Spooky Action: Scientific and Philosophical Challenges in the Era of Quantum Technology

David W. Lyons

Professor of Mathematical Sciences, Lebanon Valley College

Perry Lecture, Eastern Illinois University
31 October 2019

Outline

1. Introduction
   - Aims of This Talk
   - Misconceptions versus truth that is stranger than fiction
2. Classical Information Processing
   - Encoding
   - Logic gates and circuits
3. Quantum Information Processing
   - The Hadamard gate: superposition and measurement
   - Entanglement
   - Reality
4. Summary

Outline

1. Introduction
   - Aims of This Talk
   - Misconceptions versus truth that is stranger than fiction
2. Classical Information Processing
   - Encoding
   - Logic gates and circuits
3. Quantum Information Processing
   - The Hadamard gate: superposition and measurement
   - Entanglement
   - Reality
4. Summary

Aims of This Talk

This talk will attempt to shed some light on fundamental concepts in quantum mechanics:

- superposition and measurement
- entanglement
- what all this is good for
- philosophical problems

Outline

1. Introduction
   - Aims of This Talk
   - Misconceptions versus truth that is stranger than fiction
2. Classical Information Processing
   - Encoding
   - Logic gates and circuits
3. Quantum Information Processing
   - The Hadamard gate: superposition and measurement
   - Entanglement
   - Reality
4. Summary

Popular misconceptions

- Entanglement makes it possible to communicate instantly over arbitrarily large distances

Popular misconceptions

- Entanglement makes it possible to communicate instantly over arbitrarily large distances
- An observer can control experiments, the world, etc, by conscious thought alone

Popular misconceptions

- Entanglement makes it possible to communicate instantly over arbitrarily large distances
- An observer can control experiments, the world, etc, by conscious thought alone
- Quantum entanglement explains telepathy

Popular misconceptions

- Entanglement makes it possible to communicate instantly over arbitrarily large distances
- An observer can control experiments, the world, etc, by conscious thought alone
- Quantum entanglement explains telepathy

FALSE!!!

What quantum devices will (and already can) do

- Lasers!

What quantum devices will (and already can) do

- Lasers!
- Secure communication

What quantum devices will (and already can) do

- Lasers!
- Secure communication
  - Today's internet standard secure communication uses the RSA protocol

What quantum devices will (and already can) do

- Lasers!
- Secure communication
  - Today's internet standard secure communication uses the RSA protocol
  - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer

What quantum devices will (and already can) do

- Lasers!
- Secure communication
  - Today's internet standard secure communication uses the RSA protocol
  - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer
  - By contrast, existing quantum secure communication is secure based on the laws of physics, therefore not breakable by any present or future means (unless the laws of physics change)

What quantum devices will (and already can) do

- Lasers!
- Secure communication
  - Today's internet standard secure communication uses the RSA protocol
  - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer
  - By contrast, existing quantum secure communication is secure based on the laws of physics, therefore not breakable by any present or future means (unless the laws of physics change)
- Simulation of physical systems (quantum chemistry, potential applications to drug design)

What quantum devices will (and already can) do

- Lasers!
- Secure communication
  - Today's internet standard secure communication uses the RSA protocol
  - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer
  - By contrast, existing quantum secure communication is secure based on the laws of physics, therefore not breakable by any present or future means (unless the laws of physics change)
- Simulation of physical systems (quantum chemistry, potential applications to drug design)
- Measurement devices in new realms of accuracy

What quantum devices will (and already can) do

- Lasers!
- Secure communication
    - Today's internet standard secure communication uses the RSA protocol
    - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer
    - By contrast, existing quantum secure communication is secure based on the laws of physics, therefore not breakable by any present or future means (unless the laws of physics change)
- Simulation of physical systems (quantum chemistry, potential applications to drug design)
- Measurement devices in new realms of accuracy
    - Example: clocks (today) resolve 10^{-18} seconds

What quantum devices will (and already can) do

- Lasers!
- Secure communication
    - Today's internet standard secure communication uses the RSA protocol
    - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer
    - By contrast, existing quantum secure communication is secure based on the laws of physics, therefore not breakable by any present or future means (unless the laws of physics change)
- Simulation of physical systems (quantum chemistry, potential applications to drug design)
- Measurement devices in new realms of accuracy
    - Example: clocks (today) resolve 10^{-18} seconds
    - (compare to 10^{-15} five years ago)

What quantum devices will (and already can) do

- Lasers!
- Secure communication
  - Today's internet standard secure communication uses the RSA protocol
  - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer
  - By contrast, existing quantum secure communication is secure based on the laws of physics, therefore not breakable by any present or future means (unless the laws of physics change)
- Simulation of physical systems (quantum chemistry, potential applications to drug design)
- Measurement devices in new realms of accuracy
  - Example: clocks (today) resolve 10^{-18} seconds
  - (compare to 10^{-15} five years ago)
  - when we get to 10^{-21} seconds we will be able to time a gravity wave passing through a small molecular lattice!

