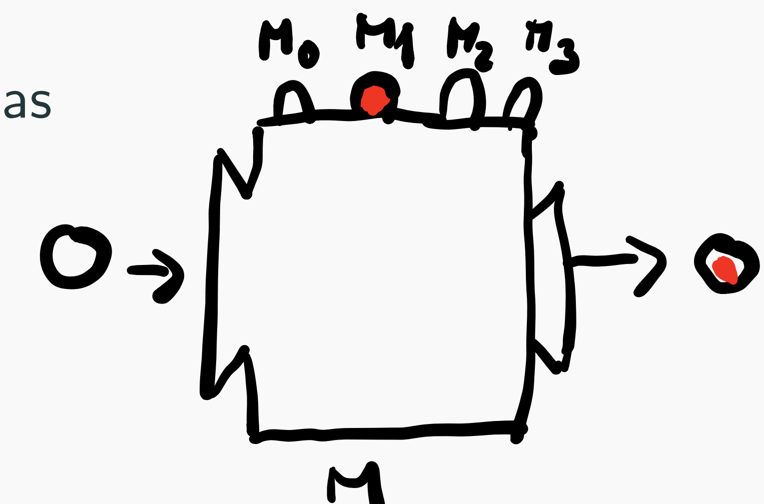
probabilities

$$p_i := \mathrm{Tr}(M_i \rho). \qquad (2)$$

Born's rule

The state after measurement will be altered as

$$\text{(3)} \quad \rho_i := \frac{M_i \rho}{p_i}.$$



Example

$M_0 = |0\rangle\langle 0|$

$M_1 = \mathbb{1} - (|0\rangle\langle 0|) = |1\rangle\langle 1|$

$M_0 + M_1 = \mathbb{1}$

$$\boxed{\begin{aligned} M_0 &= |00\rangle\langle 00| \\ M_1 &= \mathbb{1} - |00\rangle\langle 00| \end{aligned}}$$

$M_0 = \frac{1}{2}|0\rangle\langle 0|$

$M_1 = \frac{1}{2}|1\rangle\langle 1|$

$M_2 = \frac{1}{2}\mathbb{1}$

M_0, M_1 are projectors $\Rightarrow$ eigenvalues are 0 and 1. $\Rightarrow M_0, M_1$ are positive semi-definite

$M_0|0\rangle = 1\,|1\rangle$

$M_0|1\rangle = 0\,|0\rangle = 0$

$\gg$ 0 & 1

$|b\rangle = \alpha|0\rangle + \beta|1\rangle$

number

$$p_0 = \mathrm{Tr}(|b\rangle\langle b|0\rangle\langle 0|) = \mathrm{Tr}(|1\rangle\langle b|0\rangle\langle 1|) = |\beta|^2$$

$$\rho = \frac{M_0|\beta\rangle\langle\beta|}{p_0} = |0\rangle\langle 0|$$

Projective measurement

Each M_i is a projector

$$p_j := \mathrm{Tr}\left(P_j|\phi\rangle\langle\phi|\right)$$

as the example before

and the resulting state

$$\frac{P_j|\phi\rangle}{\sqrt{p_j}}.$$

exercise

A single qubit is fully characterized by a vector $\vec{r}, |r| \leq 1$ such that

$$\rho = \frac{1}{2}\left(I + r_0\sigma_x + r_1\sigma_y + r_2\sigma_z\right) \tag{3}$$

Take a set of operators

$$M = \left\{\frac{I+X}{6}, \frac{I-X}{6}, \frac{I+Y}{6}, \frac{I-Y}{6},, \frac{I+Z}{6}, \frac{I-Z}{6}\right\}. \tag{4}$$

Show that

1. M is a POVM (operators are positive and sum to identity).
2. M is tomographically complete i.e. measuring enough times will allow us to learn the vector r.

State discrimination

Take $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ and measurement statistics for $M = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. Given an unknowns state $|\psi\rangle$, is it $|+\rangle$ or $|-\rangle$?

