# Book review: "Q is for Quantum" by Terry Rudolf

David W. Lyons

Professor of Mathematical Sciences, Lebanon Valley College

Cornwall Manor, 5 August 2019

# Outline

# Outline

# Rudolf's motivation for the book

## (from the Preface)

"This book is written for my 15-year old self [. . . ] I was interested in [. . . ] science, and I distinctly recall being frustrated by the lack of concrete explanations within "pop-sci" accounts of modern physics.

# Rudolf's motivation for the book

## (from the Preface)

"This book is written for my 15-year old self [. . . ] I was interested in [. . . ] science, and I distinctly recall being frustrated by the lack of concrete explanations within "pop-sci" accounts of modern physics.

The exciting descriptions [. . . ] were ultimately hollow. They were vague on details and they came loaded with jargon, questionable analogies, and [. . . ] mysterious pontifications [. . . ]

# Rudolf's intentions for the book

Rudolf hopes to shed some light, without technical obstructions, on

- quantum computers
- quantum entanglement
- philosophical questions

# Rudolf's intentions for the book

Rudolf hopes to shed some light, without technical obstructions, on

- quantum computers
- quantum entanglement
- philosophical questions

**(p. 23)**

"It is fascinating that we have this incredibly precise theory, which [. . . ] is going to let us build marvelous new devices, and yet we are still arguing about what it all really means."

