Distinguishing Quantum States & Matrix norms

Suppose you are given a state ρ_0 or ρ_1 and want to know which you have & how best to distinguish them. What's the optimum measurement? & How does your ability to distinguish them depend on the properties of ρ_0 & ρ_1?

In the absence of prior information about whether the state is ρ_0 or ρ_1, and before performing any measurements, the two states are equally likely.

Then suppose you perform a binary POVM measurement $\{M_0, M_1\}$ to answer the question
"Is the system in state ρ_0 or ρ_1?"

The probability of guessing the correct output state is given by

$$P_{\text{correct guess}} = \sum_{b=0,1} P(S \text{ in } \rho_b) \times P(\text{gets outcome } b \mid \rho_b)$$

$$= \frac{1}{2} \operatorname{Tr}(M_0 \rho_0) + \frac{1}{2} \operatorname{Tr}(\underbrace{M_1}_{I - M_0} \rho_1)$$

$$\Big(\quad = \frac{1}{2}\left(1 + \mathrm{Tr}\left(M_0(\rho_0 - \rho_1)\right)\right)$$

assuming you were equally likely to have been given ρ_0 & ρ_1.

Max probability of distinguishing by picking M_0 to maximise $\mathrm{Tr}(M_0(\rho_0 - \rho_1))$

Simplest case: Computational basis states of single qubit

$$\rho_0 = |0\rangle\langle 0| \ \& \ \rho_1 = |1\rangle\langle 1|$$

then $M_0 = |0\rangle\langle 0| \quad (M_1 = |1\rangle\langle 1|)$

& $\mathrm{Tr}(|0\rangle\langle 0|(|0\rangle\langle 0| - |1\rangle\langle 1|)) = 1$

$$P_{\substack{\text{correct}\\\text{guess}}} = \frac{1}{2}(1 + 1) = 1$$

Generalisation to arbitrary single qubit states

$$\rho_0 = \tfrac{1}{2}(I + \underline{r}_0 \cdot \underline{\sigma})$$

$$\rho_1 = \tfrac{1}{2}(I + \underline{r}_1 \cdot \underline{\sigma})$$

We can also expand M in Pauli bases as

$$M = a(I + bX + cY + dZ) = a(I + \underline{s} \cdot \sigma)$$

$$\underline{s} = \begin{pmatrix} b \\ c \\ d \end{pmatrix}$$

then we can write

$$P_{\substack{\text{correct}\\\text{guess}}} = \frac{1}{4}\operatorname{Tr}\left(M\left(\underline{r}_0 - \underline{r}_1\right)\cdot\underline{\sigma}\right) + \frac{1}{2}$$

$$= \frac{a}{4}\operatorname{Tr}\left(\left(\cancel{I} + \underline{x}\cdot\underline{\sigma}\right)\left(\underline{r}_0 - \underline{r}_1\right)\cdot\underline{\sigma}\right) + \frac{1}{2}$$

$$= \frac{a}{4}\operatorname{Tr}\left(\left(\underline{x}\cdot\underline{\sigma}\right)\left(\underline{r}_0 - \underline{r}_1\right)\cdot\underline{\sigma}\right) + \frac{1}{2}$$

$$= \frac{a}{2}\,\underline{x}\cdot\left(\underline{r}_0 - \underline{r}_1\right) + \frac{1}{2}$$

Cross terms vanish as $\operatorname{Tr}(\sigma_i \sigma_j) = 2\delta_{ij}$

So want to pick $\underline{x}$ that maximises $\underline{x}\cdot(\underline{r}_0 - \underline{r}_1)$

This is the standard dot product between two vectors which is maximised when the two vectors are alligned

$$\underline{v}\cdot\underline{u} = \underbrace{|\underline{v}|\,|\underline{u}|\cos(\theta)}_{\text{Max when } \theta = 0}$$

So want $\underline{x} \propto (\underline{r}_0 - \underline{r}_1)$

Norm of $|\underline{x}|$ & a are determined by the constraint that

M is +ve & that $M \leq I$

But we know from writing any state ρ as a sum of Pauli operators that this is equivalent to requiring that $|\underline{x}| \leq 1$ & $a = 1/2$

