

Title: The Strange Quantum: What does it mean and how can we use it? ISSYP Keynote Session

Date: Aug 25, 2007 09:00 AM

URL: <http://pirsa.org/07080062>

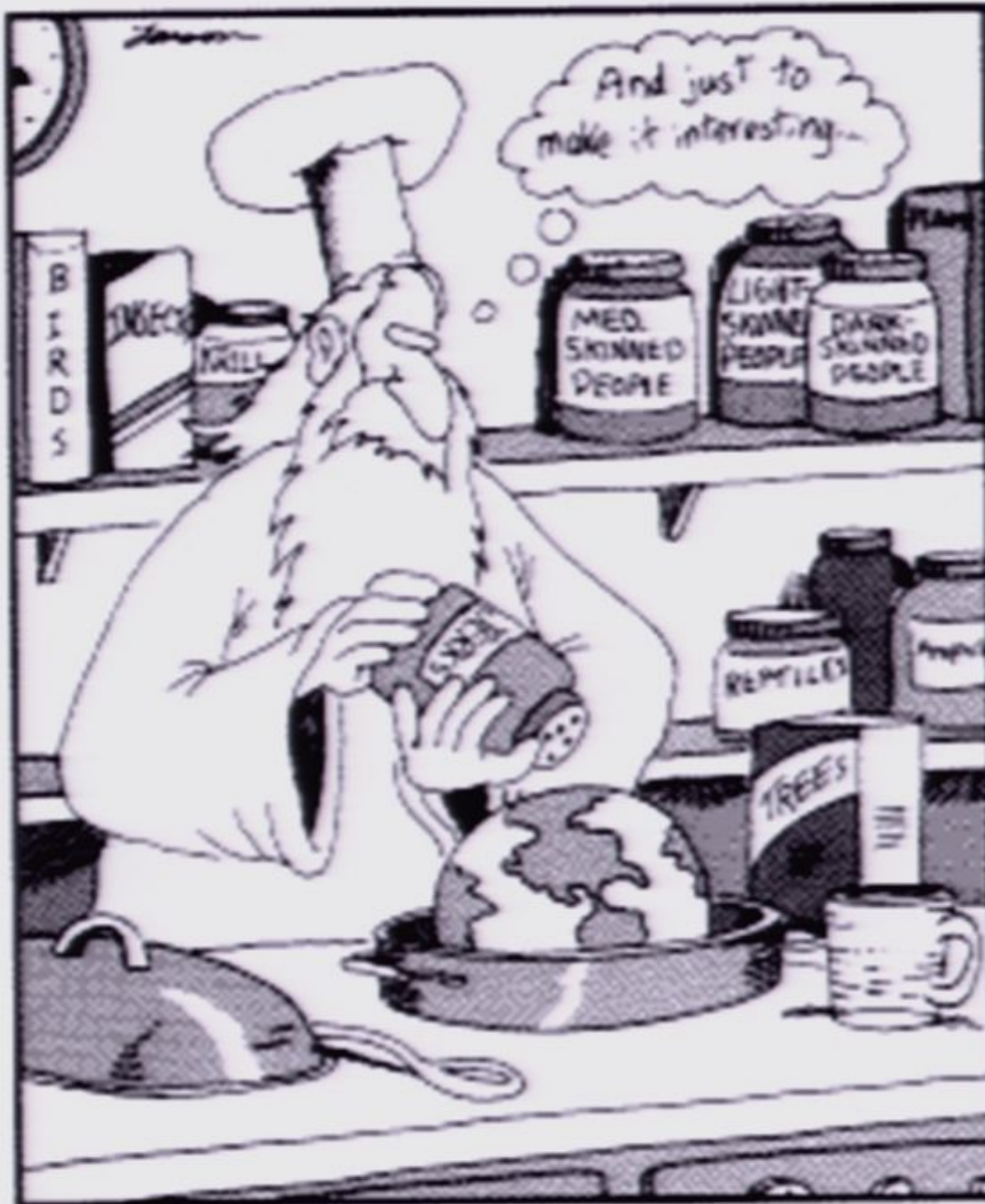
Abstract: In this talk, I describe some very simple but significant phenomena predicted by quantum theory. These are described simply in terms of what is observed in the laboratory, without making any presumptions about what sort of microscopic picture of reality might account for these observations.

With these phenomena in hand, I demonstrate two simple applications of quantum theory to cryptography: how to build counterfeit-proof money and how to detect eavesdroppers on a channel (and thereby distribute a secret key which can be used to encode messages in a way that cannot be deciphered by one who does not have the key). Moving from quantum information theory to quantum foundations, I show how the qualitative features of these phenomena can be reproduced in a toy theory wherein systems have well-defined properties but observers can only come to know a limited amount about them.

This shows the merits of the notion of "hidden variables" underlying quantum theory. Finally, I describe a phenomenon that is predicted by quantum theory but that \*cannot\* be reproduced by a natural class of hidden variable models, namely, those that are \*local\* in the sense that changes in one region cannot instantaneously affect the state of affairs in another. The phenomenon in question is the existence of certain strange correlations between the measurement outcomes on distant systems. It is illustrated in terms of a two-party game that is played out by a few lucky members of the audience.

