Lecture March 31

- Question: Can we distinguish two q states (distributions)
  - ↳ Check if density ops equal

Example:

- Alice has secret bit b
- If $b=0$, A sends $|0\rangle @ 0.499$, $|1\rangle @ 0.501$
- If $b=1$, A sends $|+\rangle @ 0.499$ $|-\rangle @ 0.501$

How well can adv Bob distinguish $b=0$, $b=1$?

$$\rho_0 = 0.499\, \underbrace{|0\rangle\langle 0|}_{\begin{pmatrix}1 & \\ & 0\end{pmatrix}} + 0.501 \cdot \underbrace{|1\rangle\langle 1|}_{\begin{pmatrix}0 & \\ & 1\end{pmatrix}} = \begin{pmatrix}0.499 & \\ & 0.501\end{pmatrix} \approx \tfrac{1}{2}I$$

$\ne$

$$\rho_1 = 0.499\, \underbrace{|+\rangle\langle +|}_{\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}} + 0.501\, \underbrace{|-\rangle\langle -|}_{\frac{1}{2}\begin{pmatrix}1 & -1\\ -1 & 1\end{pmatrix}} = \begin{pmatrix}1/2 & -0.01\\ -0.01 & 1/2\end{pmatrix} \approx \tfrac{1}{2}I$$

$\Rightarrow$ Not phys. dist.

Excursion: Statistical Distance

Given random vars / distribs X, Y

Ask: How well can we dist. X, Y?

$$SD(X,Y) \overset{\text{(informal)}}{=} \max_{Adv} \left| \Pr[Adv(X) \to \text{"yes"}] - \Pr[Adv(Y) \to \text{"yes"}] \right|$$

Precise: Instead of Adv, we have a set T

$$SD(X\,Y) := \max_{(\text{set})\, T} \left| \Pr[X \in T] - \Pr[Y \in T] \right|$$

$$SD(X,Y) = \frac{1}{2} \sum_a \left| \Pr[X=a] - \Pr[Y=a] \right|$$

Example: $0 @ 0.499$, $1 @ 0.501$ $\to X$
$0 @ 1/2$ $\quad 1 @ 1/2$ $\to Y$

$$SD(X,Y) = \frac{1}{2}\Big(\underbrace{|0.499 - \tfrac{1}{2}|}_{0.001} + \underbrace{|0.501 - \tfrac{1}{2}|}_{0.001} \Big) = 0.001$$

Properties

- SD is a metric ($SD=0$ iff $X=Y$, $SD \geq 0$, triangle ineq.)
- For any (possibly randomized) function F
  $$SD(F(X), F(Y)) \leq SD(X,Y)$$
- If Z indep of X,Y
  $$SD((X,Z),(Y,Z)) = SD(X,Y)$$

Trace distance

Given two density ops ρ, σ

Ask: How well can we distinguish?

$$TD(\rho,\sigma) \overset{\text{(informal)}}{=} \max_{Adv} \big| \Pr[Adv(\rho) \to yes] - \Pr[Adv(\sigma) \to yes] \big|$$

<u>Case 1</u> ρ, σ are classical $\quad$ ($\{|1\rangle @ p_1, |2\rangle @ p_2, \dots\}$)

ρ: $|i\rangle @ p_i \to \rho = \sum p_i |i\rangle\langle i| = \begin{pmatrix} p_1 & & & \\ & p_2 & & \\ & & \ddots & \\ & & & p_n \end{pmatrix}$

σ: $|i\rangle @ r_i \to \sigma = \begin{pmatrix} r_1 & & & \\ & r_2 & & \\ & & \ddots & \\ & & & r_n \end{pmatrix}$

Want: $TD(\rho,\sigma) = SD(X,Y)$ $\qquad X \sim p_i \quad Y \sim r_i$

$$SD(X,Y) = \frac{1}{2}\sum_i |p_i - r_i| = \frac{1}{2}\operatorname{tr}|\rho - \sigma|$$

$$|\rho-\sigma| = \begin{pmatrix} |p_1-r_1| & & & \\ & |p_2-r_2| & & \\ & & \ddots & \\ & & & |p_n - r_n| \end{pmatrix}$$

($\sum_i p_i - r_i = \operatorname{tr}(\rho - \sigma)$)

(For diag A: $|A| := A$ with each diag. elem $\to$ abs val)

Case 2: General ρ, σ.

What is $|\rho - \sigma|$ if $\rho - \sigma$ is not diag?

