On the distinguishability of random quantum states

Ashley Montanaro[1]

[1]Department of Computer Science
University of Bristol
Bristol, UK

quant-ph/0607011

University of BRISTOL

Distinguishing quantum states

Question

Consider a known ensemble $\mathcal{E}$ of n quantum states $\{|\psi_i\rangle\}$ with a priori probabilities p_i. Given an unknown state $|\psi_?\rangle$, picked at random from $\mathcal{E}$, what is the optimal probability P^{opt} of identifying $|\psi_?\rangle$? That is,

$$P^{opt} = \max_M \sum_i p_i \langle\psi_i|M_i|\psi_i\rangle$$

where we maximise over all POVMs $M = \{M_i\}$.

- Considered by many authors under titles like "quantum hypothesis testing", "quantum detection", etc.
- In general, producing an analytic expression for P^{opt} appears to be intractable (although good numerical solutions can be found)

This talk

I will discuss:

1. Two analytic lower bounds recently obtained for this optimal probability.
2. The application of one of them to distinguishing *random* quantum states.
3. An application to the "oracle identification problem" in quantum computation.

Methods

The lower bounds are obtained by putting a lower bound on the probability of success of a specific measurement that can be defined for any ensemble of states, the *Pretty Good Measurement* (PGM). Set $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Then the PGM is defined by the set of measurement operators $\{|\mu_i\rangle\langle\mu_i|\}$, where $|\mu_i\rangle = \sqrt{p_i}\rho^{-1/2}|\psi_i\rangle$.

Methods

The lower bounds are obtained by putting a lower bound on the probability of success of a specific measurement that can be defined for any ensemble of states, the *Pretty Good Measurement* (PGM). Set $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Then the PGM is defined by the set of measurement operators $\{|\mu_i\rangle\langle\mu_i|\}$, where $|\mu_i\rangle = \sqrt{p_i}\rho^{-1/2}|\psi_i\rangle$.

Key fact

Let G be the rescaled Gram matrix of the ensemble $\mathcal{E}$, $G_{ij} = \sqrt{p_i p_j}\langle\psi_i|\psi_j\rangle$. Then the probability of success of the PGM is

$$P^{pgm}(\mathcal{E}) = \sum_i p_i |\langle\psi_i|\mu_i\rangle|^2 = \sum_i (\sqrt{G})^2_{ii}$$

The pairwise inner product bound

- The first lower bound is based on the pairwise distinguishability of the states in $\mathcal{E}$.
- The strategy is to put a lower bound on the square root function by an "easier" function (a parabola), and then optimise the parabola.
- Works because $\sqrt{x} \geq ax + bx^2 \Rightarrow (\sqrt{G})_{ii} \geq aG_{ii} + b\sum_j |G_{ij}|^2$.

Pairwise inner product bound

Let $\mathcal{E}$ be an ensemble of n states $\{|\psi_i\rangle\}$ with a priori probabilities p_i.

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

The eigenvalue bound

- The second lower bound is based on a global measure of distinguishability of the states in $\mathcal{E}$: the eigenvalues of the Gram matrix G.
- Using a Cauchy-Schwarz inequality, we can show the following:

Eigenvalue bound

Let G be the Gram matrix of an ensemble $\mathcal{E}$ of n states and let G have eigenvalues $\{\lambda_i\}$. Then

$$P^{pgm}(\mathcal{E}) \geq \frac{1}{n}\left(\sum_i \sqrt{\lambda_i}\right)^2 = \frac{1}{n}\mathrm{tr}(\sqrt{G})^2$$

Comparison with previous bounds

- Previous authors (e.g. Burnashev and Holevo [1]) have used bounds based on similar principles.
- But the bounds here are stronger, especially for low values of $P^{pgm}(\mathcal{E})$, and always give a non-trivial value.

[1] M. V. Burnashev and A. S. Holevo, On reliability function of quantum communication channel, quant-ph/9703013

Comparison with previous bounds

- Previous authors (e.g. Burnashev and Holevo [1]) have used bounds based on similar principles.
- But the bounds here are stronger, especially for low values of $P^{pgm}(\mathcal{E})$, and always give a non-trivial value.
- Assuming the states in $\mathcal{E}$ have equal probabilities:

Comparison of bounds

Previously known lower bound	**New lower bound**
$P^{pgm}(\mathcal{E}) \geq 1 - \frac{1}{n} \sum_{i \neq j} \lvert\langle\psi_i\vert\psi_j\rangle\rvert^2$	$P^{pgm}(\mathcal{E}) \geq \frac{1}{n} \sum_{i=1}^{n} \frac{1}{\sum_{j=1}^{n} \lvert\langle\psi_i\vert\psi_j\rangle\rvert^2}$
$P^{pgm}(\mathcal{E}) \geq \frac{2}{\sqrt{n}} \mathrm{tr}(\sqrt{G}) - 1$	$P^{pgm}(\mathcal{E}) \geq \frac{1}{n} \mathrm{tr}(\sqrt{G})^2$

[1] M. V. Burnashev and A. S. Holevo, On reliability function of quantum communication channel, quant-ph/9703013

Random quantum states

- What is an ensemble of random quantum states?
- Here, we mean a set of n d-dimensional pure states whose components (in some basis) are i.i.d. complex random variables with mean 0 and variance $1/d$.
- This is a quite general notion of randomness that includes pure states distributed uniformly at random (according to Haar measure), in which case the components (in any basis!) are Gaussians.