# Outline

# 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

# Coding 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 |

# Coding information in strings of bits

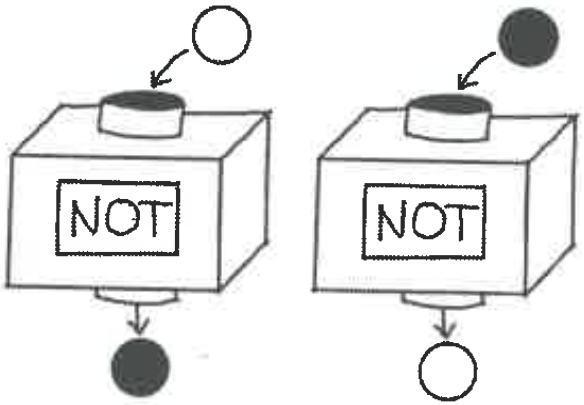
## ASCII - Binary Character Table

| 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 |

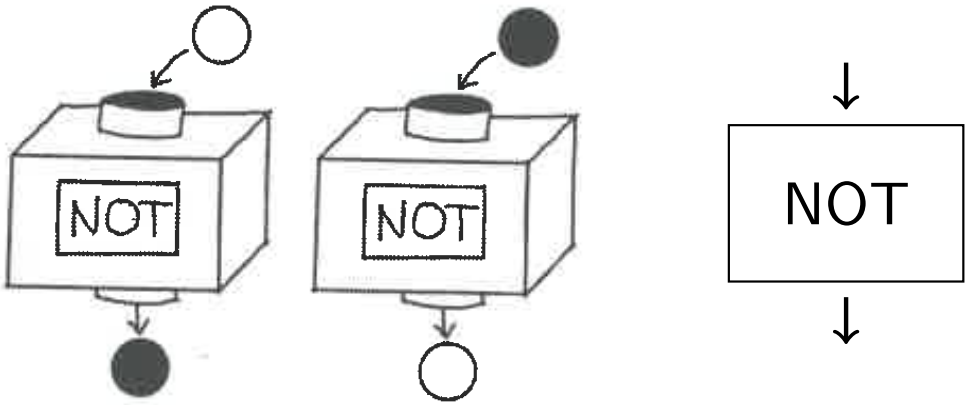
$G = 01000111 =$ ○●○○○●●●

# Outline

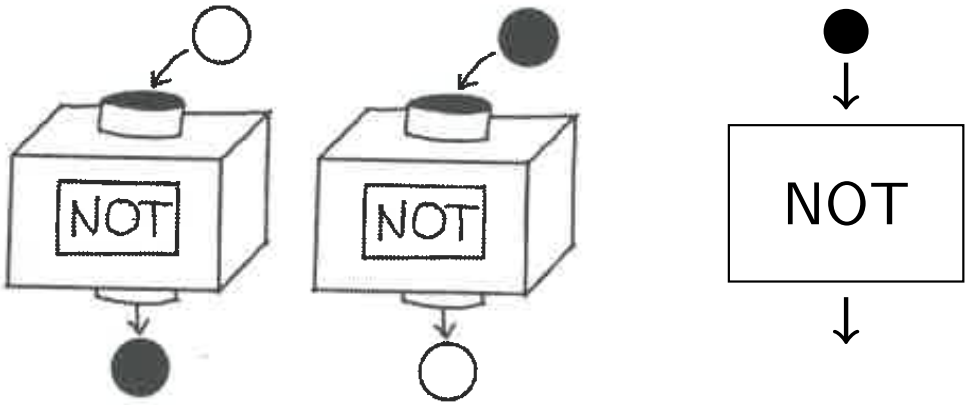
# NOT gates



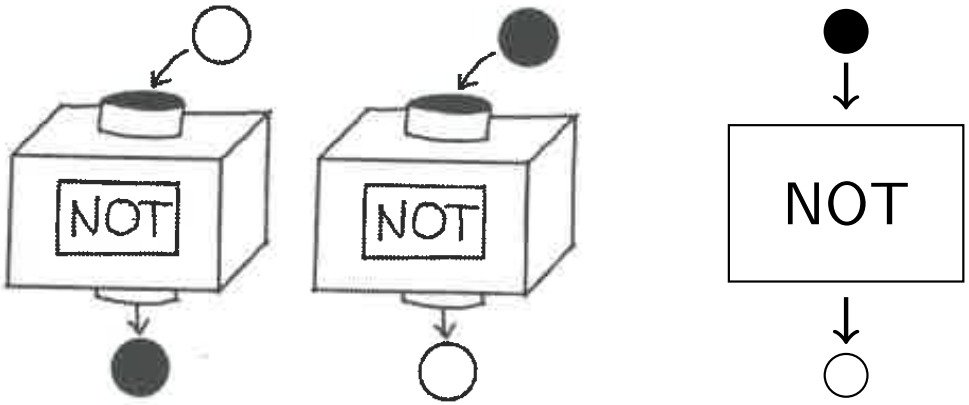
# NOT gates



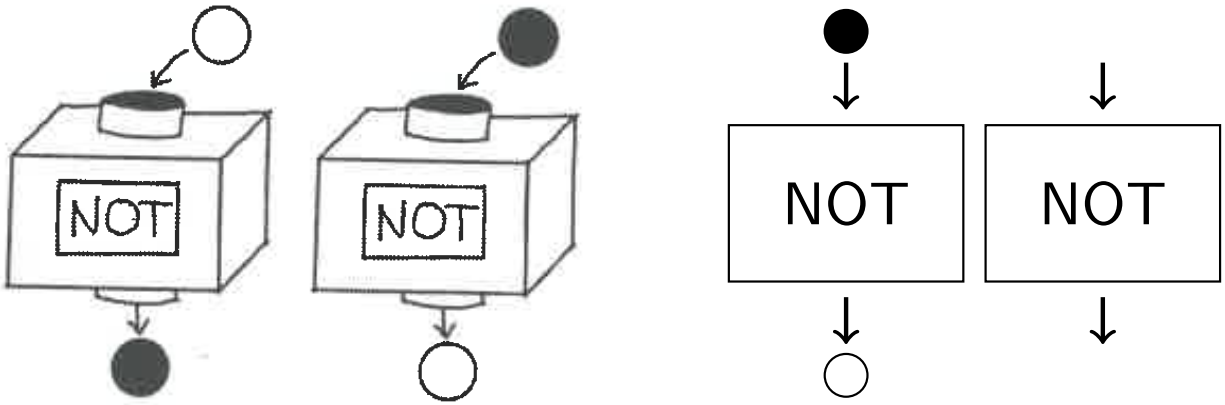
# NOT gates



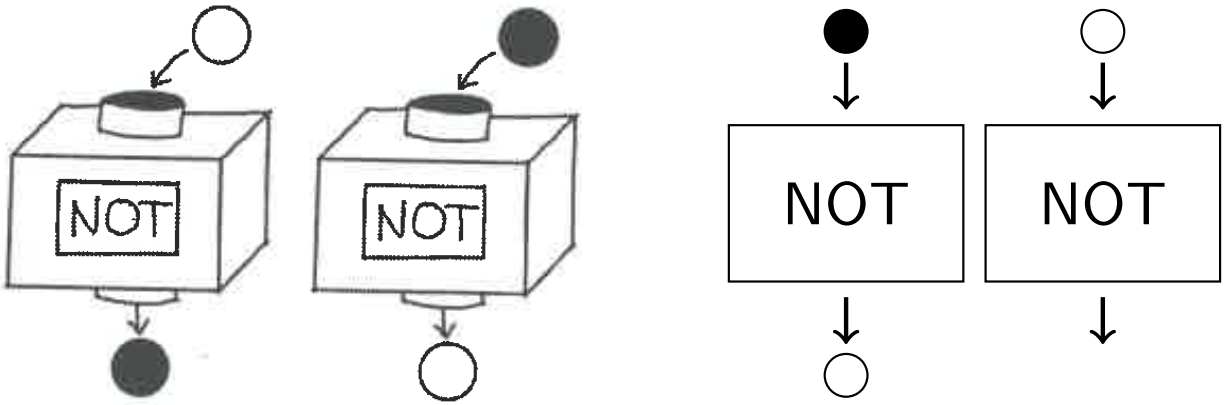
# NOT gates



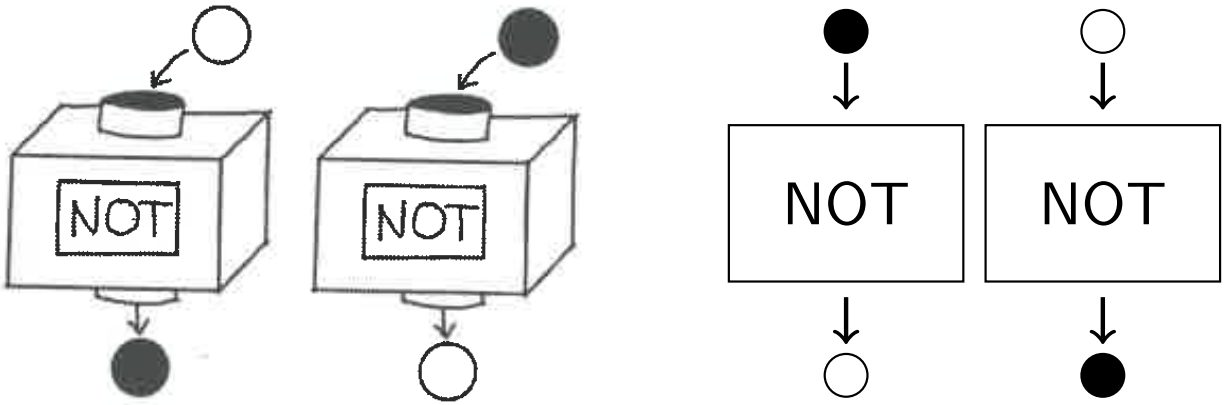
# NOT gates



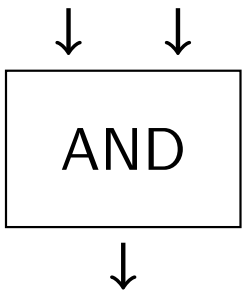
# NOT gates



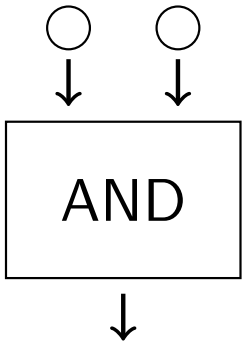
# NOT gates



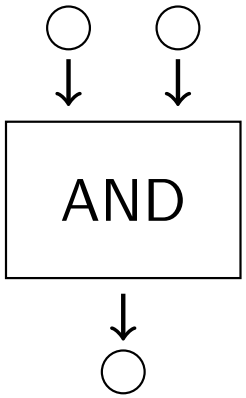
# More gates



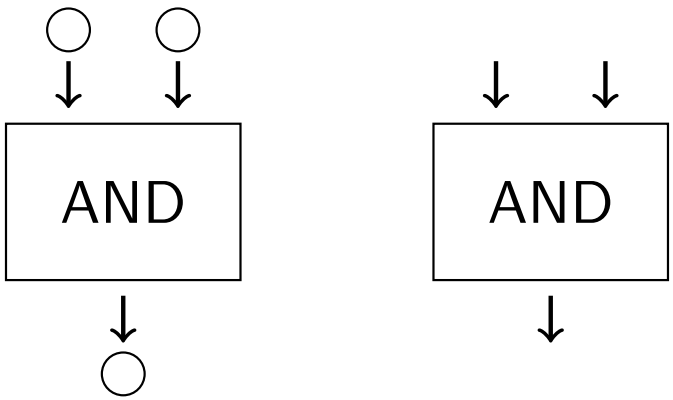
# More gates



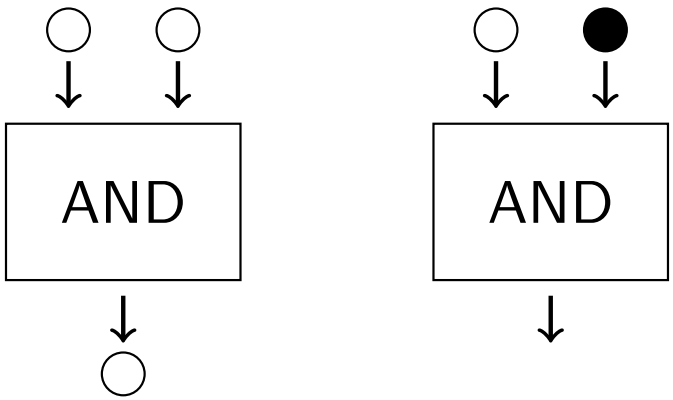
# More gates



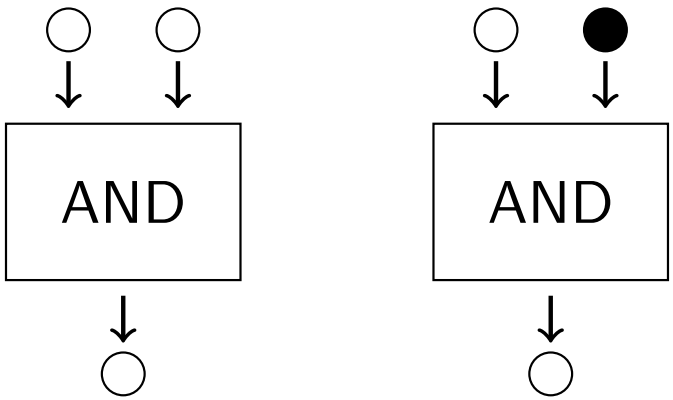
# More gates



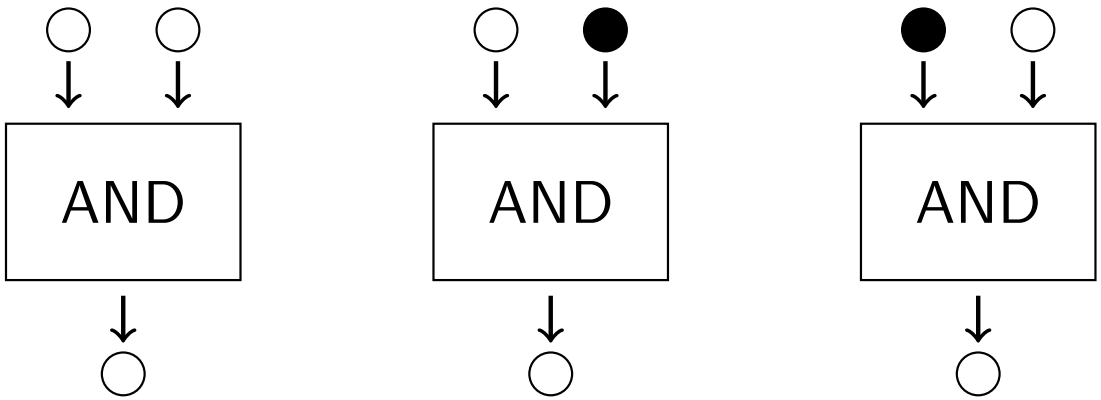