Def: $|A| := \sqrt{A^\dagger A}$

$\sqrt{X}$ (with $X \geq 0$) is the unique $Y \geq 0$ s.t. $Y^\dagger Y = X$

Want: $|A| = U^\dagger |UAU^\dagger| U$

Want: $|A|$ = elementwise abs val if A diag

Def: $TD(\rho,\sigma) = \frac{1}{2}\operatorname{tr}|\rho - \sigma|$

$$TD(\rho,\sigma) = \frac{1}{2}\operatorname{tr}\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}$$

$A := \rho - \sigma$, $\quad A = U^\dagger D U$ (U unitary, D diag)

$$TD(\rho,\sigma) = \frac{1}{2}\operatorname{tr}|A| = \frac{1}{2}\operatorname{tr} U^\dagger |\underbrace{UAU^\dagger}_{D}| U = \frac{1}{2}\operatorname{tr} U^\dagger |D| U = \frac{1}{2}\operatorname{tr}|D| = \frac{1}{2}\sum |\text{eigenvalue}|$$

Properties of TD

- $TD(\rho,\sigma) = SD(X,Y)$ if ρ, σ are the class. dens. op. corresponding to X, Y

Properties

- SD is a metric ($SD=0$ iff $X=Y$, sym, $SD \geq 0$, triangle ineq.)
- For any (possibly randomized) function F
  $SD(F(X), F(Y)) \leq SD(X,Y)$
- If Z indep of X,Y
  $SD((X,Z),(Y,Z)) = SD(X,Y)$

- TD is a metric
- For any q. oper. $\mathcal{E}$
  $$TD(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq TD(\rho,\sigma)$$
- $TD(\rho \otimes \tau, \sigma \otimes \tau) = TD(\rho,\sigma)$

<u>Toy example:</u> $\rho_0 = \begin{pmatrix}0.499 & \\ & 0.501\end{pmatrix}$ $\quad \rho_1 = \begin{pmatrix}1/2 & -0.001\\ -0.001 & 1/2\end{pmatrix}$

$TD(\rho_0, \rho_1) = ?$

$$A := \rho_0 - \rho_1 = \begin{pmatrix}-0.001 & 0.001\\ 0.001 & 0.001\end{pmatrix} = \frac{1}{1000}\overbrace{\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix}}^{B}$$

$$\det(B - xI) = \det\begin{pmatrix}-1-x & 1\\ 1 & 1-x\end{pmatrix} = (-1-x)(1-x) - 1\cdot 1$$

$$= -1 + x - x + x^2 - 1 = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

EV of B: $\sqrt{2}$, $-\sqrt{2}$

EV of A: $\frac{\sqrt{2}}{1000}$ $\quad \frac{-\sqrt{2}}{1000}$

$$TD(\rho,\sigma) = \frac{1}{2}\left(\left|\frac{\sqrt{2}}{1000}\right| + \left|\frac{-\sqrt{2}}{1000}\right| \right) = \frac{\sqrt{2}}{1000}$$

$\Rightarrow$ "Distinguishing advantage" of adv. Bob $\leq \frac{\sqrt{2}}{1000}$

Other distance measures?

<u>"Fidelity"</u>

Say $|\psi\rangle, |\phi\rangle$ are pure states.

If $|\psi\rangle = |\phi\rangle$, $\langle\psi|\phi\rangle = 1$

If $|\psi\rangle, |\phi\rangle$ orthog, $\langle\psi|\phi\rangle = 0$

In all other cases: $|\langle\psi|\phi\rangle| \in (0,1)$

$\Rightarrow$ $|\langle\psi|\phi\rangle|$ is a measure of similarity!

$$F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|$$

(or: $= |\langle\psi|\phi\rangle|^2$ for some authors)

Can also be defined for density ops.

Best possible distinguisher?

Given ρ, σ with $TD(\rho,\sigma) = \varepsilon$

Find meas. that dist ρ, σ optimally.

If ρ, σ diag: $\rho - \sigma = \begin{pmatrix} + & & & & & \\ & + & & & & \\ & & + & & & \\ & & & - & & \\ & & & & - & \\ & & & & & - \end{pmatrix}$ (plus entries, then minus entries)

$$TD(\rho,\sigma) = \frac{1}{2}\left(\sum \text{plus} - \sum \text{minus}\right) = \varepsilon$$

$$M = \left\{ P := \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots\ 0 \end{pmatrix},\ I - P \right\}$$

$\Pr[\text{outcome } M(\rho) = 1] = \operatorname{tr} P\rho$

$\Pr[\quad\quad \sigma \quad] = \operatorname{tr} P\sigma$

$$|\Pr[\dots\rho] - \Pr[\dots\sigma]| = \operatorname{tr} P(\rho - \sigma) = \operatorname{tr}\begin{pmatrix} + & & & \\ & + & & \\ & & 0 & \\ & & & \ddots\ 0 \end{pmatrix} = \sum \text{plus} = \varepsilon$$

Fact: $\sum \text{plus} + \sum \text{minus} = \operatorname{tr}(\rho - \sigma) = \operatorname{tr}\rho - \operatorname{tr}\sigma = 0$

$$\varepsilon = \frac{1}{2}\left(\sum \text{plus} - \sum \text{minus}\right) = \frac{1}{2}\left(\sum \text{plus} - \left(-\sum \text{plus}\right)\right) = \sum \text{plus}$$

General case: Diagonalize $\rho - \sigma$

In that basis, $P := \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 0 & \\ & & & \ddots\ 0 \end{pmatrix}$

$\Rightarrow$ success of $M = \varepsilon$