Introduction to Quantum Information Processing

CS 667 / PH 767 / CO 681 / AM 871

Lecture 19 (2009)

Richard Cleve
DC 2117
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"

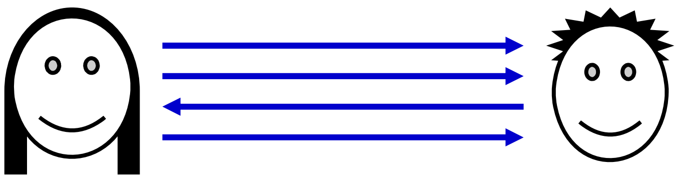
Any operation performed on one system has no affect on the state of the other system (its reduced density matrix)

Basic communication scenario

Goal: convey n bits from Alice to Bob

Basic communication scenario

Bit communication:

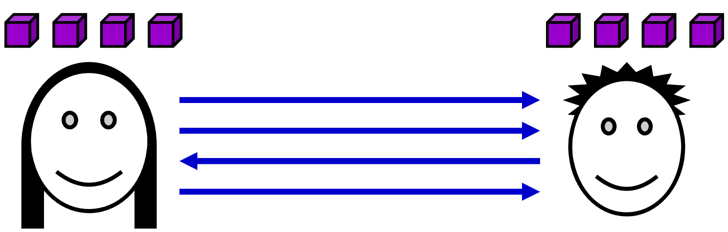


Cost: n

Qubit communication:

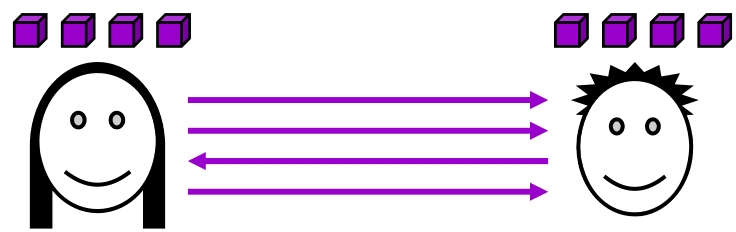
Cost: n [Holevo's Theorem, 1973]

Bit communication & prior entanglement:



Cost: n (can be deduced)

Qubit communication & prior entanglement:



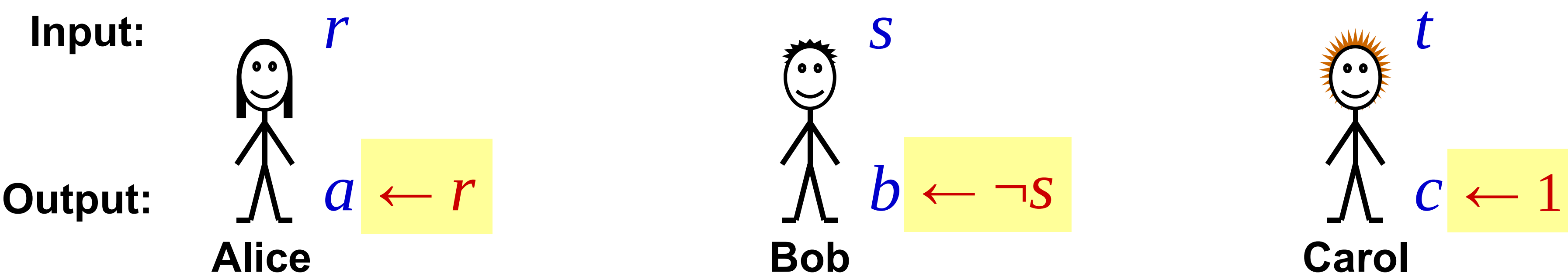
Cost: $n/2$ superdense coding

[Bennett & Wiesner, 1992]

The GHZ “paradox”

GHZ scenario

[Greenberger, Horne, Zeilinger, 1980]



Rules of the game:

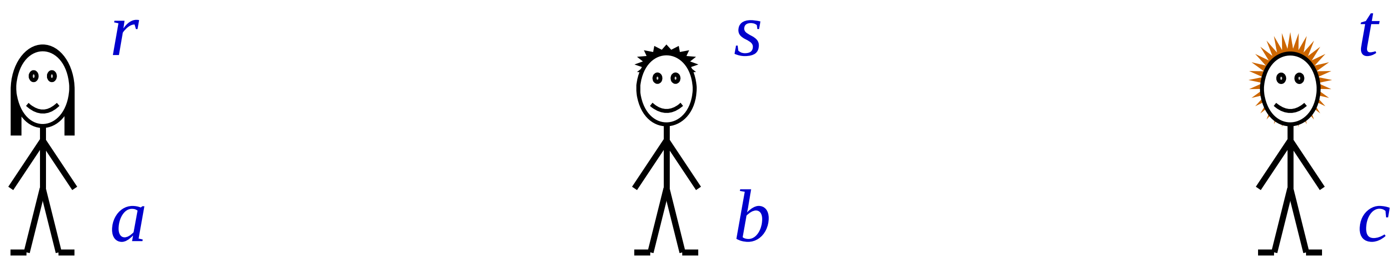
1. It is promised that $r \oplus s \oplus t = 0$
2. No communication after inputs received
3. They ***win*** if $a \oplus b \oplus c = r \vee s \vee t$

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

No perfect strategy for GHZ

Input:

Output:



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

General deterministic strategy:

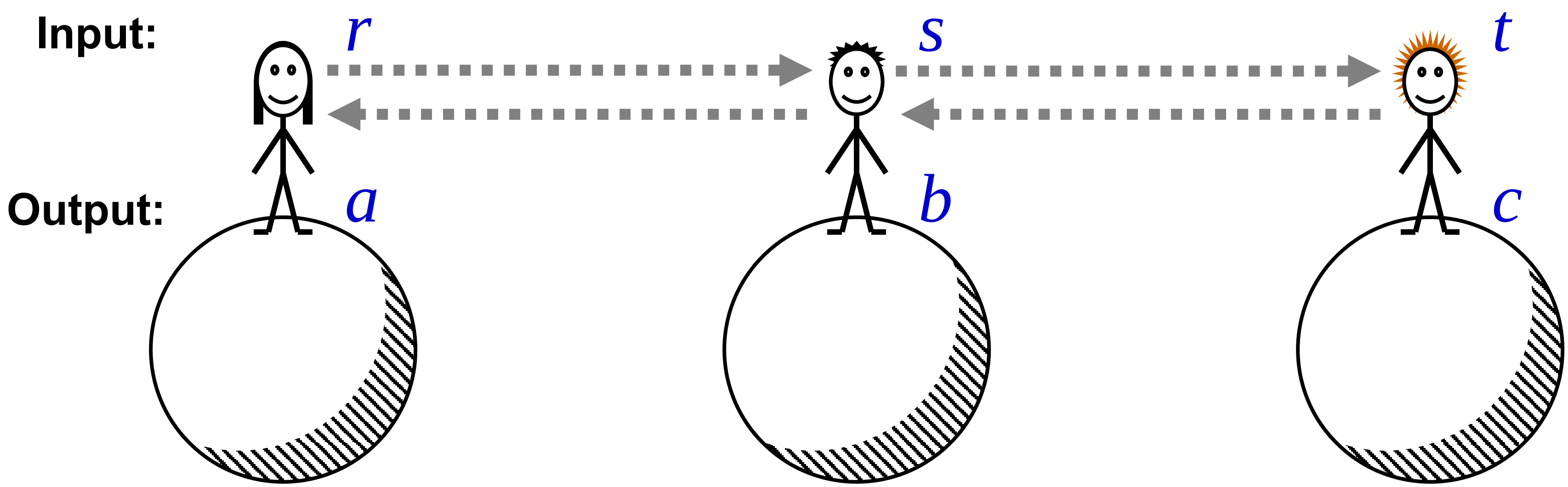
$a_0, a_1, b_0, b_1, c_0, c_1$

Winning conditions:

$$\begin{cases} a_0 \oplus b_0 \oplus c_0 = 0 \\ a_0 \oplus b_1 \oplus c_1 = 1 \\ a_1 \oplus b_0 \oplus c_1 = 1 \\ a_1 \oplus b_1 \oplus c_0 = 1 \end{cases}$$