Random quantum states

- What is an ensemble of random quantum states?
- Here, we mean a set of n d-dimensional pure states whose components (in some basis) are i.i.d. complex random variables with mean 0 and variance $1/d$.
- This is a quite general notion of randomness that includes pure states distributed uniformly at random (according to Haar measure), in which case the components (in any basis!) are Gaussians.
- The pairwise inner product bound (above) can be applied to random quantum states directly, but we can get better results from the eigenvalue bound.
- In order to apply this bound, we need a powerful result from random matrix theory.

The Marčenko-Pastur law

- If the states in $\mathcal{E}$ are random and $p_i = 1/n$ for all i, the Gram matrix G is known to statisticians (since the 1930s!) as a rescaled complex *Wishart matrix*.
- The density of the eigenvalues of G is known and is given by the Marčenko-Pastur law.
    - This is the equivalent of the famous Wigner semicircle law for random Hermitian matrices...
- This allows us to calculate a lower bound on the expected probability of success for the PGM!

Technical issues

- The Marčenko-Pastur law can be applied to random states in the asymptotic regime where:
  - The number of states n and the dimension d approach infinity.
  - The ratio n/d approaches a constant, r.
- We need to modify the Marčenko-Pastur law slightly.
  - It gives the density of the eigenvalues of the Gram matrix; we need the density of the square roots of the eigenvalues.
- The lower bound we get for $\mathbb{E}(P^{pgm}(\mathcal{E}))$ turns out to be given by an intractable elliptic integral.
- However, a good lower bound may be proven on this integral, giving the main result...

The finished lower bound

Main 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

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

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

The finished lower bound

Main 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

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

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

- Concentration of measure results may be used to show that almost all states obey this lower bound!

Comparison with numerical results (1)

$(0 \leq n \leq 2d)$

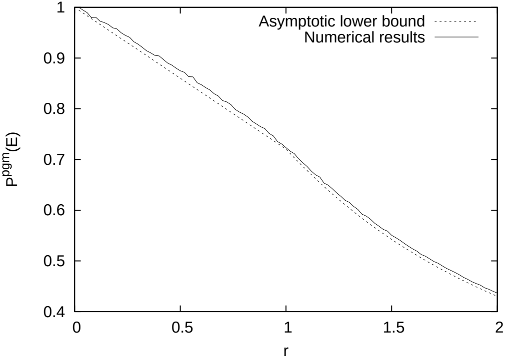

Figure: Asymptotic bound on $P^{pgm}(\mathcal{E})$ vs. numerical results (averaged over 10 runs) for ensembles of $n = 50r$ 50-dimensional uniformly random states.

Comparison with numerical results (2)

($0 \leq n \leq 10d$)

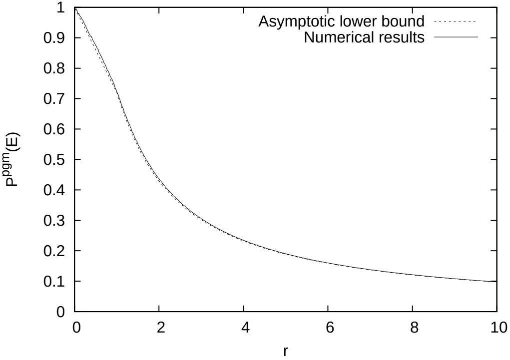

Figure: Asymptotic bound on $P^{pgm}(\mathcal{E})$ vs. numerical results (averaged over 10 runs) for ensembles of $n = 50r$ 50-dimensional uniformly random states.

Oracle identification

Problem

Given an unknown Boolean function f, picked uniformly at random from a set S of N Boolean functions on n bits, identify f with the minimum number of uses of f.

- This is a particular case of the oracle identification problem studied by Ambainis et al[2].
- We consider the case where we must identify f with a bounded probability of error.

[2] A. Ambainis et al, Quantum identification of Boolean oracles, quant-ph/0403056

Oracle identification

- Consider the following single-query "algorithm":
  1. Create the state $|\psi_f\rangle = \sum_x (-1)^{f(x)} |x\rangle$.
  2. Apply the PGM.
- When S is a random set of functions, the states $\{|\psi_f\rangle\}$ are random quantum states.
- So the results here can be used to put the same lower bound on the probability of success of distinguishing these states.
- Concentration of measure is used again to show that this bound holds for almost all sets of functions.
- When the probability of success is a constant $> 1/2$, we can repeat the algorithm a constant number of times for an arbitrarily good probability of success.

Summary

- Good lower bounds have been obtained on the probability of distinguishing pure quantum states.
- These bounds can be applied to distinguishing random quantum states.
- Asymptotically, n random states in n dimensions can be distinguished with probability > 0.72.
- Almost all sets of 2^n Boolean functions on n bits can be distinguished with a constant number of quantum queries.

Summary

- Good lower bounds have been obtained on the probability of distinguishing pure quantum states.
- These bounds can be applied to distinguishing random quantum states.
- Asymptotically, n random states in n dimensions can be distinguished with probability > 0.72.
- Almost all sets of 2^n Boolean functions on n bits can be distinguished with a constant number of quantum queries.

- Further reading: quant-ph/0607011

Summary

- Good lower bounds have been obtained on the probability of distinguishing pure quantum states.
- These bounds can be applied to distinguishing random quantum states.
- Asymptotically, n random states in n dimensions can be distinguished with probability > 0.72.
- Almost all sets of 2^n Boolean functions on n bits can be distinguished with a constant number of quantum queries.
- Further reading: quant-ph/0607011
- Thank you for your time!