# The Strange Quantum: What does it mean and how can we use it?

Robert Spekkens  
University of Cambridge





# The Solvay Congress of 1927

Werner Heisenberg

Louis de Broglie

Erwin Schrödinger



H. A. Lorentz

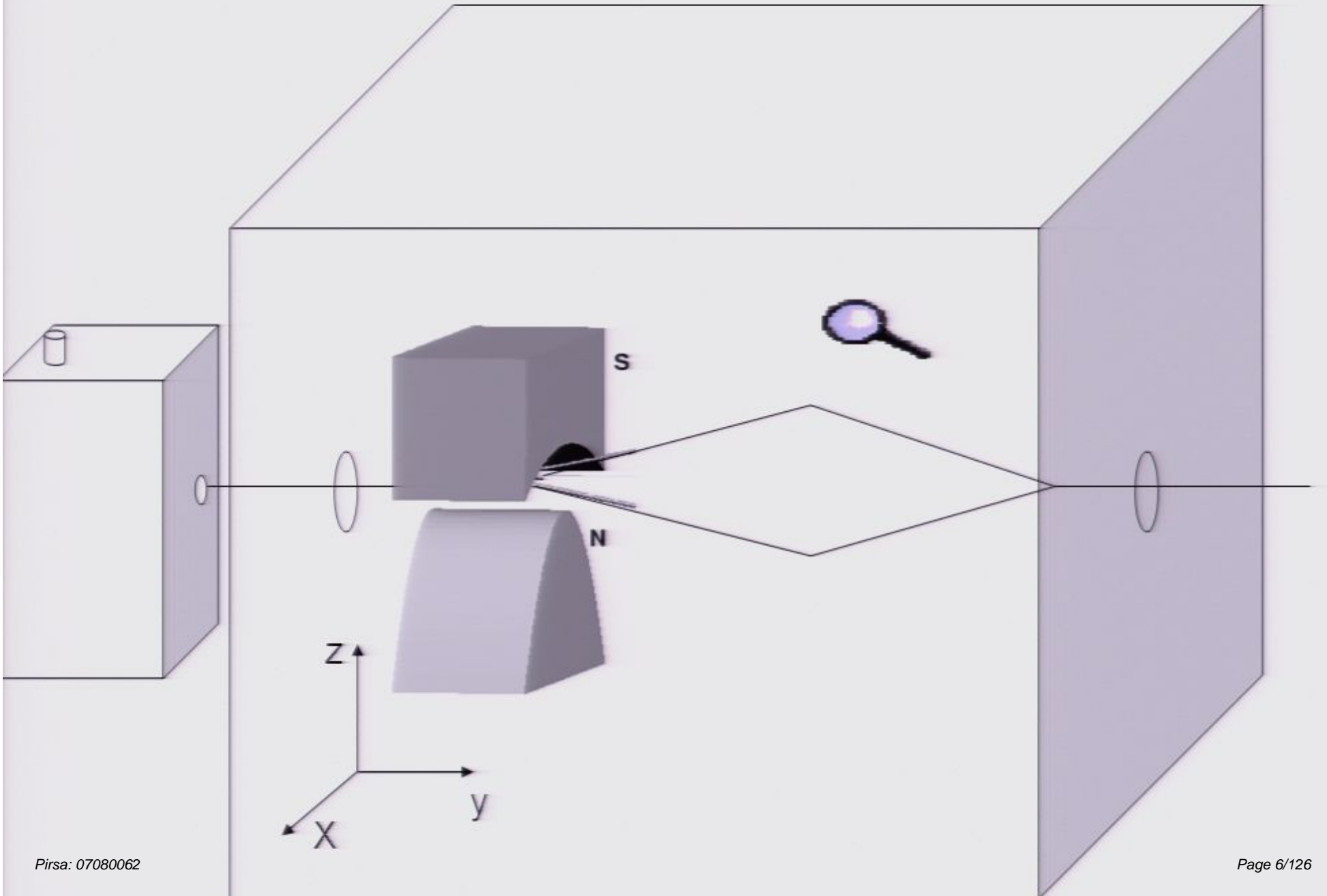
Max Born

