

Local Information and Nonorthogonal States

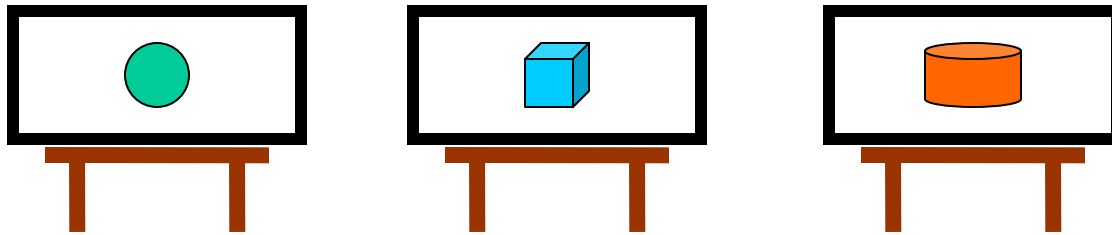
Jonathan Walgate



ALBERTA
INGENUITY
FUND



Different Things



State discrimination is the most fundamental task in physics, and in information theory.

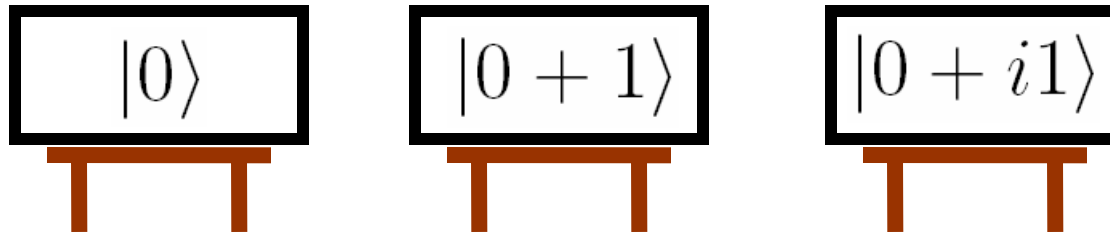
Classically, it's an easy task.

- Different classical states are completely distinguishable.

Quantum mechanically, it's not so easy.

- Orthogonal states are completely distinguishable.
- Nonorthogonal states are not completely distinguishable.

Different Things



State discrimination is the most fundamental task in physics, and in information theory.

Classically, it's an easy task.

- Different classical states are completely distinguishable.

Quantum mechanically, it's not so easy.

- Orthogonal states are completely distinguishable.
- Nonorthogonal states are not completely distinguishable.

But this isn't the only problem...

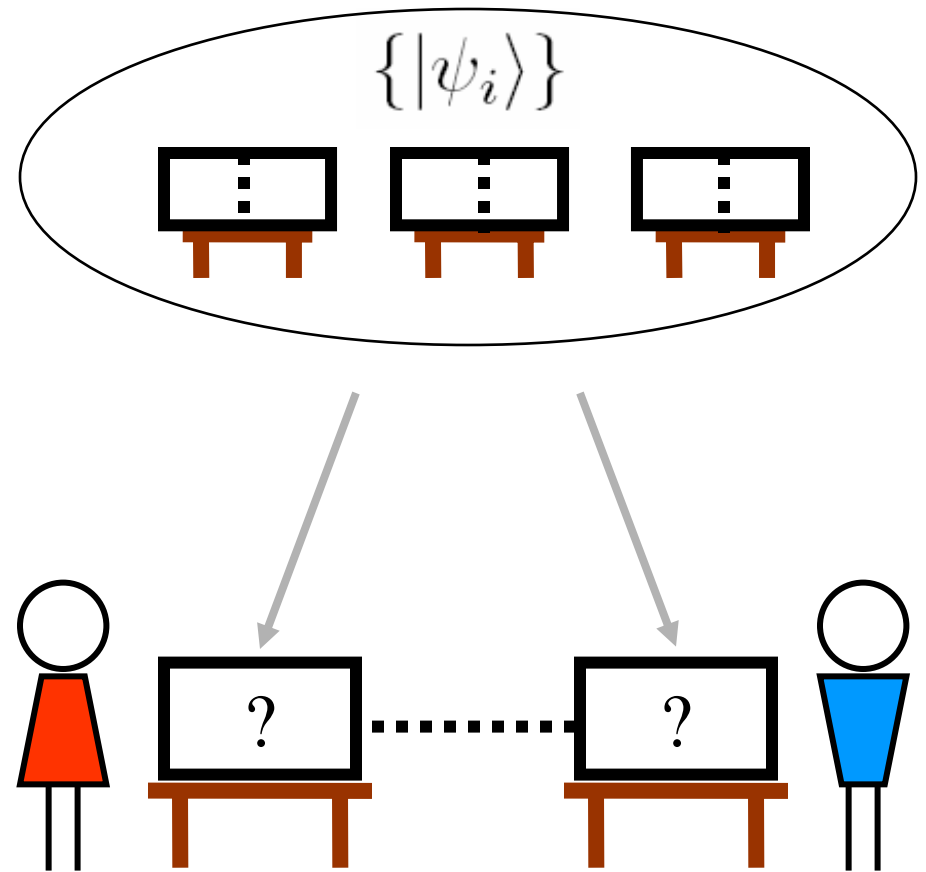
Local Indistinguishability

The system is prepared in one of n known states, $\{|\psi_i\rangle\}$.

One copy of the the system is shared between Alice and Bob.

Can Alice and Bob discover the which state they have been given, using LOCC?

Not in general, *even if the states are orthogonal.*



Local Indistinguishability

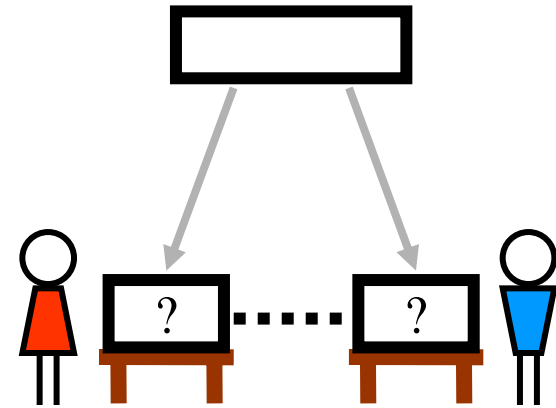
The four Bell states form a locally indistinguishable set.

$$\mathbf{00} = |\Phi^+\rangle = |0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B$$

$$\mathbf{01} = |\Phi^-\rangle = |0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B$$

$$\mathbf{10} = |\Psi^+\rangle = |0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B$$

$$\mathbf{11} = |\Psi^-\rangle = |0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B$$



If Alice or Bob project into the $\{|0\rangle, |1\rangle\}$ basis, they *delete* the second bit of information.

