

Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lectures 13–14 (2019)

Richard Cleve

QNC 3129

cleve@cs.uwaterloo.ca

Preliminary remarks about quantum communication

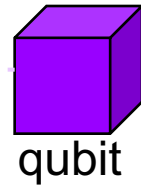
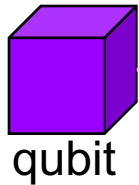
Quantum information can apparently be used to substantially reduce ***computation*** costs for a number of interesting problems

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”

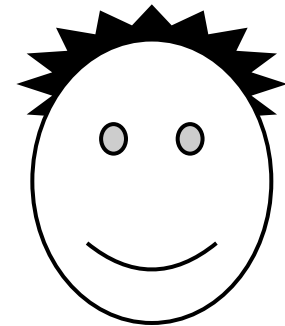
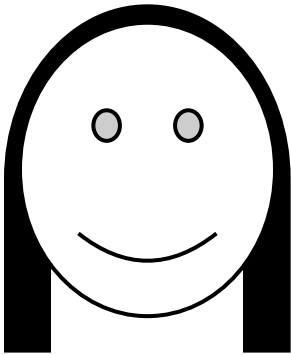
Any operation performed on one system has no affect on the state of the other system (its reduced density matrix)

Basic communication scenario

Goal: convey n bits from Alice to Bob

$x_1 x_2 \dots x_n$

Alice

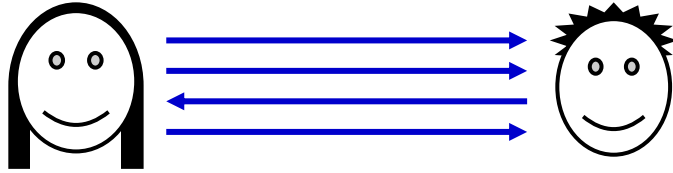


Bob

$x_1 x_2 \dots x_n$

Basic communication scenario

Bit communication:



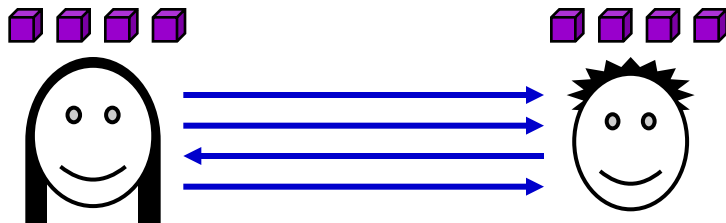
Cost: n

Qubit communication:



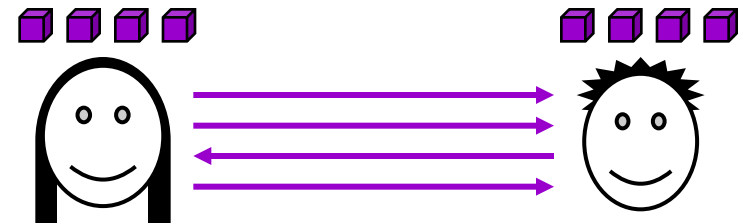
Cost: n [Holevo's Theorem, 1973]

Bit communication
& prior entanglement:



Cost: n (can be deduced)

Qubit communication
& prior entanglement:



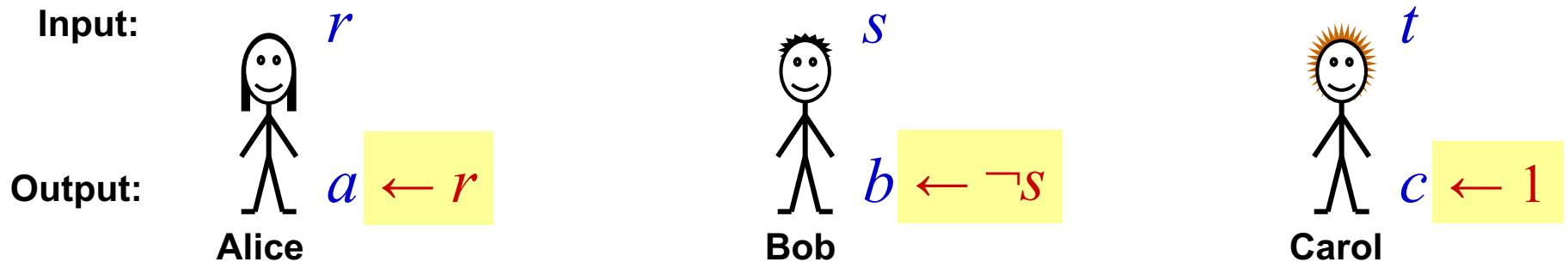
Cost: $n/2$ superdense coding
[Bennett & Wiesner, 1992]

