Introduction to Quantum Information Processing

QIC 710 / CS 678 / PH 767 / CO 681 / AM 871

Lectures 12–13 (2013)

Richard Cleve
DC 2117 / QNC 3129
cleve@cs.uwaterloo.ca

Recap ...

Characterizing density matrices

$$\rho = \sum_{k=1}^{d} p_k |\psi_k\rangle\langle\psi_k|$$

Three properties of ρ :

- $\mathrm{Tr}\rho = 1$ ($\mathrm{Tr}M = M_{11} + M_{22} + \ldots + M_{dd}$)
- $\rho = \rho^{\dagger}$ (i.e. ρ is *Hermitian)*
- $\langle\varphi|\rho|\varphi\rangle \geq 0$, for all states $|\varphi\rangle$ (i.e. ρ is *positive semidefinite*)

Moreover, for ***any*** matrix ρ satisfying the above properties, there exists a probabilistic mixture whose density matrix is ρ

Exercise: show this

Recap of general quantum operations

General quantum operations (1)

Also known as:
"quantum channels"
"completely positive trace preserving maps",
"admissible operations"

Let $A_1, A_2, \ldots, A_m$ be matrices satisfying $\sum_{j=1}^{m} A_j^\dagger A_j = I$

Then the mapping $\rho \mapsto \sum_{j=1}^{m} A_j \rho A_j^\dagger$ is a general quantum op

Note: $A_1, A_2, \ldots, A_m$ do not have to be square matrices

Example 1 (unitary op): applying U to ρ yields $U\rho U^\dagger$

General quantum operations (2)

Example 2 (decoherence): let $A_0 = |0\rangle\langle 0|$ and $A_1 = |1\rangle\langle 1|$

This quantum op maps ρ to $|0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|$

For $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $\begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{bmatrix} \mapsto \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}$

Corresponds to measuring ρ "without looking at the outcome"

After looking at the outcome, ρ becomes $\begin{cases} |0\rangle\langle 0| & \text{with prob. } |\alpha|^2 \\ |1\rangle\langle 1| & \text{with prob. } |\beta|^2 \end{cases}$

General quantum operations (3)

Example 3 (discarding the second of two qubits):

Let $A_0 = I \otimes \langle 0| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ and $A_1 = I \otimes \langle 1| = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

States of the form $\rho \otimes \sigma$ (product states) become ρ

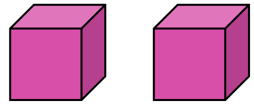
State $\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)\left(\frac{1}{\sqrt{2}}\langle 00| + \frac{1}{\sqrt{2}}\langle 11|\right)$ becomes $\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Note 1: it's the same density matrix as for $((½, |0\rangle), (½, |1\rangle))$

Note 2: the operation is called the ***partial trace*** $\mathrm{Tr}_2\, \rho$

Partial trace

More about the partial trace

Two quantum registers  in states σ and μ (resp.) are ***independent*** when the combined system is in state $\rho = \sigma \otimes \mu$

If the 2nd register is discarded, state of the 1st register remains σ

In general, the state of a two-register system may not be of the form $\sigma \otimes \mu$ (it may contain ***entanglement*** or ***correlations***)

The ***partial trace*** Tr_2 gives the effective state of the first register

For d-dimensional registers, Tr_2 is defined with respect to the operators $A_k = I \otimes \langle \phi_k |$, where $|\phi_0\rangle, |\phi_1\rangle, \ldots, |\phi_{d-1}\rangle$ can be any orthonormal basis

The **partial trace** $\mathrm{Tr}_2 \, \rho$, can also be characterized as the unique linear operator satisfying the identity $\mathrm{Tr}_2(\sigma \otimes \mu) = \sigma$

Partial trace continued

For 2-qubit systems, the partial trace is explicitly

$$\mathrm{Tr}_2\begin{bmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{00,10} & \rho_{00,11} \\ \rho_{01,00} & \rho_{01,01} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{10,10} & \rho_{10,11} \\ \rho_{11,00} & \rho_{11,01} & \rho_{11,10} & \rho_{11,11} \end{bmatrix} = \begin{bmatrix} \rho_{00,00}+\rho_{01,01} & \rho_{00,10}+\rho_{01,11} \\ \rho_{10,00}+\rho_{11,01} & \rho_{10,10}+\rho_{11,11} \end{bmatrix}$$

and

$$\mathrm{Tr}_1\begin{bmatrix} \rho_{00,00} & \rho_{00,01} & \rho_{00,10} & \rho_{00,11} \\ \rho_{01,00} & \rho_{01,01} & \rho_{01,10} & \rho_{01,11} \\ \rho_{10,00} & \rho_{10,01} & \rho_{10,10} & \rho_{10,11} \\ \rho_{11,00} & \rho_{11,01} & \rho_{11,10} & \rho_{11,11} \end{bmatrix} = \begin{bmatrix} \rho_{00,00}+\rho_{10,10} & \rho_{00,01}+\rho_{10,11} \\ \rho_{01,00}+\rho_{11,10} & \rho_{01,01}+\rho_{11,11} \end{bmatrix}$$

General quantum operations (4)

Example 4 (adding an extra qubit):

Just one operator $A_0 = I \otimes |0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$

States of the form ρ become $\rho \otimes |0\rangle\langle 0|$

More generally: to add a register in state $|\phi\rangle$, use the single operator $A_0 = I \otimes |\phi\rangle$

POVM measurements

(POVM = Positive Operator Valued Measure)

POVM measurements (1)

Let $A_1, A_2, \ldots, A_m$ be matrices satisfying $\sum_{j=1}^{m} A_j^\dagger A_j = I$

Corresponding ***POVM measurement*** is a stochastic operation on ρ that, with probability $\mathrm{Tr}\left(A_j \rho A_j^\dagger\right)$, produces outcome:

$$\begin{cases} j & \text{(classical information)} \\ \dfrac{A_j \rho A_j^\dagger}{\mathrm{Tr}\left(A_j \rho A_j^\dagger\right)} & \text{(the collapsed quantum state)} \end{cases}$$

Example 1: $A_j = |\phi_j\rangle\langle\phi_j|$ (orthogonal projectors)

This reduces to our previously defined measurements …

POVM measurements (2)

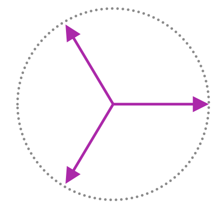
When $A_j = |\phi_j\rangle\langle\phi_j|$ are orthogonal projectors and $\rho = |\psi\rangle\langle\psi|$,

$$\begin{aligned}\mathrm{Tr}\left(A_j \rho A_j^\dagger\right) &= \mathrm{Tr}|\phi_j\rangle\langle\phi_j|\psi\rangle\langle\psi|\phi_j\rangle\langle\phi_j| \\ &= \langle\phi_j|\psi\rangle\langle\psi|\phi_j\rangle\langle\phi_j|\phi_j\rangle \\ &= |\langle\phi_j|\psi\rangle|^2\end{aligned}$$