Has no solution, thus no perfect strategy exists

GHZ: preventing communication

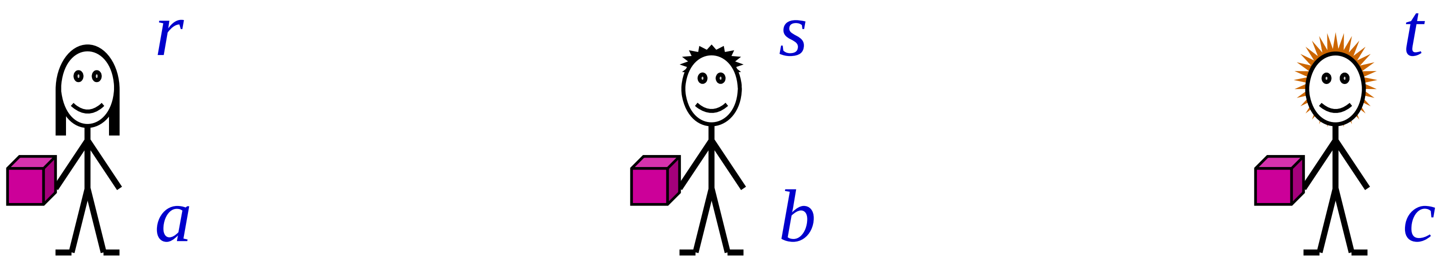


Input and output events can be ***space-like*** separated:
so signals at the speed of light are not fast enough for cheating

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

“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
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 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
- Thus, entanglement is a useful resource for the task of ***winning the GHZ game***

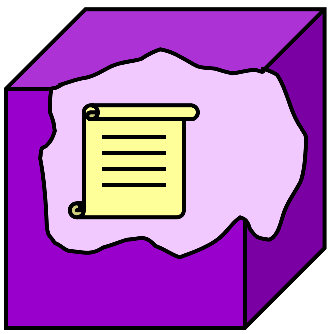
The Bell inequality and its violation
– Physicist’s perspective

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)

called ***hidden variables***

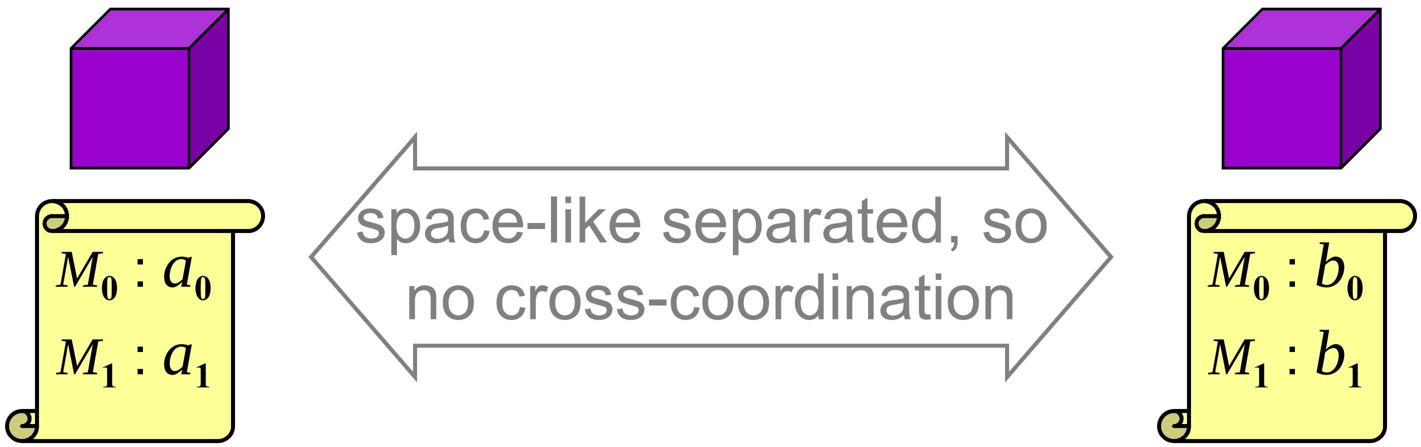
table could be implicitly given by some formula

[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?