So $\underline{x}_{opt} = \dfrac{1}{|\underline{r}_0 - \underline{r}_1|}(\underline{r}_0 - \underline{r}_1)$ $\qquad M = \frac{1}{2}(I + \underline{x}_{opt}\cdot\underline{\sigma})$

$$P_{\substack{\text{correct}\\\text{guess}}} = \frac{1}{2} + \frac{1}{4}\,\frac{(\underline{\Gamma}_0 - \underline{\Gamma}_1)\cdot(\underline{\Gamma}_0 - \underline{\Gamma}_1)}{|\underline{\Gamma}_0 - \underline{\Gamma}_1|}$$

$$= \frac{1}{2} + \frac{1}{4}\,|\underline{\Gamma}_0 - \underline{\Gamma}_1|$$

What changes if one of the states is more likely to occur than one of the others? i.e. your prior changes.

This will add an additional consideration to be taken into account when guessing (think about the extreme case when it's with 99% prob ρ_0!).
More subtly this will also effect the optimum measurement to be performed.

One of the problems for this week will cover this generalisation

What about distinguishing more complex (higher dimensional) states?

In this case a super nice / useful result is that

Claim ✡

$$\left\{\begin{aligned} P^{\text{opt}}_{\substack{\text{correct}\\\text{guess}}} &= \frac{1}{2}\left(1 + \max_{0 \le M \le I} \operatorname{Tr}\left(M(\rho_0 - \rho_1)\right)\right) \\ &= \frac{1}{2}\left(1 + \frac{1}{2}\|\rho_0 - \rho_1\|_1\right) \end{aligned}\right.$$

This gives a nice operational meaning to the 1-norm between two states.

Namely $\frac{1}{2}\|\rho_0 - \rho_1\|_1 \equiv \max_{0 \le M \le I} \operatorname{Tr}\left(M(\rho_0 - \rho_1)\right)$

$$\boxed{\|A\|_1 = \operatorname{Tr}\left(\sqrt{X^\dagger X}\right) = \sum_i \sqrt{\lambda_i(X^\dagger X)}}$$

eigenvalues of $X^\dagger X$

Handwavey

✓ Proof of Claim ✱

$$p^{opt}_{\substack{guess\\correct}} = \frac{1}{2}\left(1 + \max_{0 \le M \le I} \mathrm{Tr}(M_0(\rho_0 - \rho_1))\right)$$

The trick to optimising this is to write $\rho_0 - \rho_1$ as $\rho_0 - \rho_1 = P_+ - P_-$ where P_+ & P_- are orthogonal projectors onto the +ve and −ve parts of $\rho_0 - \rho_1$

That is, let $|\lambda_i\rangle, \lambda_i$ be the eigenvectors/values of $\rho_0 - \rho_1$, then we can write

$$\begin{aligned}\rho_0 - \rho_1 &= \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i| \\ &= \underbrace{\sum_{\substack{i \\ \text{s.t. } \lambda_i > 0}} \lambda_i |\lambda_i\rangle\langle\lambda_i|}_{P_+} + \underbrace{\sum_{\substack{i \\ \text{s.t. } \lambda_i < 0}} \lambda_i |\lambda_i\rangle\langle\lambda_i|}_{-P_-}\end{aligned}$$

$$p_{\substack{guess\\correct}} = \frac{1}{2}\left(1 + \frac{1}{2}\mathrm{Tr}(M(P_+ - P_-))\right)$$

Now to maximise this you want to pick M such that $\mathrm{Tr}(MP_+)$ is max and $\mathrm{Tr}(MP_-)$ is minimized

Since $-P_-$ has only negative eigenvalues

P_- " " positive eigenvalues

remember M is a +ve operator

So $\mathrm{Tr}(M P_-)$ is only -ve.