Moreover, $$\frac{A_j \rho A_j^\dagger}{\mathrm{Tr}\left(A_j \rho A_j^\dagger\right)} = \frac{|\varphi_j\rangle\langle\varphi_j|\psi\rangle\langle\psi|\varphi_j\rangle\langle\varphi_j|}{|\langle\varphi_j|\psi\rangle|^2} = |\varphi_j\rangle\langle\varphi_j|$$

POVM measurements (3)

Example 3 (trine state "measurent"):



Let $|\varphi_0\rangle = |0\rangle$, $|\varphi_1\rangle = -1/2|0\rangle + \sqrt{3}/2|1\rangle$, $|\varphi_2\rangle = -1/2|0\rangle - \sqrt{3}/2|1\rangle$

Define $A_0 = \sqrt{2/3}|\varphi_0\rangle\langle\varphi_0| = \sqrt{\frac{2}{3}}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

$A_1 = \sqrt{2/3}|\varphi_1\rangle\langle\varphi_1| = \frac{1}{4}\begin{bmatrix} \sqrt{2/3} & +\sqrt{2} \\ +\sqrt{2} & \sqrt{6} \end{bmatrix}$ $\quad A_2 = \sqrt{2/3}|\varphi_2\rangle\langle\varphi_2| = \frac{1}{4}\begin{bmatrix} \sqrt{2/3} & -\sqrt{2} \\ -\sqrt{2} & \sqrt{6} \end{bmatrix}$

Then $A_0^\dagger A_0 + A_1^\dagger A_1 + A_2^\dagger A_2 = I$

If the input itself is an unknown trine state, $|\varphi_k\rangle\langle\varphi_k|$, then the probability that classical outcome is k is 2/3 = 0.6666…

POVM measurements (4)

Often POVMs arise in contexts where we only care about the classical part of the outcome (not the residual quantum state)

The probability of outcome ***j*** is $\mathrm{Tr}\left(A_j \rho A_j^\dagger\right) = \mathrm{Tr}\left(\rho A_j^\dagger A_j\right)$

Simplified definition for POVM measurements:

Let E_1, E_2, …, E_m be positive semidefinite and with $\sum_{j=1}^{m} E_j = I$

The probability of outcome ***j*** is $\mathrm{Tr}\left(\rho E_j\right)$

This is usually the way POVM measurements are defined

"Mother of all operations"

Let $A_{1,1}, A_{1,2}, \ldots, A_{1,m_1}$
$A_{2,1}, A_{2,2}, \ldots, A_{2,m_2}$
$A_{k,1}, A_{k,2}, \ldots, A_{k,m_k}$

satisfy $$\sum_{j=1}^{k} \sum_{i=1}^{m_j} A_{j,i}^\dagger A_{j,i} = I$$

Then there is a quantum operation that, on input ρ, produces

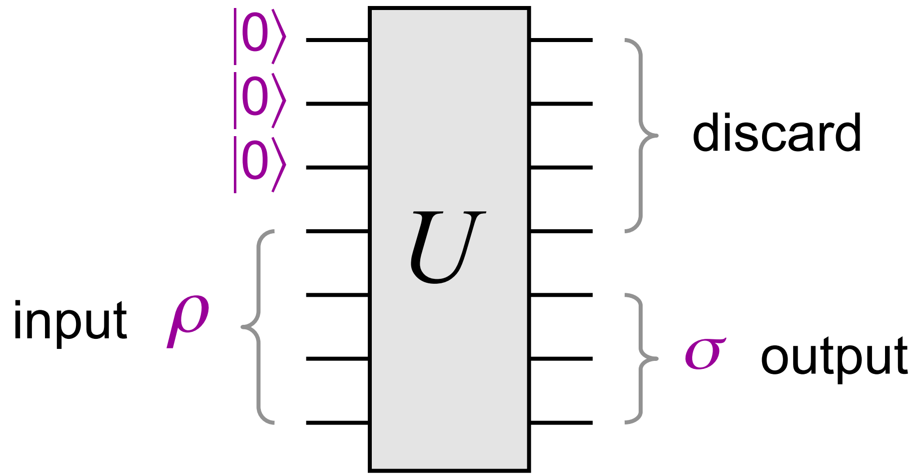
with probability $\sum_{i=1}^{m_j} \mathrm{Tr}\left(A_{j,i} \rho A_{j,i}^\dagger\right)$ the state:

$$\begin{cases} j & \text{(classical information)} \\ \dfrac{\sum_{i=1}^{m_j} A_{j,i} \rho A_{j,i}^\dagger}{\sum_{i=1}^{m_j} \mathrm{Tr}\left(A_{j,i} \rho A_{j,i}^\dagger\right)} & \text{(the collapsed quantum state)} \end{cases}$$

Simulations among operations

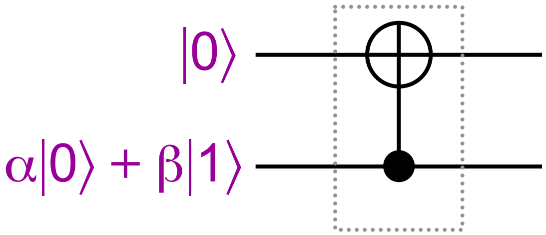
Simulations among operations (1)

Theorem 1: any ***general quantum operation*** can be simulated by applying a unitary operation on a larger quantum system:



This specification of a quantum operation is called the ***Stinespring*** form

Example: decoherence



$$\rho = \begin{bmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{bmatrix}$$

Simulations among operations (2)

Proof of Theorem 1:

Let $A_1, A_2, \ldots, A_{2^k}$ be any 2^m x 2^n matrices such that

$$\sum_{j=1}^{2^k} A_j^\dagger A_j = I$$

This defines a mapping from m qubits to n qubits:

$$\rho \mapsto \sum_{j=1}^{2^k} A_j \rho A_j^\dagger$$

This specification of the quantum operation is called the ***Krauss*** form

Simulations among operations (3)

Set $V = \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_{2^k} \end{bmatrix}$

Since $V^\dagger V = \begin{bmatrix} A_1^\dagger & A_2^\dagger & \cdots & A_{2^k}^\dagger \end{bmatrix} \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_{2^k} \end{bmatrix} = I$