The GHZ “paradox”

(Greenberger-Horne-Zeilinger)

GHZ scenario

[Greenberger, Horne, Zeilinger, 1980]

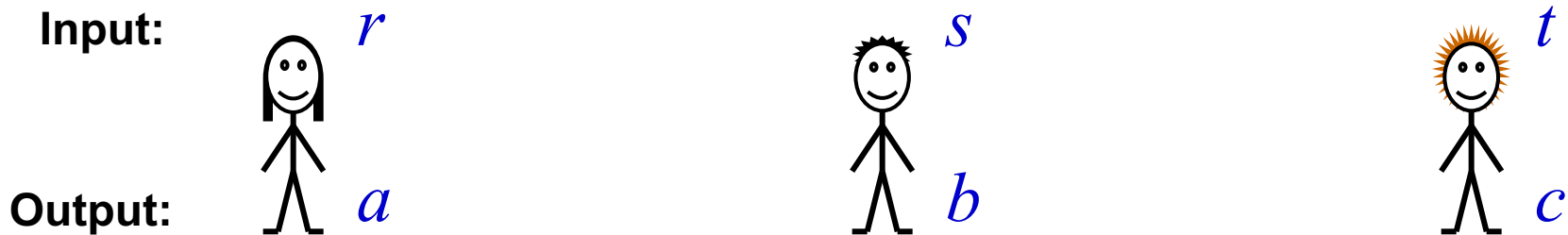


Rules of the game:

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:

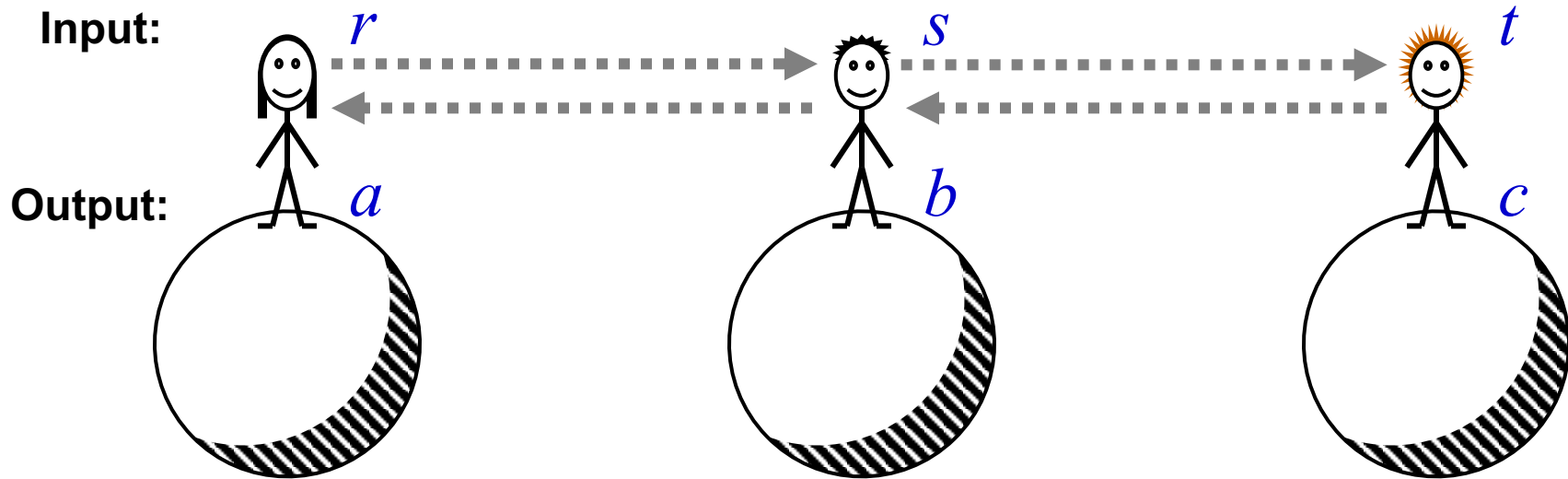
$$a_0, a_1, b_0, b_1, c_0, c_1$$

Winning conditions:

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

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 ...

