Distinguishability of Random Quantum States

Based on *Montanaro, A. Commun.Math. Phys. 3, 619–636 (2007).*

Ali Almasi

Institut Polytechnique de Paris

Introduction

Problem Set-up

Given an unknown state $\rho_? \in \mathcal{L}(\mathbb{C}^d)$, picked from a known set of states $\mathcal{E} = \{\rho_1, \ldots, \rho_n\}$ with a known prior probability distribution on $\mathcal{E}$,

We want to find an **optimal** measurement to determine $\rho_?$,

In the sense that the probability of success is optimized.

We can focus on finding a POVM measurement (Why?).

An Application: Oracle Identification Problem

Given an oracle implementing an unknown n-bit Boolean function $f : \{0, 1\}^n \mapsto \{0, 1\}$ picked uniformly at random from a known set F of functions,

Identify f with the minimum number of calls to the oracle.

An Application: Oracle Identification Problem

Given an oracle implementing an unknown n-bit Boolean function $f : \{0,1\}^n \mapsto \{0,1\}$ picked uniformly at random from a known set F of functions,

Identify f with the minimum number of calls to the oracle.

$$|\psi_f\rangle = \frac{1}{2^{n-1}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle$$

Some Notations

For $\rho_i \in \mathcal{E}$, which appears with probability p_i, define

$$\rho_i{}' := p_i \rho_i.$$

If $\rho_i = |\psi_i\rangle \langle\psi_i|$, we define

$$|\psi_i{}'\rangle = \sqrt{p_i}\, |\psi_i\rangle \,.$$

For a measurement $M = \{M_i\}_i$, we denote the probability of success in distinguishing which state is given, by $P^M(\mathcal{E})$.

$$P^{opt}(\mathcal{E}) := \sup_M P^M(\mathcal{E})$$

$$P^M(\mathcal{E}) = \sum_i \mathrm{tr}(M_i \rho_i{}')$$

Pretty Good Measurements (PGM)

What are the discrimination strategies?

- non-measurement strategy:
  The probability of sucess is $\sum_i {p_i}^2$.
- the most natural way to design a measurement:

$$M_i := {\rho_i}'.$$

However, these operators do not satisfy the completeness condition:

$$\rho := \sum_i {\rho_i}' \implies \text{tr}(\rho) = 1 \implies \rho \neq \mathbb{I}$$

$$M_i := \rho^{-\frac{1}{2}} {\rho_i}' \rho^{-\frac{1}{2}}$$

Pretty Good Measurements (PGM) for Pure States

It is a projective (?) measurement which is defined as

$$PGM = \{|v_i\rangle\langle v_i|\}_i,$$

where

$$|v_i\rangle := \rho^{-\frac{1}{2}} |\psi_i'\rangle .$$

Pretty Good Measurements (PGM) for Pure States

It is a projective (?) measurement which is defined as

$$PGM = \{|v_i\rangle \langle v_i|\}_i,$$

where

$$|v_i\rangle := \rho^{-\frac{1}{2}} |\psi_i'\rangle .$$

Our PGM is not necessarily projective!

Why is it "pretty good"?

Theorem (Barnum–Knill)

$$P^{pgm}(\mathcal{E}) \geq P^{opt}(\mathcal{E})^2.$$

Why is it "pretty good"?

Theorem (Barnum–Knill)

$$P^{pgm}(\mathcal{E}) \geq P^{opt}(\mathcal{E})^2.$$

Theorem (Barnum–Knill)

$$\sqrt{P^{pgm}(\mathcal{E})} \geq P^{opt}(\mathcal{E}).$$

Gram matrix

For a while, let's limit ourselves to the case where ρ_i's are pure states. We can encode the inner product of all the states in an $n \times n$ matrix G:

$$G_{ij} = \sqrt{p_i p_j} \langle \psi_i \mid \psi_j \rangle$$

$$S := (|\psi'_1\rangle, \ldots, |\psi'_n\rangle) \implies G = S^\dagger S$$

Gram matrix

For a while, let's limit ourselves to the case where ρ_i's are pure states. We can encode the inner product of all the states in an $n \times n$ matrix G:

$$G_{ij} = \sqrt{p_i p_j} \langle \psi_i \mid \psi_j \rangle$$

$$S := (|\psi'_1\rangle, \ldots, |\psi'_n\rangle) \implies G = S^\dagger S$$

We may similarly encode the probability of getting outcome i and receiving state j in a matrix P:

$$P_{i,j} := \langle v_i | \psi_j{}' \rangle$$

Then the success probability is

$$P^{pgm}(\mathcal{E}) = \sum_{i=1}^{n} |\langle v_i \mid \psi'_i \rangle|^2 = \sum_{i=1}^{n} |P_{ii}|^2.$$

Gram matrix and PGM

We have:

$$\begin{aligned}
\left(P^2\right)_{ij} &= \sum_{k=1}^{n} \left\langle \psi_i' \middle| \rho^{-1/2} \middle| \psi_k' \right\rangle \left\langle \psi_k' \middle| \rho^{-1/2} \middle| \psi_j' \right\rangle \\
&= \left\langle \psi_i' \middle| \left(\rho^{-1/2} \sum_{k=1}^{n} |\psi_k'\rangle \langle \psi_k'| \, \rho^{-1/2} \right) \middle| \psi_j' \right\rangle \\
&= G_{ij}
\end{aligned}$$

Thus,

$$P = \sqrt{G}.$$

Corollary

$$P^{pgm}(\mathcal{E}) = \sum_{i=1}^{n} (\sqrt{G})_{ii}^2$$

Two Lower Bounds for State Discrimination

Two Lower Bounds

In this part, we give the two lower bounds for the success probability of PGM:

- A bound obtained from the pairwise inner products
- A bound from the eigenvalues of the Gram matrix

A Bound from Pairwise Inner Products (1)

Lemma

If for any $x > 0$, $\sqrt{x} \geq ax + bx^2$, then $(\sqrt{G})_{ii} \geq aG_{ii} + b\sum_{j=1}^{n} |G_{ij}|^2$.

