QUANTUM STATES DISTINGUISHABILITY USING LOCC

Institute for Quantum Information Science
Department of Physics and Astronomy
University of Calgary

Institute for Quantum Information Science at the University of Calgary

University of Calgary
Department of Physics and Astronomy

Informatics iCORE Circle of Research Excellence

OUTLINE

- Introduction – What is distinguishability?
- Why distinguishability?
- Locally – one party
- Locally – many parties – w/o communication
- Multi-partite with communication
- Unextendible product bases (UPBs)
- Distinguishability of a UPB

WHAT IS DISTINGUISHABILITY?

CLASSICALLY

We can (at least in principle), distinguish between the different states of an entity (e.g. a macroscopic object)

Example: A die has six distinguishable states.

WHAT IS DISTINGUISHABILITY?

QUANTUMLY

Given a state $|\phi_i\rangle$ from a set of known states $\{|\phi_i\rangle\}$, can we find a protocol that will identify with probability 100% which of the states it is? (i.e. its index *i*)

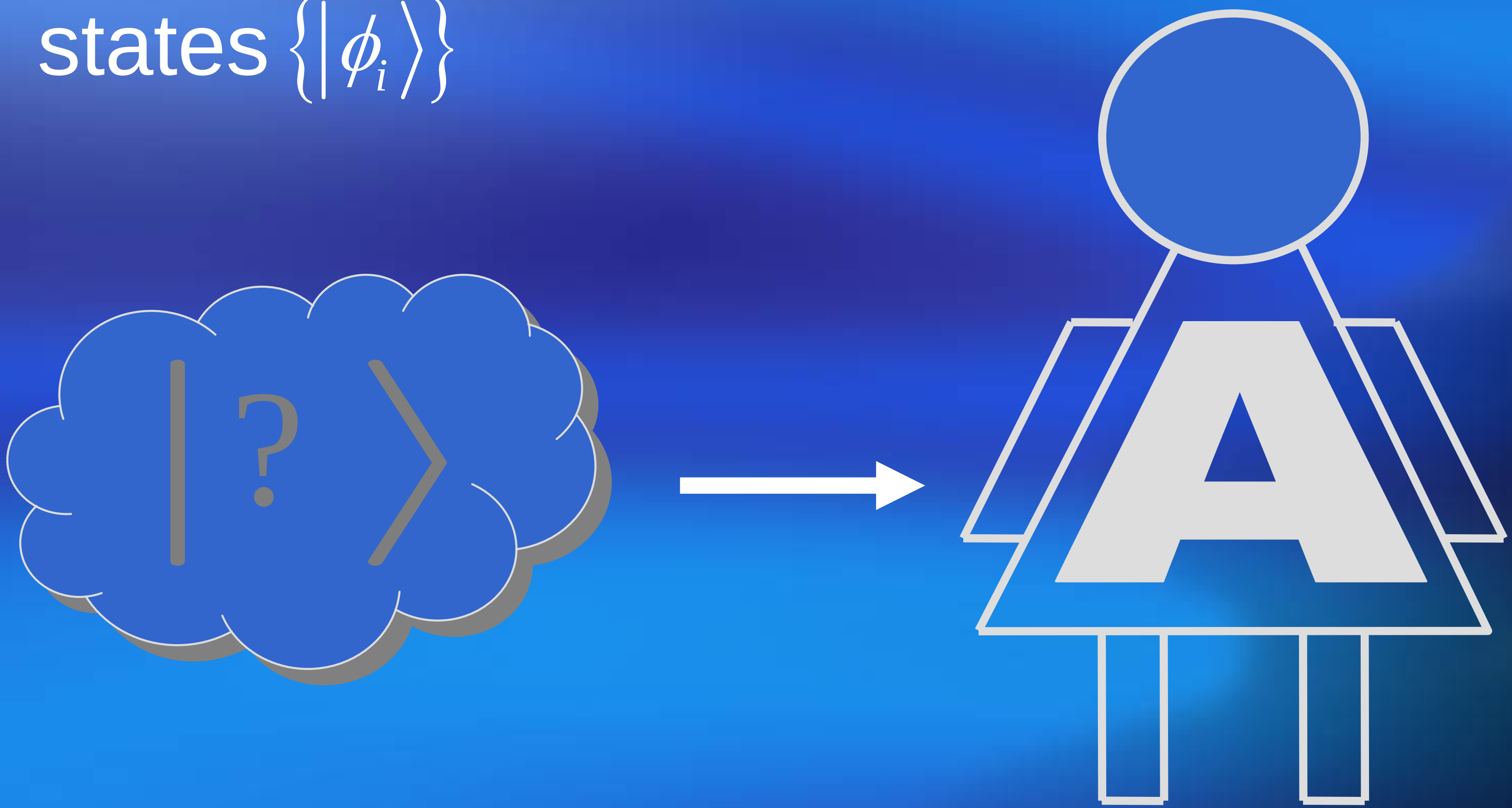
WHY DISTINGUISHABILITY?