State discrimination task: what M to choose to be able to decide which one of quantum states we are given with the highest probability.

$$\langle \psi | Z | \psi \rangle = 0.7(+1) + 0.3(-1)$$

$|0\rangle\langle 0| \rightarrow 70\%$

$|1\rangle\langle 1| \rightarrow 30\%$

Norm of states and state distance

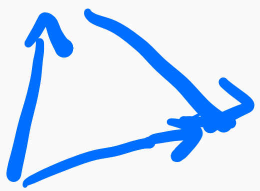
For pure states: Norm $\|\psi\| = \langle\psi|\psi\rangle$

How to extend the concept of the norm to matrices? How to calculate distance between quantum channels and operators?

Norm

Every norm $\|\cdot\|$ must satisfy the following conditions.

- $\|A\| \geq 0$ with equality if and only if $A = 0$.
- $\|\alpha A\| = |\alpha|\|A\|$ for any $\alpha \in \mathbb{C}$.
- Triangle inequality: $\|A + B\| \leq \|A\| + \|B\|$.



Examples: $\sqrt{a^2 + b^2}$ Euclidian on $\mathbb{R}^2$

$\|\alpha\|^2 + \|B\|^2$

$|\alpha| + |B|$

Matrix Schatten norms

Shatten p-norm of a matrix $A \in \mathbb{C}^{m\times n}$ is defined as

$$\|A\|_p := \left(\operatorname{Tr}\left(|A|^p\right)\right)^{\frac{1}{p}} \tag{5}$$

where $|A| := \sqrt{A^\dagger A}$. We extend $p \to \infty$ as follows

$$\|A\|_\infty := \max\left\{\|A\boldsymbol{x}\| : \forall \boldsymbol{x} \in \mathbb{C}^n,\ \|\boldsymbol{x}\| = 1\right\}. \tag{6}$$

$p = 1, 2, \infty$

Exercise

or eigenvalue

Denote by $\sigma_i(A)$ the i-th (non-zero) singular value of A. Show that

$$\|A\|_p = \left(\sum_i (\sigma_i(A))^p\right)^{\frac{1}{p}}. \tag{7}$$

$$A = \sum_i \sigma_i |i\rangle\langle i|$$

$$A^p = \sum_i \sigma_i^p |i\rangle\langle i|$$

Matrix Schatten norm, p=1

$$\|A\|_{p=1} = \operatorname{Tr}\left(|A|^p\right)^{\frac{1}{p}} = \operatorname{Tr}\left(|A|\right) \tag{8}$$

This is known as the **trace norm**.

Schatten norm, $p = 2$

$$\|A\|_{p=2} := \operatorname{Tr}\left(|A|^2\right)^{\frac{1}{2}} = \left(\sum_i (\sigma_i(A))^2\right)^{\frac{1}{2}} \tag{9}$$

This is known as the **Hilbert–Schmidt norm** or Frobenius norm. It can be also defined as

$$\|A\|_2 \equiv \|A\|_F = \sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} |A_{i,j}|^2}. \tag{10}$$

Notice that it corresponds to the norm of the vector of singular values.

$A = \sum_i \sigma_i |i\rangle\langle i|$ (in the basis of its eigenvectors)

$\vec{\sigma} = (\sigma_0, \sigma_1, \ldots \sigma_n)$ vector of eigenvalues

$\|\sigma\|^2 = \sigma_1^2 + \sigma_2^2 + \ldots + \sigma_n^2$

Schatten norm, $p = \infty$

$$\|A\|_\infty := \max\{\|A\boldsymbol{x}\| : \forall \boldsymbol{x} \in \mathbb{C}^n, \|\boldsymbol{x}\| = 1\} \tag{11}$$

This is called the operator norm and corresponds to the largest singular value.

$\|v\| = 1$

$$A = \sum_i \lambda_i |i\rangle\langle i|$$

$$\max_v \|Av\| = \max_v \left\| \sum_i \lambda_i |i\rangle\langle i| v \right\|$$

pick v to be the eigenvector with the largest eigenvalue

$$\|Av\| = \lambda_{max}$$

Properties

1. unitarily invariant: for any unitary operators U and V

$$\|UAV\|_p = \|A\|_p \tag{12}$$

   for any $p \in [1, \infty]$.