What quantum devices will (and already can) do

- Lasers!
- Secure communication
  - Today's internet standard secure communication uses the RSA protocol
  - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer
  - By contrast, existing quantum secure communication is secure based on the laws of physics, therefore not breakable by any present or future means (unless the laws of physics change)
- Simulation of physical systems (quantum chemistry, potential applications to drug design)
- Measurement devices in new realms of accuracy
  - Example: clocks (today) resolve 10^{-18} seconds
  - (compare to 10^{-15} five years ago)
  - when we get to 10^{-21} seconds we will be able to time a gravity wave passing through a small molecular lattice!
- Efficient computation of currently unfeasible problems (many optimization problems of theoretical and commercial interest)

What quantum devices will (and already can) do

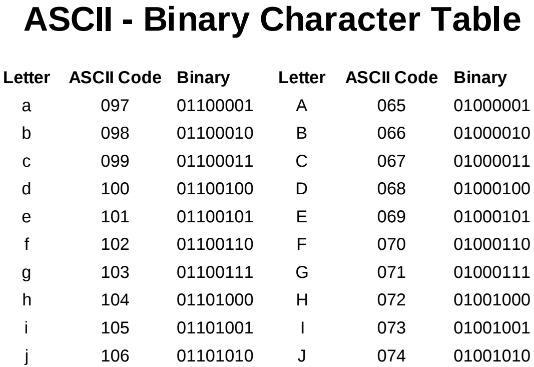
- Lasers!
- Secure communication
    - Today's internet standard secure communication uses the RSA protocol
    - "unbreakable" by (today's) classical computers but breakable by a (future) quantum computer
    - By contrast, existing quantum secure communication is secure based on the laws of physics, therefore not breakable by any present or future means (unless the laws of physics change)
- Simulation of physical systems (quantum chemistry, potential applications to drug design)
- Measurement devices in new realms of accuracy
    - Example: clocks (today) resolve 10^{-18} seconds
    - (compare to 10^{-15} five years ago)
    - when we get to 10^{-21} seconds we will be able to time a gravity wave passing through a small molecular lattice!
- Efficient computation of currently unfeasible problems (many optimization problems of theoretical and commercial interest)

(amazing but) TRUE!!!

Outline

1. Introduction
   - Aims of This Talk
   - Misconceptions versus truth that is stranger than fiction
2. Classical Information Processing
   - Encoding
   - Logic gates and circuits
3. Quantum Information Processing
   - The Hadamard gate: superposition and measurement
   - Entanglement
   - Reality
4. Summary

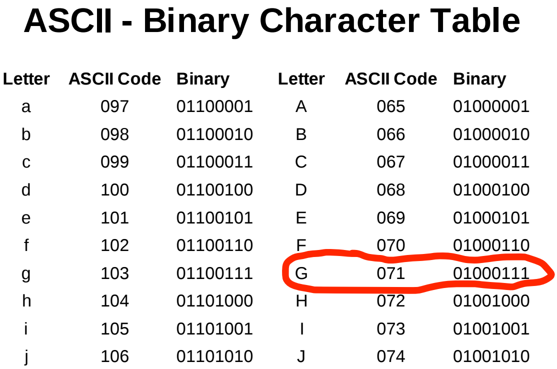
Encoding information in strings of bits



ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010

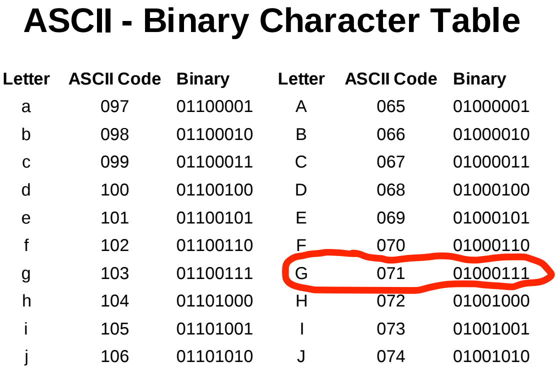
Encoding information in strings of bits



ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010

Encoding information in strings of bits



ASCII - Binary Character Table

Letter	ASCII Code	Binary	Letter	ASCII Code	Binary
a	097	01100001	A	065	01000001
b	098	01100010	B	066	01000010
c	099	01100011	C	067	01000011
d	100	01100100	D	068	01000100
e	101	01100101	E	069	01000101
f	102	01100110	F	070	01000110
g	103	01100111	G	071	01000111
h	104	01101000	H	072	01001000
i	105	01101001	I	073	01001001
j	106	01101010	J	074	01001010

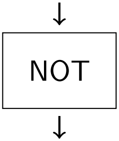
$$G = 01000111 = \text{○●○○○●●●}$$

Outline

1. Introduction
   - Aims of This Talk
   - Misconceptions versus truth that is stranger than fiction
2. Classical Information Processing
   - Encoding
   - Logic gates and circuits
3. Quantum Information Processing
   - The Hadamard gate: superposition and measurement
   - Entanglement
   - Reality
4. Summary