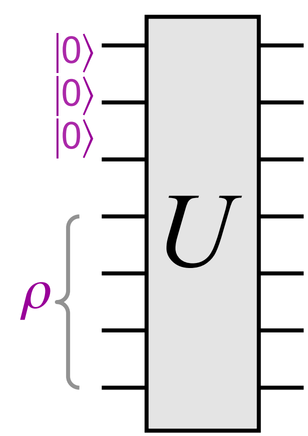
the columns of V are ***orthonormal***

Let U be any unitary matrix with first 2^n columns from V

$$U = [\ V \,\vdots\, W]$$

U is a 2^{m+k} x 2^{m+k} matrix (and its columns partition into 2^{m-n+k} blocks of size 2^n)

Now, consider the circuit:



Simulations among operations (4)

The output state of the circuit is $U(|00\cdots 0\rangle\langle 00\cdots 0| \otimes \rho)U^\dagger$

$$
= \left[\begin{array}{c|c} A_1 & \\ A_2 & \\ \vdots & W \\ A_{2^k} & \end{array}\right]
\begin{bmatrix} \rho & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}
\left[\begin{array}{cccc} A_1^\dagger & A_1^\dagger & \cdots & A_{2^k}^\dagger \\ \hline \multicolumn{4}{c}{W^\dagger} \end{array}\right]
$$

$$
= \begin{bmatrix} A_1\rho & 0 & \cdots & 0 \\ A_2\rho & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ A_{2^k}\rho & 0 & \cdots & 0 \end{bmatrix}
\left[\begin{array}{cccc} A_1^\dagger & A_1^\dagger & \cdots & A_{2^k}^\dagger \\ \hline \multicolumn{4}{c}{W^\dagger} \end{array}\right]
$$

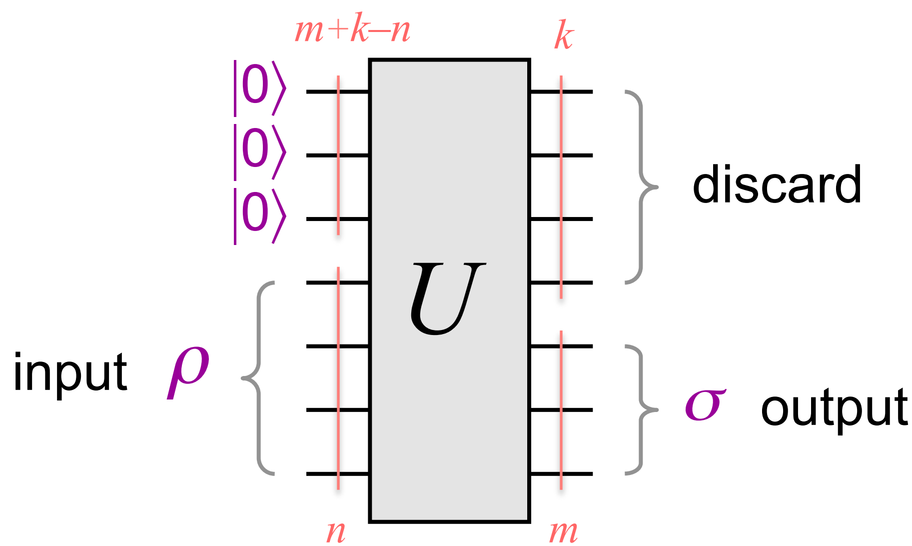
$$
= \begin{bmatrix} A_1\rho A_1^\dagger & A_1\rho A_2^\dagger & \cdots & A_1\rho A_{2^k}^\dagger \\ A_2\rho A_1^\dagger & A_2\rho A_2^\dagger & \cdots & A_2\rho A_{2^k}^\dagger \\ \vdots & \vdots & \ddots & \vdots \\ A_{2^k}\rho A_1^\dagger & A_{2^k}\rho A_2^\dagger & \cdots & A_{2^k}\rho A_{2^k}^\dagger \end{bmatrix}
$$

Simulations among operations (5)

Tracing out the high-order k qubits of this state yields

$$A_1 \rho A_1^\dagger + A_2 \rho A_2^\dagger + \cdots + A_{2^k} \rho A_{2^k}^\dagger$$

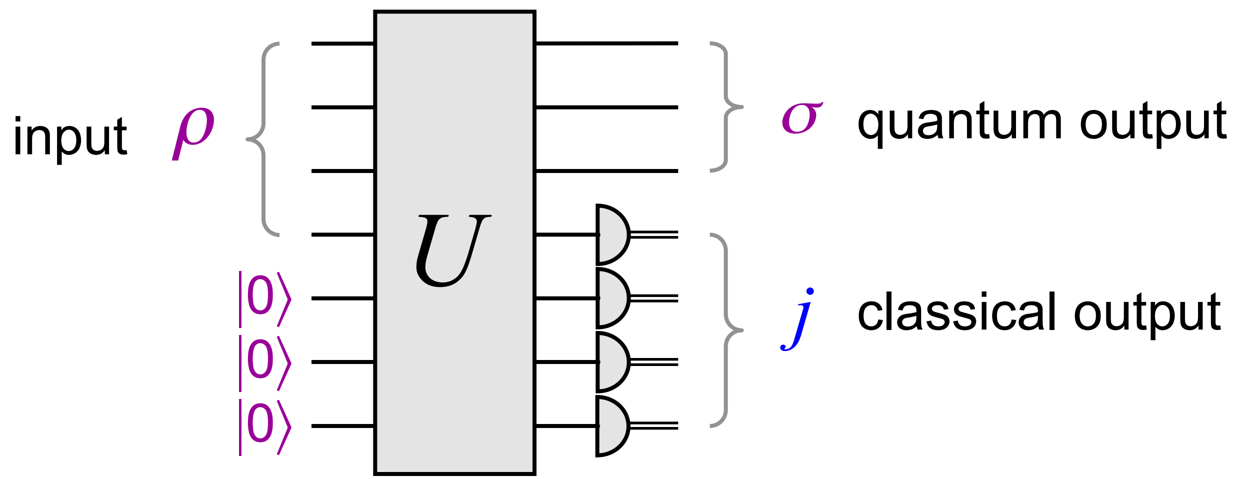
exactly the output of mapping that we want to simulate



Note: this approach is ***not***, in general, optimal in the number of ancilliary qubits used—there are more efficient methods

Simulations among operations (6)

Theorem 2: any ***POVM measurement*** can also be simulated by applying a unitary operation on a larger quantum system and then measuring:



This is the same diagram as for Theorem 1 (drawn with the extra qubits at the bottom) but where the “discarded” qubits are measured and part of the output

Separable states

(very briefly)