If Alice or Bob project into the $\{|+\rangle, |-\rangle\}$ basis, they *delete* the first bit of information.

One bit of information is hidden from local observers.

Local Indistinguishability

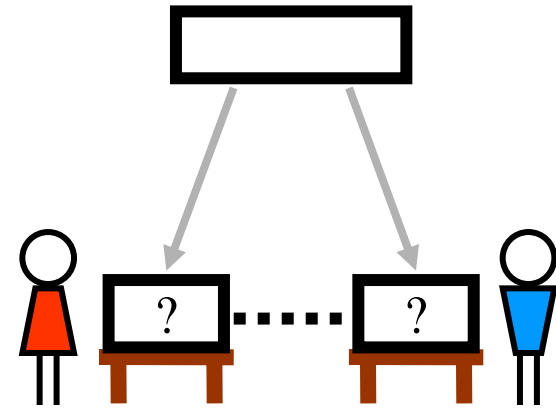
The four Bell states form a locally indistinguishable set.

$$00 = |\Phi^+\rangle = |0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B$$

$$01 = |\Phi^-\rangle = |0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B$$

$$10 = |\Psi^+\rangle = |0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B$$

$$11 = |\Psi^-\rangle = |0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B$$



- Nature of entanglement.
- Ubiquity of LOCC in quantum information theory.
- Economize quantum communication.
- Role of nonorthogonality, locality.

Local Indistinguishability

Distinguishable

Any 2 states.

JW, A. Short, L. Hardy, V. Vedral, *PRL* **84** (2000)

Any 3 states, two of which are separable.

JW, L. Hardy, *PRL* **89** (2002)

Any 3 maximally entangled states ($\dim. > 2$).

M. Nathanson, quant-ph/0411110 (2004)

Indistinguishable

A set of nine $3 \otimes 3$ product states (nonlocality without entanglement).

Bennett et al., *PRA* **59** (1999)

Three Bell states.

Ghosh et al., *PRL* **87** (2001)

LOCC and Nonorthogonality

‘Local’ nonorthogonality can render orthogonal product states indistinguishable.

Every LOCC indistinguishable set of orthogonal states can be rendered completely LOCC distinguishable simply by adding one nonorthogonal subsystem.

We can create a set of orthogonal states that are completely LOCC distinguishable, yet the only *essential* distinguishing measurement is performed on a nonorthogonal subsystem.

Building LOCC Indistinguishability

$$|\psi_1\rangle = |0\rangle_A |0\rangle_B$$

$$|\psi_2\rangle = |1\rangle_A |0\rangle_B$$

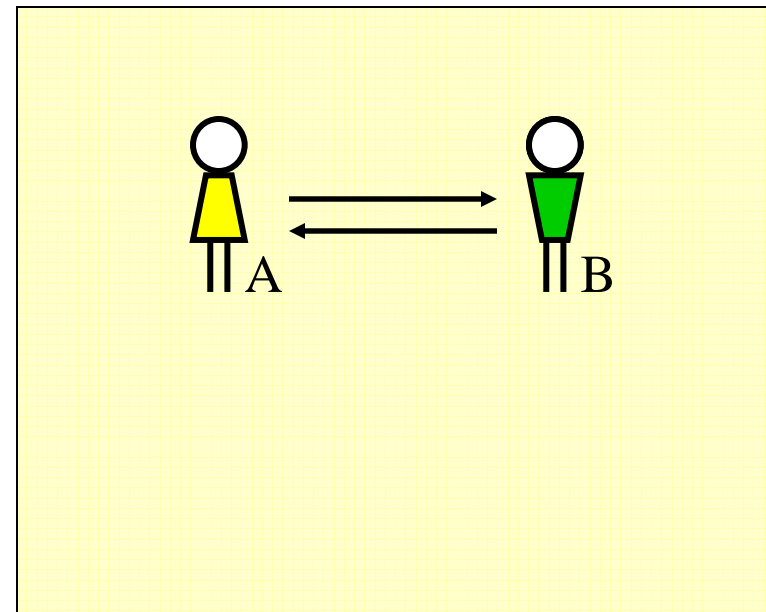
$$|\psi_3\rangle = |0\rangle_A |1\rangle_B$$

$$|\psi_4\rangle = |1\rangle_A |1\rangle_B$$

These four states exactly mimic classical behaviour.

Local projections in one basis are sufficient to perfectly distinguish between the states.

The order in which Alice and Bob measure their qubits doesn't matter.



Building LOCC Indistinguishability

$$|\psi_1\rangle = |0\rangle_A |0\rangle_B$$

$$|\psi_2\rangle = |1\rangle_A |+\rangle_B \quad \leftrightarrow$$

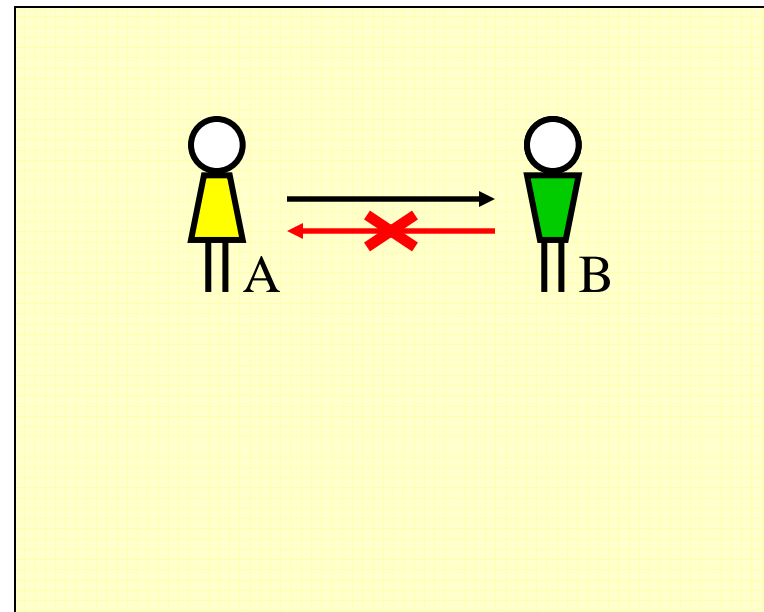
$$|\psi_3\rangle = |0\rangle_A |1\rangle_B$$

$$|\psi_4\rangle = |1\rangle_A |-\rangle_B \quad \leftrightarrow$$

These orthogonal states behave nonclassically.