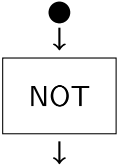
NOT gates

NOT gates



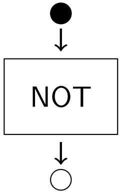
NOT

NOT gates



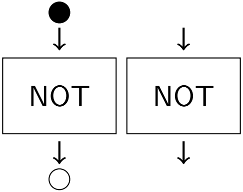
NOT

NOT gates

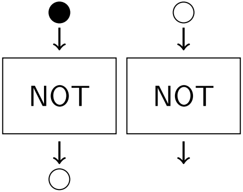


NOT

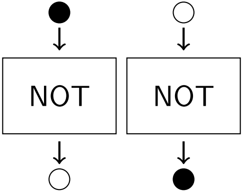
NOT gates



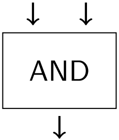
NOT gates



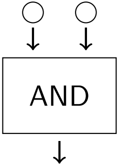
NOT gates



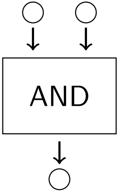
More gates



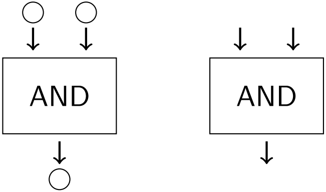
More gates



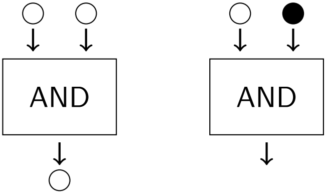
More gates



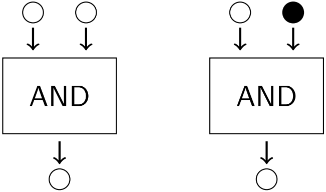
More gates



More gates



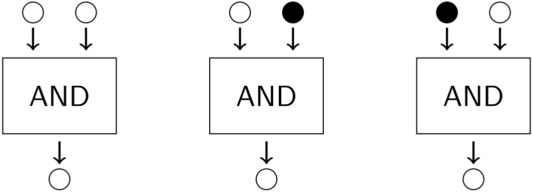
More gates



AND

AND

More gates

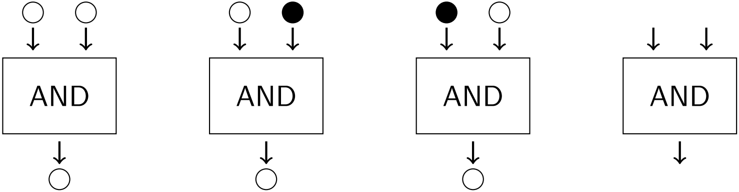


AND

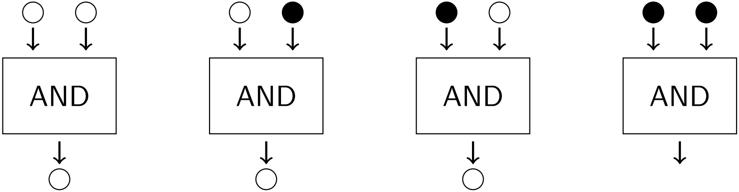
AND

AND

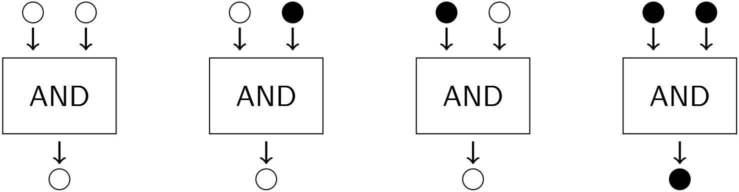
More gates



More gates



More gates



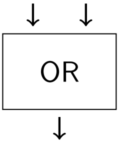
AND

AND

AND

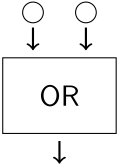
AND

More gates, cont’d

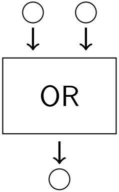


OR

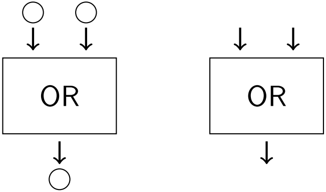
More gates, cont'd



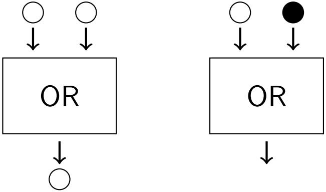
More gates, cont'd



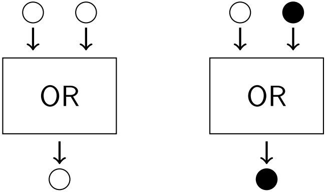
More gates, cont'd



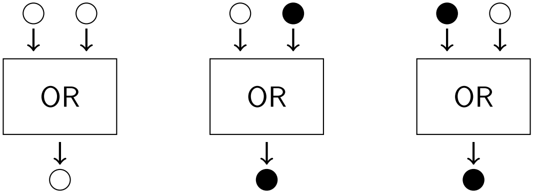
More gates, cont'd



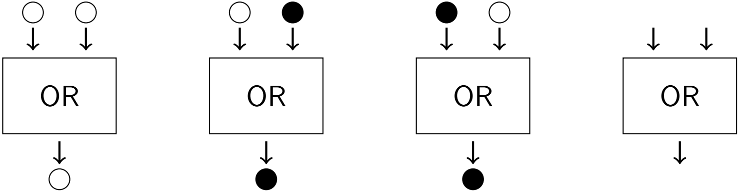
More gates, cont'd



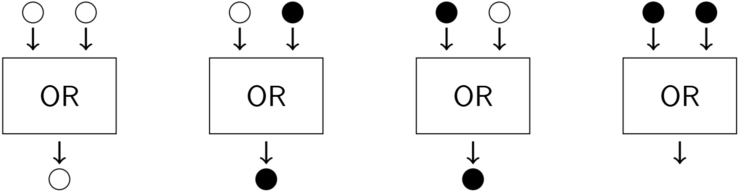
More gates, cont'd



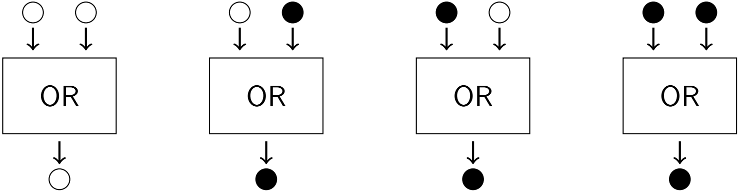
More gates, cont'd



More gates, cont'd



More gates, cont'd



More gates, cont'd

What's the point of all these boxes?

A classical computer is made entirely of NOT, AND, and OR boxes. The balls that pass through the boxes are bits.

More gates, cont'd

What's the point of all these boxes?

A classical computer is made entirely of NOT, AND, and OR boxes. The balls that pass through the boxes are bits.