Separable states

A bipartite (i.e. two register) state ρ is a:

- ***product state*** if $\rho = \sigma \otimes \xi$
- ***separable state*** if $\rho = \sum_{j=1}^{m} p_j \sigma_j \otimes \xi_j \quad (p_1, \ldots, p_m \geq 0)$

  (i.e. a probabilistic mixture of product states)
- ***entangled*** = not separable

Since mixed states might be expressible as a mixture in several different ways, determining whether they are separable is tricky

Question: which of the following states are separable?

$$\rho_1 = \tfrac{1}{2}\big(|00\rangle + |11\rangle\big)\big(\langle 00| + \langle 11|\big)$$

$$\rho_2 = \tfrac{1}{2}\big(|00\rangle + |11\rangle\big)\big(\langle 00| + \langle 11|\big) + \tfrac{1}{2}\big(|00\rangle - |11\rangle\big)\big(\langle 00| - \langle 11|\big)$$

Introduction to Quantum Information Processing

QIC 710 / CS 678 / PH 767 / CO 681 / AM 871

Lecture 13 (2013)

Richard Cleve
DC 2117 / QNC 3129
cleve@cs.uwaterloo.ca

Distance measures for quantum states

Distance measures

Some simple (and often useful) measures:

- **Euclidean distance:** $\| |\psi\rangle - |\varphi\rangle \|_2$
- **Fidelity:** $| \langle\varphi|\psi\rangle |$

Small Euclidean distance implies "closeness" but large Euclidean distance need not (for example, $|\psi\rangle$ vs $-|\psi\rangle$)

Not so clear how to extend these for mixed states …

… though fidelity does generalize, to $\mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$

Trace norm – preliminaries (1)

For a normal matrix M and a function $f : \mathbf{C} \to \mathbf{C}$, we define the matrix $f(M)$ as follows:

$M = U^\dagger D U$, where D is diagonal (i.e. unitarily diagonalizable)

Now, define $f(M) = U^\dagger f(D)\, U$, where

$$D = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_d \end{bmatrix} \qquad f(D) = \begin{bmatrix} f(\lambda_1) & 0 & \cdots & 0 \\ 0 & f(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & f(\lambda_d) \end{bmatrix}$$

Trace norm – preliminaries (2)

For a normal matrix $M = U^{\dagger} D U$, define $|M|$ in terms of replacing D with

$$|D| = \begin{bmatrix} |\lambda_1| & 0 & \cdots & 0 \\ 0 & |\lambda_2| & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & |\lambda_d| \end{bmatrix}$$

This is the same as defining $|M| = \sqrt{M^{\dagger} M}$ and the latter definition extends to ***all*** matrices (not necessarily normal ones), since $M^{\dagger} M$ is positive definite

Trace norm/distance – definition

The ***trace norm*** of M is $\|M\|_{\text{tr}} = \text{Tr}|M| = \text{Tr}\sqrt{M^\dagger M}$

Intuitively, it's the 1-norm of the eigenvalues (or, in the non-normal case, the *singular values*) of M

The ***trace distance*** between ρ and σ is defined as $\|\rho - \sigma\|_{\text{tr}}$

Why is this a meaningful distance measure between quantum states?

Theorem: for any two quantum states ρ and σ, the ***optimal*** measurement procedure for distinguishing between them succeeds with probability $\frac{1}{2} + \frac{1}{4}\|\rho - \sigma\|_{\text{tr}}$

Distinguishing between two arbitrary quantum states

Holevo-Helstrom Theorem (1)

Theorem: for any two quantum states ρ and σ, the optimal measurement procedure for distinguishing between them succeeds with probability $\frac{1}{2} + \frac{1}{4}\|\rho - \sigma\|_{\mathrm{tr}}$ (equal prior probs.)

Proof* (the attainability part):

Since $\rho - \sigma$ is Hermitian, its eigenvalues are real

Let Π_+ be the projector onto the positive eigenspaces

Let Π_- be the projector onto the non-positive eigenspaces

Take the POVM measurement specified by Π_+ and Π_- with the associations $+ \equiv \rho$ and $- \equiv \sigma$

* The other direction of the theorem (optimality) is omitted here

Holevo-Helstrom Theorem (2)

Claim: this succeeds with probability $\frac{1}{2} + \frac{1}{4}\|\rho - \sigma\|_{\mathrm{tr}}$

Proof of Claim:

A key observation is $\mathrm{Tr}(\Pi_+ - \Pi_-)(\rho - \sigma) = \|\rho - \sigma\|_{\mathrm{tr}}$

The success probability is $p_s = \frac{1}{2}\mathrm{Tr}(\Pi_+ \rho) + \frac{1}{2}\mathrm{Tr}(\Pi_- \sigma)$

& the failure probability is $p_f = \frac{1}{2}\mathrm{Tr}(\Pi_+ \sigma) + \frac{1}{2}\mathrm{Tr}(\Pi_- \rho)$

Therefore, $p_s - p_f = \frac{1}{2}\mathrm{Tr}(\Pi_+ - \Pi_-)(\rho - \sigma) = \frac{1}{2}\|\rho - \sigma\|_{\mathrm{tr}}$

From this, the result follows $\blacksquare$

Purifications & Ulhmann's Theorem

Any density matrix ρ, can be obtained by tracing out part of some larger ***pure*** state:

$$\rho = \sum_{j=1}^{d} \lambda_j |\varphi_j\rangle\langle\varphi_j| = \mathrm{Tr}_2\left(\sum_{j=1}^{m}\sqrt{\lambda_j}|\varphi_j\rangle|j\rangle\right)\left(\sum_{j=1}^{m}\sqrt{\lambda_j}\langle\varphi_j|\langle j|\right)$$

a purification of ρ

Ulhmann's Theorem*: The ***fidelity*** between ρ and σ is the maximum of $\langle\varphi|\psi\rangle$ taken over all purifications $|\psi\rangle$ and $|\varphi\rangle$

* See [Nielsen & Chuang, pp. 410-411] for a proof of this

Recall our previous definition of fidelity as

$$\mathrm{F}(\rho, \sigma) = \mathrm{Tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}} \equiv \|\rho^{1/2}\sigma^{1/2}\|_{\mathrm{tr}}$$

Relationships between fidelity and trace distance

$$1 - F(\rho,\sigma) \le \|\rho - \sigma\|_{tr} \le \sqrt{1 - F(\rho,\sigma)^2}$$

See [Nielsen & Chuang, pp. 415-416] for more details

Preliminary remarks about quantum communication

Quantum information can apparently be used to substantially reduce ***computation*** costs for a number of interesting problems

How does quantum information affect the ***communication costs*** of information processing tasks?