The order in which Alice and Bob measure their qubits *does* matter.

Alice *has* to measure before Bob, or else the states are indistinguishable!



Building LOCC Indistinguishability

$$|\psi_1\rangle = |0\rangle_A |0\rangle_B |0\rangle_C,$$

$$|\psi_2\rangle = |1\rangle_A |+\rangle_B |+\rangle_C,$$

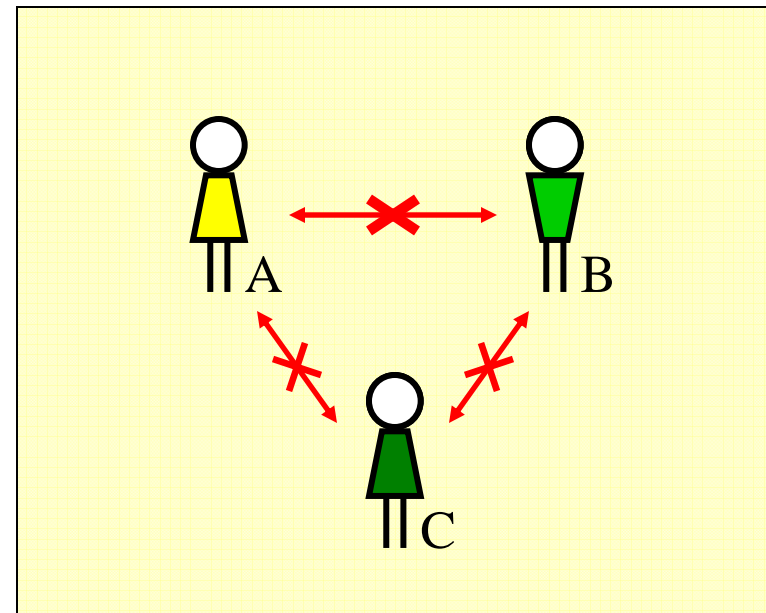
$$|\psi_3\rangle = |+\rangle_A |1\rangle_B |-\rangle_C,$$

$$|\psi_4\rangle = |-\rangle_A |-\rangle_B |1\rangle_C.$$

These orthogonal tripartite states are locally indistinguishable.

No qubit can be measured without disturbing the system into a set of globally nonorthogonal states.

'Nonlocality without entanglement.'



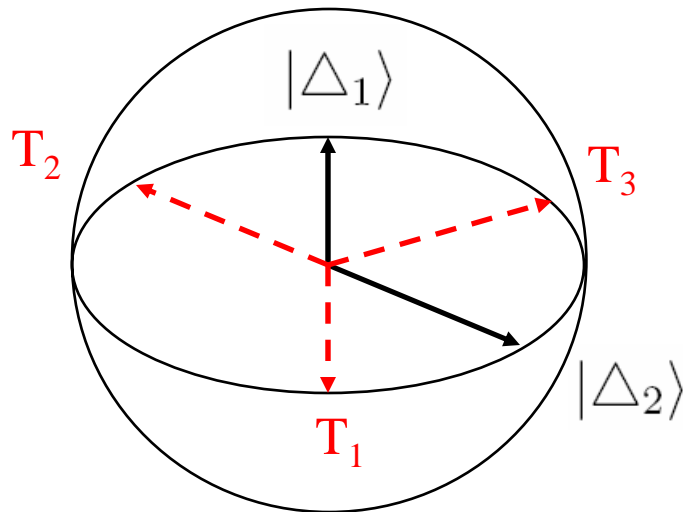
LOCC and Nonorthogonality

‘Local’ nonorthogonality can render orthogonal product states indistinguishable.

Every LOCC indistinguishable set of orthogonal states can be rendered completely LOCC distinguishable by adding just *one* nonorthogonal subsystem.

We can create a set of orthogonal states that are completely LOCC distinguishable, yet the only *essential* distinguishing measurement is performed on a nonorthogonal subsystem.

Conclusive Qubit Measurements



$$|\Delta_1\rangle = |0\rangle,$$

$$|\Delta_2\rangle = \cos \frac{\pi}{3} |0\rangle + \sin \frac{\pi}{3} |1\rangle$$

$$T_1^\dagger T_1 = \frac{2}{3} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

Qubit was not in state $|\Delta_1\rangle$.

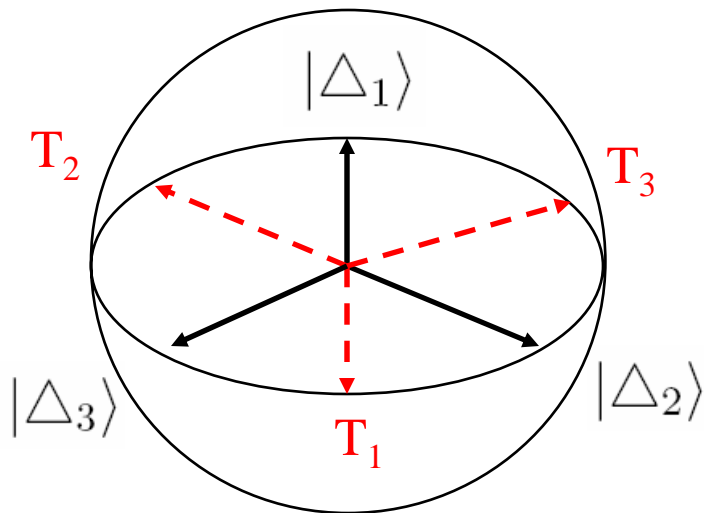
$$T_2^\dagger T_2 = \frac{2}{3} \begin{pmatrix} \frac{3}{4} & -\frac{\sqrt{3}}{4} \\ -\frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix},$$

Qubit was not in state $|\Delta_2\rangle$.

$$T_3^\dagger T_3 = \frac{2}{3} \begin{pmatrix} \frac{3}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix}.$$

Inconclusive.