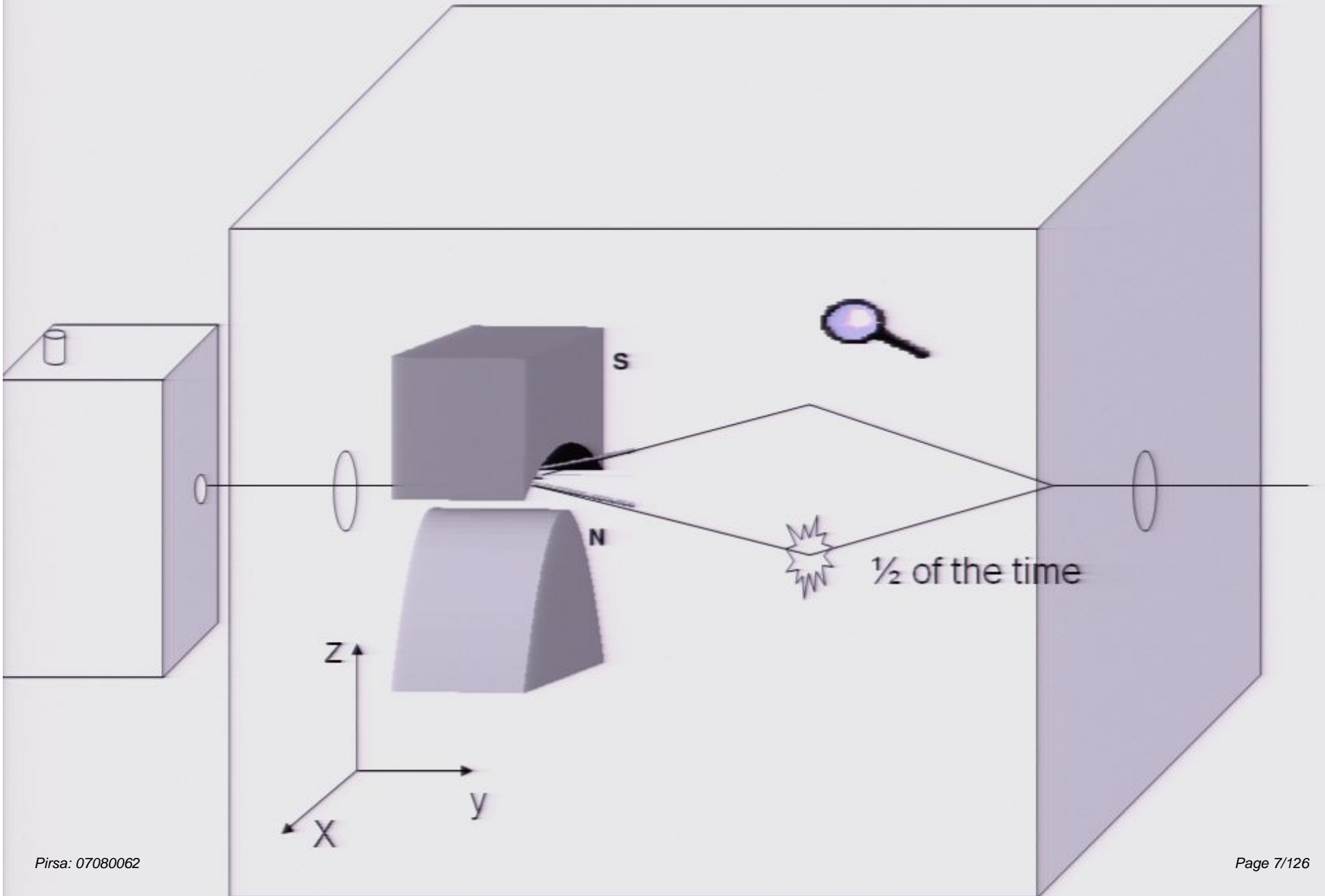
Max Planck

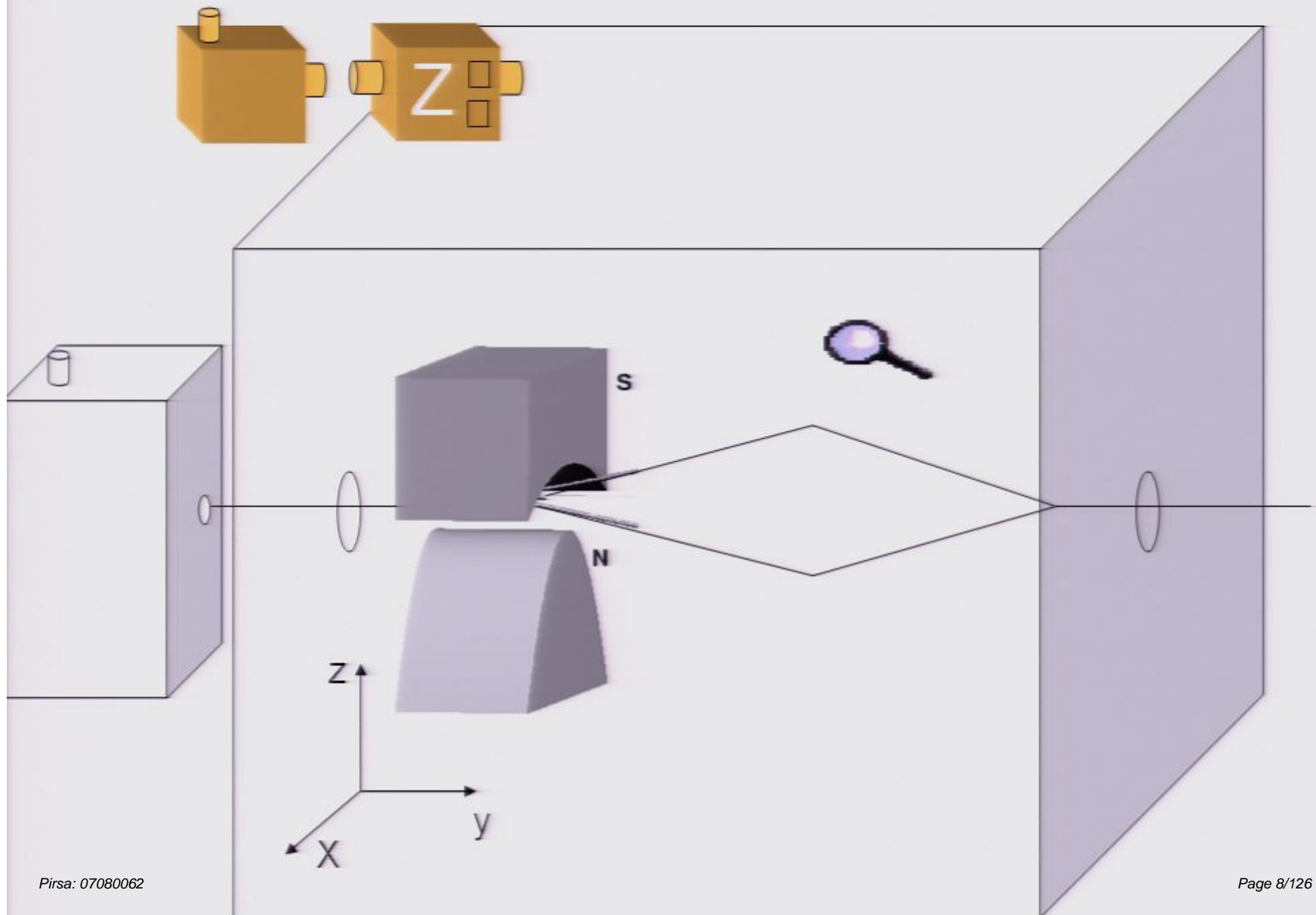
Einstein

Niels Bohr

# Some simple quantum phenomena









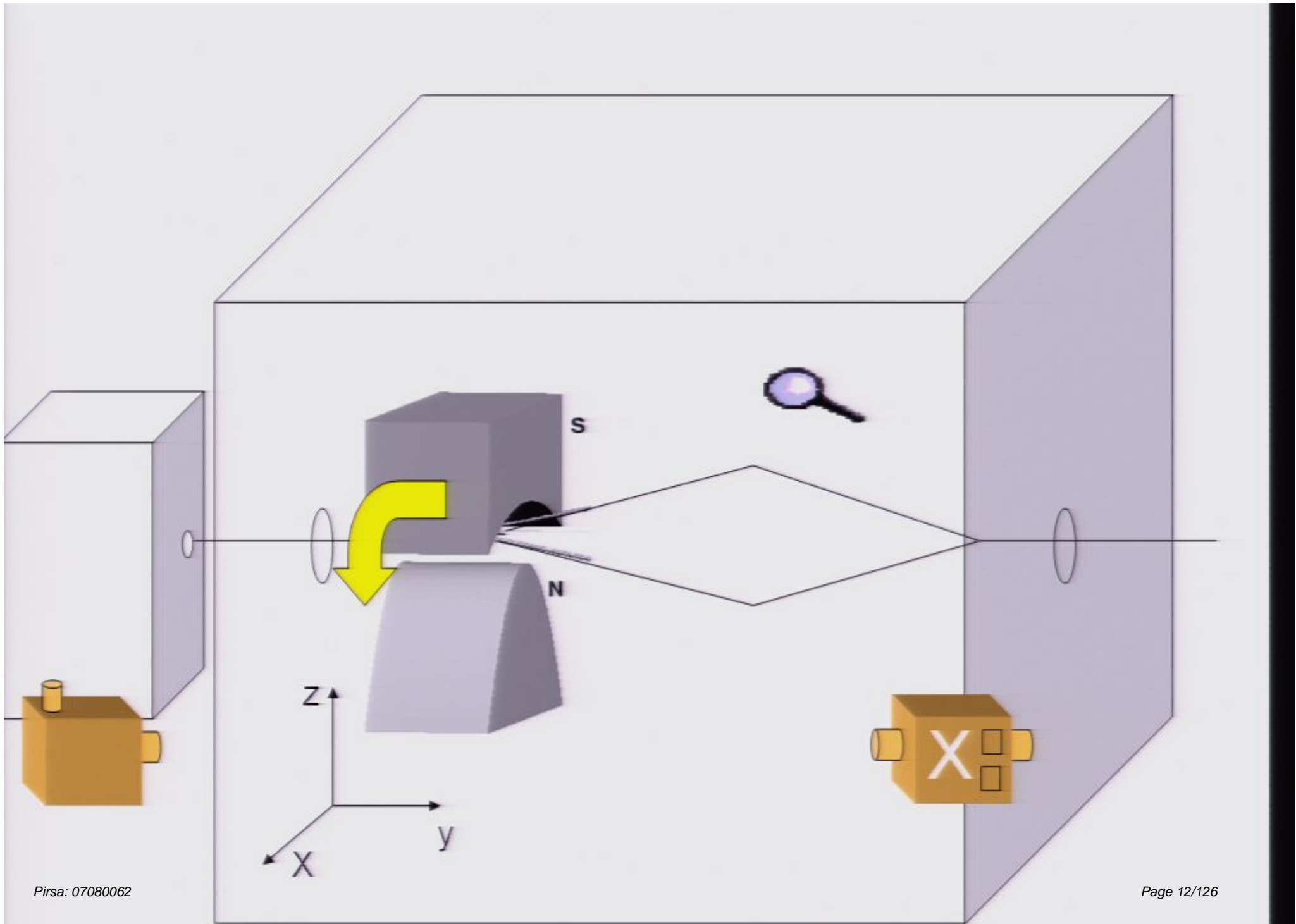




$\frac{1}{2}$  of the time



$\frac{1}{2}$  of the time