Quantum computers

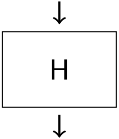
A quantum computer is also made of boxes, but new kinds of boxes are available. The balls that pass through the boxes are *quantum* bits, or qubits.

Outline

1. Introduction
   - Aims of This Talk
   - Misconceptions versus truth that is stranger than fiction
2. Classical Information Processing
   - Encoding
   - Logic gates and circuits
3. Quantum Information Processing
   - The Hadamard gate: superposition and measurement
   - Entanglement
   - Reality
4. Summary

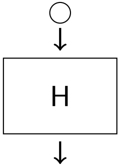
The quantum Hadamard gate

The quantum Hadamard gate

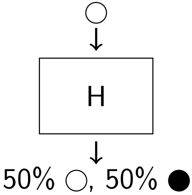


H

The quantum Hadamard gate



The quantum Hadamard gate



○

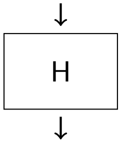
↓

H

↓

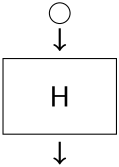
50% ○, 50% ●

Hadamard gate, cont’d



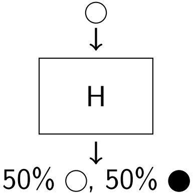
H

Hadamard gate, cont'd



H

Hadamard gate, cont'd



○

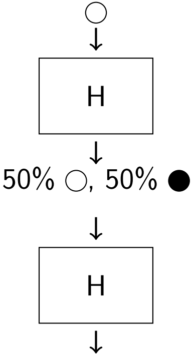
↓

H

↓

50% ○, 50% ●

Hadamard gate, cont'd



○

↓

H

↓

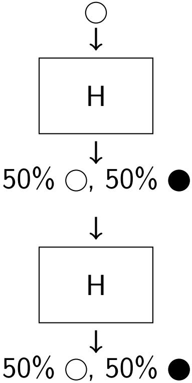
50% ○, 50% ●

↓

H

↓

Hadamard gate, cont'd



○

↓

H

↓

50% ○, 50% ●

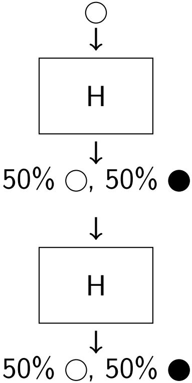
↓

H

↓

50% ○, 50% ●

Hadamard gate, cont'd



○

↓

H

↓

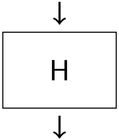
50% ○, 50% ●

↓

H

↓

50% ○, 50% ●

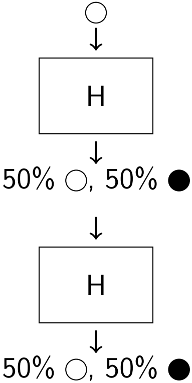


↓

H

↓

Hadamard gate, cont'd



○

↓

H

↓

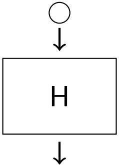
50% ○, 50% ●

↓

H

↓

50% ○, 50% ●



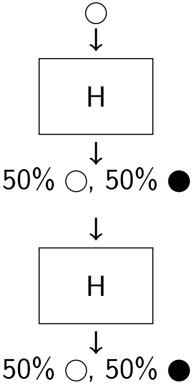
○

↓

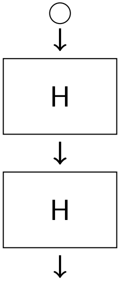
H

↓

Hadamard gate, cont'd

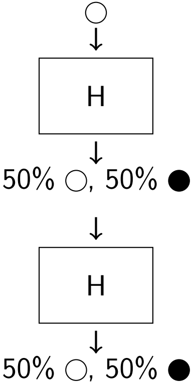


○
↓
H
↓
50% ○, 50% ●
↓
H
↓
50% ○, 50% ●



○
↓
H
↓
H
↓

Hadamard gate, cont’d



○

↓

H

↓

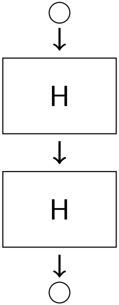
50% ○, 50% ●

↓

H

↓

50% ○, 50% ●



○

↓

H

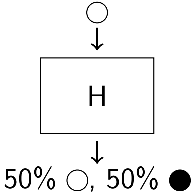
↓

H

↓

○

“Explanation” of the Hadamard paradox



○

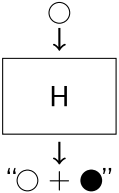
↓

H

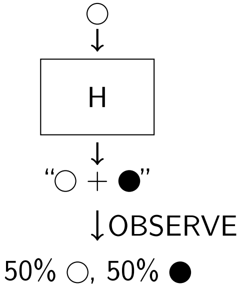
↓

50% ○, 50% ●

“Explanation” of the Hadamard paradox



"Explanation" of the Hadamard paradox



○

↓

H

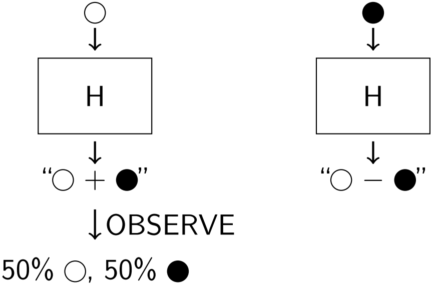
↓

"○ + ●"