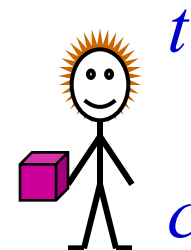
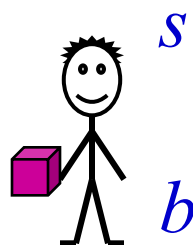
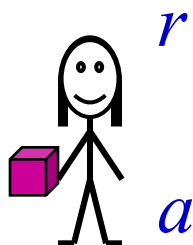
Continuation of:

The GHZ “paradox”

(Greenberger-Horne-Zeilinger)

“GHZ Paradox” explained

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



Alice's strategy:

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

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

Bob's & Carol's strategies: 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 $\frac{3}{4}$
- 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

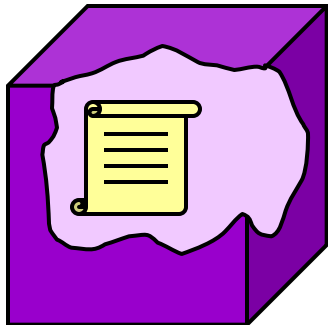
– Physicist's perspective

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:

called *hidden variables*

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

[Bell, 1964]

[Clauser, Horne, Shimony, Holt, 1969]

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?

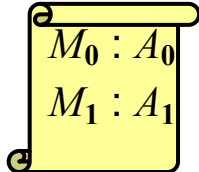
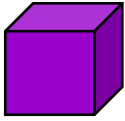
Answer 1: no, not directly, because A_0, A_1, B_0, B_1 cannot all be measured (only **one** $A_s B_t$ term can be measured)

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 $A_s B_t$

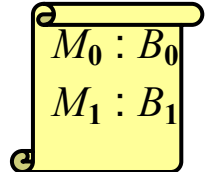
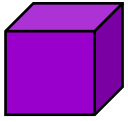
The **average** of $A_0 B_0, A_0 B_1, A_1 B_0, -A_1 B_1$ should be $\leq \frac{1}{2}$

* also called CHSH Inequality

Recap of Bell Inequality



Assume local hidden variables framework is correct



Consider the following experiment:

1. pick a random $st \in \{00, 01, 10, 11\}$ (uniform distribution)
2. perform M_s measurement on 1st qubit (outcome $A_s \in \{+1, -1\}$)
3. perform M_t measurement on 2nd qubit (outcome $B_t \in \{+1, -1\}$)
4. output the value of $(-1)^{s \cdot t} A_s B_t$

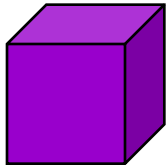
In any run of this experiment, the output is an element of $\{+1, -1\}$ (according to probabilities that depend on what A_0, A_1, B_0, B_1 are)

How large can the *expected* value of the outcome be?

$$\begin{aligned} & \frac{1}{4} (A_0 B_0) + \frac{1}{4} (A_0 B_1) + \frac{1}{4} (A_1 B_0) + \frac{1}{4} (-A_1 B_1) \\ & = \frac{1}{4} (A_0 B_0 + A_0 B_1 + A_1 B_0 - A_1 B_1) \leq \frac{1}{4} 2 = \frac{1}{2} \end{aligned}$$

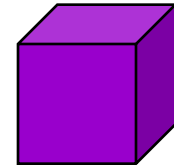
Violating the Bell Inequality

Assume the quantum mechanical framework is correct



Two-qubit system in state

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



It can be shown that, applying rotations θ_A and θ_B ($R_{\theta_A} \otimes R_{\theta_B}$) yields:

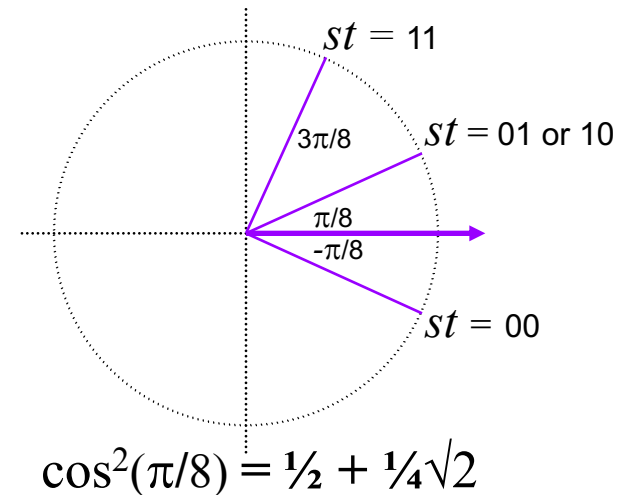
$$\underbrace{\cos(\theta_A + \theta_B)}_{AB = +1} (|00\rangle - |11\rangle) + \underbrace{\sin(\theta_A + \theta_B)}_{AB = -1} (|01\rangle + |10\rangle)$$