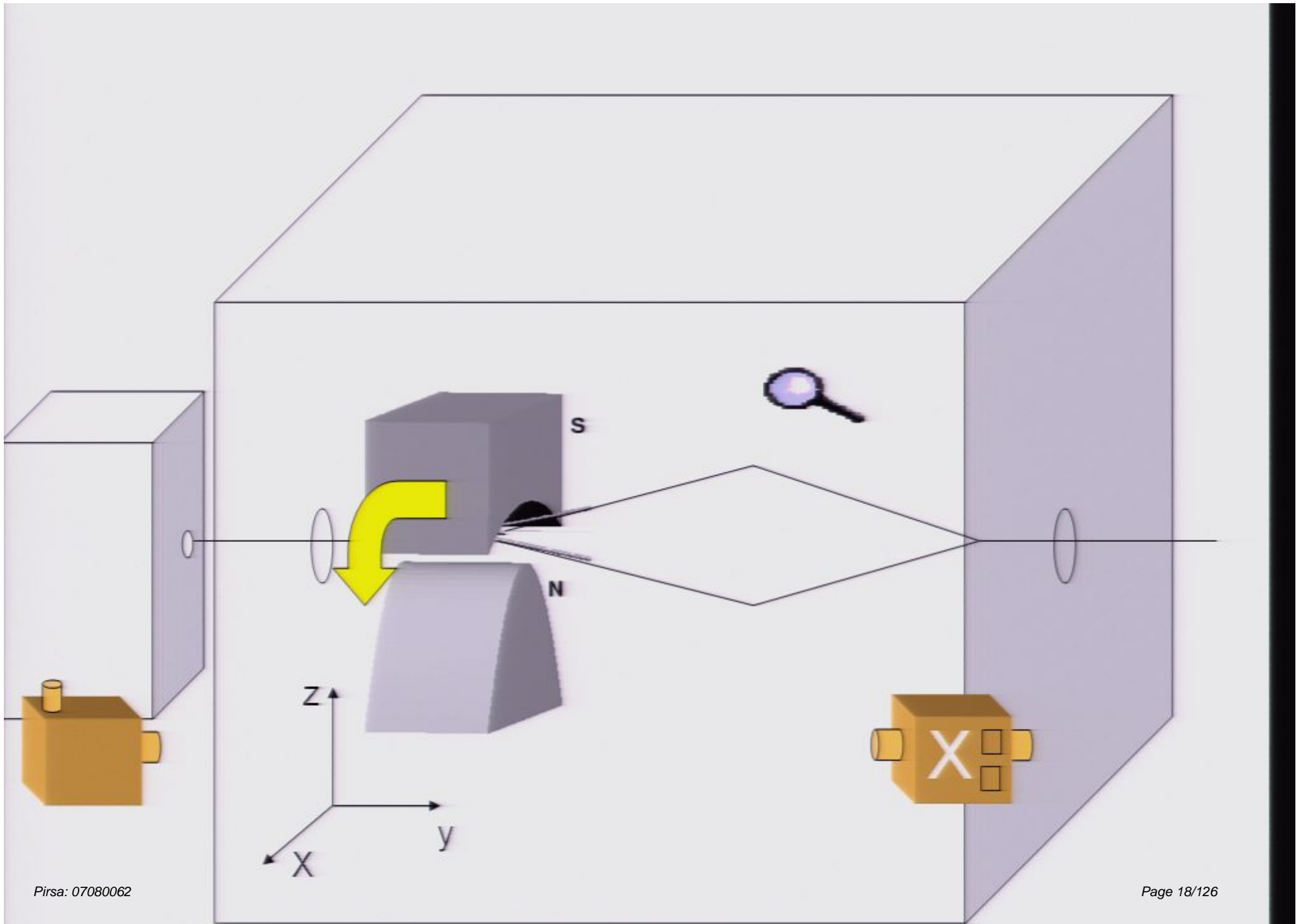
$\frac{1}{2}$  of the time





$\frac{1}{2}$  of the time





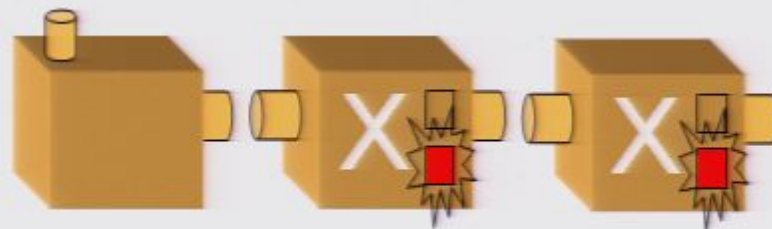




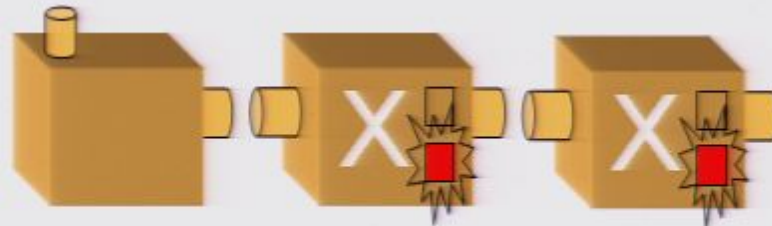






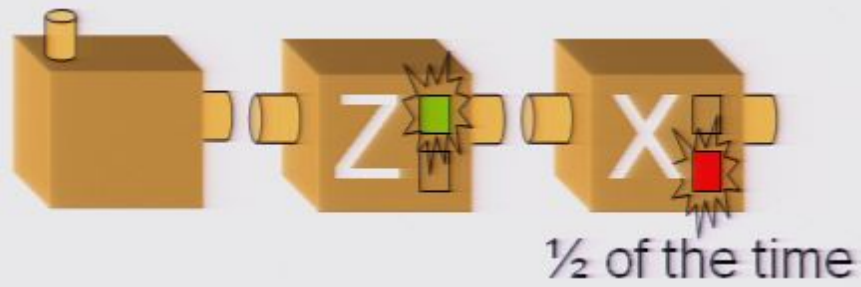


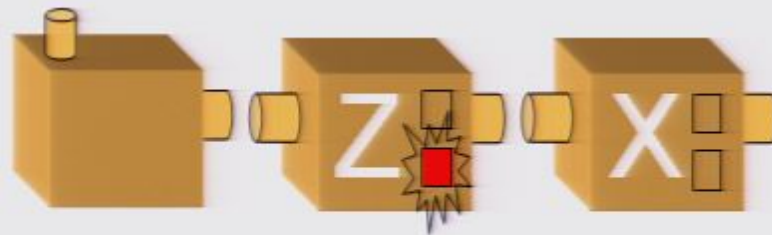