- Distinguish different physical states → extract information
- Data hiding
- Metaphysical implications (locality/causality)
- Difference between classical and quantum communication
- Test our knowledge/comprehension of QM

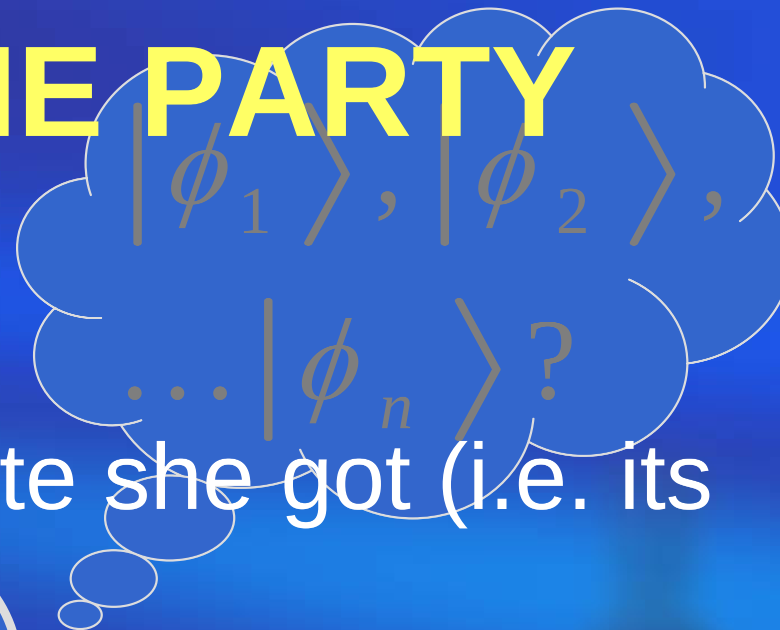
LOCALLY – ONE PARTY

SETTING

Alice is given a state $|\phi_i\rangle$ from a known set of states $\{|\phi_i\rangle\}$



LOCALLY – ONE PARTY



PROBLEM

Can Alice identify which state she got (i.e. its index *i*)?