Define

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

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

Then $A_0 B_0$, $A_0 B_1$, $A_1 B_0$, $-A_1 B_1$ all have expected value $\frac{1}{2}\sqrt{2}$, which **contradicts** the upper bound of $\frac{1}{2}$

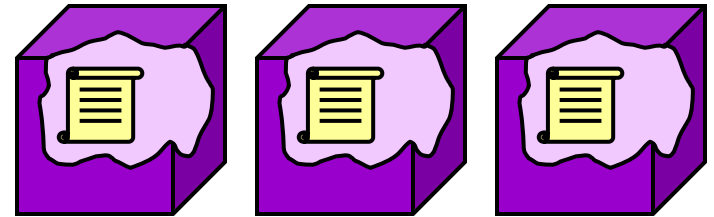


Therefore, QM framework implies LHV framework is false

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



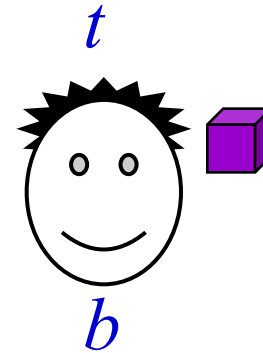
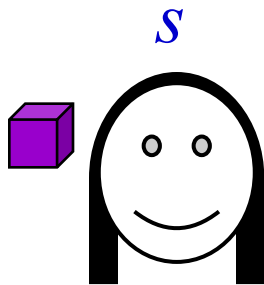
The Bell inequality and its violation

- Computer Scientist's perspective

Bell's Inequality and its violation

Part II: computer scientist's view:

input:



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

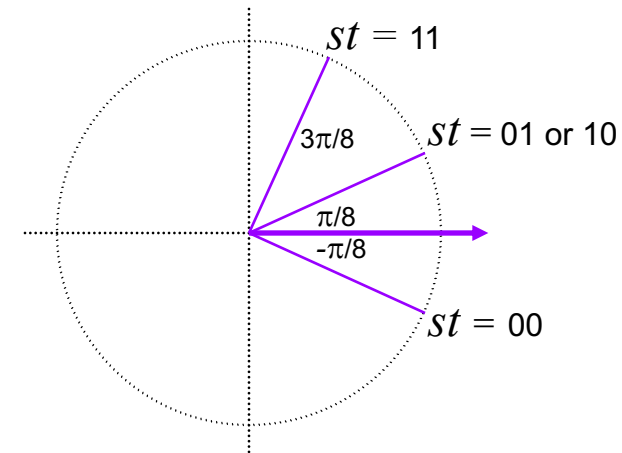
With classical resources, $\Pr[a \oplus b = s \wedge t] \leq 0.75$

But, with prior entanglement state $|00\rangle - |11\rangle$,

$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = \frac{1}{2} + \frac{1}{4}\sqrt{2} = 0.853\dots$