# More gates



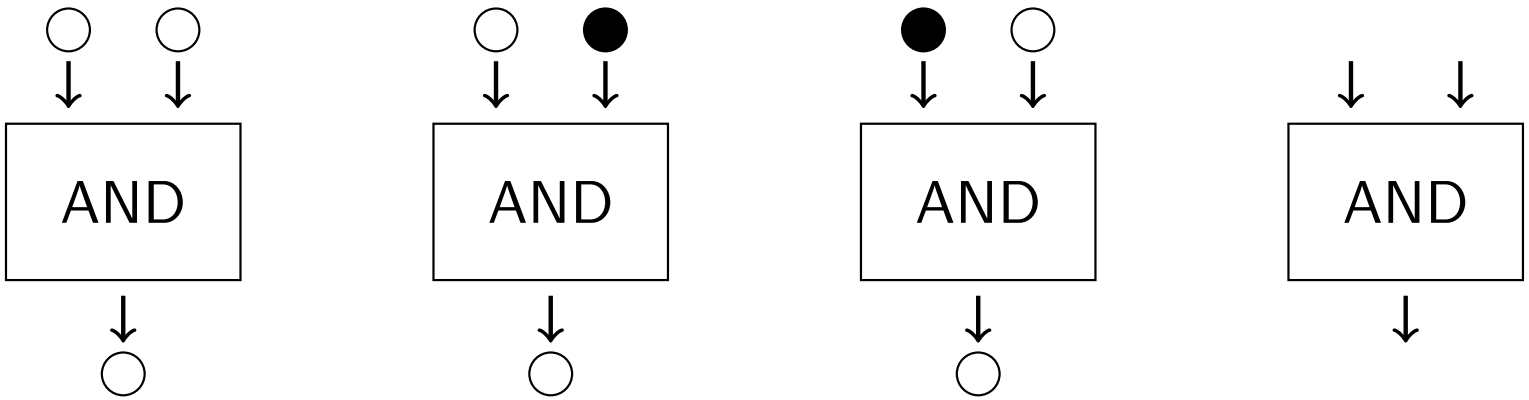
# More gates



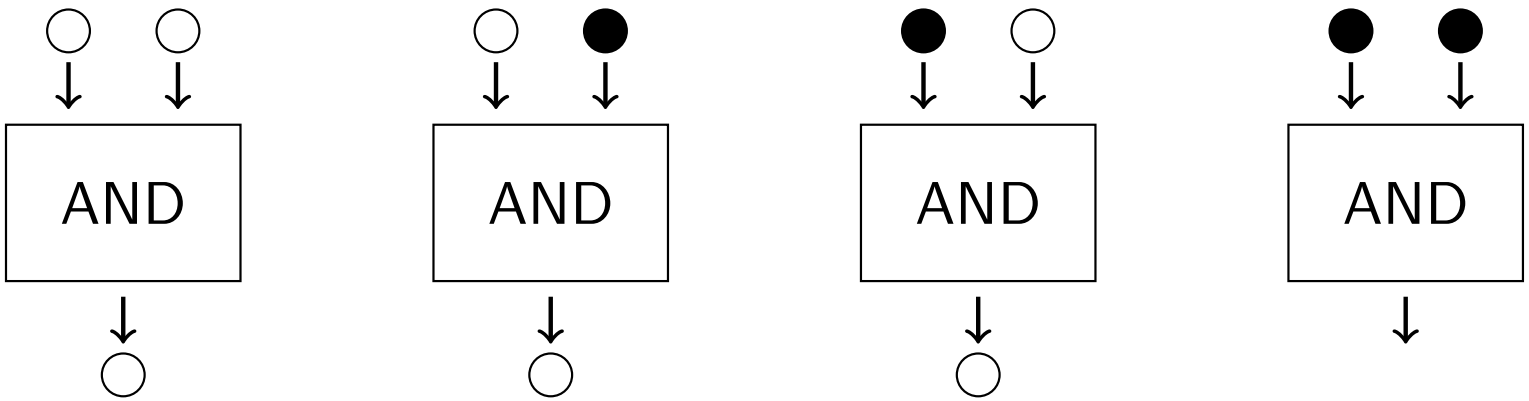
# More gates



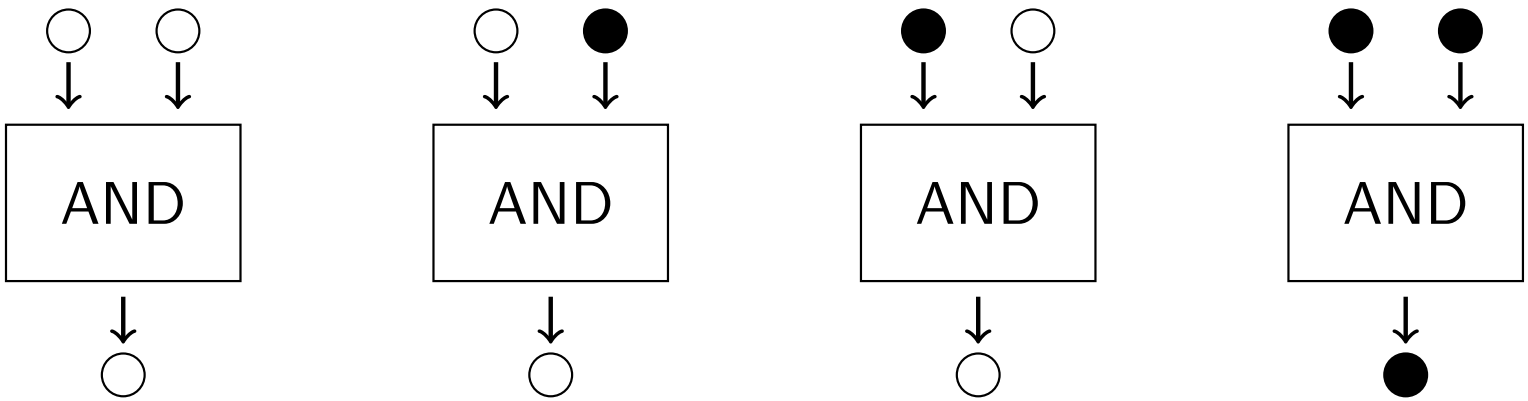
# More gates



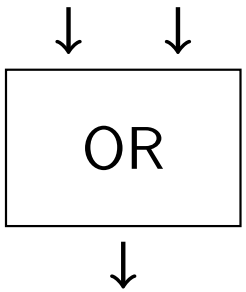
# More gates



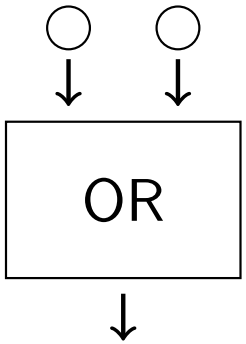
# More gates



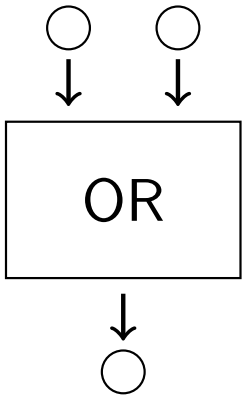
# More gates, cont'd



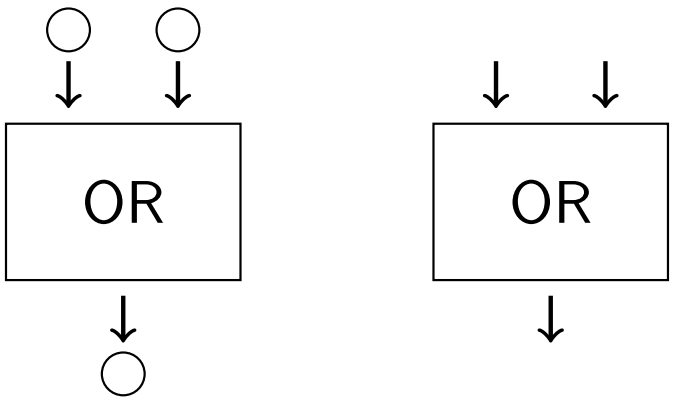
# More gates, cont'd



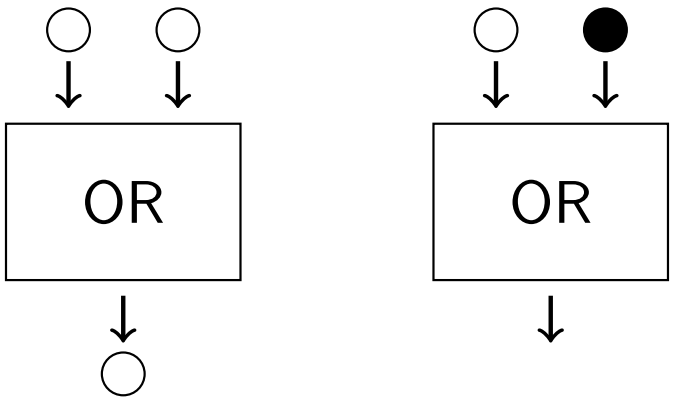
# More gates, cont'd



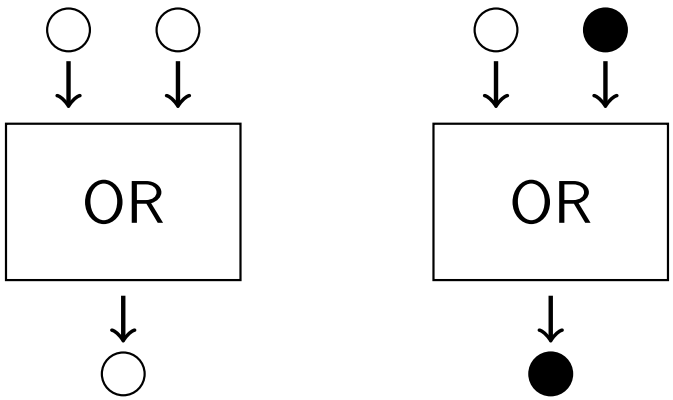
# More gates, cont'd



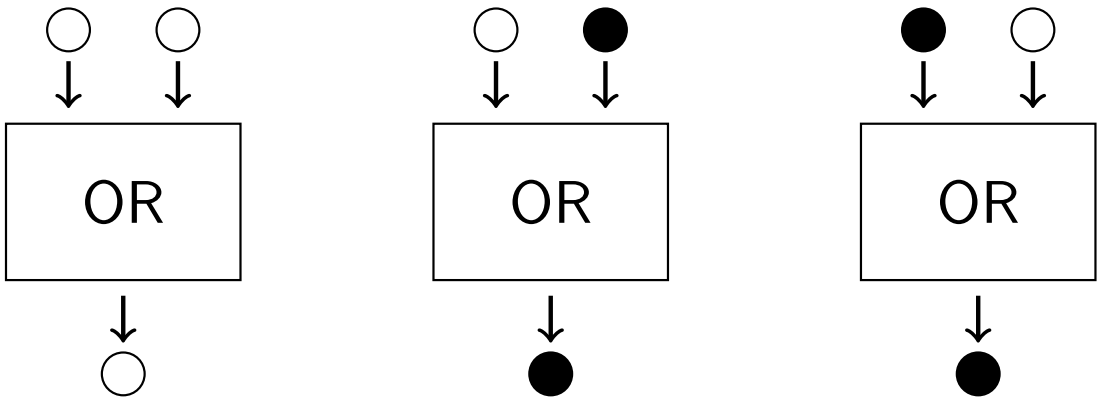
# More gates, cont'd



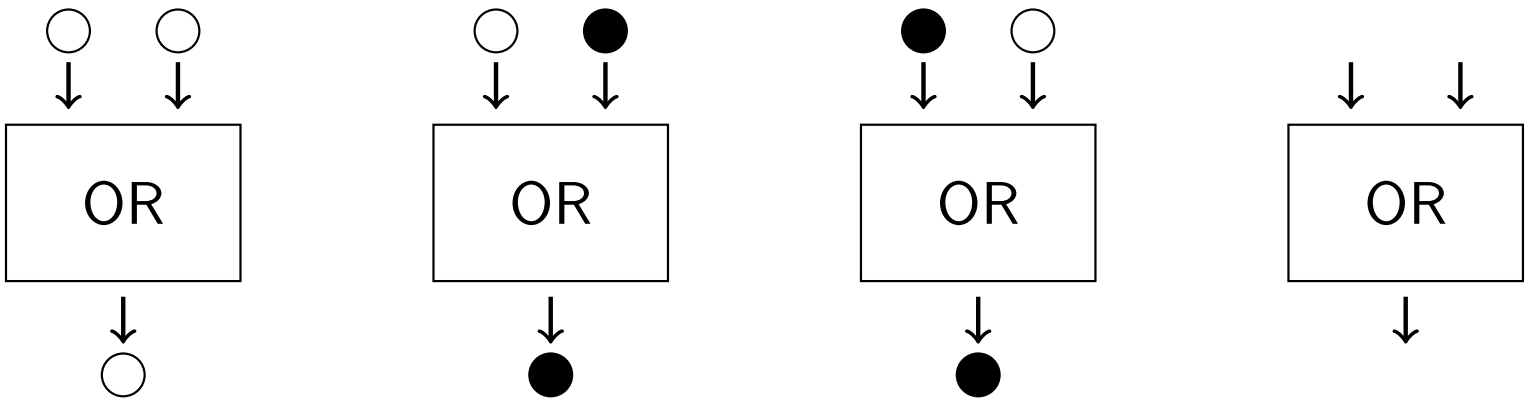
# More gates, cont'd



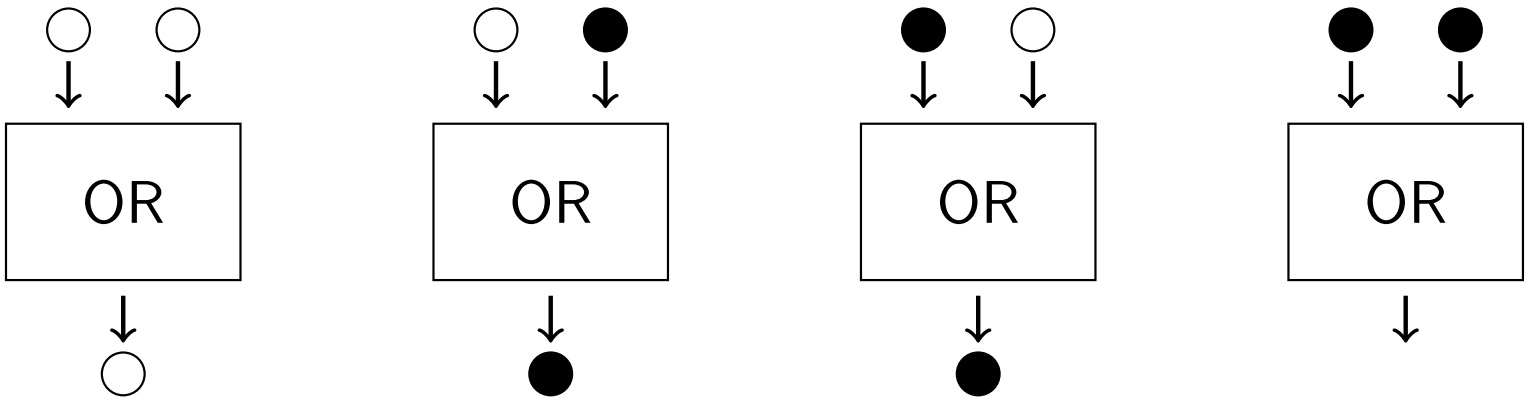
# More gates, cont'd



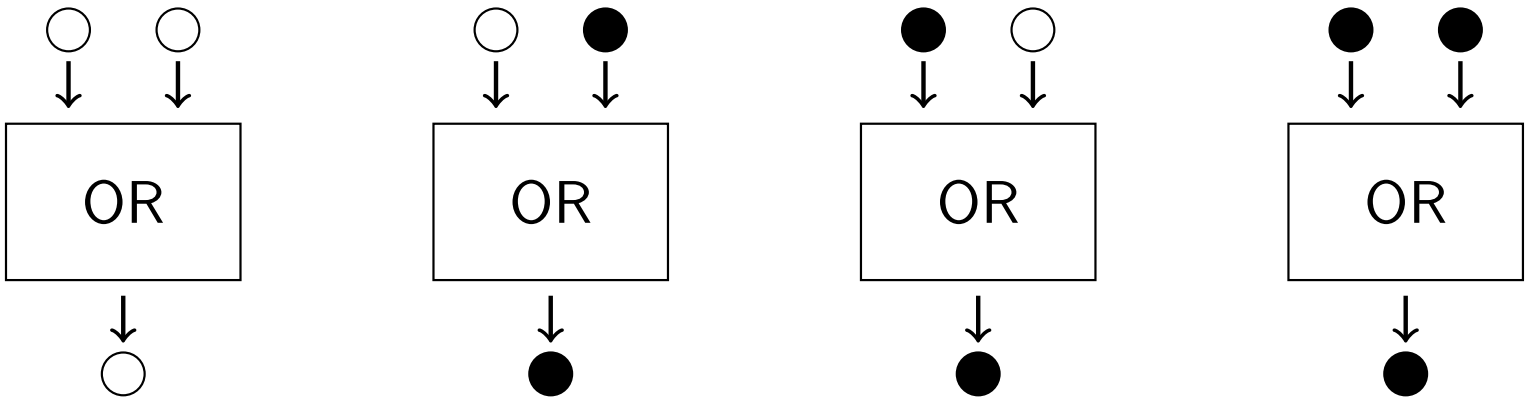
# More gates, cont'd



# More gates, cont'd



# More gates, cont'd



# 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?

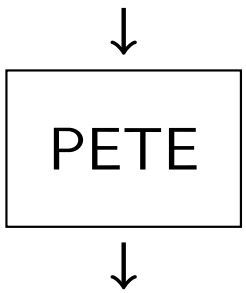
A classical computer is made entirely of NOT, AND, and OR boxes. The balls that pass through the boxes are bits.