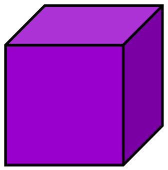
Answer 1: ***no, not directly***, because A_0, A_1, B_0, B_1 cannot all be measured (only ***one*** $A_s B_t$ term can be measured)

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

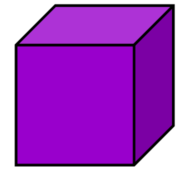
* also called CHSH Inequality

Violating the Bell Inequality



Two-qubit system in state

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



Applying rotations θ_A and θ_B yields:

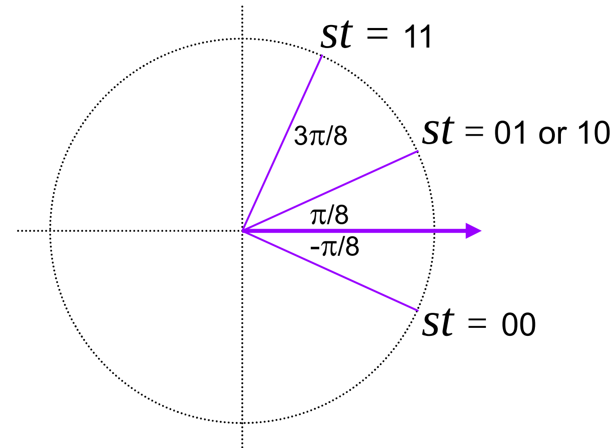
$$\cos(\theta_A + \theta_B)\,\underbrace{(|00\rangle - |11\rangle)}_{AB\,=\,+1} + \sin(\theta_A + \theta_B)\,\underbrace{(|01\rangle + |10\rangle)}_{AB\,=\,-1}$$

Define

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

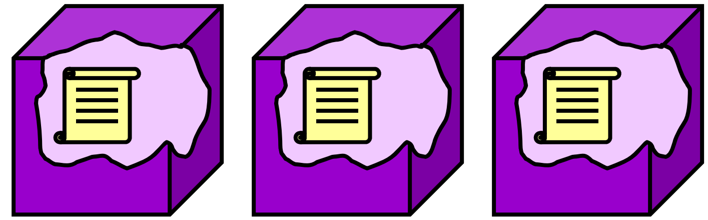
M_1: rotate by $+3\pi/16$ then measure

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 ½



$\cos^2(\pi/8) = \frac{1}{2} + \frac{1}{4}\sqrt{2}$

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

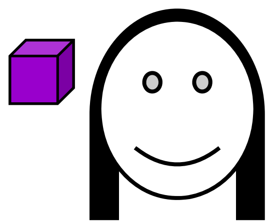
This is, in principle, experimentally verifiable, and experiments along these lines have actually been conducted

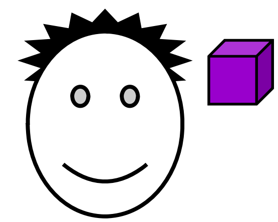
The Bell inequality and its violation – Computer Scientist’s perspective