LOCALLY – ONE PARTY

PROBLEM

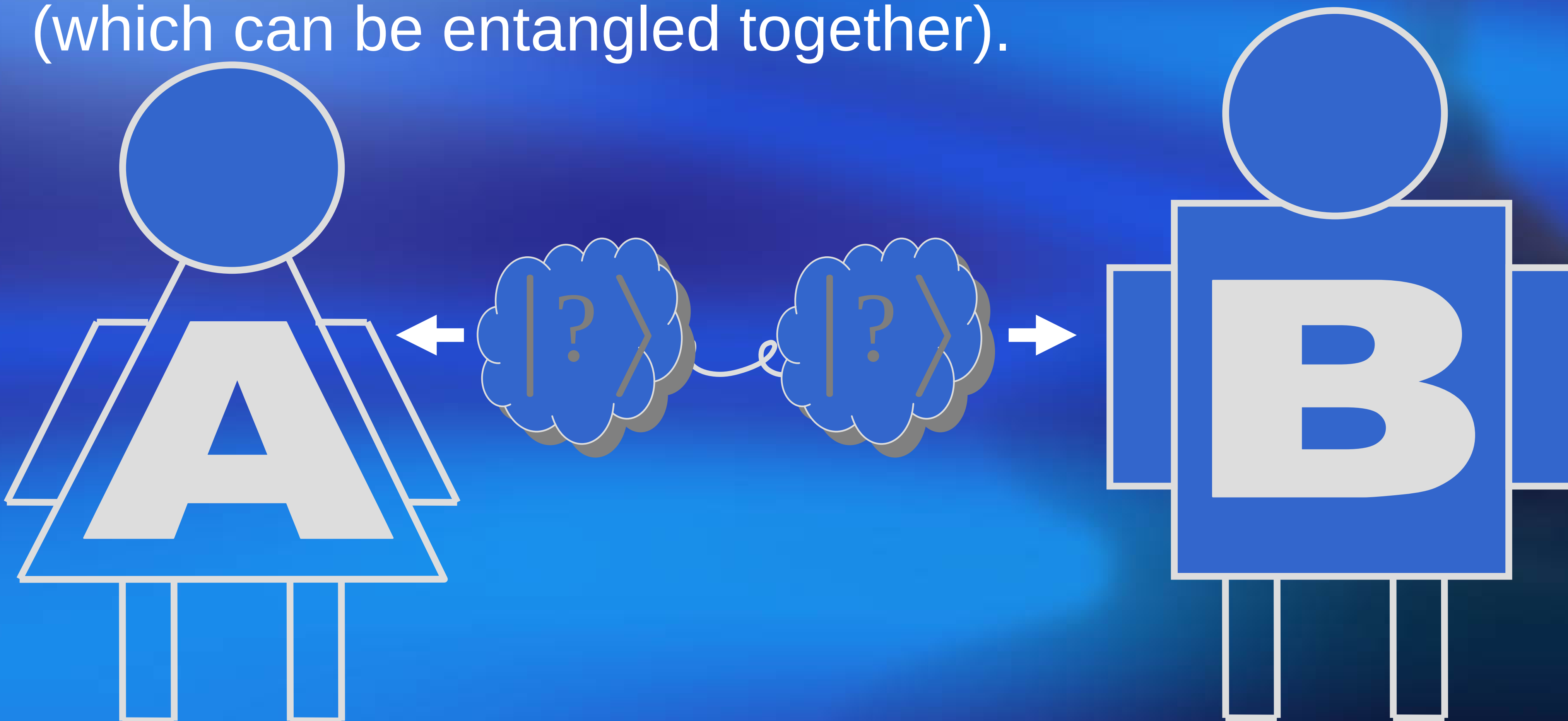
Given a state $|\phi_i\rangle$ from a set of known states $\{|\phi_i\rangle\}$, can we identify which one it is? (i.e. its index *i*)

YES, iff the $|\phi_i\rangle$s are orthogonal *(even if we consider generalized measurements i.e. POVMs)*

MULTI-PARTITE – W/O COMM.

