Distinguishing Quantum States and Operations

John Watrous

School of Compupter Science
and
Institute for Quantum Computing

University of Waterloo

August 11, 2006

Overview of Talk

In this talk I will discuss the following general tasks, attempted by one or more **collaborating** players:

State Identification

- A set of two or more quantum states of equal dimension is fixed in advance, and assumed to be completely known to all players.
- One of the states from the set is selected (secretly), and a single copy is given to the players.
- The goal: **to determine which one of the states was selected**.

Operation Identification

Similar to the State Identification task, except with operations rather than states. . . more details later.

Basic Examples: State Identification for a single player

1. Orthogonal pure states: suppose the set of states is

$$\{|\psi_0\rangle, \ldots, |\psi_{m-1}\rangle\},$$

where these are n-qubit states (and so $m \leqslant 2^n$). Then a selected state can be identified with certainty.

Define a unitary matrix U as:

$$U = \begin{pmatrix} | & | & & | & | & & | \\ |\psi_0\rangle & |\psi_1\rangle & \cdots & |\psi_{m-1}\rangle & ? & \cdots & ? \\ | & | & & | & | & & | \end{pmatrix}$$

Then $U|j\rangle = |\psi_j\rangle$ for $0 \leqslant j \leqslant m-1$, so $U^\dagger |\psi_j\rangle = |j\rangle$.

Method: Perform $U^\dagger$ and measure in the standard basis.

Basic Examples: State Identification for a single player

2. Two mixed states: suppose the set of states is $\{\rho_0, \rho_1\}$.

If each state is selected with probability 1/2:

There is a (projective) measurement that correctly identifies whether the state was ρ_0 or ρ_1 with probability

$$\frac{1}{2} + \frac{1}{4} \left\| \rho_0 - \rho_1 \right\|_{\mathrm{tr}} .$$

($\|X\|_{\mathrm{tr}} =$ sum of absolute values of eigenvalues for $X = X^\dagger$.)

This is optimal.

If an adversary chooses which of ρ_0 or ρ_1 to select:

The above measurement will be correct with probability at least

$$\frac{1}{2} \left\| \rho_0 - \rho_1 \right\|_{\mathrm{tr}} .$$

Basic Examples: State Identification for a single player

Example: suppose the set of states is

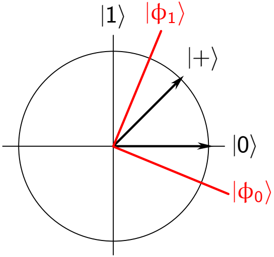
$$\{|0\rangle, |+\rangle\},$$

where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

We already know that these states cannot be distinguished perfectly.

Optimal probability of success (for $|0\rangle$ and $|+\rangle$ chosen uniformly):

$$\frac{1}{2} + \frac{1}{4} \| |0\rangle\langle 0| - |+\rangle\langle +| \|_{\mathrm{tr}} = \frac{1}{2} + \frac{1}{2\sqrt{2}} = 0.85\cdots$$



Unambiguous state identification

Sometimes we may associate different payoffs with different results. . .

Consider the previous example where the set was

$$\{|0\rangle, |+\rangle\}.$$

You are given one of the two states, and may answer:

“$|0\rangle$”, “$|+\rangle$”, or “don’t know”.

Here are the payoffs:

Correct guess:	win $100
Incorrect guess:	lose $1,000,000
Answer “don’t know”:	lose $1

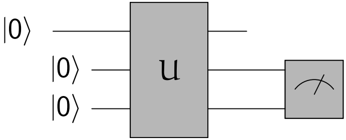
Would you play this game?

Unambiguous state identification

If you consider only projective measurements applied to the given qubit alone, you should expect to lose a lot of money.

You can, however, perform a **POVM-type measurement** (POVM = positive operator-valued measure) and expect to make a lot of money.

In different terms, there exists a three-qubit unitary U with the following properties:



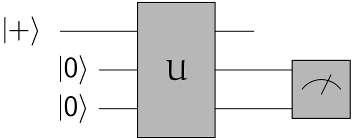
00	with probability ≈ 0.29
11	with probability = 0
01 or 10	with probability ≈ 0.71

Unambiguous state identification

If you consider only projective measurements applied to the given qubit alone, you should expect to lose a lot of money.