Consecutive identical measurements  
always yield the same outcome









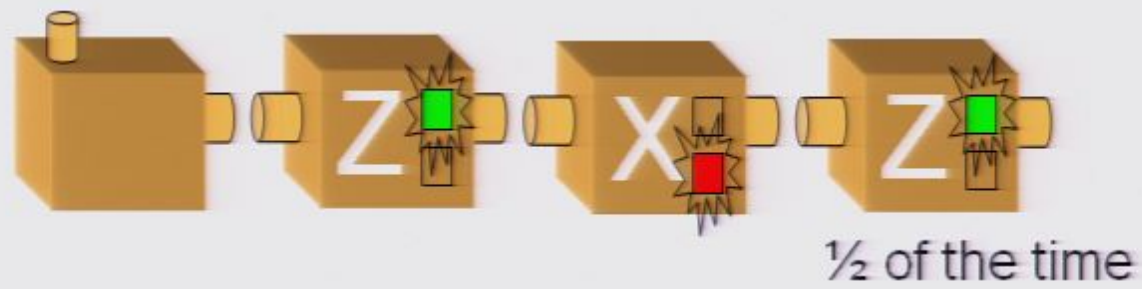


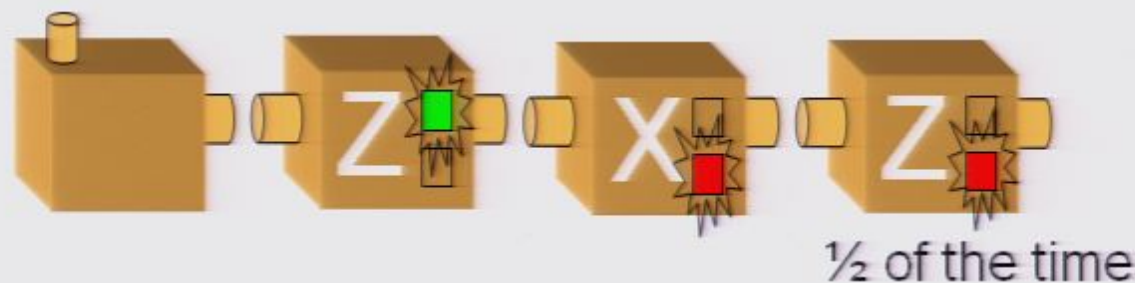


The outcome of an X measurement is uncorrelated with the outcome of an immediately preceding Z measurement