We find the parameters a and b such that $aG_{ii} + b\sum_{j=1}^{n} |G_{ij}|^2$ is maximized.

The maximum is attained when $a = \frac{3}{2\sqrt{r}}$ and $b = -\frac{1}{2r^{3/2}}$, where

$$r = \frac{\sum_{j=1}^{n} |G_{ij}|^2}{G_{ii}}.$$

A Bound from Pairwise Inner Products (2)

Plugging it in our lemma:

$$P^{pgm}(\mathcal{E}) \geq \sum_{i=1}^{n} \frac{p_i^2}{\sum_{j=1}^{n} p_j \left|\langle \psi_i \mid \psi_j \rangle\right|^2}$$

A Bound from Eigenvalues

$$\sum_{i=1}^{n}(\sqrt{G})_{ii} = \sum_{i=1}^{n}\sqrt{\lambda_i}$$

$$\Rightarrow \left(\sum_{i=1}^{n}(\sqrt{G})_{ii}\right)^2 = \left(\sum_{i=1}^{n}\sqrt{\lambda_i}\right)^2$$

$$\Rightarrow n\sum_{i=1}^{n}(\sqrt{G})_{ii}^2 \geq \left(\sum_{i=1}^{n}\sqrt{\lambda_i}\right)^2$$

$$P^{pgm}(\mathcal{E}) \geq \frac{1}{n}\left(\sum_{i=1}^{n}\sqrt{\lambda_i}\right)^2$$

What about Mixed States?

Let $\mathcal{E}$ be an ensemble of n mixed states $\{\rho_i\}$ with a priori probabilities $\{p_i\}$, and having spectral decompositions $\rho_i = \sum_{k=1}^{d} \lambda_{ik} |v_{ik}\rangle \langle v_{ik}|$. Define $\mathcal{F}$ to be the ensemble of the nd pure states $\{|v_{ik}\rangle\}$ with a priori probabilities $\{p_i \lambda_{ik}\}$. Then $P^{pgm}(\mathcal{E}) \geq P^{\mathrm{pgm}}(\mathcal{F})$.

Distinguishing Random Quantum States

Discrimination for Random Ensembles (Expectation)

Theorem

Let $\mathcal{E}$ be an ensemble of n equiprobable d-dimensional quantum states $\{|\psi_i\rangle\}$ with $n/d \to r \in (0,\infty)$ as $n, d \to \infty$, and let the components of $|\psi_i\rangle$ in some basis be i.i.d. complex random variables with mean 0 and variance $1/d$. Then

$$\mathbb{E}\left(P^{pgm}\left(\mathcal{E}\right)\right) \geq \begin{cases} \frac{1}{r}\left(1 - \frac{1}{r}\left(1 - \frac{64}{9\pi^2}\right)\right) & \text{if } n \geq d \\ 1 - r\left(1 - \frac{64}{9\pi^2}\right)^2 & \text{otherwise} \end{cases}$$

and in particular $\mathbb{E}\left(P^{pgm}\left(\mathcal{E}\right)\right) > 0.720$ when $n \leq d$.

Discrimination for Random Ensembles (Expectation)

Theorem

Let $\mathcal{E}$ be an ensemble of n equiprobable d-dimensional quantum states $\{|\psi_i\rangle\}$ with $n/d \to r \in (0, \infty)$ as $n, d \to \infty$, and let the components of $|\psi_i\rangle$ in some basis be i.i.d. complex random variables with mean 0 and variance $1/d$. Then

$$\mathbb{E}\left(P^{pgm}\left(\mathcal{E}\right)\right) \geq \begin{cases} \frac{1}{r}\left(1 - \frac{1}{r}\left(1 - \frac{64}{9\pi^2}\right)\right) & \text{if } n \geq d \\ 1 - r\left(1 - \frac{64}{9\pi^2}\right)^2 & \text{otherwise} \end{cases}$$

and in particular $\mathbb{E}\left(P^{pgm}\left(\mathcal{E}\right)\right) > 0.720$ when $n \leq d$.

What is the point here?

- We have random ensembles.
- We need to bound the **expectation** of the probability of success.
- The premises of the theorem provide us the possibility of applying some nice results from random matrix theory.
- States are being chosen according to the Haar measure.

Discrimination for Random Ensembles (Concentration of Measure)

Theorem

Let $\mathcal{E}$ be an ensemble of n d-dimensional quantum states picked uniformly at random. Set $p = \mathbb{E}\left(P^{pgm}\left(\mathcal{E}\right)\right) = \frac{1}{r}\left(1 - \frac{1}{r}\left(1 - \frac{64}{9\pi^2}\right)\right)$ if $n \geq d$, and $p = 1 - r\left(1 - \frac{64}{9\pi^2}\right)$ otherwise. Then

$$\Pr\left[P^{pgm}(\mathcal{E}) \leq p - \epsilon\right] \leq 2\exp\left(\frac{-C(2nd+1)\epsilon^2}{2}\right)$$

where $C = 1/\left(18\pi^3\right)$.

Conclusion

Conclusion

- The importance of this work is:
  - finding analytic lower bounds for the success probability of pretty good measurements
  - using the theory of random matrices to apply the bounds in the case of random ensembles
- If my talk went well, you should probably know that:
  - what is the state discrimination problem.
  - the state discrimination problem has many applications.
  - pretty good measurement are indeed pretty good strategies.
  - obtaining lower (upper) bounds for the success probability of pretty good measurements might be useful to solve other problems.

Thank you!