You can, however, perform a **POVM-type measurement** (POVM = positive operator-valued measure) and expect to make a lot of money.

In different terms, there exists a three-qubit unitary U with the following properties:



00	with probability = 0
11	with probability ≈ 0.29
01 or 10	with probability ≈ 0.71

This phenomenon is known as **unambiguous state identification**, and is studied for various types of state sets.

The general case: not so simple

In the **general case** where a finite set of three or more non-orthogonal states is given, the picture is not so simple as for the previous special cases.

For example: it is possible to define a set of pure states

$$\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$$

that are pairwise far apart:

$$\left|\langle\psi_i|\psi_j\rangle\right| < 10^{-6} \quad\Rightarrow\quad \left\| |\psi_i\rangle\langle\psi_i| - |\psi_j\rangle\langle\psi_j| \right\|_{\mathrm{tr}} > 2 - 10^{-6}.$$

But the optimal measurement correctly identifies which state was given with very small probability:

$$\Pr[\text{successful identification}] < 10^{-6}.$$

The “pretty good” measurement

There is, however a very useful measurement for the general case: the pretty good measurement. (Also called the “least squares” measurement.)

Suppose the set of states to distinguish is

$$\{\rho_1, \dots, \rho_m\}.$$

Let $R = \sum_{j=1}^{m} \rho_j$.

The pretty good measurement for this set is a POVM $\{P_1, \dots, P_m\}$, where

$$P_j = R^{-1/2} \rho_j R^{-1/2}.$$

Theorem [BARNUM AND KNILL, 2000]

$$\Pr[\text{pretty good measurement correct}] \geqslant \Pr[\text{optimal measurement correct}]^2.$$

Multiple players: LOCC identification

Suppose now that the set of states to be distinguished is **shared** between Alice and Bob:

$$\{|\psi_1\rangle, \ldots, |\psi_m\rangle\} \subset \mathcal{A} \otimes \mathcal{B}.$$

Alice and Bob would like to identify which one of these states they are given, but we will restrict their capabilities:

- Alice can perform any **local quantum operations** on her part of the given state, along with any number of additional ancillary qubits.
- Likewise for Bob.
- They can communicate with one another, but **only classically**.

This paradigm is known as **LOCC** (local operations and classical communication).

Impossibility of LOCC distinguishing Bell states

Even if the set $\{|\psi_1\rangle, \ldots, |\psi_m\rangle\}$ is orthonormal, it might **not** be possible for Alice and Bob to perfectly distinguish the states.

For example, consider the Bell states:

$$
\begin{aligned}
|\phi^+\rangle &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle \\
|\psi^+\rangle &= \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle \\
|\psi^-\rangle &= \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle
\end{aligned}
$$

These states form an orthonormal set: the Bell basis.

It is **not possible** for Alice and Bob to perfectly distinguish these states.

Impossibility of LOCC distinguishing Bell states

The proof is by contradiction. . .

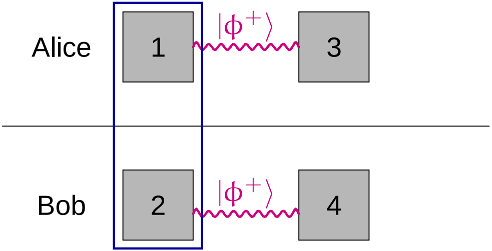
We will assume it **is possible** for Alice and Bob to perfectly distinguish the Bell states using LOCC, and conclude that this allows them to do something that is **definitely impossible**:

To **create** entanglement
using local operations and classical communication.

You may not believe that this is impossible, but trust me for now. . . it is intuitive and not difficult to prove (but you should verify it for yourself).

Impossibility of LOCC distinguishing Bell states

Suppose that Alice and Bob share four qubits as follows:



Assume Alice's two qubits and Bob's two qubits are in state

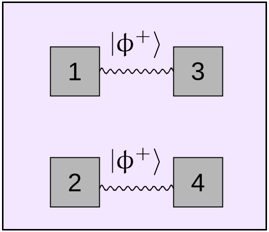
$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\,|00\rangle + \frac{1}{\sqrt{2}}\,|11\rangle\,.$$

There is **no entanglement** between Alice and Bob at this point.