2. Hölder's inequality: for $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times \ell}$, it holds that

$$\|AB\|_1 \leq \|A\|_p \|B\|_q, \tag{13}$$

   where $p, q \geq 1$ and $\frac{1}{p} + \frac{1}{q} = 1$.

3. Sub-multiplicativity: for $A \in \mathbb{C}^{m\times n}$ and $B \in \mathbb{C}^{n\times \ell}$, it holds that

$$\|AB\|_p \leq \|A\|_p \|B\|_p. \tag{14}$$

4. Monotonicity: for $1 \leq p \leq q \leq \infty$, it holds that

$$\|A\|_1 \geq \|A\|_p \geq \|A\|_q \geq \|A\|_\infty. \tag{15}$$

Warning

There are other norms, including induced norms, entry-wise norms, etc often with conflicting notation.

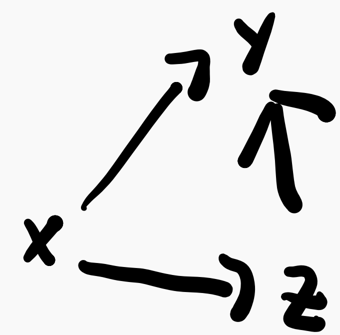
Wikipedia article "Matrix norm" can be very helpful.

$$\|A\|_2$$

$$\|A\|_{max} = \max_{i,j} |A_{i,j}|$$

Use a norm to define metric

- The distance between an object and itself is always zero.
- The distance between distinct objects is always non-negative.
- Distance is symmetric: the distance from x to y is always the same as the distance from y to x.
- Triangle inequality: $d(x, y) \leq d(x, z) + d(z, y)$



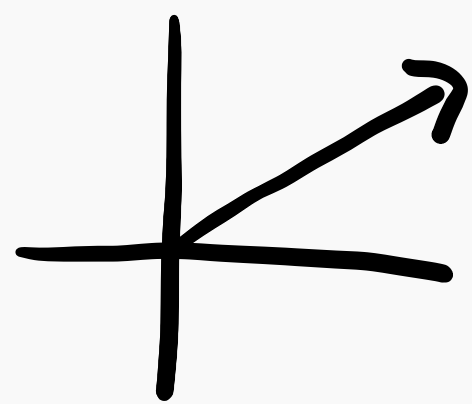
$d(a, a) = 0$

$d(a, b) = 0 \Leftrightarrow a = b$

$d(a, b) \geq 0$

$d \quad \mathbb{C}^{n \times m} \times \mathbb{C}^{n \times m} \to \mathbb{R}_{+,0}$