↓OBSERVE

50% ○, 50% ●

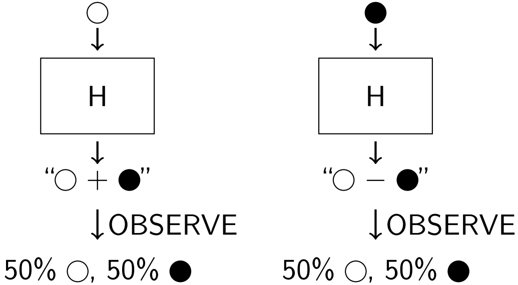
“Explanation” of the Hadamard paradox



○
↓
H
↓
“○ + ●”
↓OBSERVE
50% ○, 50% ●

●
↓
H
↓
“○ − ●”

“Explanation” of the Hadamard paradox



○

↓

H

↓

“○ + ●”

↓OBSERVE

50% ○, 50% ●

●

↓

H

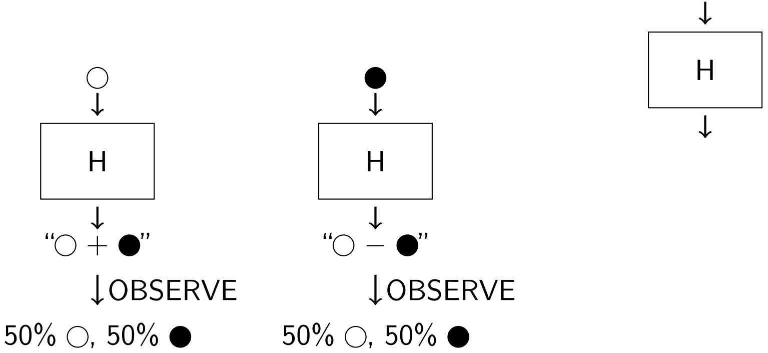
↓

“○ − ●”

↓OBSERVE

50% ○, 50% ●

“Explanation” of the Hadamard paradox



○

↓

H

↓

“○ + ●”

↓OBSERVE

50% ○, 50% ●

●

↓

H

↓

“○ − ●”

↓OBSERVE

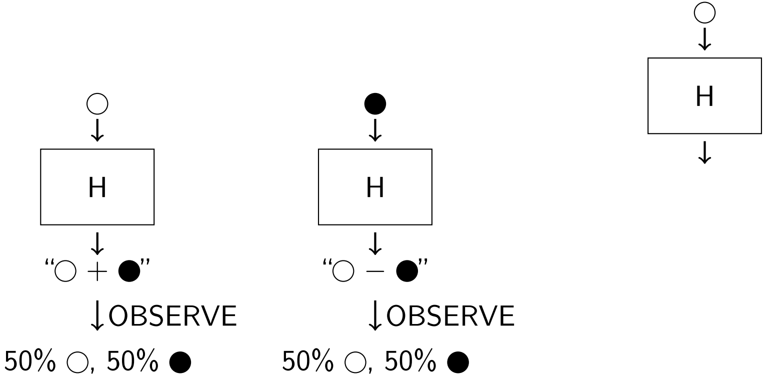
50% ○, 50% ●

↓

H

↓

“Explanation” of the Hadamard paradox

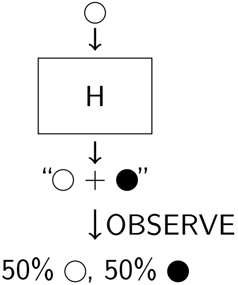


○ ↓ H ↓ “○ + ●” ↓OBSERVE 50% ○, 50% ●

● ↓ H ↓ “○ − ●” ↓OBSERVE 50% ○, 50% ●

○ ↓ H ↓

“Explanation” of the Hadamard paradox



○

↓

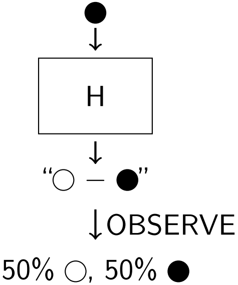
H

↓

“○ + ●”

↓OBSERVE

50% ○, 50% ●



●

↓

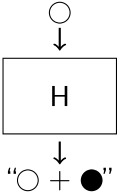
H

↓

“○ − ●”

↓OBSERVE

50% ○, 50% ●



○

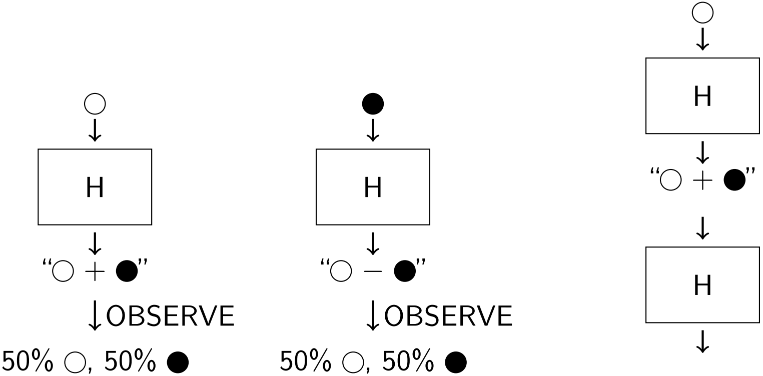
↓

H

↓

“○ + ●”