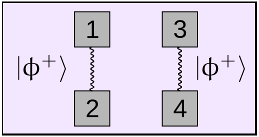
They use their LOCC protocol to measure which of the four Bell states the pair of qubits 1 and 2 are in. . .

Impossibility of LOCC distinguishing Bell states

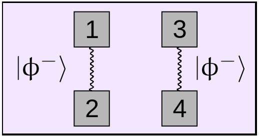
The key to analyzing what happens is the following identity:



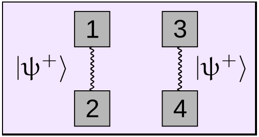
$= \frac{1}{2}$



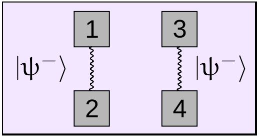
$+ \frac{1}{2}$



$+ \frac{1}{2}$

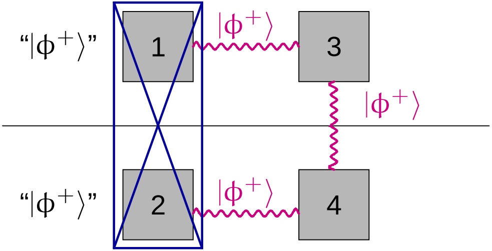


$+ \frac{1}{2}$



Impossibility of LOCC distinguishing Bell states

Consider the left-over state of the pair (3,4) after the measurement protocol is run. (Assume qubits 1 and 2 are destroyed by the measurement protocol.)



Each possible outcome appears with probability 1/4, and the state of the pair (3,4) will be identical to the state indicated by the measurement.

In all four cases, Alice and Bob are left with a known entangled state on qubits 3 and 4. . . **impossible**.

Indistinguishability of unentangled states

It is not entanglement that forbids the Bell states from being LOCC distinguished.

For example, these 9 orthogonal **product** states (the “sausage states”) **cannot** be perfectly distinguished by an LOCC procedure:

$$
\begin{aligned}
|\psi_1\rangle &= |0\rangle\,(|0\rangle + |1\rangle) & |\psi_2\rangle &= (|1\rangle + |2\rangle)\,|0\rangle \\
|\psi_3\rangle &= |0\rangle\,(|0\rangle - |1\rangle) & |\psi_4\rangle &= (|1\rangle - |2\rangle)\,|0\rangle \\
|\psi_5\rangle &= |2\rangle\,(|1\rangle + |2\rangle) & |\psi_6\rangle &= (|0\rangle + |1\rangle)\,|2\rangle \\
|\psi_7\rangle &= |2\rangle\,(|1\rangle - |2\rangle) & |\psi_8\rangle &= (|0\rangle - |1\rangle)\,|2\rangle \\
|\psi_9\rangle &= |1\rangle\,|1\rangle
\end{aligned}
$$

[Bennett, DiVincenzo, Fuchs, Mor, Rains, Shor, Smolin & Wootters, 1998].

LOCC distinguishability of any two orthogonal states

Theorem [Walgate, Short, Hardy & Vedral, 2000]

Any two orthogonal pure states $|\psi_0\rangle, |\psi_1\rangle \in \mathcal{A} \otimes \mathcal{B}$ can be perfectly distinguished by an LOCC measurement protocol.

- The idea of the proof is to show that there is a good orthonormal basis for Alice:

  $$\{|\phi_1\rangle, \ldots, |\phi_d\rangle\} \subset \mathcal{A}$$

  so that if she measures with respect to this basis then the two possibilities for Bob's left-over state are always orthogonal:

  $$(\langle\phi_i| \otimes I)|\psi_0\rangle \;\perp\; (\langle\phi_i| \otimes I)|\psi_1\rangle \qquad (\text{for all } i = 1, \ldots, d)$$

- Equivalent condition:

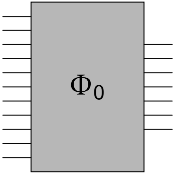
  $$\langle\phi_i| \left(\mathrm{tr}_{\mathcal{A}} |\psi_1\rangle\langle\psi_0|\right) |\phi_i\rangle = 0 \qquad (\text{for all } i = 1, \ldots, d).$$

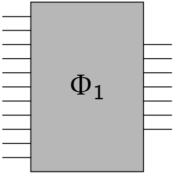
- The existence of such a basis follows from $\mathrm{tr}\left(\mathrm{tr}_{\mathcal{A}} |\psi_1\rangle\langle\psi_0|\right) = 0$ and the *Toeplitz-Hausdorff Theorem*.