$\|\cdot\| \quad \mathbb{C}^{n \times m} \to \mathbb{R}_{+,0}$

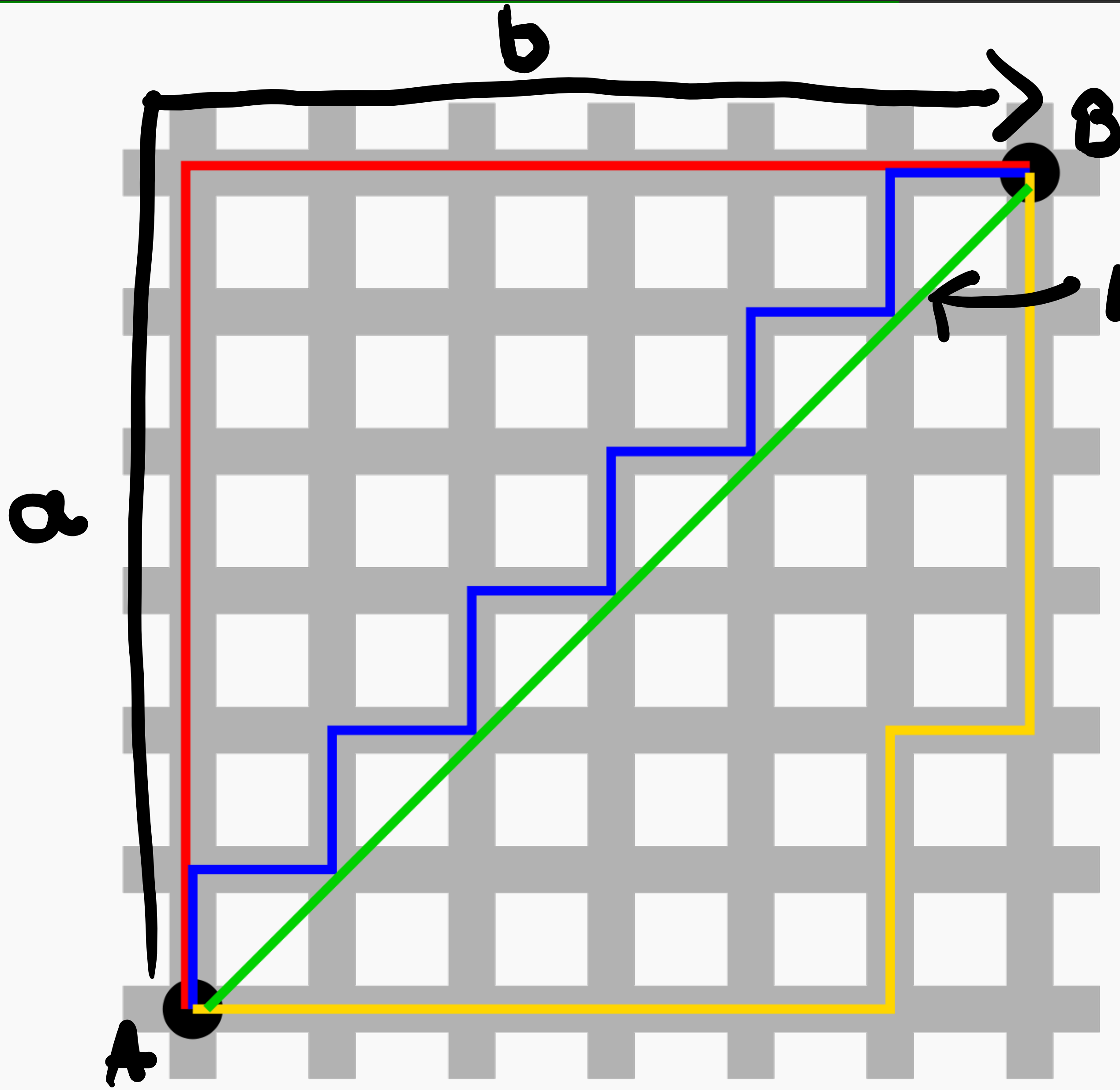


Examples

red, blue
yellow

L_1

$a+b$



Euclidian distance

L^2

$\sqrt{a^2+b^2}$

Trace Distance

The *trace distance* between two operators A and B is given by

$$T(A,B) := \frac{1}{2}\operatorname{Tr}(A - B). \quad = \frac{1}{2}\|A - B\|_1$$

Related to the maximum probability of distinguishing between two quantum states.

$$\frac{1}{2}\operatorname{Tr}\left(|\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\right)$$

$p_{success} = \frac{1}{2}(1 + T(A,B))$

$$\frac{1}{2}\sum_i |\langle i|\psi\rangle|^2 - |\langle i|\phi\rangle|^2$$

Quantum analogue of total variational distance.

$$1 - \sqrt{F(\rho,\sigma)} \leq T(\rho,\sigma) \leq \sqrt{1 - F(\rho,\sigma)}$$

Fidelity

$$F(\rho, \sigma) := \left(\mathrm{Tr} \sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \right)^2 .$$

Sometimes the square is missing

Not a distance, but infidelity (1-F) is.

maximize fidelity $\Leftrightarrow$ minimize distance from the target

If $\rho = |\psi\rangle\langle\psi|$

$F(\rho, \sigma) = \langle\psi|\sigma|\psi\rangle$

POVM

$M_0 = |\psi\rangle\langle\psi|$

$M_1 = \mathbb{1} - |\psi\rangle\langle\psi|$

Exercise

1. $0 \leq F(\rho, \sigma) \leq 1$.
2. $F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma)$.
3. $F(|\psi_\rho\rangle, |\psi_\sigma\rangle) = |\langle\psi_\rho|\psi_\sigma\rangle|^2$.
4. Symmetry: $F(\rho, \sigma) = F(\sigma, \rho)$.