SETTING

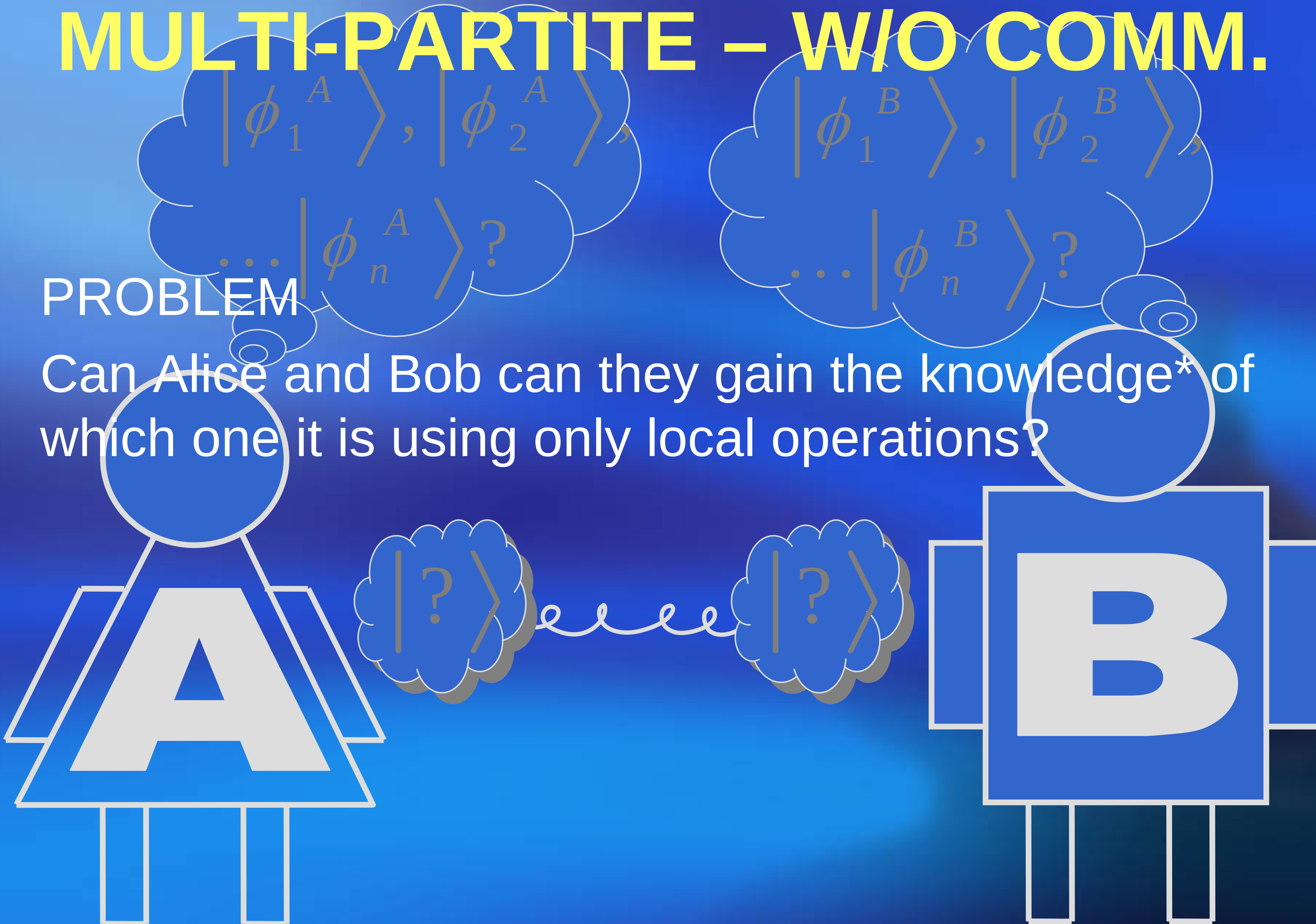
A state $\left|\phi_i\right\rangle$ from a set $\left\{\left|\phi_i\right\rangle\right\}$ is seperated into two parts. Alice and Bob are each given one part (which can be entangled together).



MULTI-PARTITE – W/O COMM.

PROBLEM

Can Alice and Bob can they gain the knowledge* of which one it is using only local operations?



MULTI-PARTITE – W/O COMM.

RESTRICTIONS

- The two parties have only one copy of their part of the state
- They can only perform local operations
- They cannot communicate

EXAMPLE 1

$$\{|\phi_i\rangle\} = \begin{cases} |\phi_1\rangle = |0\rangle_A |0\rangle_B \\ |\phi_2\rangle = |0\rangle_A |1\rangle_B \\ |\phi_3\rangle = |1\rangle_A |0\rangle_B \\ |\phi_4\rangle = |1\rangle_A |1\rangle_B \end{cases}$$

EXAMPLE 1

$$\left|\phi_1\right\rangle = \left|0\right\rangle_A \left|0\right\rangle_B$$

$$\left|\phi_2\right\rangle = \left|0\right\rangle_A \left|1\right\rangle_B$$

$$\left|\phi_3\right\rangle = \left|1\right\rangle_A \left|0\right\rangle_B$$

$$\left|\phi_4\right\rangle = \left|1\right\rangle_A \left|1\right\rangle_B$$

Alice measures in the $\{\left|0\right\rangle, \left|1\right\rangle\}$ basis and gets a 1, she now knows what was the state of the first qubit.

EXAMPLE 1

$$|\phi_1\rangle = |0\rangle_A |0\rangle_B$$

$$|\phi_2\rangle = |0\rangle_A |1\rangle_B$$

$$|\phi_3\rangle = |1\rangle_A |0\rangle_B$$

$$|\phi_4\rangle = |1\rangle_A |1\rangle_B$$

Bob measures in the same basis and gets a 0, so he knows what was the state of the second qubit. Together they know the state.