Conclusive Qubit Measurements



$$|\Delta_1\rangle = |0\rangle,$$

$$|\Delta_2\rangle = \cos \frac{\pi}{3} |0\rangle + \sin \frac{\pi}{3} |1\rangle,$$

$$|\Delta_3\rangle = \cos \frac{\pi}{3} |0\rangle - \sin \frac{\pi}{3} |1\rangle.$$

$$T_1^\dagger T_1 = \frac{2}{3} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

Qubit was not in state $|\Delta_1\rangle$.

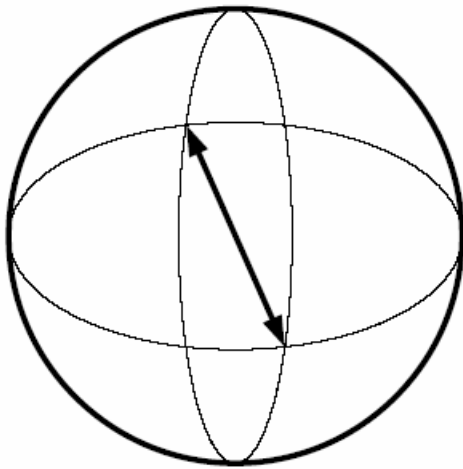
$$T_2^\dagger T_2 = \frac{2}{3} \begin{pmatrix} \frac{3}{4} & -\frac{\sqrt{3}}{4} \\ -\frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix},$$

Qubit was not in state $|\Delta_2\rangle$.

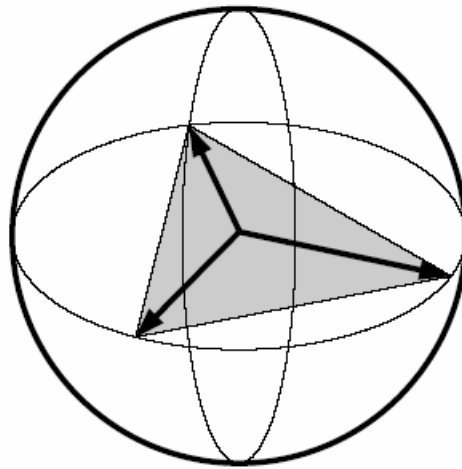
$$T_3^\dagger T_3 = \frac{2}{3} \begin{pmatrix} \frac{3}{4} & \frac{\sqrt{3}}{4} \\ \frac{\sqrt{3}}{4} & \frac{1}{4} \end{pmatrix}.$$

Qubit was not in state $|\Delta_3\rangle$.

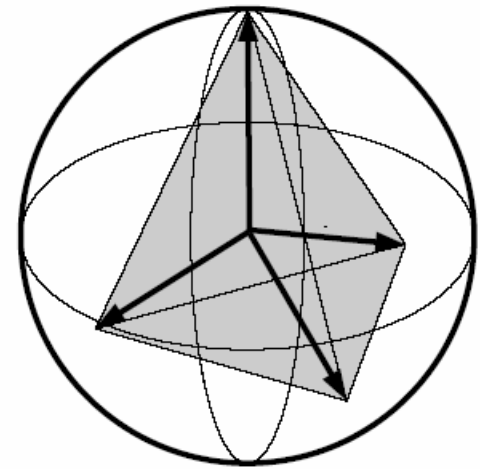
Conclusive Qubit Measurements



Two State Eliminations



Three State Eliminations



Four State Eliminations

A conclusive ‘elimination’ measurement: $\{M_i\} : \sum_i M_i^\dagger M_i = 1$
upon a set of states $\{|\psi_i\rangle\}$ always satisfies the following:

$$\langle \psi_i | M_i^\dagger M_i | \psi_i \rangle = 0$$

Building Sets of Qubits

Theorem: Let n and m be any positive integers. A set of n m -partite quantum states $\{|\psi_i\rangle\}$ can be constructed with the following properties:

The states are completely nonorthogonal: $\forall i, j \quad \langle \psi_i | \psi_j \rangle \neq 0$.

A measurement exists every outcome of which has zero expectation value for all but two members of $\{|\psi_i\rangle\}$.

Sketch of proof:

If there are n states, then there are ${}^n C_3$ triplets of states.

Use trine states:

$$\begin{aligned} |\Delta_1\rangle &= |0\rangle, \\ |\Delta_2\rangle &= \cos \frac{\pi}{3} |0\rangle + \sin \frac{\pi}{3} |1\rangle, \\ |\Delta_3\rangle &= \cos \frac{\pi}{3} |0\rangle - \sin \frac{\pi}{3} |1\rangle. \end{aligned}$$

Building Sets of Qubits

$$|\psi_1\rangle = |\Delta_1\rangle_A$$

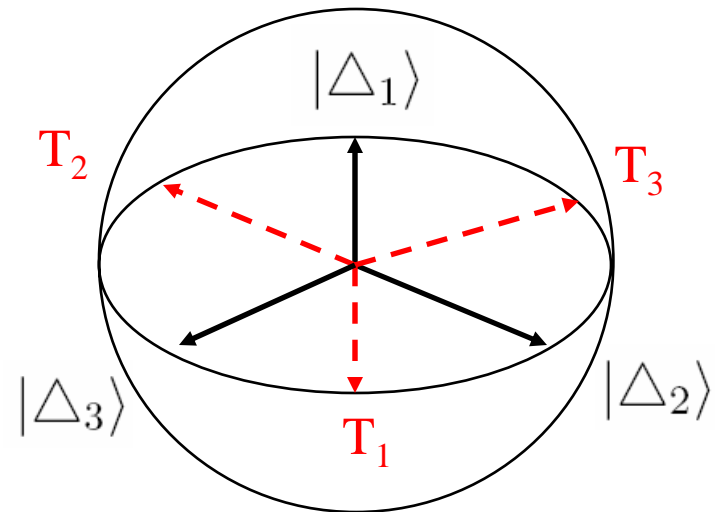
$$|\psi_2\rangle = |\Delta_2\rangle_A$$

$$|\psi_3\rangle = |\Delta_3\rangle_A$$

$$|\psi_4\rangle = |\Delta_1\rangle_A$$

$$|\psi_5\rangle = |\Delta_2\rangle_A$$

$$|\psi_6\rangle = |\Delta_3\rangle_A$$



Nonorthogonal states yield definite information with certainty.

We can always rule out $n - 2$ possible states.

- Number of qubits required increases with n .
- No multipartite constraint.