We explore this issue ...

Entanglement and signaling

Recall that Entangled states, such as $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$,

can be used to perform some intriguing feats, such as ***teleportation*** and ***superdense coding***

—but they ***cannot*** be used to "signal instantaneously"

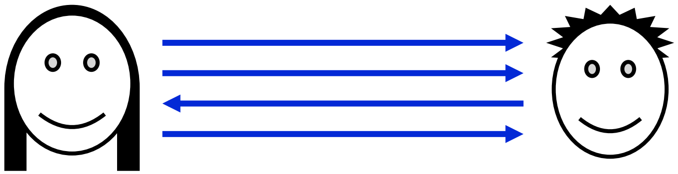
Any operation performed on one system has no affect on the state of the other system (its reduced density matrix)

Basic communication scenario

Goal: convey n bits from Alice to Bob

Basic communication scenario

Bit communication:

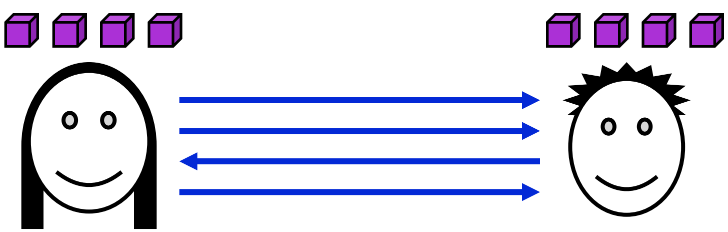


Cost: n

Qubit communication:

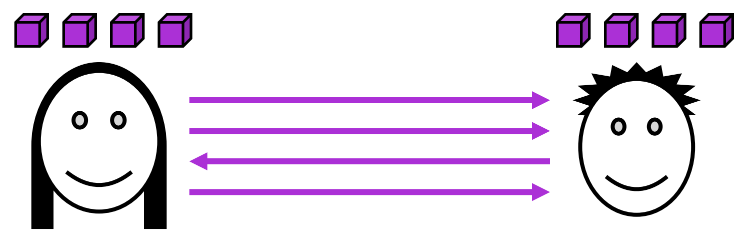
Cost: n [Holevo's Theorem, 1973]

Bit communication & prior entanglement:



Cost: n (can be deduced)

Qubit communication & prior entanglement:



Cost: $n/2$ superdense coding

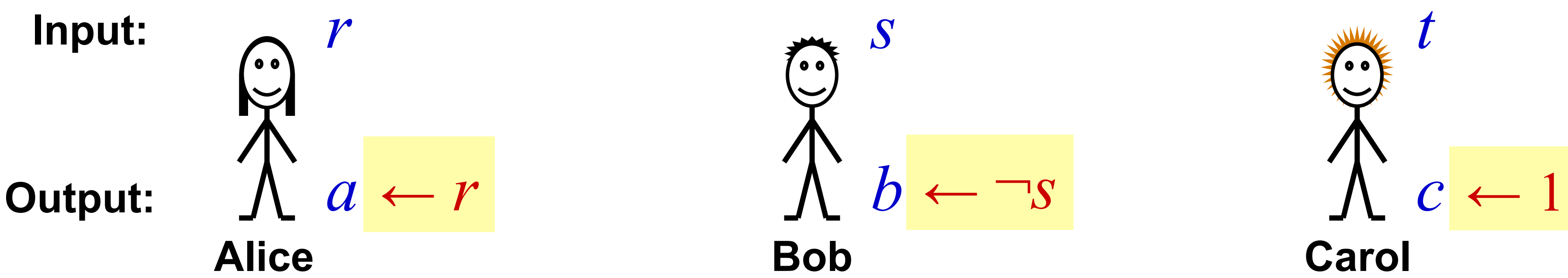
[Bennett & Wiesner, 1992]

The GHZ “paradox”

(Greenberger-Horne-Zeilinger)

GHZ scenario

[Greenberger, Horne, Zeilinger, 1980]

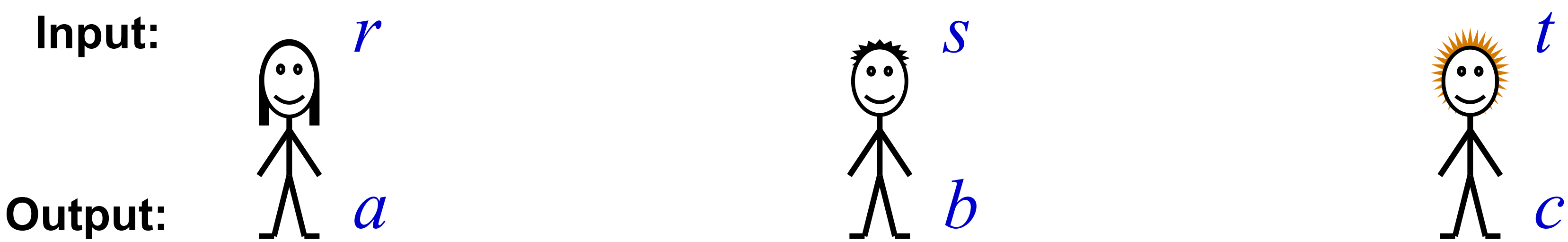


Rules of the game:

1. It is promised that $r \oplus s \oplus t = 0$
2. No communication after inputs received
3. They ***win*** if $a \oplus b \oplus c = r \vee s \vee t$

rst	$a \oplus b \oplus c$	abc
000	0	011
011	1	001
101	1	111
110	1	101

No perfect strategy for GHZ



rst	$a \oplus b \oplus c$
000	0
011	1
101	1
110	1

General deterministic strategy:

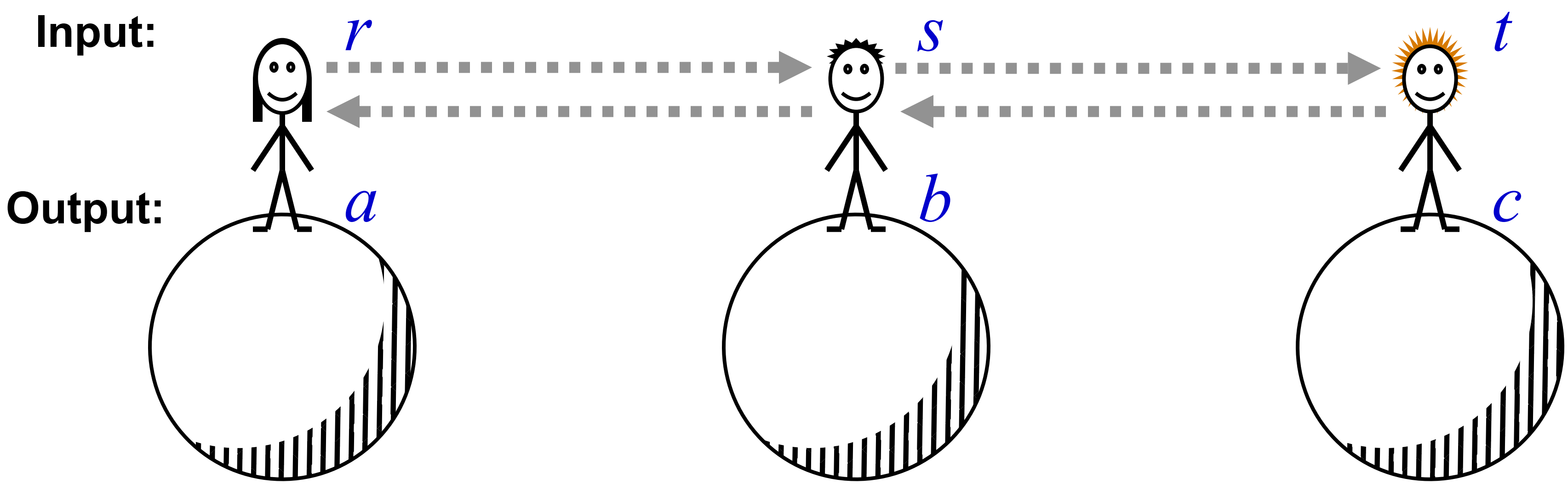
$$a_0, a_1, b_0, b_1, c_0, c_1$$

Winning conditions:

$$\left\{\begin{aligned} a_0 \oplus b_0 \oplus c_0 &= 0 \\ a_0 \oplus b_1 \oplus c_1 &= 1 \\ a_1 \oplus b_0 \oplus c_1 &= 1 \\ a_1 \oplus b_1 \oplus c_0 &= 1 \end{aligned}\right.$$

Has no solution, thus no perfect strategy exists

GHZ: preventing communication



Input and output events can be ***space-like*** separated:
so signals at the speed of light are not fast enough for cheating

What if Alice, Bob, and Carol ***still*** keep on winning?

To be continued …

Introduction to Quantum Information Processing
QIC 710 / CS 678 / PH 767 / CO 681 / AM 871

Lecture 14 (2013)

Richard Cleve
DC 2117 / QNC 3129
cleve@cs.uwaterloo.ca

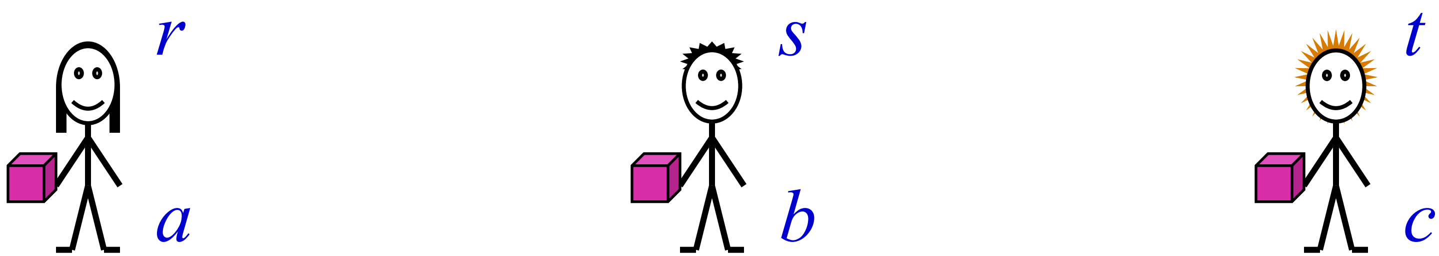
Continuation of:

The GHZ “paradox”

(Greenberger-Horne-Zeilinger)

“GHZ Paradox” explained

Prior entanglement: $|\psi\rangle = |000\rangle - |011\rangle - |101\rangle - |110\rangle$



<u>Alice’s strategy:</u>

1. if $r = 1$ then apply H to qubit (else I)
2. measure qubit and set a to result

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

<u>Bob’s & Carol’s strategies:</u> similar

Case 1 ($rst = 000$)**:** state is measured directly …

Case 2 ($rst = 011$)**:** new state $|001\rangle + |010\rangle - |100\rangle + |111\rangle$

Cases 3 & 4 ($rst = 101$ & 110)**:** similar by symmetry

GHZ: conclusions

- For the GHZ game, any ***classical*** team succeeds with probability at most ¾
- Allowing the players to communicate would enable them to succeed with probability 1
- Entanglement cannot be used to communicate
- Nevertheless, allowing the players to have entanglement enables them to succeed with probability 1 (but not by using entanglement to communicate)
- Thus, entanglement is a useful resource for the task of ***winning the GHZ game***

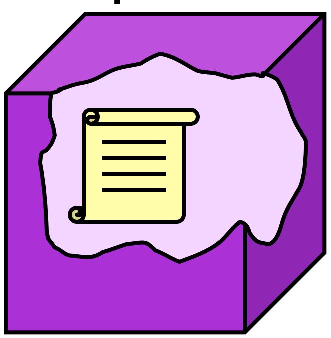
The Bell inequality and its violation
– Physicist's perspective

Bell's Inequality and its violation

Part I: physicist's view:

Can a quantum state have ***pre-determined*** outcomes for each possible measurement that can be applied to it?

qubit:



where the "manuscript" is something like this:

if $\{|0\rangle,|1\rangle\}$ measurement then output **0**

if $\{|+\rangle,|-\rangle\}$ measurement then output **1**

if **...** (etc)