EXAMPLE 2

$$\{|\phi_i\rangle\} = \begin{cases} |\phi_1\rangle = |0\rangle_A |0\rangle_B \\ |\phi_2\rangle = |1\rangle_A |+\rangle_B \\ |\phi_3\rangle = |0\rangle_A |1\rangle_B \\ |\phi_4\rangle = |1\rangle_A |-\rangle_B \end{cases}$$

EXAMPLE 2.1

$$\left|\phi_1\right\rangle = \left|0\right\rangle_A \left|0\right\rangle_B$$

$$\left|\phi_2\right\rangle = \left|1\right\rangle_A \left|+\right\rangle_B$$

$$\left|\phi_3\right\rangle = \left|0\right\rangle_A \left|1\right\rangle_B$$

$$\left|\phi_4\right\rangle = \left|1\right\rangle_A \left|-\right\rangle_B$$

Alice measures in the $\{\left|0\right\rangle, \left|1\right\rangle\}$ basis and gets a 1, the states 1 and 3 are eliminate as known by Alice.

EXAMPLE 2.1

$$|\phi_1\rangle = \cancel{|0\rangle_A}|0\rangle_B$$

$$|\phi_2\rangle = |1\rangle_A|+\rangle_B$$

$$|\phi_3\rangle = \cancel{|0\rangle_A}|1\rangle_B$$

$$|\phi_4\rangle = |1\rangle_A|-\rangle_B$$

Now, Bob doesn't know if he should measure in the $\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\}$ basis. Even if he picks the right one, he still doesn't know if the result is right.

EXAMPLE 2.1

$$|\phi_1\rangle = \xcancel{|0\rangle_A}|0\rangle_B = \xcancel{|0\rangle_A}\left(|+\rangle_B + |-\rangle_B\right)$$

$$|\phi_2\rangle = |1\rangle_A|+\rangle_B = |1\rangle_A\left(|0\rangle_B + |1\rangle_B\right)$$

$$|\phi_3\rangle = \xcancel{|0\rangle_A}|1\rangle_B = \xcancel{|0\rangle_A}\left(|+\rangle_B - |-\rangle_B\right)$$

$$|\phi_4\rangle = |1\rangle_A|-\rangle_B = |1\rangle_A\left(|0\rangle_B - |1\rangle_B\right)$$

Now, Bob doesn't know if he should measure in the $\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\}$ basis. Even if he picks the right one, he still doesn't know if the result is right.

➔ Need for communication

EXAMPLE 2.2

$$|\phi_1\rangle = |0\rangle_A |0\rangle_B$$

$$|\phi_2\rangle = |1\rangle_A |+\rangle_B = |1\rangle_A \left(|0\rangle_B + |1\rangle_B\right)$$

$$|\phi_3\rangle = |0\rangle_A |1\rangle_B$$

$$|\phi_4\rangle = |1\rangle_A |-\rangle_B = |1\rangle_A \left(|0\rangle_B - |1\rangle_B\right)$$

Now, what about if Bob measures first? If he measures in the $\{|0\rangle, |1\rangle\}$ basis, he only eliminates one state. Same thing for $\{|+\rangle, |-\rangle\}$.

➔ Need for communication.

MULTI-PARTITE – W/ COMM.

SETTING

A state $|\phi_i\rangle$ from a set $\{|\phi_i\rangle\}$ is seperated into two parts. Alice and Bob are each given one part (which can be entangled together).

MULTI-PARTITE – W/ COMM.

$$|\phi_1\rangle, |\phi_2\rangle, \ldots |\phi_n\rangle ?$$

PROBLEM

Can Alice and Bob can they gain the knowledge* of which one it is using only local operations and classical communication?

MULTI-PARTITE – W/ COMM.

LESS RESTRICTIONS

- They have only one copy
- They can only perform local operations
- The two parties **can** communicate but only **classically** (they can't exchange qubits)

EXAMPLE 2 (revisited)

Now, If Alice and Bob call each other to schedule their measurements and Alice tells her measurement result to Bob, they can distinguish the states perfectly.

$$|\phi_1\rangle = |0\rangle_A |0\rangle_B$$

$$|\phi_2\rangle = |1\rangle_A |+\rangle_B = |1\rangle_A \left(|0\rangle_B + |1\rangle_B\right)$$

$$|\phi_3\rangle = |0\rangle_A |1\rangle_B$$

$$|\phi_4\rangle = |1\rangle_A |-\rangle_B = |1\rangle_A \left(|0\rangle_B - |1\rangle_B\right)$$