## Quantum computers

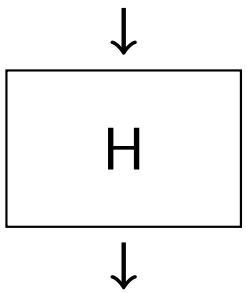
A quantum computer is also made of boxes, but new kinds of boxes are available. The balls that pass through the boxes are *quantum* bits, or qubits.

# Outline

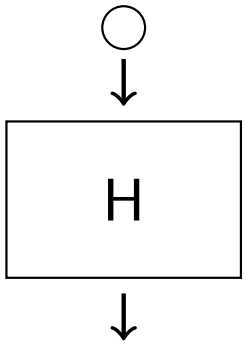
# A quantum gate called “PETE”



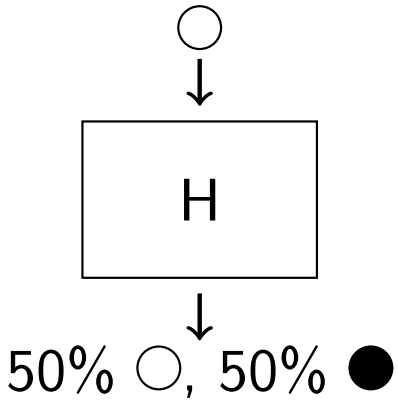
# A quantum gate called “PETE”



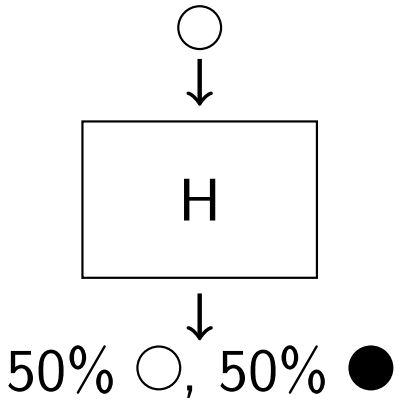
# A quantum gate called “PETE”