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 $a \oplus b = s \wedge t$

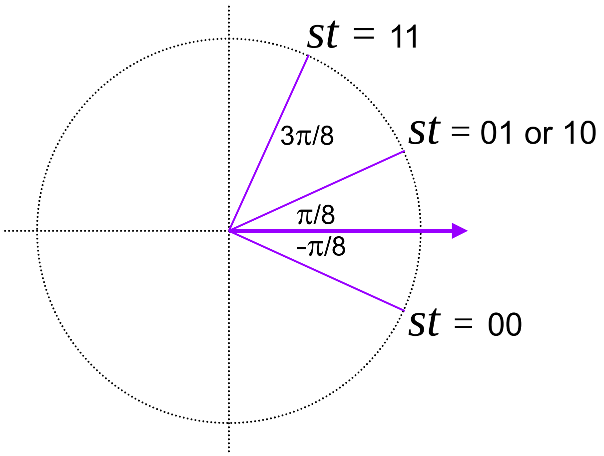
st	$a \oplus b$
00	0
01	0
10	0
11	1

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

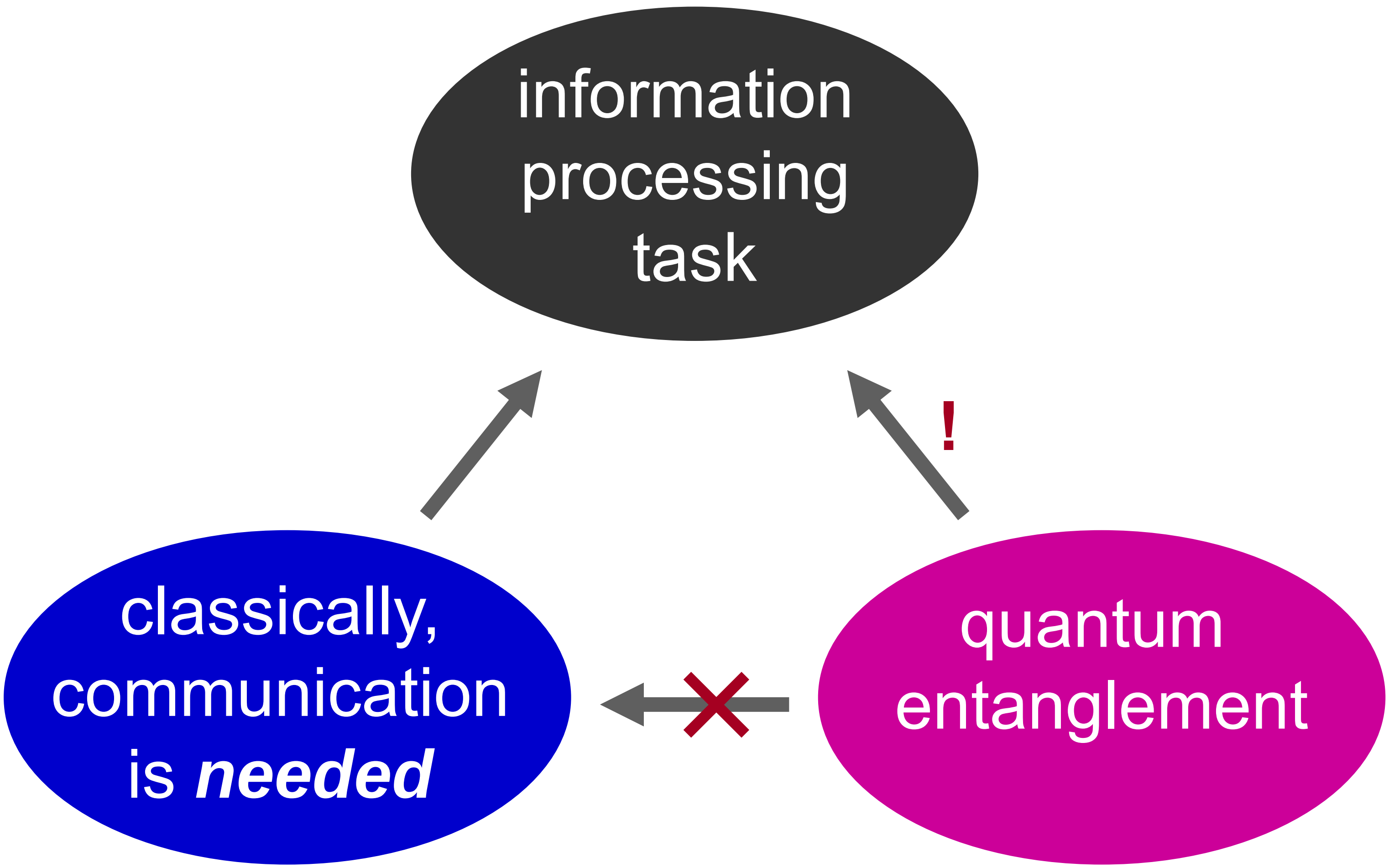


$$\cos(\theta_A - \theta_B)\,(|00\rangle - |11\rangle) + \sin(\theta_A - \theta_B)\,(|01\rangle + |10\rangle)$$

Success probability:

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

Nonlocality in operational terms



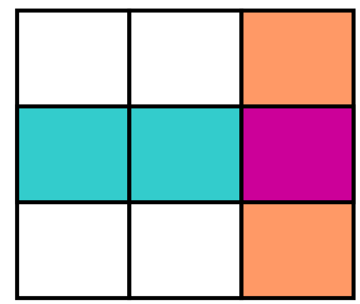
The magic square game

Magic square game

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

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

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)