$\sqrt{\sigma} = \sum_i p_i |i\rangle\langle i|$ go to the eigenbasis of σ

Exercise

What is the fidelity and total trace distance between a maximally mixed state and any pure state?

Quantum channels

last time:

$$\Phi(\sigma) = \sum_i B_i \sigma B_i^\dagger \quad \text{where} \quad \sum_i B_i^\dagger B_i = \mathbf{1}. \tag{16}$$

Examples of channels

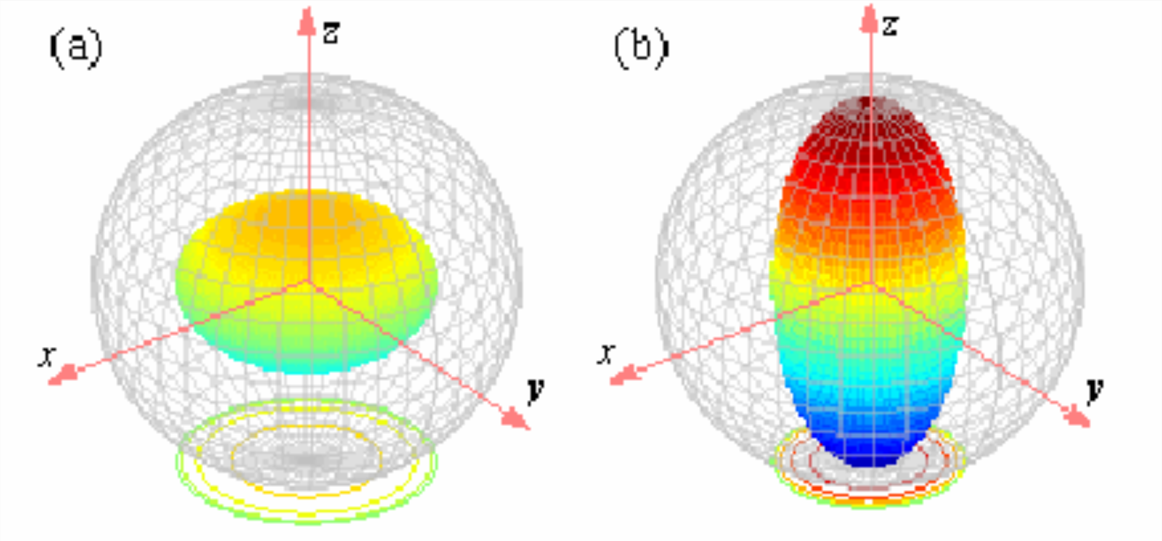
- Depolarizing Channel:

$$\mathcal{N}(\rho) = (1-p)\rho + p\pi,$$

where π is the completely mixed state.

- Dephasing Channel:

$$\mathcal{N}(\rho) = (1-p)\rho + pZ\rho Z.$$



Average Fidelity of a quantum channel

Defined with respect to the identity channel

$$F(\mathcal{E}) = \int d\psi \, \langle\psi| \, \mathcal{E}(\psi) \, |\psi\rangle \tag{17}$$

as an average over all state fidelities. To obtain the average, we must integrate over all the quantum states in a given Hilbert space with equal weightings and satisfy $\int d\psi = 1$. This is known as integration over Haar measure.

Exercise

Compute the fidelity of a qubit depolarizing channel

$\mathcal{E}(\rho) = (1 - p) |\psi\rangle \langle\psi| + p\frac{I}{d}$.

Unitary channel

The special case of fidelity between a unitary and the identity can be simplified through the Nielsen's equation:

$$F(U) = \frac{d + |Tr(U)|^2}{d + d^2}. \tag{18}$$

Exercise

1. Verify that $F(I)=1$ in (18).
2. 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?
3. What if they replace all m-controlled-NOT gates with the identity?