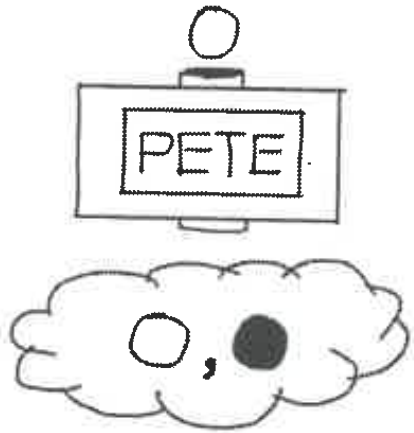


# A quantum gate called “PETE”

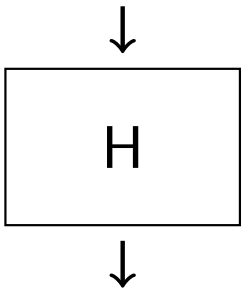


# A quantum gate called “PETE”

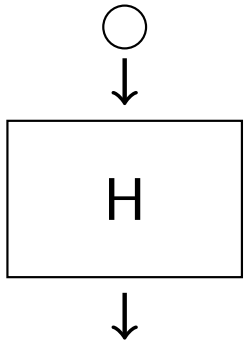


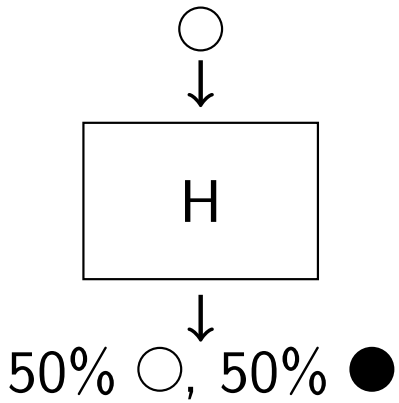
# Hadamard ("PETE") gate, cont'd



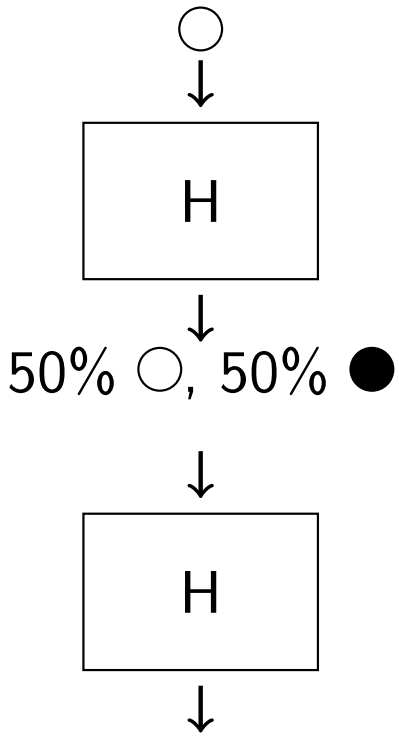
# Hadamard ("PETE") gate, cont'd



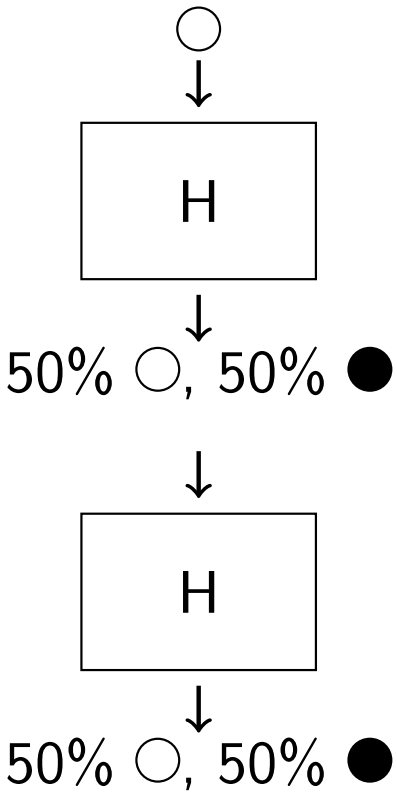
# Hadamard ("PETE") gate, cont'd



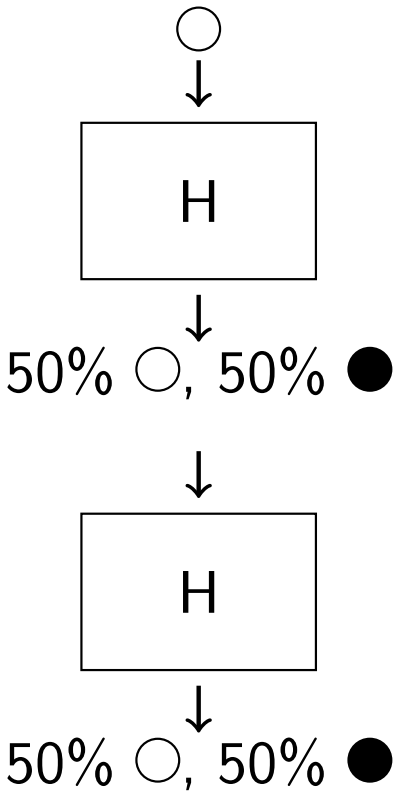
# Hadamard ("PETE") gate, cont'd

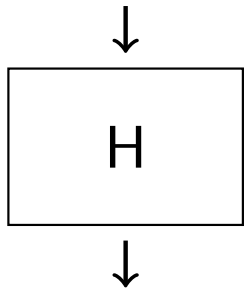


# Hadamard ("PETE") gate, cont'd

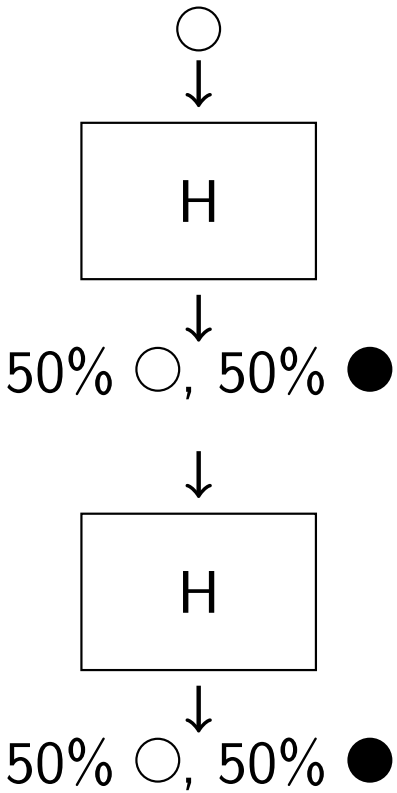


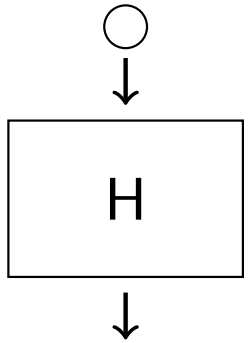
# Hadamard ("PETE") gate, cont'd



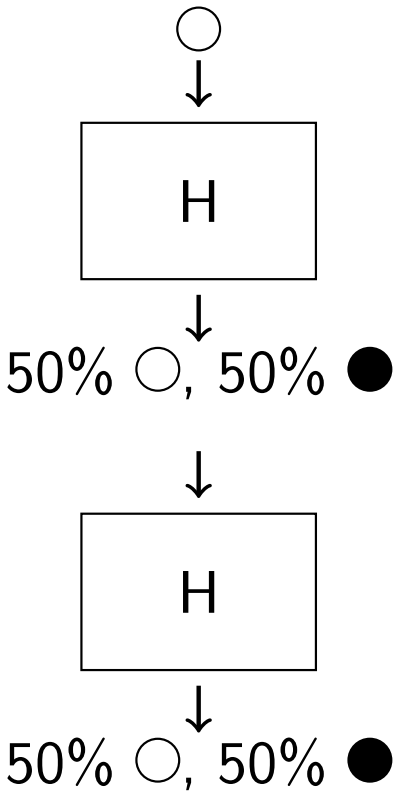



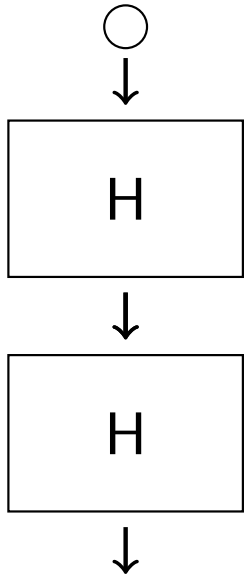
# Hadamard ("PETE") gate, cont'd



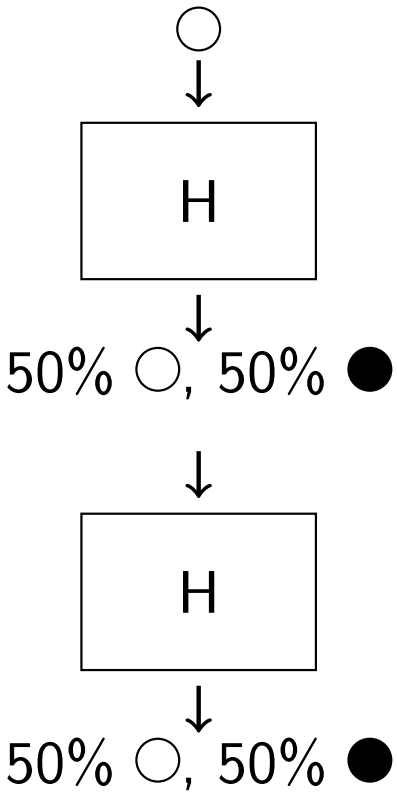



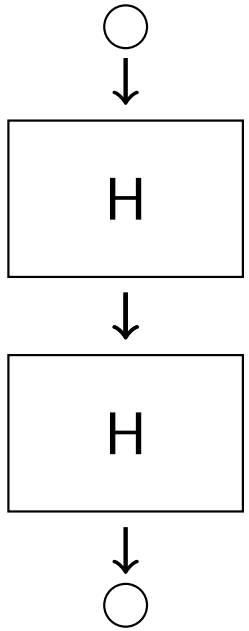
# Hadamard ("PETE") gate, cont'd



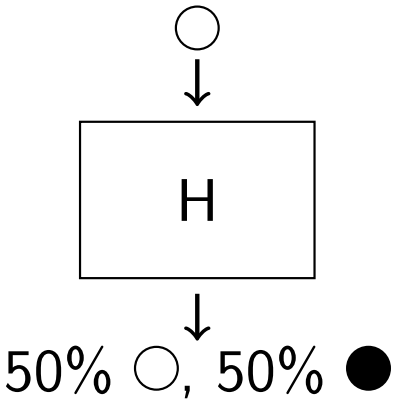



# Hadamard ("PETE") gate, cont'd

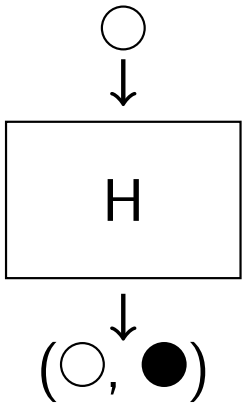


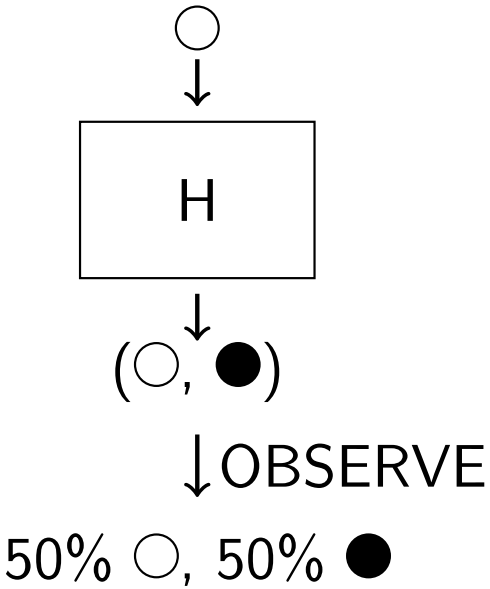