Building Sets of Qubits

$$|\psi_1\rangle = |\Delta_1\rangle_A |\Delta_1\rangle_B$$

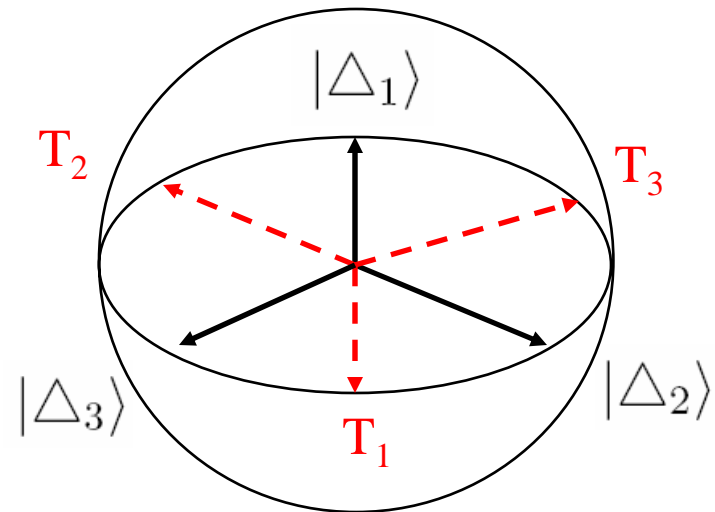
$$|\psi_2\rangle = |\Delta_2\rangle_A |\Delta_2\rangle_B$$

$$|\psi_3\rangle = |\Delta_3\rangle_A |\Delta_3\rangle_B$$

$$|\psi_4\rangle = |\Delta_1\rangle_A |\Delta_2\rangle_B$$

$$|\psi_5\rangle = |\Delta_2\rangle_A |\Delta_3\rangle_B$$

$$|\psi_6\rangle = |\Delta_3\rangle_A |\Delta_1\rangle_B$$



Nonorthogonal states yield definite information with certainty.

We can always rule out $n - 2$ possible states.

- Number of qubits required increases with n .
- No multipartite constraint.

Building Sets of Qubits

$$|\psi_1\rangle = |\Delta_1\rangle_A |\Delta_1\rangle_B |\Delta_1\rangle_C,$$

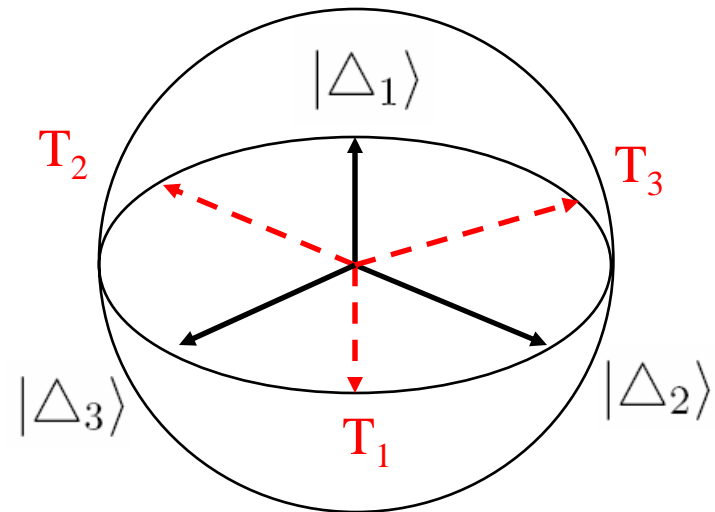
$$|\psi_2\rangle = |\Delta_2\rangle_A |\Delta_2\rangle_B |\Delta_2\rangle_C,$$

$$|\psi_3\rangle = |\Delta_3\rangle_A |\Delta_3\rangle_B |\Delta_3\rangle_C,$$

$$|\psi_4\rangle = |\Delta_1\rangle_A |\Delta_2\rangle_B |\Delta_3\rangle_C,$$

$$|\psi_5\rangle = |\Delta_2\rangle_A |\Delta_3\rangle_B |\Delta_1\rangle_C,$$

$$|\psi_6\rangle = |\Delta_3\rangle_A |\Delta_1\rangle_B |\Delta_2\rangle_C.$$



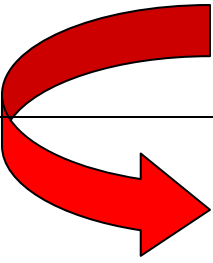
Nonorthogonal states yield definite information with certainty.

We can always rule out $n - 2$ possible states.

- Number of qubits required increases with n .
- No multipartite constraint.

Any Two States are Distinguishable

JW, A. Short, L. Hardy, V. Vedral, *PRL* **84** (2000)

	$ \Psi_1\rangle = \sum_i a_i i\rangle_A \eta_i\rangle_{BCD\dots}$ $ \Psi_2\rangle = \sum_i b_i i\rangle_A \nu_i\rangle_{BCD\dots}$
<p>Alice can always change her basis.</p>	 $ \Psi_1\rangle = \sum_j c_j j\rangle_A \eta_j\rangle_{BCD\dots}$ $ \Psi_2\rangle = \sum_j d_j j\rangle_A \eta_j^\perp\rangle_{BCD\dots}$

Distinguishability via Nonorthogonality

Theorem: Let $\{|\psi_i\rangle\}$ be any set of n LOCC *indistinguishable* orthogonal states. There exists an extended set of n states $\{|\psi_i\rangle \otimes |\phi_i\rangle\}$ such that the states $\{|\phi_i\rangle\}$ are completely nonorthogonal, and the extended set of states $\{|\psi_i\rangle \otimes |\phi_i\rangle\}$ is completely locally distinguishable.

Proof:

Let $\{|\phi_i\rangle\}$ be an $n - 2$ eliminable set of trine states.

Measuring only the states $\{|\phi_i\rangle\}$ we can narrow down to two possibilities, $|\psi_x\rangle \otimes |\phi_x\rangle$ or $|\psi_y\rangle \otimes |\phi_y\rangle$.

$|\psi_x\rangle$ and $|\psi_y\rangle$ are still orthogonal, and so can be LOCC distinguished. \square

Locally Distinguishing Bell States

$$|\Phi^+\rangle = (|00\rangle_{AB} + |11\rangle_{AB})$$

$$|\Phi^-\rangle = (|00\rangle_{AB} - |11\rangle_{AB})$$

$$|\Psi^+\rangle = (|01\rangle_{AB} + |10\rangle_{AB})$$

$$|\Psi^-\rangle = (|01\rangle_{AB} - |10\rangle_{AB})$$

The Bell states are locally indistinguishable.