“Explanation” of the Hadamard paradox

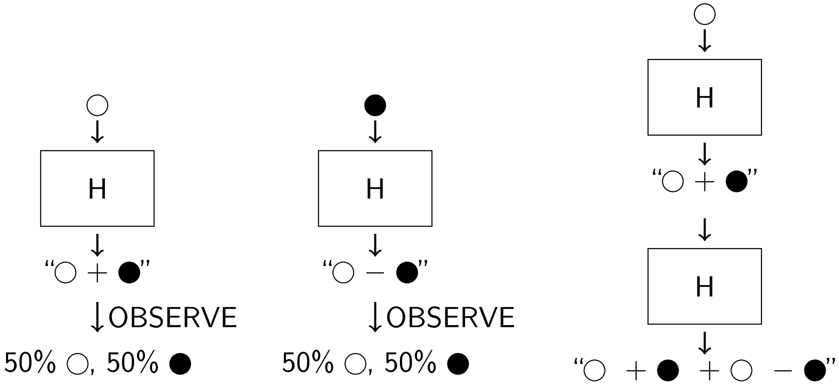


○ ↓ H ↓ “○ + ●” ↓OBSERVE 50% ○, 50% ●

● ↓ H ↓ “○ − ●” ↓OBSERVE 50% ○, 50% ●

○ ↓ H ↓ “○ + ●” ↓ H ↓

“Explanation” of the Hadamard paradox

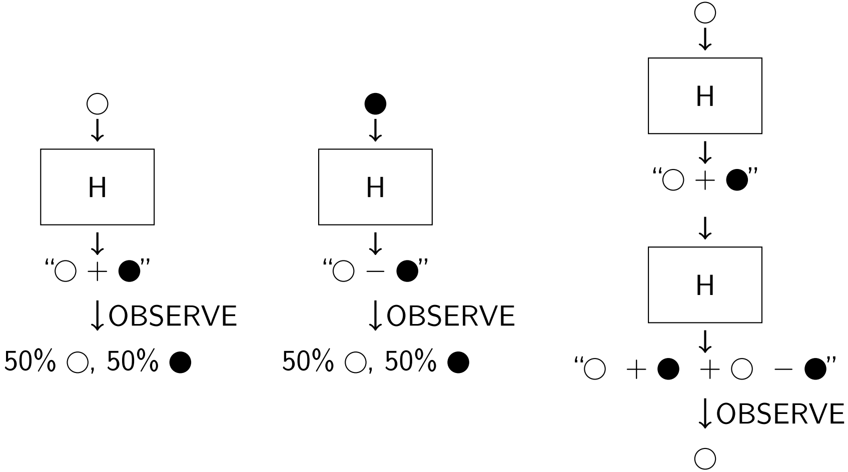


○
↓
H
↓
“○ + ●”
↓OBSERVE
50% ○, 50% ●

●
↓
H
↓
“○ − ●”
↓OBSERVE
50% ○, 50% ●

○
↓
H
↓
“○ + ●”
↓
H
↓
“○ + ● + ○ − ●”

“Explanation” of the Hadamard paradox



○
↓
H
↓
“○ + ●”
↓OBSERVE
50% ○, 50% ●

●
↓
H
↓
“○ − ●”
↓OBSERVE
50% ○, 50% ●

○
↓
H
↓
“○ + ●”
↓
H
↓
“○ + ● + ○ − ●”
↓OBSERVE
○

Bits and Qubits

Classical bit "states"

$\bigcirc, \bullet$

Bits and Qubits

Classical bit "states"

$\bigcirc, \bullet$

Quantum Bit (qubit) states

(some amount of)$\bigcirc$ + (some amount of)$\bullet$

Bits and Qubits

Classical bit “states”

$$\bigcirc, \bullet$$

Quantum Bit (qubit) states

$$\text{(some amount of)}\bigcirc + \text{(some amount of)}\bullet$$

Superposition

$$\text{qubit state} \;=\; \text{superposition of classical bit states}$$

2 Bits and 2 Qubits

States of 2 classical bits

○○, ○●, ●○, ●●

2 Bits and 2 Qubits

States of 2 classical bits

○○, ○●, ●○, ●●

States of 2 quantum bits

a○○ + b○● + c●○ + d●●

2 Bits and 2 Qubits

States of 2 classical bits

○○, ○●, ●○, ●●

States of 2 quantum bits

a○○ + *b*○● + *c*●○ + *d*●●

Superposition

2-qubit state = superposition of classical 2-bit states

2 Bits and 2 Qubits

States of 2 classical bits

○○, ○●, ●○, ●●

States of 2 quantum bits

a○○ + b○● + c●○ + d●●

Superposition

2-qubit state = superposition of classical 2-bit states

Composite systems and subsystems

Putting qubits together forms a *composite* system. The individual qubits in the composite system are *subsystems*.

Outline

1. Introduction
   - Aims of This Talk
   - Misconceptions versus truth that is stranger than fiction
2. Classical Information Processing
   - Encoding
   - Logic gates and circuits
3. Quantum Information Processing
   - The Hadamard gate: superposition and measurement
   - Entanglement
   - Reality
4. Summary

Entangled versus not entangled quantum states

Two examples of 2-qubit states

the "plus-plus" state = ○○ + ○● + ●○ + ●●

the EPR state = ○○ + ●●

Entangled versus not entangled quantum states

Two examples of 2-qubit states

the “plus-plus” state = ○○ + ○● + ●○ + ●●

= (○ + ●)(○ + ●)

the EPR state = ○○ + ●●

Entangled versus not entangled quantum states

Two examples of 2-qubit states

$$\begin{aligned} \text{the ``plus-plus'' state} &= ○○ + ○● + ●○ + ●● \\ &= (○ + ●)(○ + ●) \\ \text{the EPR state} &= ○○ + ●● \\ &\neq \text{(some 1-qubit state)(another 1-qubit state)} \end{aligned}$$

Entangled versus not entangled quantum states

Two examples of 2-qubit states

$$\begin{aligned}\text{the ``plus-plus'' state} &= \bigcirc\bigcirc + \bigcirc\bullet + \bullet\bigcirc + \bullet\bullet \\ &= (\bigcirc + \bullet)(\bigcirc + \bullet) \\ \text{the EPR state} &= \bigcirc\bigcirc + \bullet\bullet \\ &\neq \text{(some 1-qubit state)(another 1-qubit state)}\end{aligned}$$

Product state

A state (like plus-plus) that can be described by states of its subsystems

Entangled versus not entangled quantum states

Two examples of 2-qubit states

the “plus-plus” state = ○○ + ○● + ●○ + ●●

= (○ + ●)(○ + ●)

the EPR state = ○○ + ●●

≠ (some 1-qubit state)(another 1-qubit state)

Product state

A state (like plus-plus) that can be described by states of its subsystems

Entangled state

A state (like EPR) that can*not* be described by states of its subsystems

Computation and Communication

Computation and Communication

What is computation?