table could be implicitly given by some formula

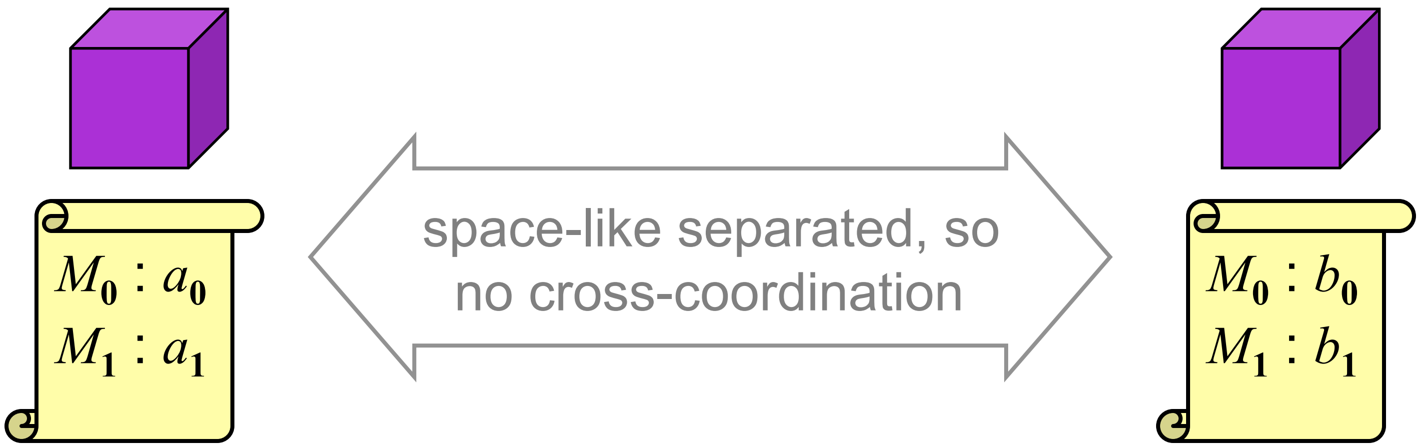
called ***hidden variables***

[Bell, 1964]

[Clauser, Horne, Shimony, Holt, 1969]

Bell Inequality

Imagine a two-qubit system, where one of two measurements, called M_0 and M_1, will be applied to each qubit:



Define:

$A_0 = (-1)^{a_0}$

$A_1 = (-1)^{a_1}$

$B_0 = (-1)^{b_0}$

$B_1 = (-1)^{b_1}$

Claim: $A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \leq 2$

Proof: $A_0 \underbrace{(B_0 + B_1)} + A_1 \underbrace{(B_0 - B_1)} \leq 2$

one is ± 2 and the other is 0

Bell Inequality

$A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \leq 2$ is called a ***Bell Inequality****

Question: could one, in principle, design an experiment to check if this Bell Inequality holds for a particular system?

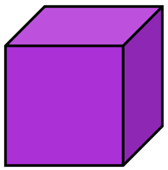
Answer 1: ***no, not directly***, because A_0, A_1, B_0, B_1 cannot all be measured (only ***one*** $A_s B_t$ term can be measured)

Answer 2: ***yes, indirectly***, by making many runs of this experiment: pick a random $st \in \{00, 01, 10, 11\}$ and then measure with M_s and M_t to get the value of $A_s B_t$

The ***average*** of $A_0 B_0$, $A_0 B_1$, $A_1 B_0$, $-A_1 B_1$ should be ≤ ½

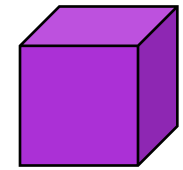
* also called CHSH Inequality

Violating the Bell Inequality



Two-qubit system in state

$|\phi\rangle = |00\rangle - |11\rangle$



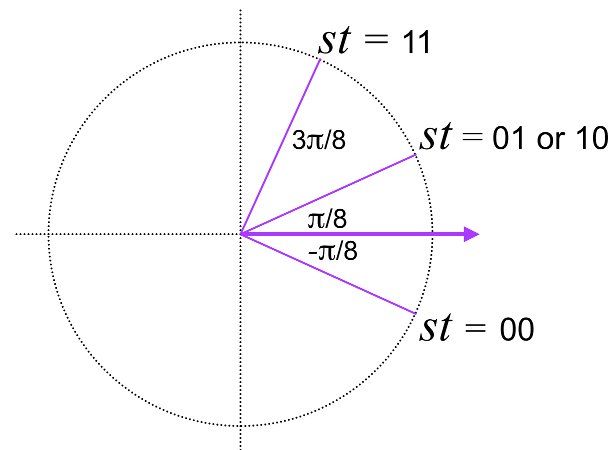
Applying rotations θ_A and θ_B yields:

$$\cos(\theta_A + \theta_B)\,\underbrace{(|00\rangle - |11\rangle)}_{AB\,=\,+1} + \sin(\theta_A + \theta_B)\,\underbrace{(|01\rangle + |10\rangle)}_{AB\,=\,-1}$$

Define

M_0: rotate by $-\pi/16$ then measure

M_1: rotate by $+3\pi/16$ then measure

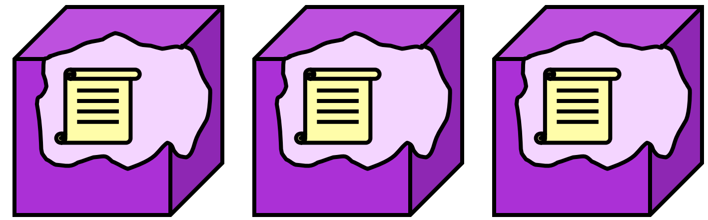


$\cos^2(\pi/8) = ½ + ¼\sqrt{2}$

Then $A_0 B_0$, $A_0 B_1$, $A_1 B_0$, $-A_1 B_1$ all have expected value $½\sqrt{2}$, which ***contradicts*** the upper bound of ½

Bell Inequality violation: summary

Assuming that quantum systems are governed by ***local hidden variables*** leads to the Bell inequality

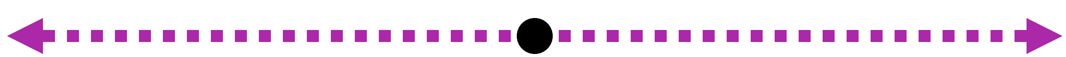


$$A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1 \leq 2$$

But this is ***violated*** in the case of Bell states (by a factor of $\sqrt{2}$)

Therefore, no such hidden variables exist

This is, in principle, experimentally verifiable, and experiments along these lines have actually been conducted

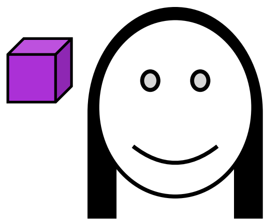


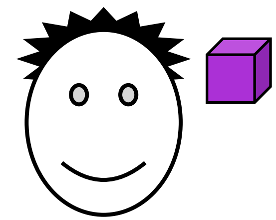
The Bell inequality and its violation – Computer Scientist’s perspective