Two bits of information are locally hidden – they are physically real, but cannot be discovered by LOCC.

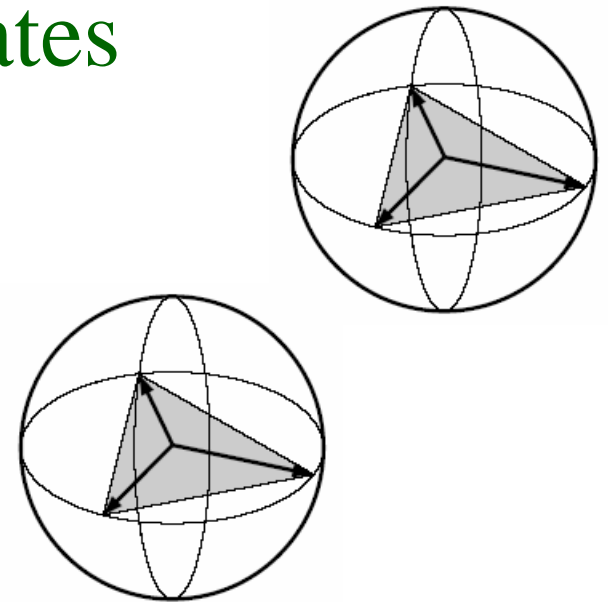
Locally Distinguishing Bell States

$$|\Phi^+\rangle = (|00\rangle_{AB} + |11\rangle_{AB}) \otimes |\Delta_1\Delta_1\rangle_C,$$

$$|\Phi^-\rangle = (|00\rangle_{AB} - |11\rangle_{AB}) \otimes |\Delta_1\Delta_2\rangle_C,$$

$$|\Psi^+\rangle = (|01\rangle_{AB} + |10\rangle_{AB}) \otimes |\Delta_2\Delta_3\rangle_C,$$

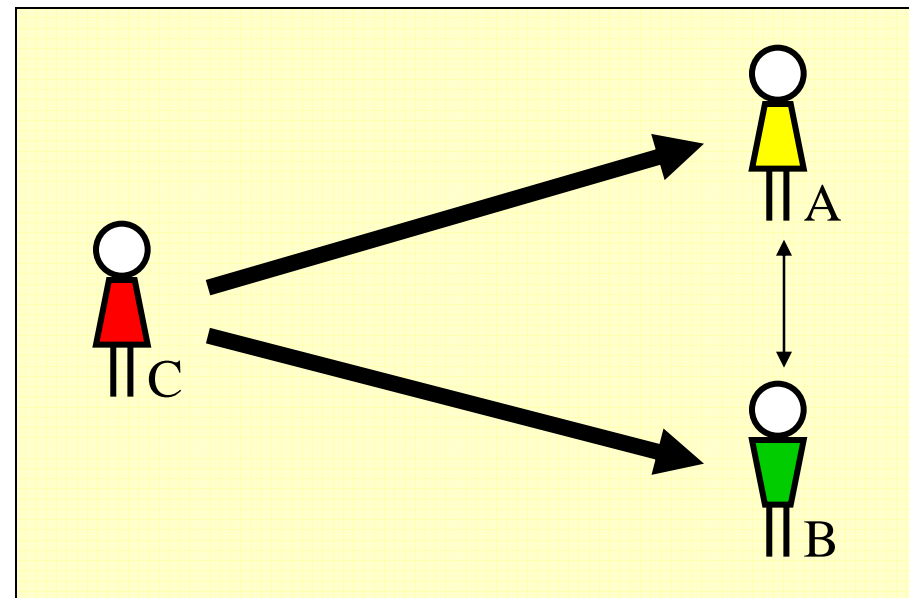
$$|\Psi^-\rangle = (|01\rangle_{AB} - |10\rangle_{AB}) \otimes |\Delta_3\Delta_3\rangle_C.$$



We can introduce a third party, Carol, to reveal the hidden information.

Globally, Carol holds nothing of value, as her possible states are all nonorthogonal.

Locally, Carol is vital – only she can reveal the locally hidden information to Alice, Bob and Carol.



Nonlocality without Entanglement

$$|\psi_1\rangle = |0\rangle_A |0\rangle_B |0\rangle_C$$

$$|\psi_2\rangle = |1\rangle_A |+\rangle_B |+\rangle_C$$

$$|\psi_3\rangle = |+\rangle_A |1\rangle_B |-\rangle_C$$

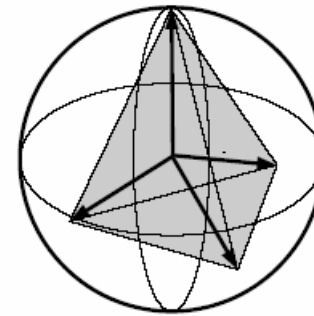
$$|\psi_4\rangle = |-\rangle_A |-\rangle_B |1\rangle_C$$

These $2 \otimes 2 \otimes 2$ product states mimic the Bell state structure: any local measurement by Alice, Bob or Carol will render one of the six pairs of states indistinguishable.

Two bits of information are locally hidden – they are physically real, but cannot be discovered by LOCC.

Nonlocality without Entanglement

$$\begin{aligned} |\psi_1\rangle &= |0\rangle_A |0\rangle_B |0\rangle_C \otimes |\Delta_1\rangle_D, \\ |\psi_2\rangle &= |1\rangle_A |+\rangle_B |+\rangle_C \otimes |\Delta_2\rangle_D, \\ |\psi_3\rangle &= |+\rangle_A |1\rangle_B |-\rangle_C \otimes |\Delta_3\rangle_D, \\ |\psi_4\rangle &= |-\rangle_A |-\rangle_B |1\rangle_C \otimes |\Delta_4\rangle_D. \end{aligned}$$