Distinguishing Between Operations

Consider a similar question for **operations** rather than states.

For simplicity, let us restrict our attention to sets of just two operations:

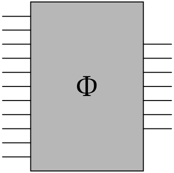




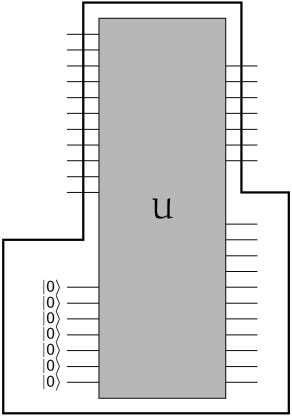
Assume that **only a single evaluation** of the given operation is permitted.

Distinguishing Between Operations

Note: it may not necessarily be the case that the operations are unitary. They might, for example, arise as follows:



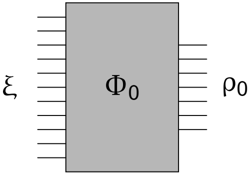
is given by

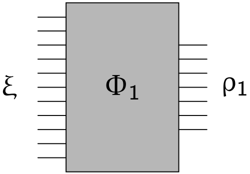


We are working with **general quantum operations** (also called admissible operations, CPSO's, etc.).

Distinguishing Between Operations

Given two such operations:





What is the best way to distinguish between them?

One possibility:

Try to optimally choose an input state ξ so that the output states ρ_0 and ρ_1 have large trace distance.

Bad choice. . .

So close and yet so far…

Let Φ_0 and Φ_1 be mappings from n qubits to n qubits defined as follows:

$$\Phi_0(X) = \frac{1}{2^n+1}\left((\operatorname{tr} X)I + X^{\mathsf{T}}\right), \ \Phi_1(X) = \frac{1}{2^n-1}\left((\operatorname{tr} X)I - X^{\mathsf{T}}\right).$$

These are both valid quantum operations.

For every mixed state ξ it holds that $\left\| \Phi_0(\xi) - \Phi_1(\xi) \right\|_{\mathrm{tr}} \leqslant \frac{4}{2^n+1}$.

Let

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle\,|i\rangle\,.$$

Then

$$\left\| (\Phi_0 \otimes I)(|\psi\rangle\langle\psi|) - (\Phi_1 \otimes I)(|\psi\rangle\langle\psi|) \right\|_{\mathrm{tr}} = 2;$$

$(\Phi_0 \otimes I)(|\psi\rangle\langle\psi|)$ and $(\Phi_1 \otimes I)(|\psi\rangle\langle\psi|)$ are **perfectly distinguishable**.

Kitaev's "diamond" norm

There is a norm defined on super-operators that perfectly handles this situation: Kitaev's "diamond" norm.

The **optimal probability** of correctly identifying which of the two operations Φ_0 and Φ_1 was given, allowing for a single evaluation on a state of arbitrary size, is

$$\Pr[\text{correct identification}] = \frac{1}{2} + \frac{1}{4} \left\| \Phi_0 - \Phi_1 \right\|_{\diamond} .$$

Kitaev's "diamond" norm has several several remarkable properties. . .

Interesting note: if Φ_0 and Φ_1 are **unitary**, then it is not necessary to use additional qubits for an optimal distinguishing procedure.

Open Questions

There are countless directions for further work relating to the topics discussed in this talk. Some examples:

1. What can be said about LOCC distinguishability of operations? (I am not aware of any work in this area.)
   For example, can Alice and Bob optimally distinguish between two unitary operations without quantum communication?
2. Obtain good bounds on the number of additional qubits needed to optimally distinguish between general quantum operations (as a function of the operations' properties).
3. There is a large body of work on LOCC distinguishability, but many specific questions are unanswered (such as identifying various properties that cause sets to not be LOCC distinguishable).