EXAMPLE 3

Bell states:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B\right)$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right)$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$$

EXAMPLE 3

1st TRY

$$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A \left|0\right\rangle_B + \left|1\right\rangle_A \left|1\right\rangle_B\right)$$

$$\left|\phi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A \left|0\right\rangle_B - \left|1\right\rangle_A \left|1\right\rangle_B\right)$$

$$\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A \left|1\right\rangle_B + \left|1\right\rangle_A \left|0\right\rangle_B\right)$$

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A \left|1\right\rangle_B - \left|1\right\rangle_A \left|0\right\rangle_B\right)$$

Alice measures in the $\{|0\rangle, |1\rangle\}$ basis and gets 0, that doesn't help them. No state is eliminated.

EXAMPLE 3

00 → $|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)$

01 → $|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B\right)$

?

10 → $|\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B\right)$

11 → $|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$

Bob measures in the same basis and gets 1, they still don't know which of two states it was. The second bit is hidden.

EXAMPLE 3

2nd TRY

$$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|0\right\rangle_B + \left|1\right\rangle_A\left|1\right\rangle_B\right)$$

$$\left|\phi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|0\right\rangle_B - \left|1\right\rangle_A\left|1\right\rangle_B\right)$$

$$\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|1\right\rangle_B + \left|1\right\rangle_A\left|0\right\rangle_B\right)$$

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|1\right\rangle_B - \left|1\right\rangle_A\left|0\right\rangle_B\right)$$

Bob measures in the $\{\left|+\right\rangle, \left|-\right\rangle\}$ basis and gets -, that eliminates 2 states

EXAMPLE 3

2nd TRY

00 → ~~$\left|\phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|0\right\rangle_B + \left|1\right\rangle_A\left|1\right\rangle_B\right)$~~

?

01 → $\left|\phi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|0\right\rangle_B - \left|1\right\rangle_A\left|1\right\rangle_B\right)$

10 → ~~$\left|\psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|1\right\rangle_B + \left|1\right\rangle_A\left|0\right\rangle_B\right)$~~

11 → $\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A\left|1\right\rangle_B - \left|1\right\rangle_A\left|0\right\rangle_B\right)$

If Alice measures in the $\{\left|+\right\rangle, \left|-\right\rangle\}$ basis then she has to get **-**. They still don't know if it was $\left|\psi^{-}\right\rangle$ or $\left|\phi^{-}\right\rangle$.

INDISTINGUISHABILITY

- The four Bell states cannot be distinguished using LOCC.
- One of the two classical bits of information will never be available to Alice and Bob.
- This is called data hiding.

UNEXTENDIBLE PRODUCT BASES

- An Unextendible Product Basis (UPB) is a basis of product states to which we cannot add any other orthogonal state lying inside our space of interest.
- An UPB is indistinguishable using only LOCC.

UPB EXAMPLE

5-dimensional subspace of $\mathcal{H}_9 = \mathcal{H}_3 \otimes \mathcal{H}_3$:

$$\left|\phi_1\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle_A \left(\left|0\right\rangle_B - \left|1\right\rangle_B\right)$$

$$\left|\phi_2\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_A - \left|1\right\rangle_A\right)\left|2\right\rangle_B$$

$$\left|\phi_3\right\rangle = \frac{1}{\sqrt{2}}\left|2\right\rangle_A \left(\left|1\right\rangle_B - \left|2\right\rangle_B\right)$$

$$\left|\phi_4\right\rangle = \frac{1}{\sqrt{2}}\left(\left|1\right\rangle_A - \left|2\right\rangle_A\right)\left|0\right\rangle_B$$

$$\left|\phi_5\right\rangle = \frac{1}{3}\left(\left|0\right\rangle_A + \left|1\right\rangle_A + \left|2\right\rangle_A\right)\left(\left|0\right\rangle_B + \left|1\right\rangle_B + \left|2\right\rangle_B\right)$$

Tiles states

A UPB OF INTEREST

4-dimensional subspace of

$\mathcal{H}_8 = \mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \mathcal{H}_2$:

$$\left|\phi_1\right\rangle = \left|0\right\rangle_A \left|0\right\rangle_B \left|0\right\rangle_C$$