# “Explanation” of the “PETE” paradox



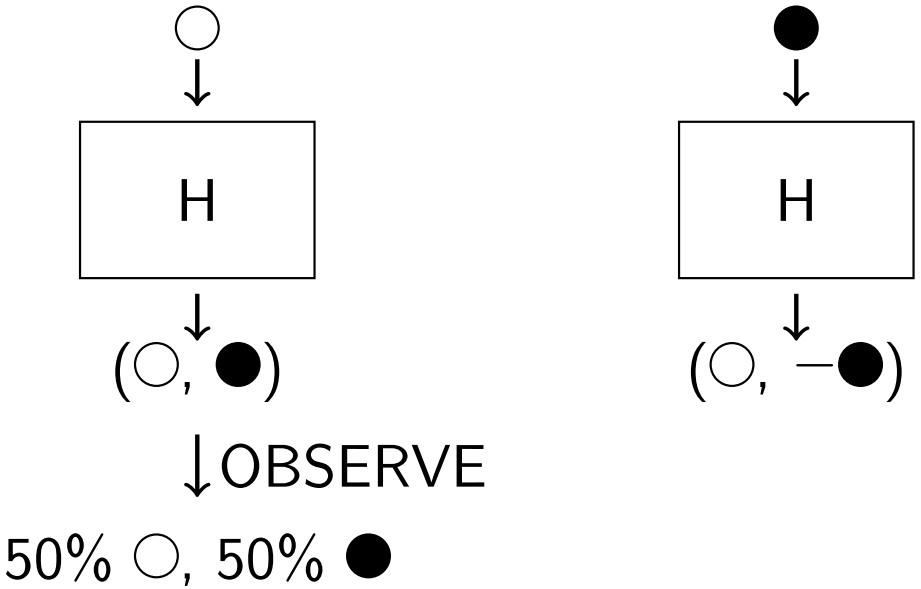
# “Explanation” of the “PETE” paradox



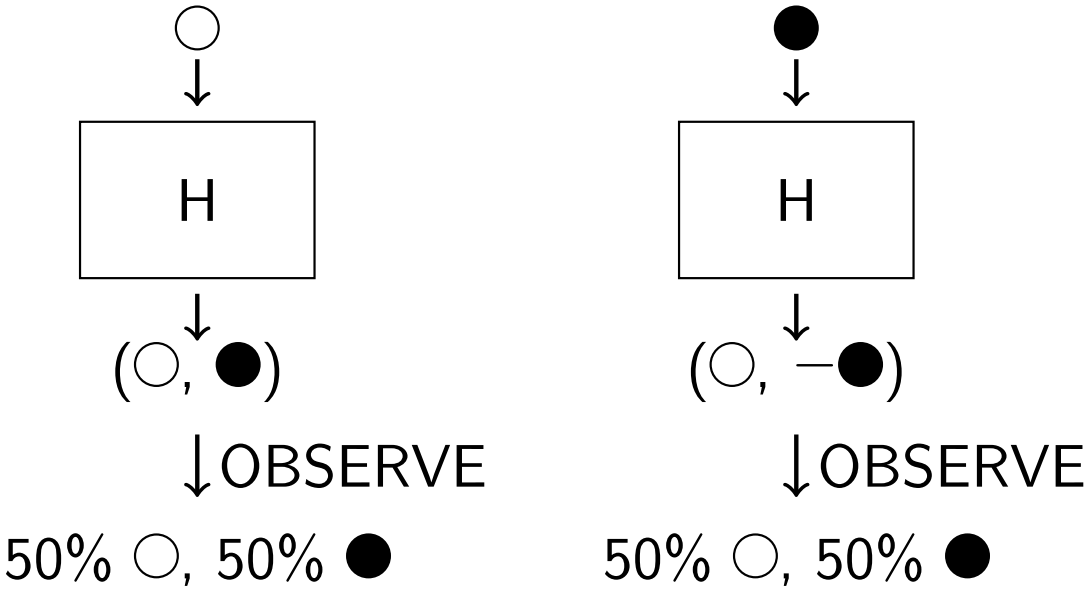
# “Explanation” of the “PETE” paradox



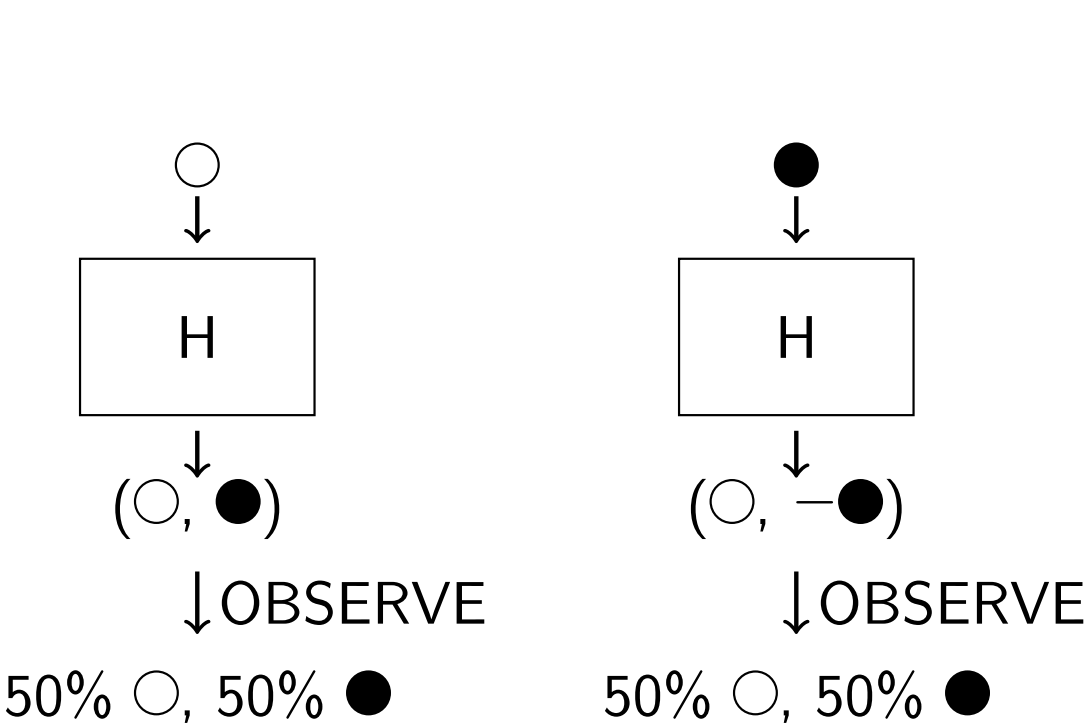
# “Explanation” of the “PETE” paradox



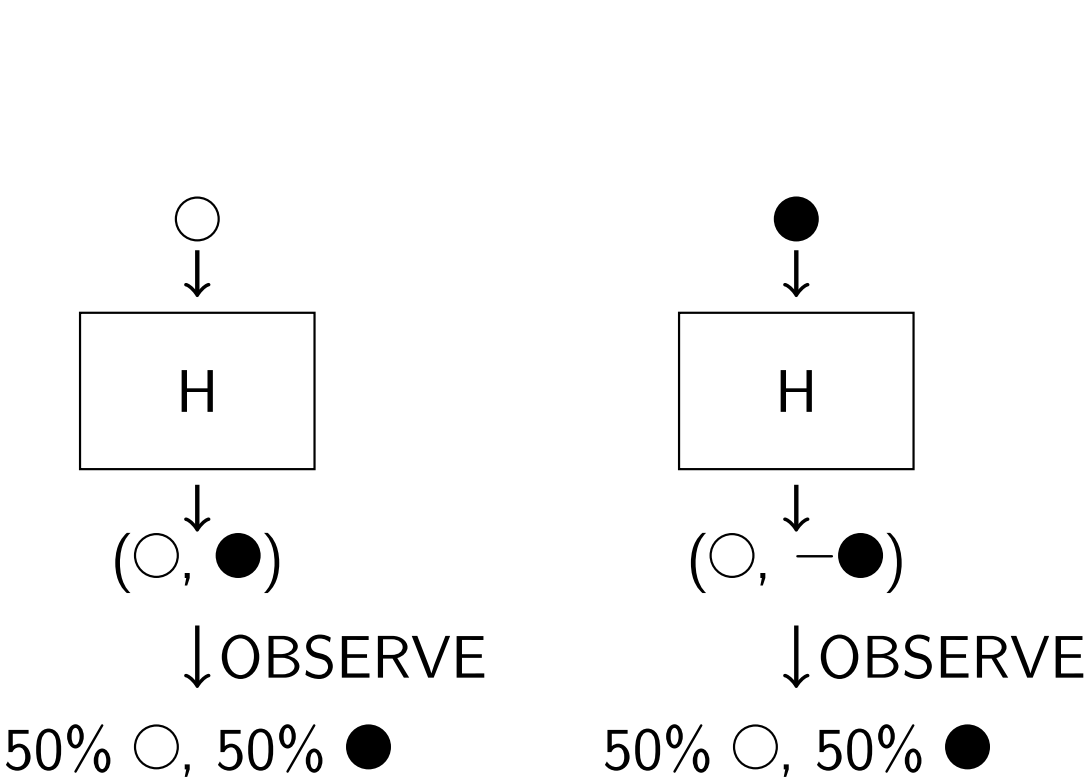
# “Explanation” of the “PETE” paradox

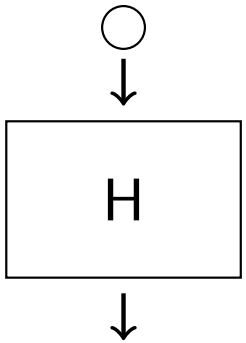


# “Explanation” of the “PETE” paradox

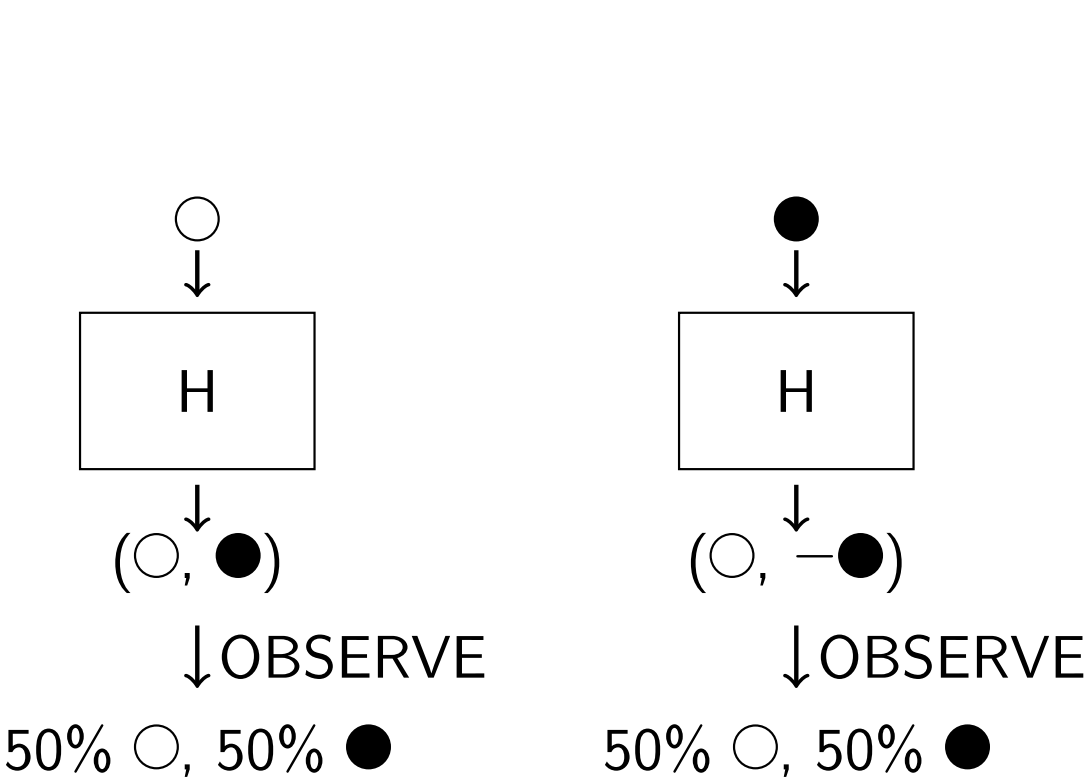


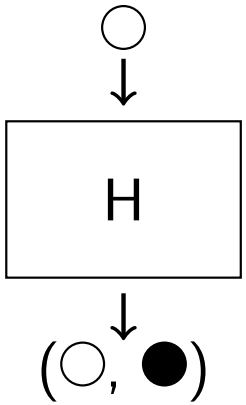
# “Explanation” of the “PETE” paradox



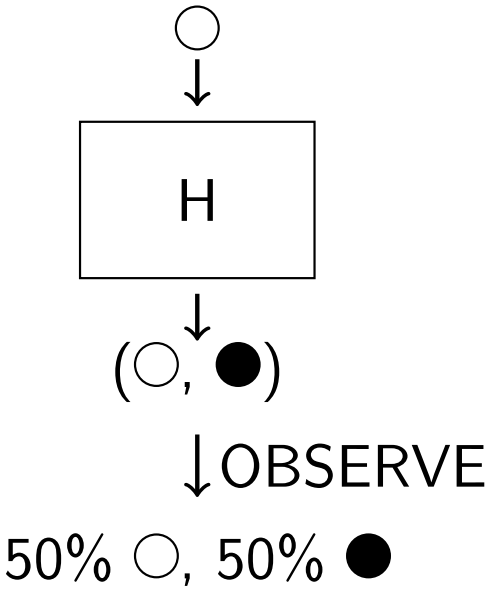



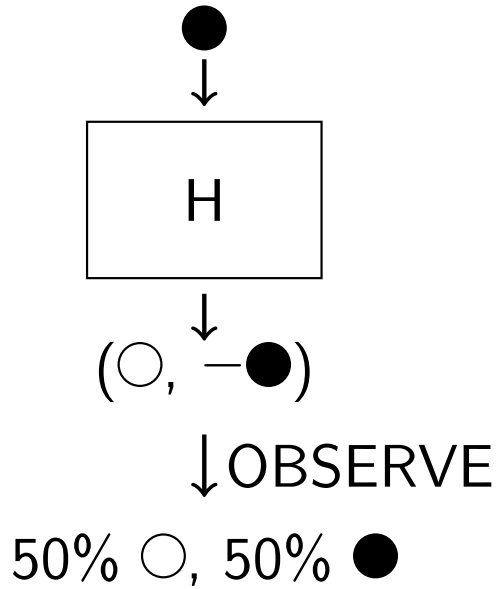
# "Explanation" of the "PETE" paradox

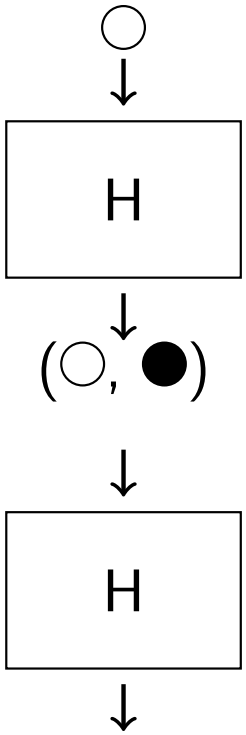


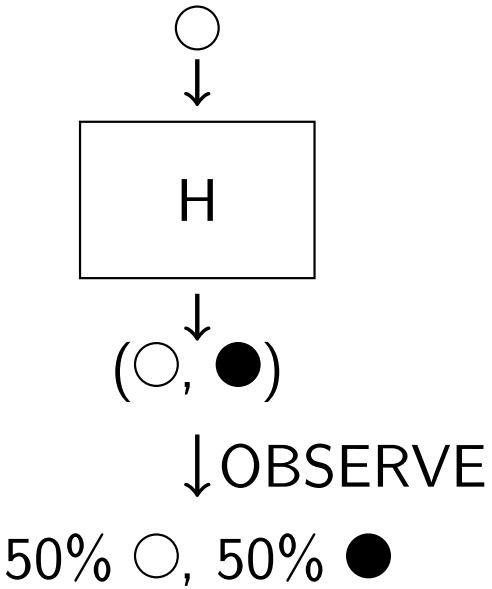
# "Explanation" of the "PETE" paradox

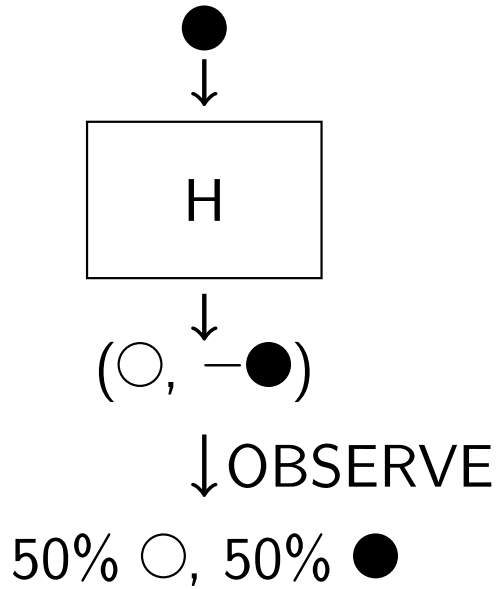


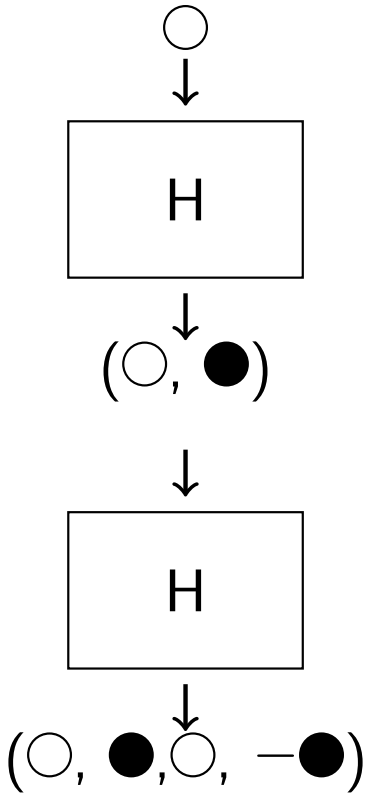



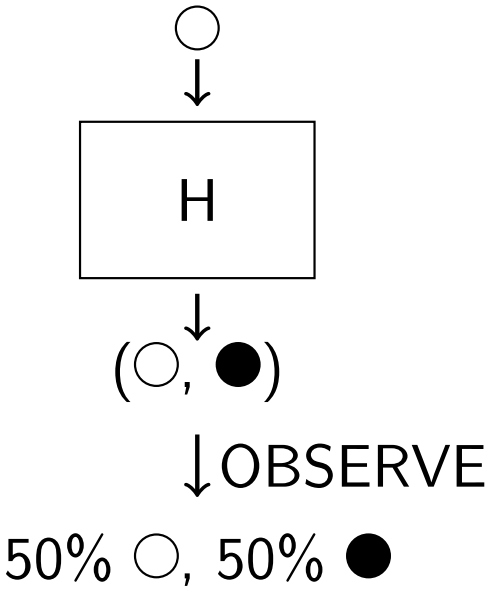
# “Explanation” of the “PETE” paradox

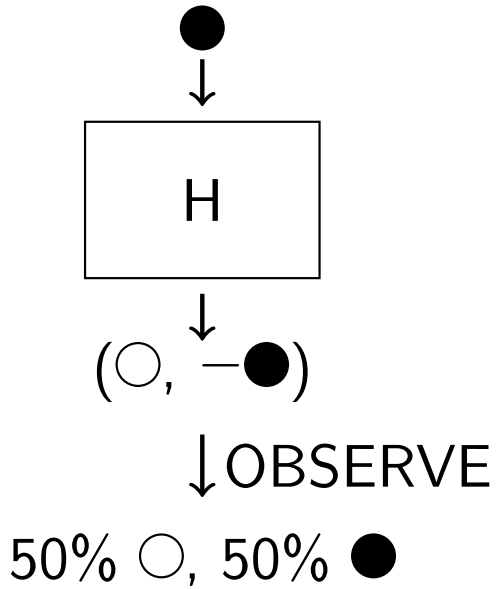


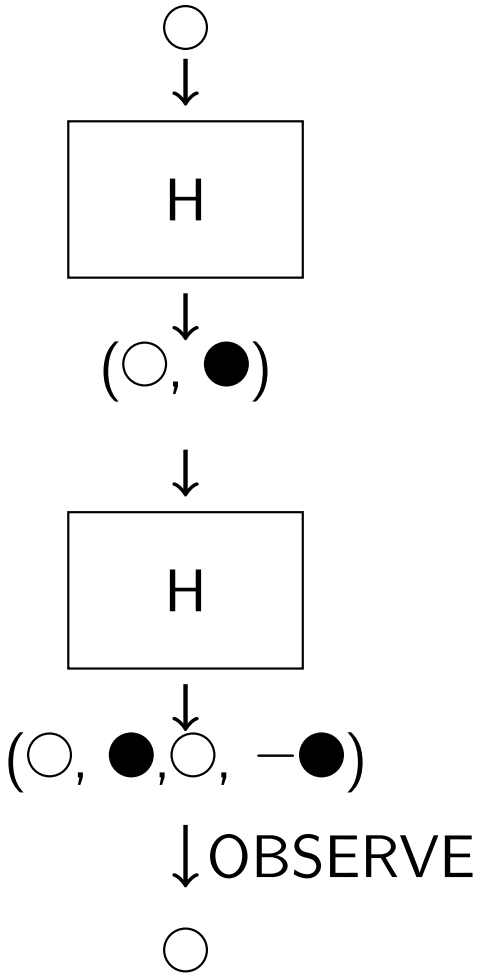