$\therefore$ it's minimised when $\mathrm{Tr}(M P_-) = 0$

This is achieved by $M = \Pi_+$ which in turn maximises $\mathrm{Tr}(M P_+)$.

$$\therefore \quad M_{opt} = \Pi_+ = \sum_{i \text{ s.t. } \lambda_i > 0} |\lambda_i\rangle\langle\lambda_i|$$

$$p^{opt}_{\text{guess correct}} = \frac{1}{2}\left(1 + \mathrm{Tr}(M_{opt}(P_+ - P_-))\right)$$

$$= \frac{1}{2}\left(1 + \mathrm{Tr}(P_+)\right)$$

Now $\|\rho - \sigma\|_1 = \sum_i |\lambda_i| = \mathrm{Tr}(P_+) + \mathrm{Tr}(P_-)$

& $\mathrm{Tr}(P_+) - \mathrm{Tr}(P_-) = \mathrm{Tr}(\rho - \sigma) = 0$

$\Rightarrow \|\rho - \sigma\|_1 = 2\,\mathrm{Tr}(P_+)$

$\Downarrow$

$$p^{opt}_{\text{guess correct}} = \frac{1}{2}\left(1 + \frac{1}{2}\|\rho_0 - \rho_1\|_1\right)$$

Question for discussion: How could you measure $\|\rho_1 - \rho_0\|_1$ on a quantum computer?

Other Matrix Norms

A matrix norm is a function $\|\cdot\| : K^{m\times n} \to \mathbb{R}$ that satisfies the following properties

- $\|A\| \geq 0$ (Positive valued)
- $\|A\| = 0 \iff A = 0$ matrix of all zeros
- $\|\alpha A\| = |\alpha| \, \|A\|$
- $\|A+B\| \leq \|A\| + \|B\|$ Subadditive / triangle inequality

Schatten p-norm

(probably the most common family of norms encountered in QI
↳ Not to be confused with the induced p-norms)

$$\|A\|_p = \left(\sum_{i=1}^{d} |\lambda_i(A)|^p \right)^{1/p}$$

norm of eigenvalues of A
$\equiv \sqrt{\text{eigs}(A^\dagger A)}$

or, for a non-square matrix, the singular values of A

$$M = U \underbrace{\Sigma}_{\text{diagonal}} V^*$$

U: $m\times m$, Σ: $m\times n$, V^*: $n\times n$

The cases you actually see:

1) 1-Norm $\quad \|A\|_1 = \sum_i |\lambda_i|$

Operationally meaningful (as previously discussed) but can be hard to work with

2) 2-Norm $\quad \|A\|_2 = \left(\sum_i |\lambda_i|^2\right)^{1/2}$

$$\equiv \sqrt{Tr(AA^\dagger)} = \sqrt{Tr(UDU^\dagger U D^\dagger U^\dagger)}$$

$$= \sqrt{Tr(DD^\dagger)}$$

$$= \sqrt{\sum_i |\lambda_i|^2}$$

Doesn't have a nice operational interpretation

But easy enough to measure on a quantum computer

e.g. $Tr\left((\rho-\sigma)(\rho-\sigma)^\dagger\right) = Tr(\rho^2) + Tr(\sigma^2) - 2\,Tr(\rho\sigma)$

can be measured in swap test or Loschmidt echo circuit

3) Infinity norm $\quad \|A\|_\infty = \max\{|\lambda_i|\}$

$$\equiv \left(\sum_i |\lambda_i|^\infty\right)^{1/\infty}$$

$$= \left(|\lambda_{max}|^\infty + |\lambda_{max-1}|^\infty + \ldots\right)^{1/\infty}$$

dominates!

λ_{max}

Often operationally meaningful

e.g. $|\mathrm{Tr}(M\rho)| \leq |\lambda_{max}| = \|M\|_\infty$

for arb. ρ i.e. $\max_\rho |\mathrm{Tr}(M\rho)| =$

But can be hard to compute

How could you compute $\|M\|_\infty$ if M was an observable?

Could max $\mathrm{Tr}(M\,\rho(\theta))$

What about $\|\rho\|_\infty$?

PCA on ρ