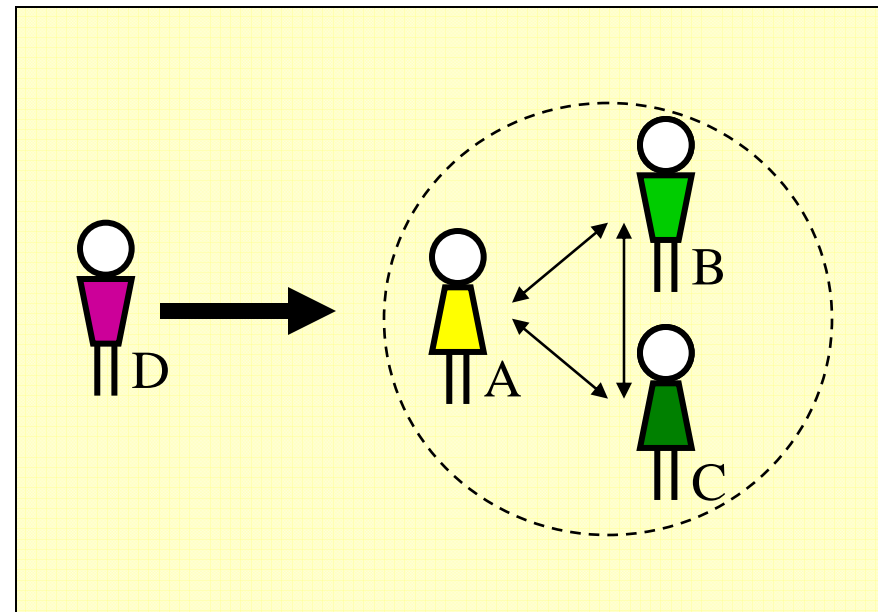


It only takes one more qubit to reveal the information.

After David measures, he can communicate the result to anyone else.

Based on the result of their measurement, one party will not be needed.

David, however, is always needed.



Complex Distinguishability

$$\begin{aligned}
 0000 &= |0\rangle_A |0\rangle_B |0\rangle_C |0\rangle_D |0\rangle_E |\Delta_1\rangle_F |0\rangle_G |0\rangle_H |0\rangle_I, \\
 0001 &= |0\rangle_A |0\rangle_B |1\rangle_C |+\rangle_D |+\rangle_E |\Delta_2\rangle_F |0\rangle_G |0\rangle_H |0\rangle_I, \\
 0010 &= |0\rangle_A |0\rangle_B |+\rangle_C |1\rangle_D |-\rangle_E |\Delta_3\rangle_F |0\rangle_G |0\rangle_H |0\rangle_I, \\
 0011 &= |0\rangle_A |0\rangle_B |-\rangle_C |-\rangle_D |1\rangle_E |\Delta_4\rangle_F |0\rangle_G |0\rangle_H |0\rangle_I, \\
 0100 &= |0\rangle_A |1\rangle_B |0\rangle_C |0\rangle_D |0\rangle_E |\Delta_1\rangle_F |1\rangle_G |+\rangle_H |+\rangle_I, \\
 0101 &= |0\rangle_A |1\rangle_B |1\rangle_C |+\rangle_D |+\rangle_E |\Delta_2\rangle_F |1\rangle_G |+\rangle_H |+\rangle_I, \\
 0110 &= |0\rangle_A |1\rangle_B |+\rangle_C |1\rangle_D |-\rangle_E |\Delta_3\rangle_F |1\rangle_G |+\rangle_H |+\rangle_I, \\
 0111 &= |0\rangle_A |1\rangle_B |-\rangle_C |-\rangle_D |1\rangle_E |\Delta_4\rangle_F |1\rangle_G |+\rangle_H |+\rangle_I, \\
 1000 &= |1\rangle_A |+\rangle_B |0\rangle_C |0\rangle_D |0\rangle_E |\Delta_1\rangle_F |+\rangle_G |1\rangle_H |-\rangle_I, \\
 1001 &= |1\rangle_A |+\rangle_B |1\rangle_C |+\rangle_D |+\rangle_E |\Delta_2\rangle_F |+\rangle_G |1\rangle_H |-\rangle_I, \\
 1010 &= |1\rangle_A |+\rangle_B |+\rangle_C |1\rangle_D |-\rangle_E |\Delta_3\rangle_F |+\rangle_G |1\rangle_H |-\rangle_I, \\
 1011 &= |1\rangle_A |+\rangle_B |-\rangle_C |-\rangle_D |1\rangle_E |\Delta_4\rangle_F |+\rangle_G |1\rangle_H |-\rangle_I, \\
 1100 &= |1\rangle_A |-\rangle_B |0\rangle_C |0\rangle_D |0\rangle_E |\Delta_1\rangle_F |-\rangle_G |-\rangle_H |1\rangle_I, \\
 1101 &= |1\rangle_A |-\rangle_B |1\rangle_C |+\rangle_D |+\rangle_E |\Delta_2\rangle_F |-\rangle_G |-\rangle_H |1\rangle_I, \\
 1110 &= |1\rangle_A |-\rangle_B |+\rangle_C |1\rangle_D |-\rangle_E |\Delta_3\rangle_F |-\rangle_G |-\rangle_H |1\rangle_I, \\
 1111 &= |1\rangle_A |-\rangle_B |-\rangle_C |-\rangle_D |1\rangle_E |\Delta_4\rangle_F |-\rangle_G |-\rangle_H |1\rangle_I.
 \end{aligned}$$

Very simple states:

- Pure
- Separable
- Orthogonal
- Qubits

Are these 16 states
locally distinguishable?