Computation and Communication

What is computation?

Minimum ingredients

- Input
- Processor or Computer
- Output

Computation and Communication

What is computation?

Minimum ingredients

- Input
- Processor or Computer
- Output

$$m \longrightarrow \boxed{\quad \mathcal{C} \quad} \longrightarrow \mathcal{C}(m)$$

Computation and Communication, cont'd

What is computation?

Computation and Communication, cont'd

What is computation?

Minimum ingredients

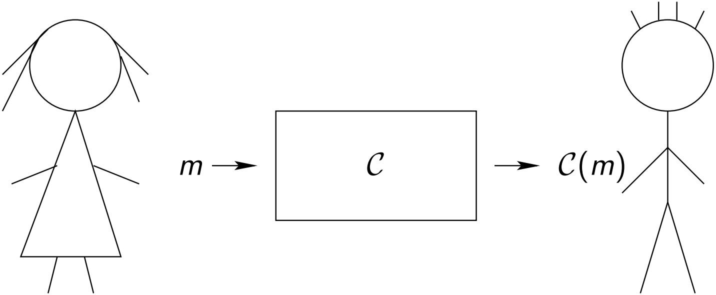
- Two parties: Sender and Receiver
- Message: Information to be sent
- Channel: Medium by which information is sent

Computation and Communication, cont'd

What is computation?

Minimum ingredients

- Two parties: Sender and Receiver
- Message: Information to be sent
- Channel: Medium by which information is sent

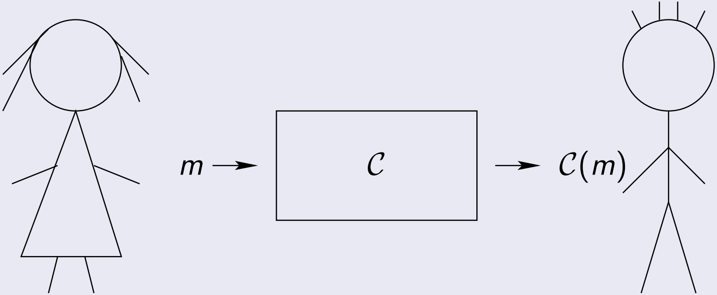


Information Processing

Computation

$$m \longrightarrow \boxed{\quad \mathcal{C} \quad} \longrightarrow \mathcal{C}(m)$$

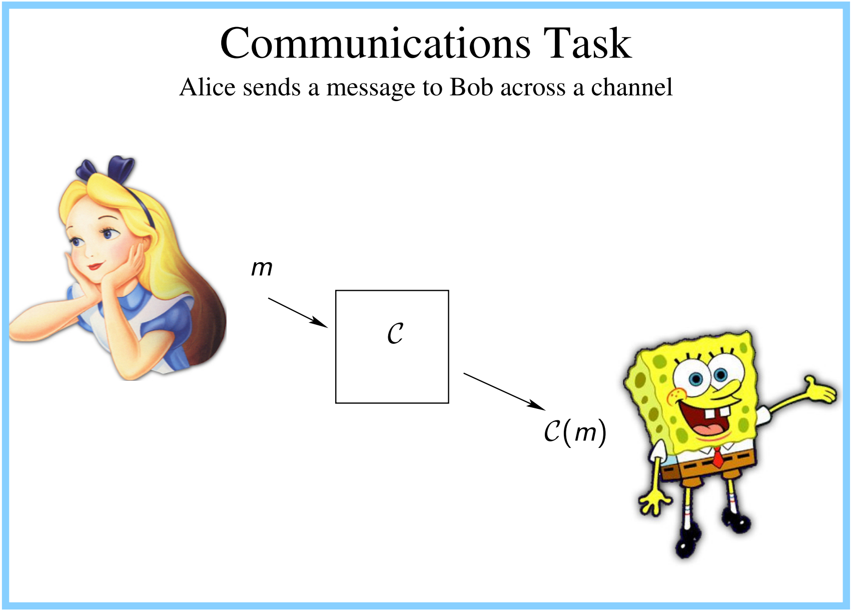
Communication



Cultural note on sender and receiver

- Sender is traditionally called “Alice”
- Receiver is traditionally called “Bob”
- Slides must be funny