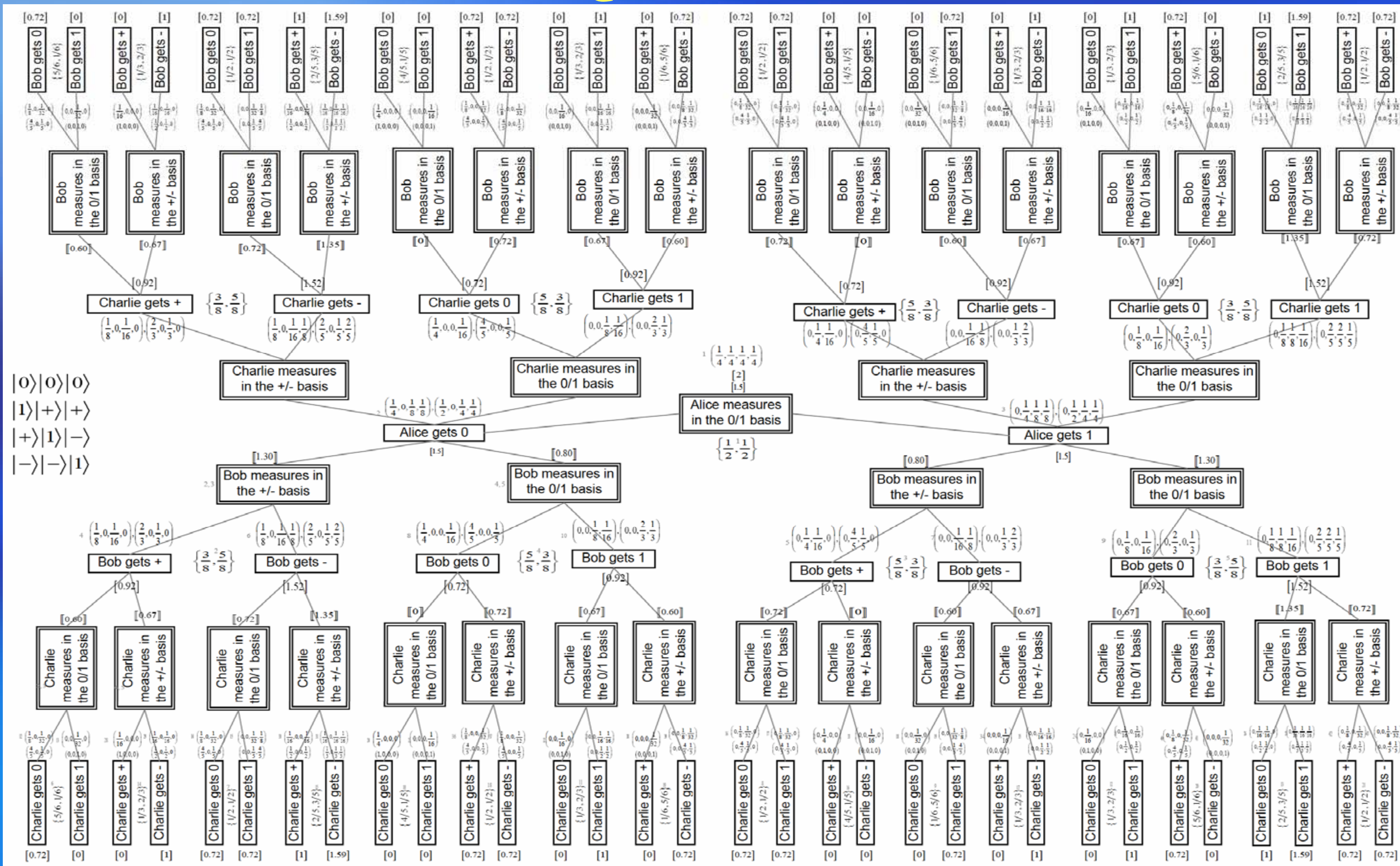
$$\left|\phi_2\right\rangle = \left|1\right\rangle_A \left|+\right\rangle_B \left|+\right\rangle_C$$

$$\left|\phi_3\right\rangle = \left|+\right\rangle_A \left|1\right\rangle_B \left|-\right\rangle_C$$

$$\left|\phi_4\right\rangle = \left|-\right\rangle_A \left|-\right\rangle_B \left|1\right\rangle_C$$