Same thing for X then Z

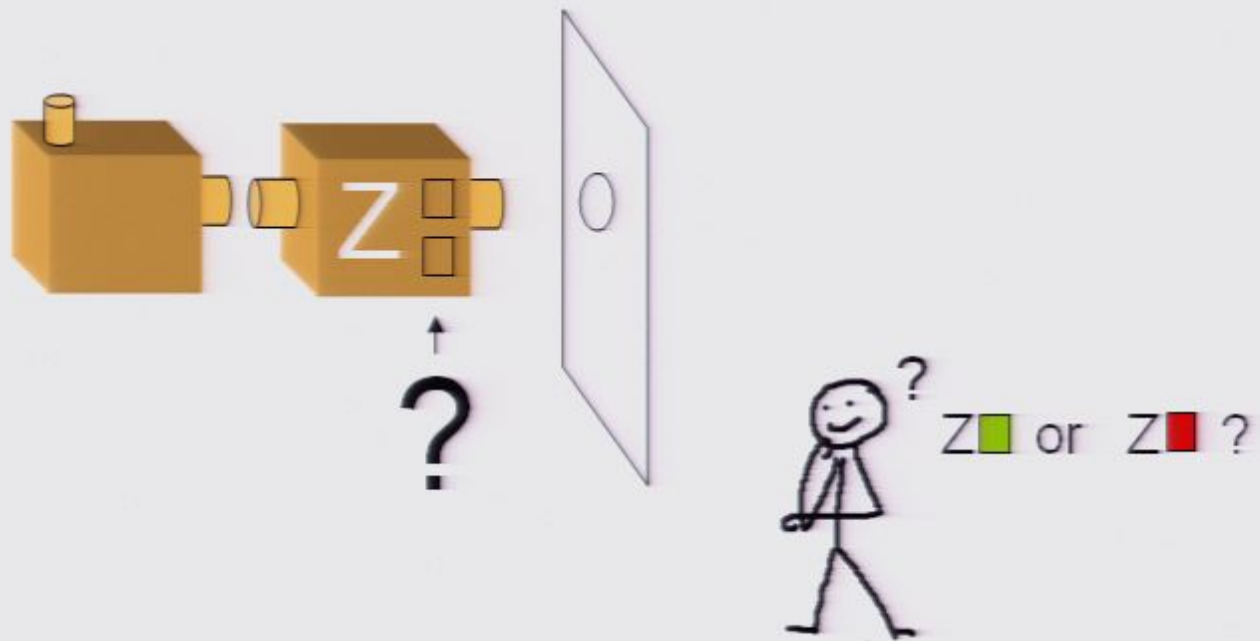


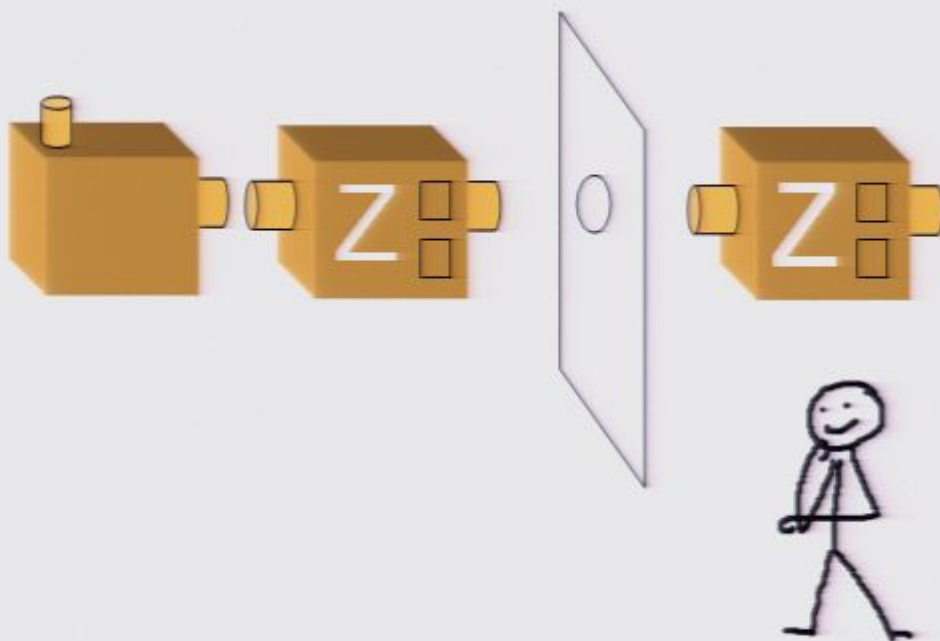


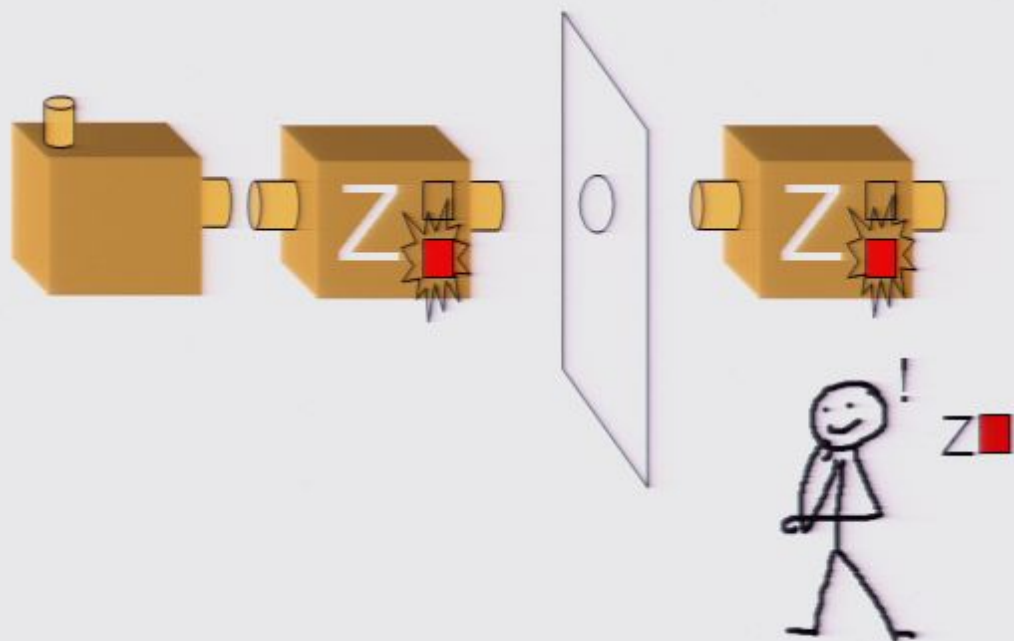


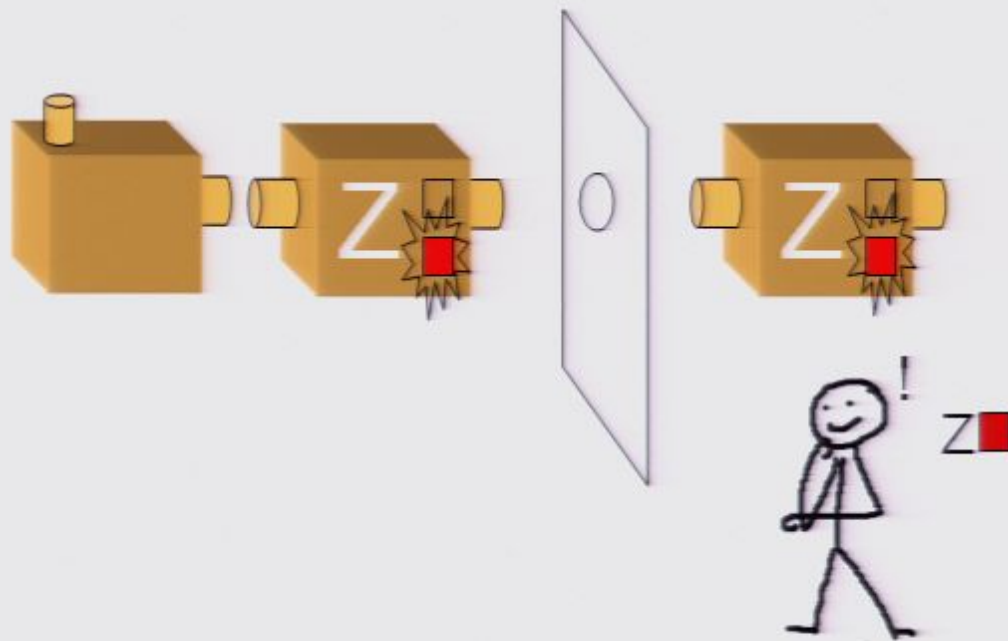
An intervening X measurement  
randomizes the outcome of a Z  
measurement

Same thing for X Z X



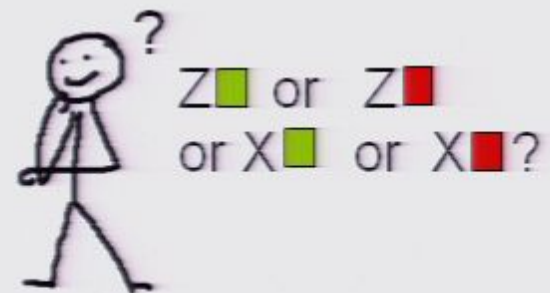
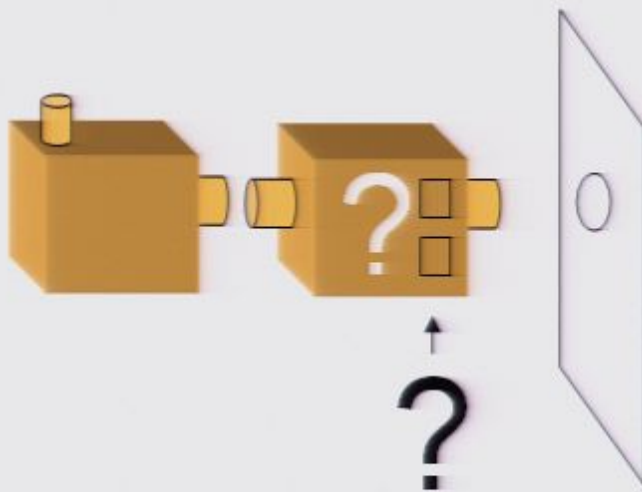