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

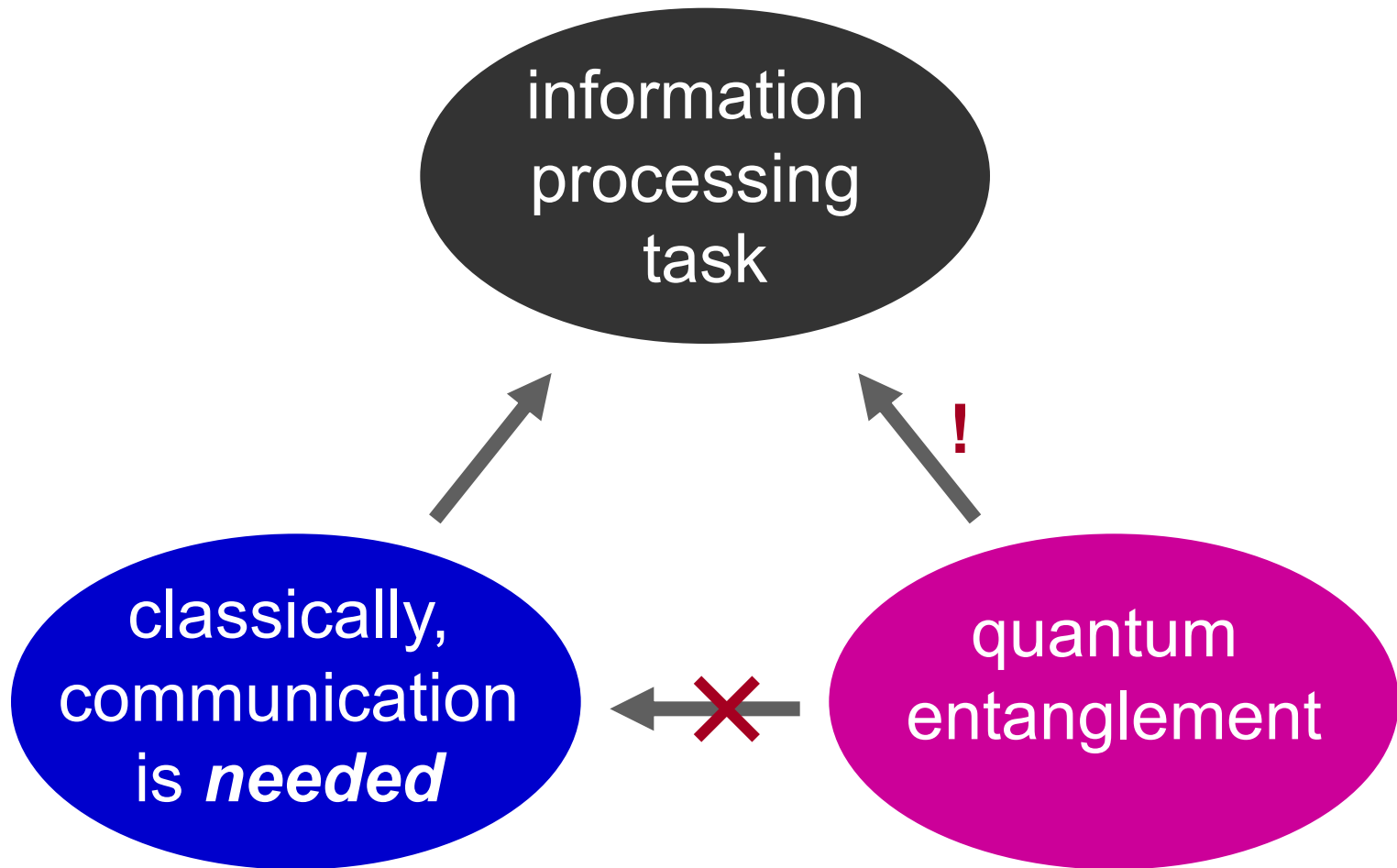


$$\cos(\theta_A + \theta_B) (|00\rangle - |11\rangle) + \sin(\theta_A + \theta_B) (|01\rangle + |10\rangle)$$

Success probability:

$$\Pr[a \oplus b = s \wedge t] = \cos^2(\pi/8) = \frac{1}{2} + \frac{1}{4}\sqrt{2} = 0.853\dots$$

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

a_{11}	a_{12}	a_{13}	even
a_{21}	a_{22}	a_{23}	even
a_{31}	a_{32}	a_{33}	even
odd	odd	odd	

IMPOSSIBLE

		orange
cyan	cyan	purple
		orange

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

Distance measures for quantum states

Distance measures

Some simple (and often useful) measures:

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

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 $\text{Tr} \sqrt{\rho^{1/2} \sigma \rho^{1/2}}$

Trace norm – preliminaries (1)

For a normal matrix M and a function $f: \mathbb{C} \rightarrow \mathbb{C}$, 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

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

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 semidefinite

Trace norm/distance – definition

The **trace norm** of M is $\|M\|_{\text{tr}} = \|M\|_1 = \text{Tr}|M| = \text{Tr}\sqrt{M^\dagger M}$

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 $\frac{1}{2} + \frac{1}{4}\|\rho - \sigma\|_{\text{tr}}$ (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 ρ and $-$ \equiv σ

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

Holevo-Helstrom Theorem (2)

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

Proof of Claim:

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

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

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

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

From this, the result follows \square

Purifications & Uhlmann's Theorem

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

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

a purification of ρ

Uhlmann'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

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

Relationships between fidelity and trace distance

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

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