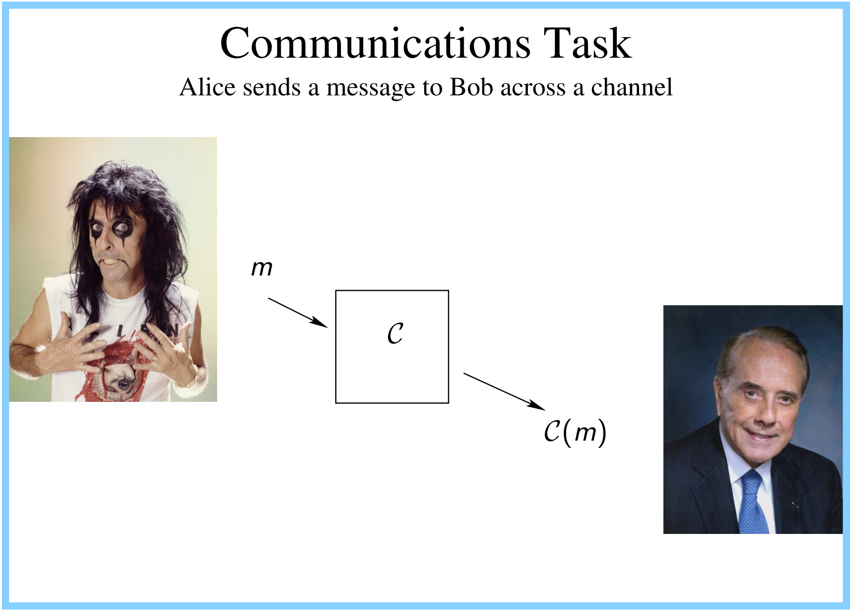
Typical information theory talk slide



Communications Task

Alice sends a message to Bob across a channel

Improved information theory talk slide



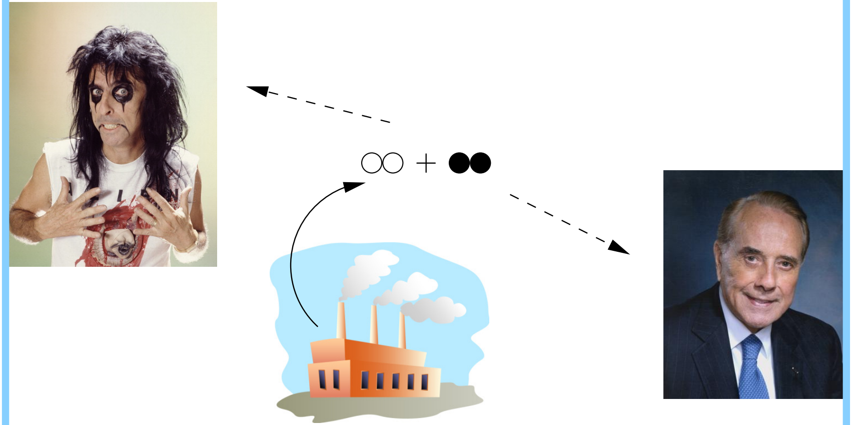
Communications Task

Alice sends a message to Bob across a channel

EPR Paradox

EPR Protocol Step 1

Factory prepares state ○○ + ●●
Sends 1 qubit to Alice, 1 to Bob



○○ + ●●

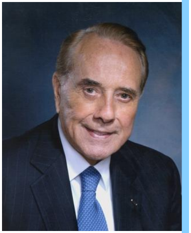
EPR Paradox

EPR Protocol Step 2

Alice measures his qubit

I got ●

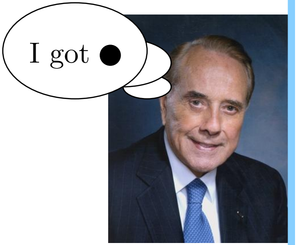
Post measurement state is ●●



EPR Protocol Step 3

Bob measures his qubit

Post measurement state is ●●



EPR Paradox

Alice's measurement determines the result of Bob's. Even if they are separated by great distance.

EPR Paradox

Alice's measurement determines the result of Bob's. Even if they are separated by great distance.

This is *not* science fiction. This EPR experiment is performed routinely in labs all over the world on a daily basis.

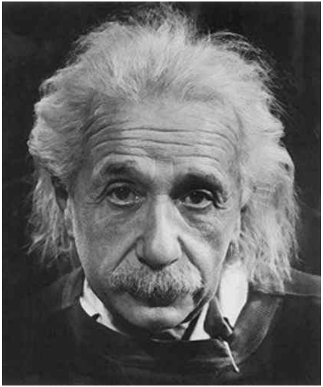
EPR Paradox

Alice's measurement determines the result of Bob's. Even if they are separated by great distance.

This is *not* science fiction. This EPR experiment is performed routinely in labs all over the world on a daily basis.

The first experiment to demonstrate the EPR measurement was by Alain Aspect in 1982.

Intellectual dissonance



“. . . spooky action at a distance”

Outline

1. Introduction
   - Aims of This Talk
   - Misconceptions versus truth that is stranger than fiction
2. Classical Information Processing
   - Encoding
   - Logic gates and circuits
3. Quantum Information Processing
   - The Hadamard gate: superposition and measurement
   - Entanglement
   - Reality
4. Summary

Some philosophical problems

- Is the quantum state real? What is the status of the objects that appear in the mathematical model?

Some philosophical problems

- Is the quantum state real? What is the status of the objects that appear in the mathematical model?
- Observation, observer, measurements—all are very troublesome.

Some philosophical problems

- Is the quantum state real? What is the status of the objects that appear in the mathematical model?
- Observation, observer, measurements—all are very troublesome.
- Nonlocality is very troublesome.

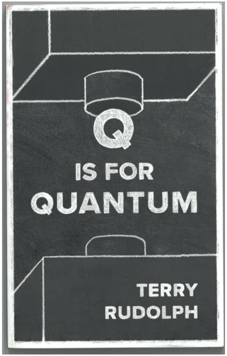
Some main points

- Quantum mechanics is a practical, successful theory.
- Our use of quantum mechanics to predict outcomes of experiments is sophisticated and precise.
- Our ability to explain its meaning is primitive.
- We live in an exciting time.

Thank you! `http://quantum.lvc.edu/mathphys`

Lebanon Valley College

NSF


Q IS FOR QUANTUM

TERRY RUDOLPH

Cool things that might be true

- Time travel can not (yet) be ruled out
- Black holes leak information
- Whether $P = NP$?
- Birds might do quantum computations for navigation