# “Explanation” of the “PETE” paradox



# Outline

# Communication and Computation

# Communication and Computation

**What is communication?**

# Communication and Computation

**What is communication?**

Minimum ingredients

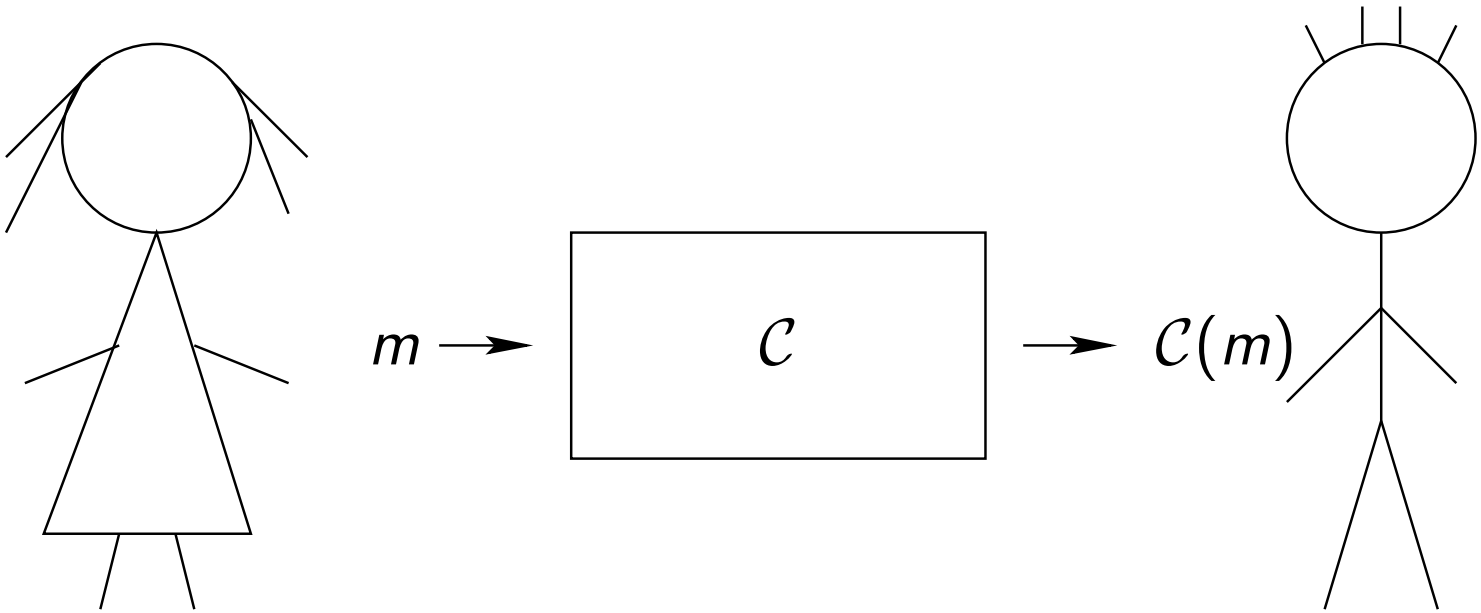
- Two parties: Sender and Receiver
- Message: Information to be sent
- Channel: Medium by which information is sent

# Communication and Computation

**What is communication?**

Minimum ingredients

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



# Theory of Computation: Abstract Study of Information Processing

**What is computation?**

# Theory of Computation: Abstract Study of Information Processing

**What is computation?**

Minimum ingredients

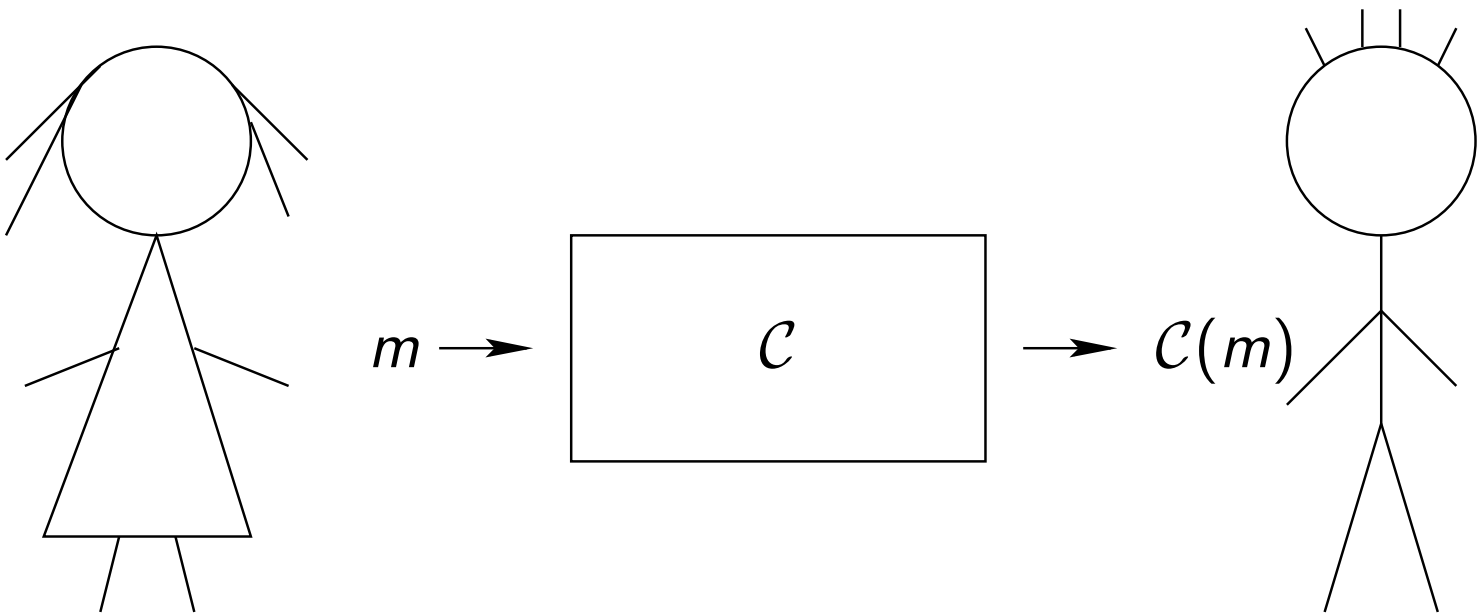
- Input
- Processor or Computer
- Output

# Theory of Computation: Abstract Study of Information Processing

**What is computation?**

Minimum ingredients

- Input
- Processor or Computer
- Output



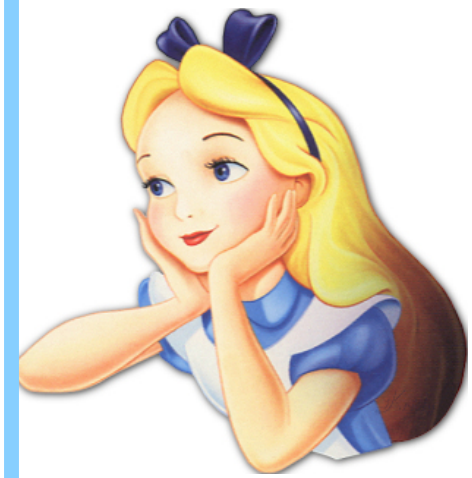
# Cultural note on sender and receiver

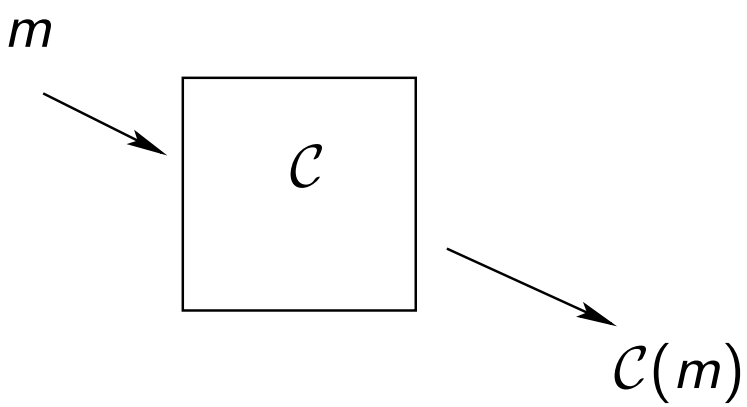
- Sender is traditionally called “Alice”
- Receiver is traditionally called “Bob”
- Slides must be funny