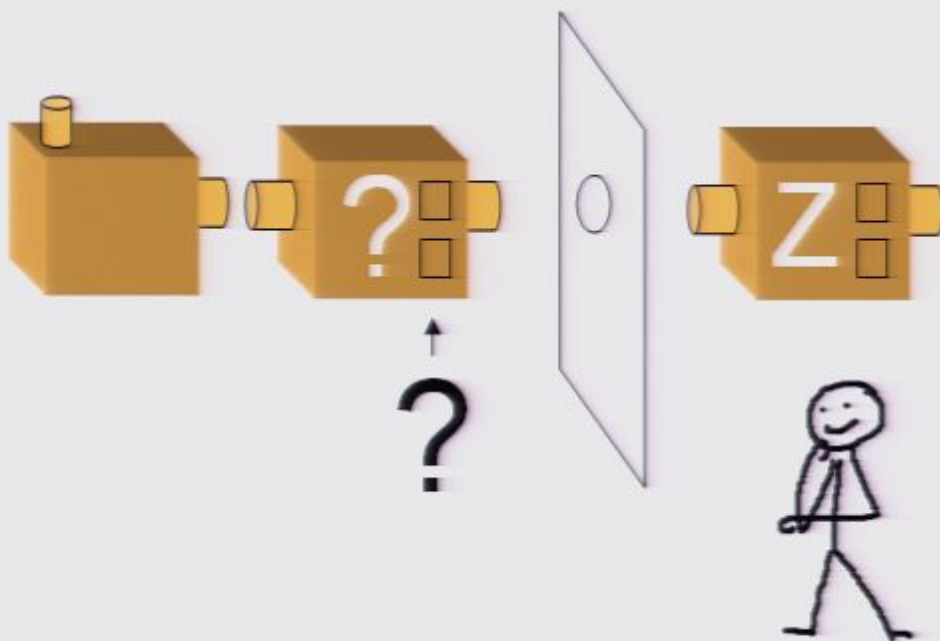


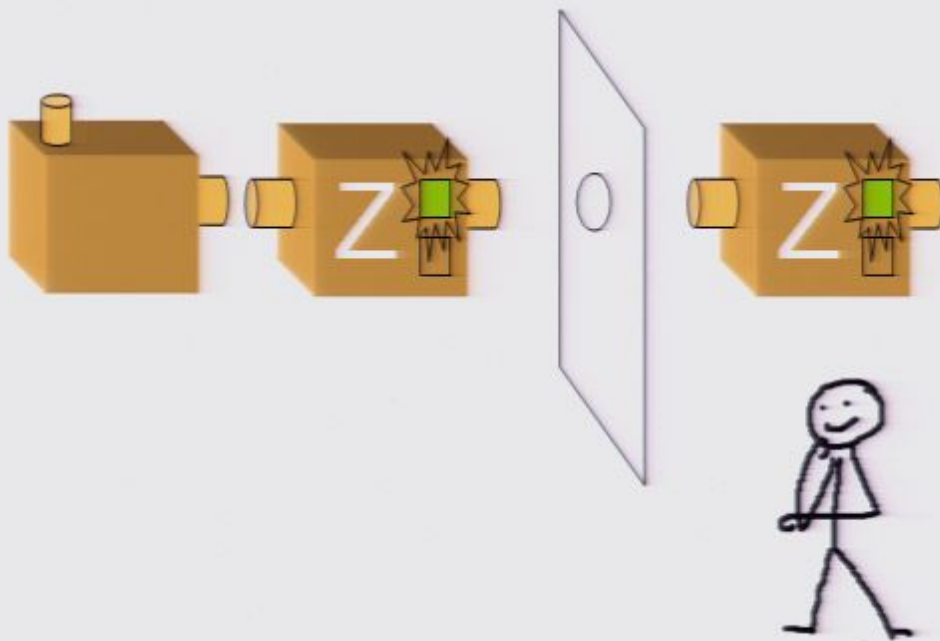


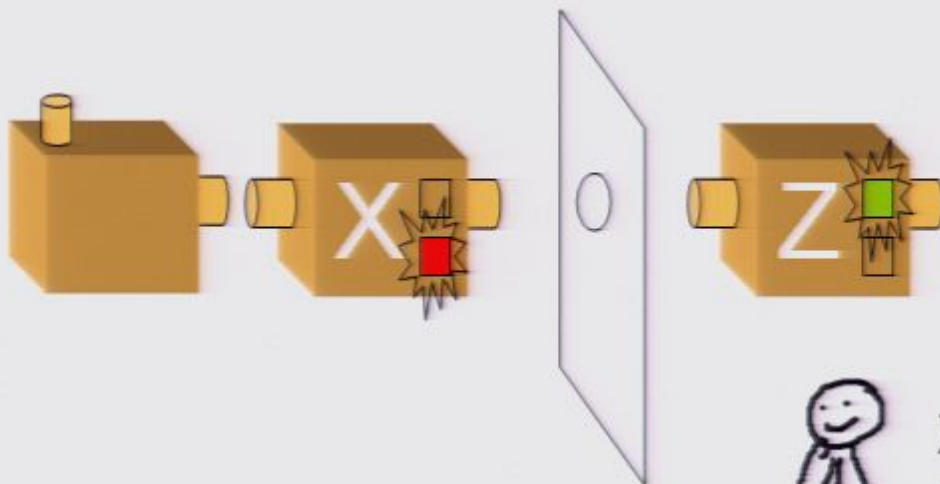
It is possible to distinguish between  
Z Green and Z Red  
(The same is true for X Green and X Red)