Complex Distinguishability

$$\begin{aligned} 0000 &= |0\rangle_A |0\rangle_B |0\rangle_C |0\rangle_D |0\rangle_E |\Delta_1\rangle_F |0\rangle_G |0\rangle_H |0\rangle_I, \\ 0001 &= |0\rangle_A |0\rangle_B |1\rangle_C |+\rangle_D |+\rangle_E |\Delta_2\rangle_F |0\rangle_G |0\rangle_H |0\rangle_I, \\ 0010 &= |0\rangle_A |0\rangle_B |+\rangle_C |1\rangle_D |-\rangle_E |\Delta_3\rangle_F |0\rangle_G |0\rangle_H |0\rangle_I, \\ 0011 &= |0\rangle_A |0\rangle_B |-\rangle_C |-\rangle_D |1\rangle_E |\Delta_4\rangle_F |0\rangle_G |0\rangle_H |0\rangle_I, \\ 0100 &= |0\rangle_A |1\rangle_B |0\rangle_C |0\rangle_D |0\rangle_E |\Delta_1\rangle_F |1\rangle_G |+\rangle_H |+\rangle_I, \\ 0101 &= |0\rangle_A |1\rangle_B |1\rangle_C |+\rangle_D |+\rangle_E |\Delta_2\rangle_F |1\rangle_G |+\rangle_H |+\rangle_I, \\ 0110 &= |0\rangle_A |1\rangle_B |+\rangle_C |1\rangle_D |-\rangle_E |\Delta_3\rangle_F |1\rangle_G |+\rangle_H |+\rangle_I, \\ 0111 &= |0\rangle_A |1\rangle_B |-\rangle_C |-\rangle_D |1\rangle_E |\Delta_4\rangle_F |1\rangle_G |+\rangle_H |+\rangle_I, \\ 1000 &= |1\rangle_A |+\rangle_B |0\rangle_C |0\rangle_D |0\rangle_E |\Delta_1\rangle_F |+\rangle_G |1\rangle_H |-\rangle_I, \\ 1001 &= |1\rangle_A |+\rangle_B |1\rangle_C |+\rangle_D |+\rangle_E |\Delta_2\rangle_F |+\rangle_G |1\rangle_H |-\rangle_I, \\ 1010 &= |1\rangle_A |+\rangle_B |+\rangle_C |1\rangle_D |-\rangle_E |\Delta_3\rangle_F |+\rangle_G |1\rangle_H |-\rangle_I, \\ 1011 &= |1\rangle_A |+\rangle_B |-\rangle_C |-\rangle_D |1\rangle_E |\Delta_4\rangle_F |+\rangle_G |1\rangle_H |-\rangle_I, \\ 1100 &= |1\rangle_A |-\rangle_B |0\rangle_C |0\rangle_D |0\rangle_E |\Delta_1\rangle_F |-\rangle_G |-\rangle_H |1\rangle_I, \\ 1101 &= |1\rangle_A |-\rangle_B |1\rangle_C |+\rangle_D |+\rangle_E |\Delta_2\rangle_F |-\rangle_G |-\rangle_H |1\rangle_I, \\ 1110 &= |1\rangle_A |-\rangle_B |+\rangle_C |1\rangle_D |-\rangle_E |\Delta_3\rangle_F |-\rangle_G |-\rangle_H |1\rangle_I, \\ 1111 &= |1\rangle_A |-\rangle_B |-\rangle_C |-\rangle_D |1\rangle_E |\Delta_4\rangle_F |-\rangle_G |-\rangle_H |1\rangle_I. \end{aligned}$$

Very simple states:

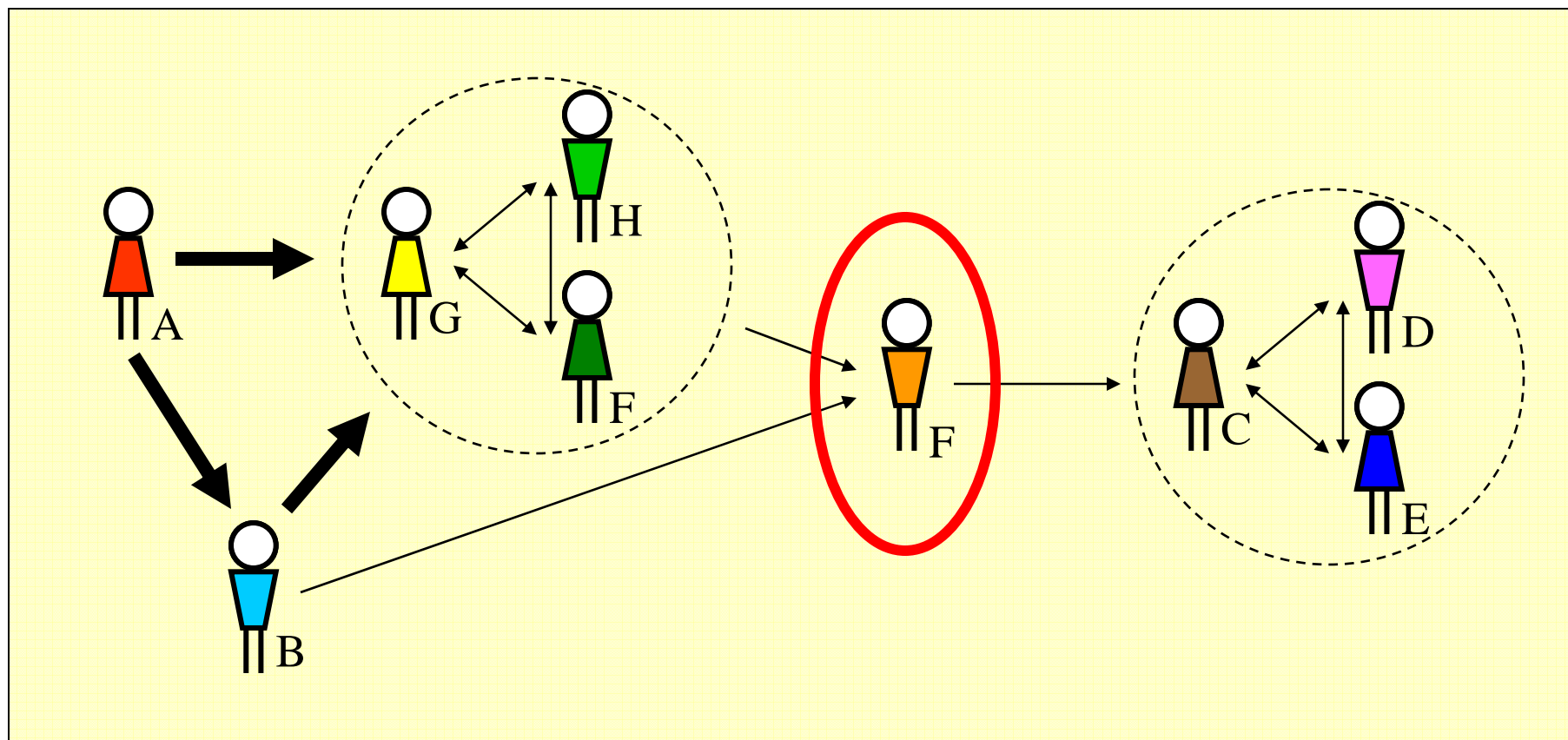
- Pure
- Separable
- Orthogonal
- Qubits

Are these 16 states
locally distinguishable?

Yes.

But only with the help
of Fred!

Complex Distinguishability



We can use nonorthogonality to create almost arbitrarily Byzantine local data hiding networks, even with qubit product states.

Nonorthogonality is vitally important for LOCC distinguishability.