# Typical information theory talk slide

## Communications Task

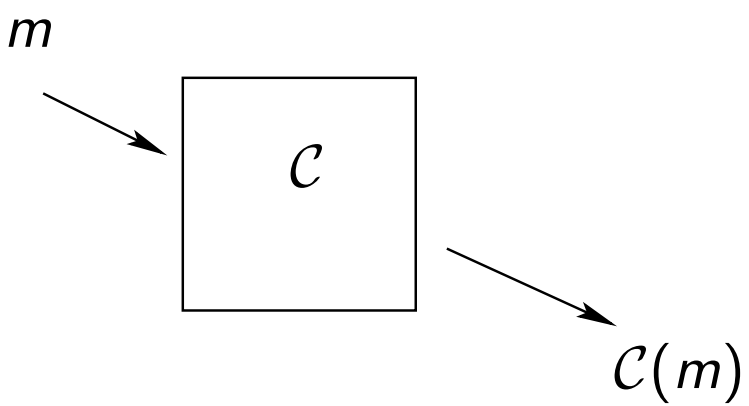
Alice sends a message to Bob across a channel

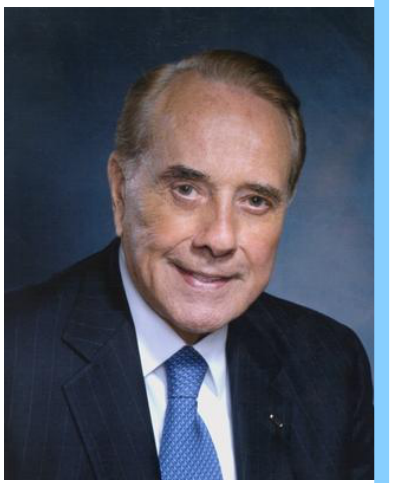





# Communications Task

Alice sends a message to Bob across a channel

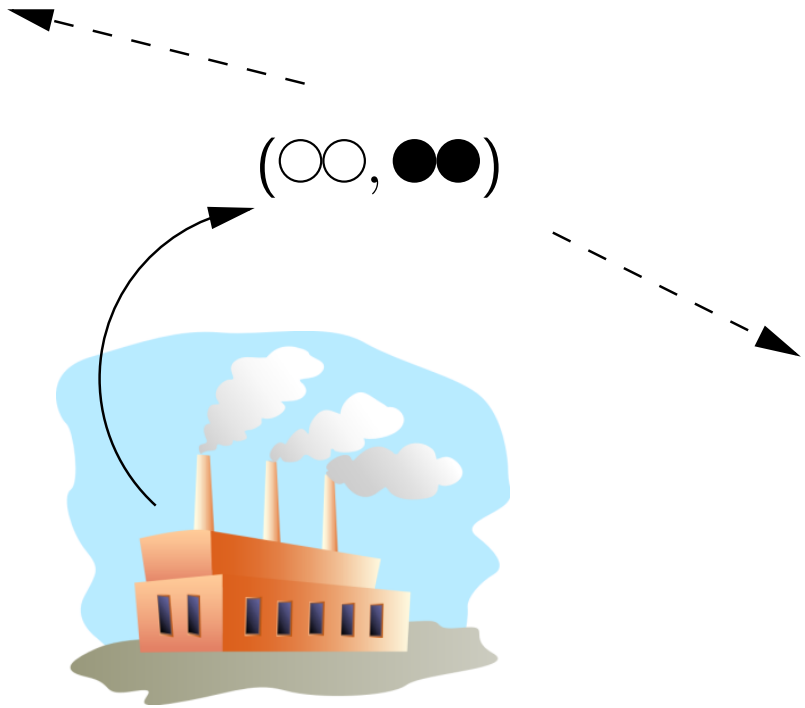


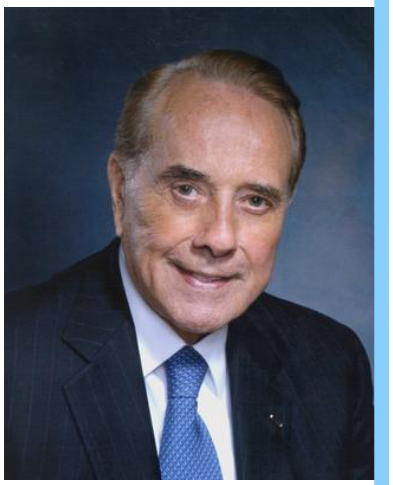



# EPR Protocol Step 1

Factory prepares state (○○, ●●)

Sends 1 qubit to Alice, 1 to Bob

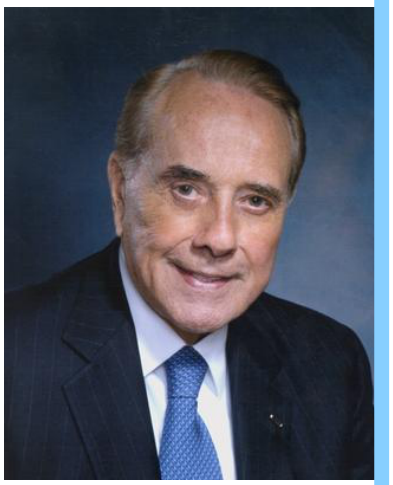


# EPR Protocol Step 2

Alice measures his qubit

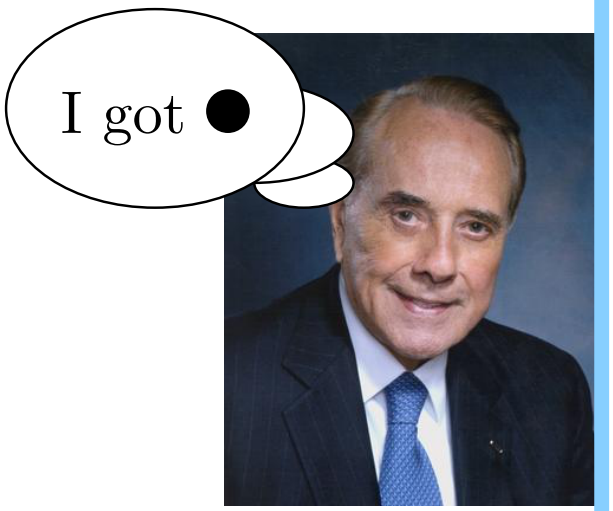

Post measurement state is (●, ●)



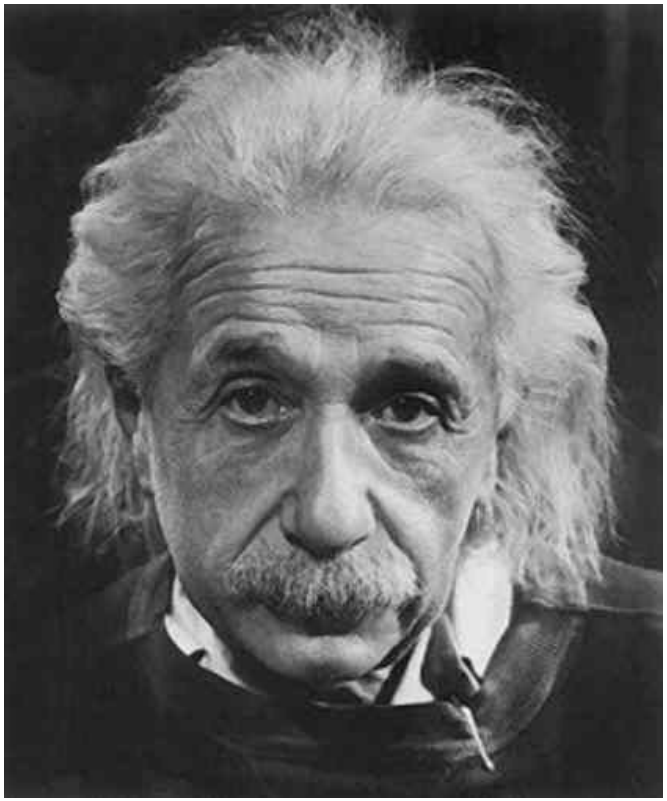
# EPR Protocol Step 3

Bob measures his qubit

Post measurement state is (●, ●)



# Intellectual dissonance



"...spooky action at a distance"

# 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.

# Outline

# 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

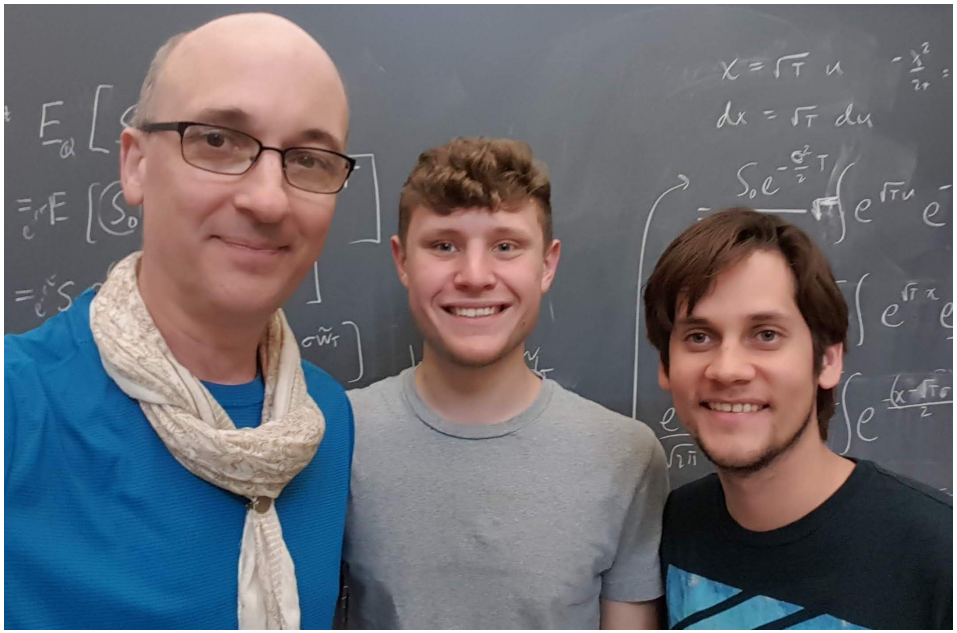
- Is the quantum state real? What is the status of the objects that appear in the mathematical model?
- Observation, observer, measurements—all are very troublesome.
- Nonlocality is very troublesome.

# 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.

# Thank you!

LVC Mathematical Physics Research Group



David Lyons  Isaac Lehman  David Campbell

`http://quantum.lvc.edu/mathphys`

# 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