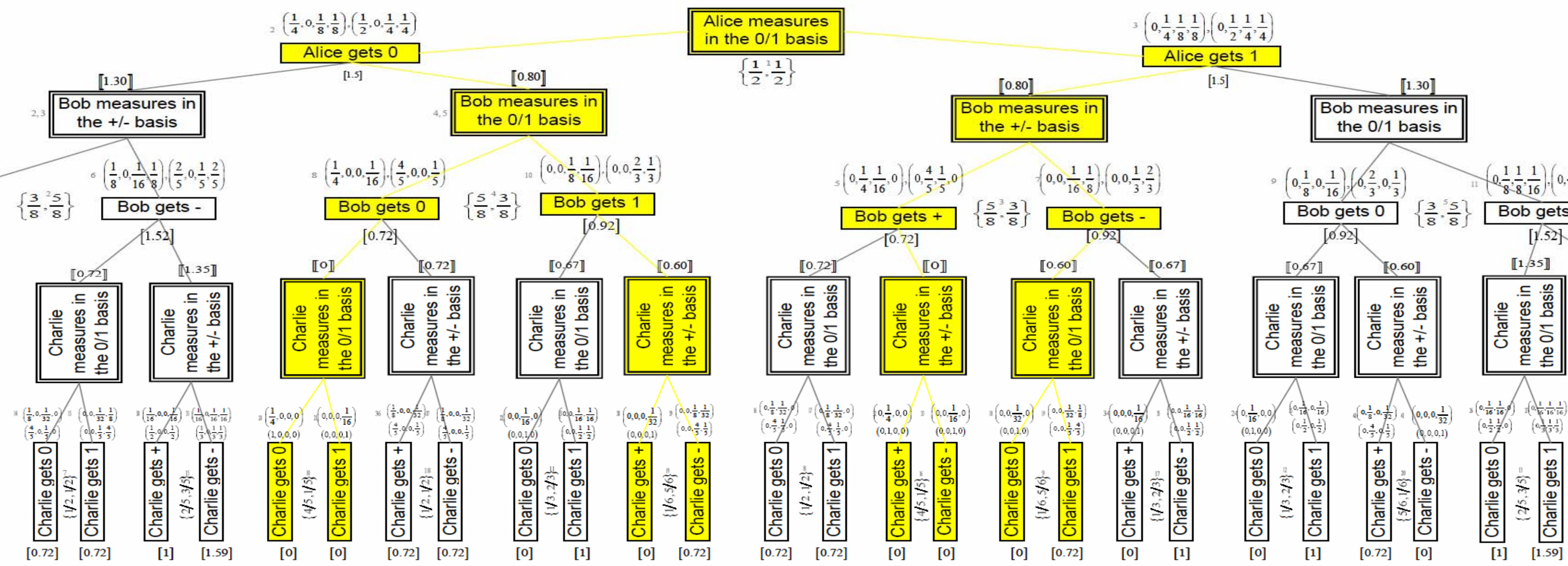
The set of four states is symmetric under permutation of A, B & C (relabeling)

DIFFERENT MEASUREMENT SEQUENCES



OPTIMAL PROTOCOL

Maximum information extraction using $\{|0\rangle,|1\rangle\}$ and $\{|+\rangle,|-\rangle\}$ measurements.



This protocol results in an average extraction of 1.775 bits of information $\left(H_{before} - H_{after}\right)$.

OPTIMAL PROTOCOL

Next step: consider POVMs and see if more information can be extracted.

Work in progress…

OTHER INTERESTING VARIATIONS

- Give multiple copies to each parties
- Communication restrictions between all or some parties
- Permit some quantum communication (transfer qubits)

INTERESTING RESULTS

- 2 orthogonal states distributed between any number of parties can be reliably distinguished (w/ probability 100%)
- Non-locality w/o entanglement
- Some states can’t be distinguished using one copy, but can using multiple copies
- Any state can be distinguished w/ *N-1* copies (for a state from a set of *N* orthogonal states)

ACKNOWLEDGEMENTS

Thank you to

Dr. Barry Sanders

Dr. Jonathan Walgate

Wan Di

REFERENCES

- C. H. Bennett et al., *PRL* **82** 5385 (1999)
- Ghosh et al., *PRL* **87** (2001)
- T.B Pedersen, *Master Thesis*, (2002)
- J. Walgate et al, *PRL* **84** (2000)
- J. Walgate, L. Hardy, *PRL* **89** (2002)