Bell's Inequality and its violation

Part II: computer scientist's view:

input: s t





output: a b

Rules: 1. No communication after inputs received

2. They ***win*** if $a \oplus b = s \wedge t$

st	$a \oplus b$
00	0
01	0
10	0
11	1

With classical resources, $\Pr[a \oplus b = s \wedge t] \leq 0.75$

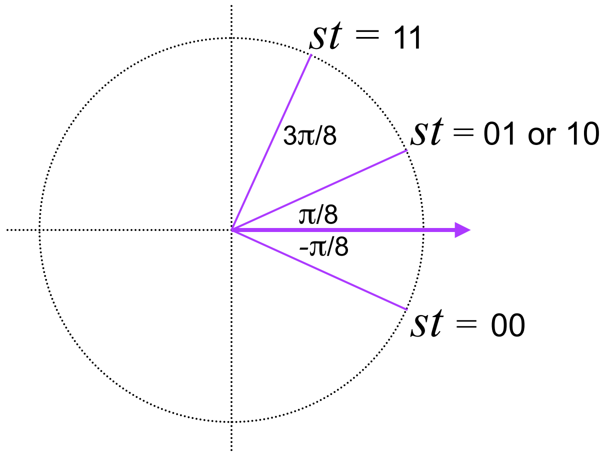
But, with prior entanglement state $|00\rangle - |11\rangle$,
$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = ½ + ¼\sqrt{2} = 0.853\ldots$

The quantum strategy

- Alice and Bob start with entanglement $|\phi\rangle = |00\rangle - |11\rangle$

- **Alice:** if $s = 0$ then rotate by $\theta_A = -\pi/16$ else rotate by $\theta_A = +3\pi/16$ and measure

- **Bob:** if $t = 0$ then rotate by $\theta_B = -\pi/16$ else rotate by $\theta_B = +3\pi/16$ and measure

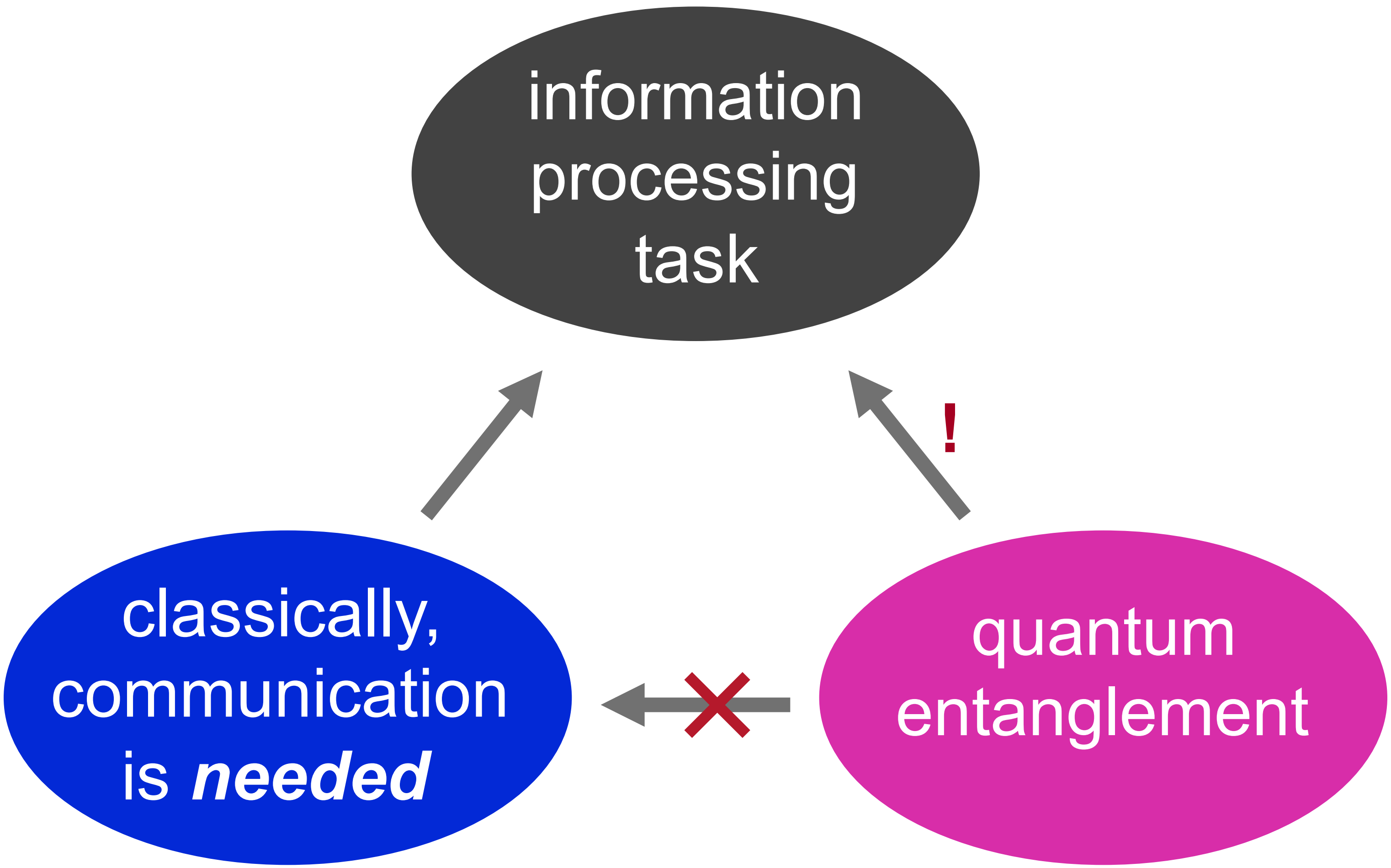


$\cos(\theta_A - \theta_B)\,(|00\rangle - |11\rangle) + \sin(\theta_A - \theta_B)\,(|01\rangle + |10\rangle)$

Success probability:

$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = ½ + ¼\sqrt{2} = 0.853\ldots$

Nonlocality in operational terms



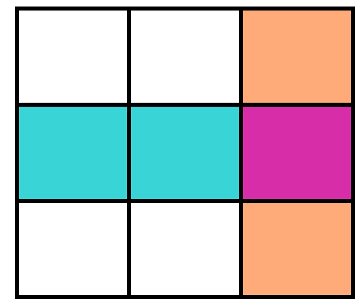
The magic square game

Magic square game

Problem: fill in the matrix with bits such that each row has even parity and each column has odd parity

$$\begin{array}{|c|c|c|l}
\hline
a_{11} & a_{12} & a_{13} & \text{even} \\
\hline
a_{21} & a_{22} & a_{23} & \text{even} \\
\hline
a_{31} & a_{32} & a_{33} & \text{even} \\
\hline
\multicolumn{1}{c}{\text{odd}} & \multicolumn{1}{c}{\text{odd}} & \multicolumn{1}{c}{\text{odd}} &
\end{array}$$

IMPOSSIBLE



Game: ask Alice to fill in one row and Bob to fill in one column

They ***win*** iff parities are correct and bits agree at intersection

Success probabilities: $^8/_9$ classical and 1 quantum

[Aravind, 2002] (details omitted here)