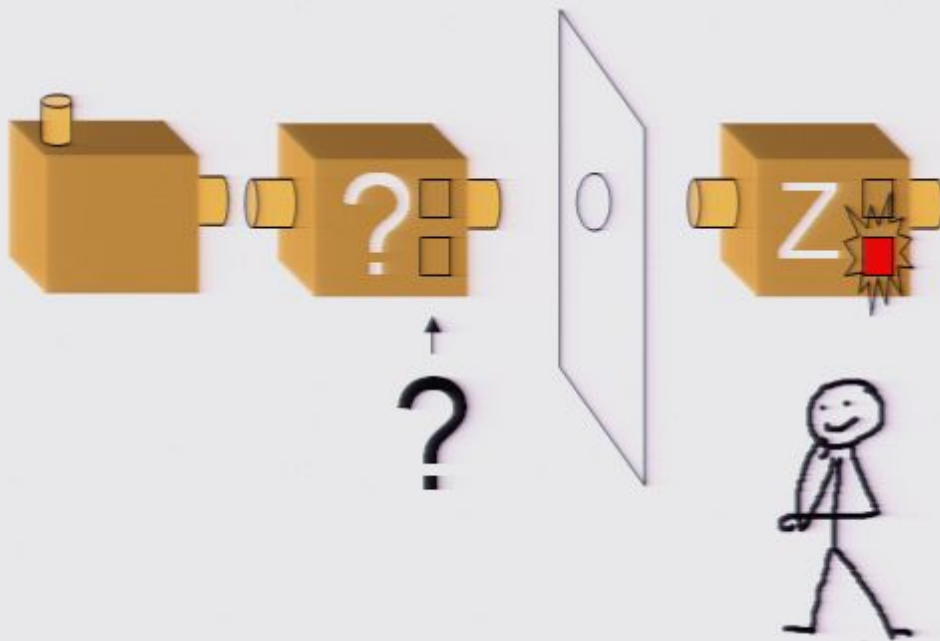


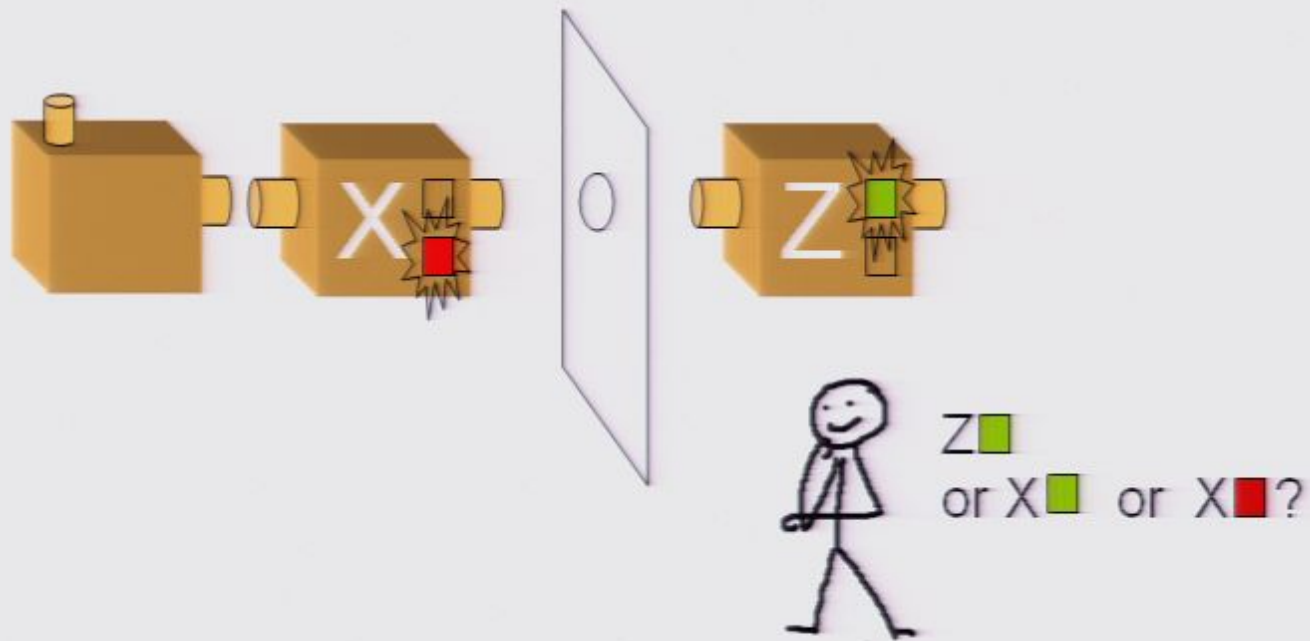


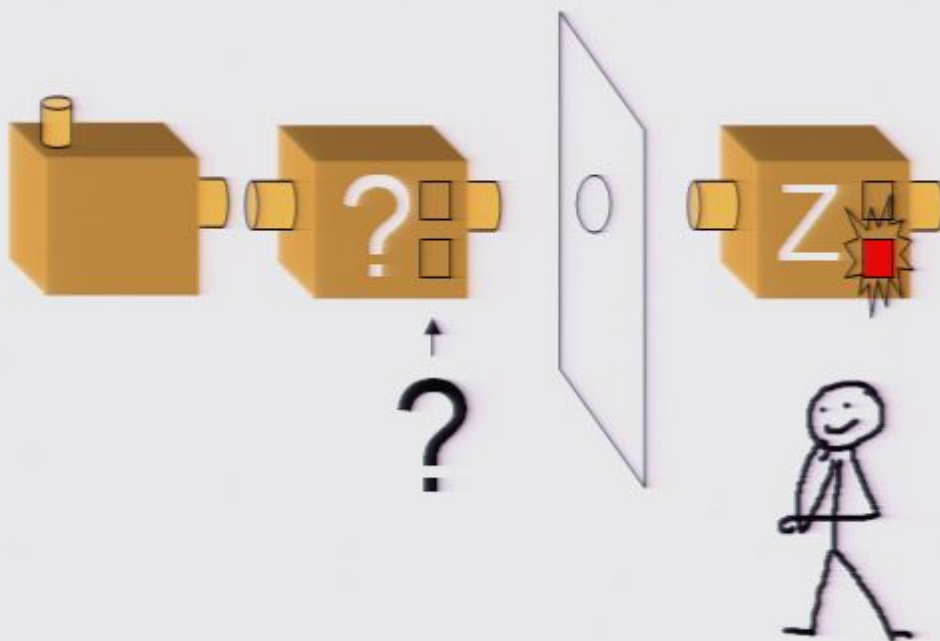


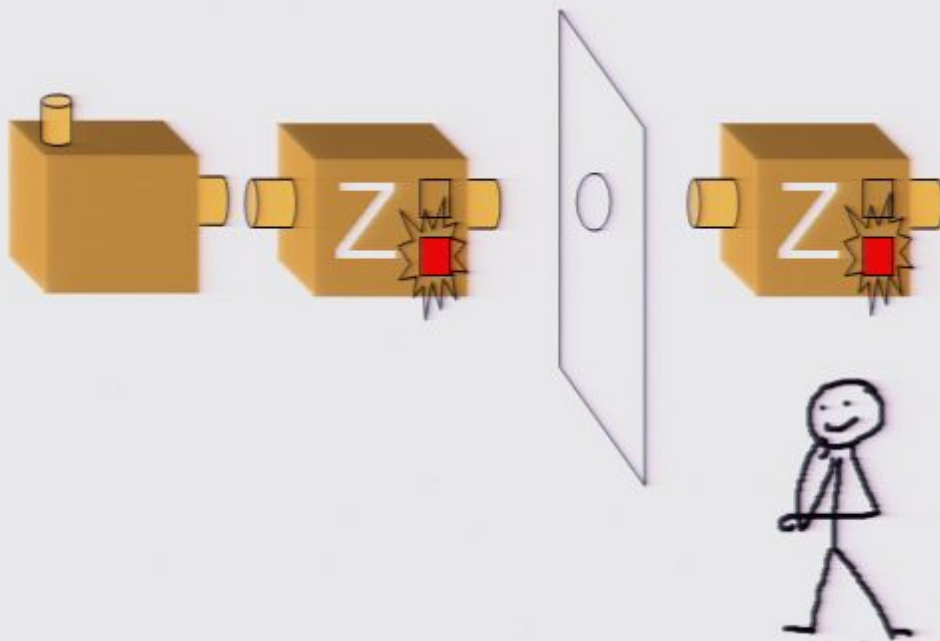


Z ■  
or X ■ or X ■?

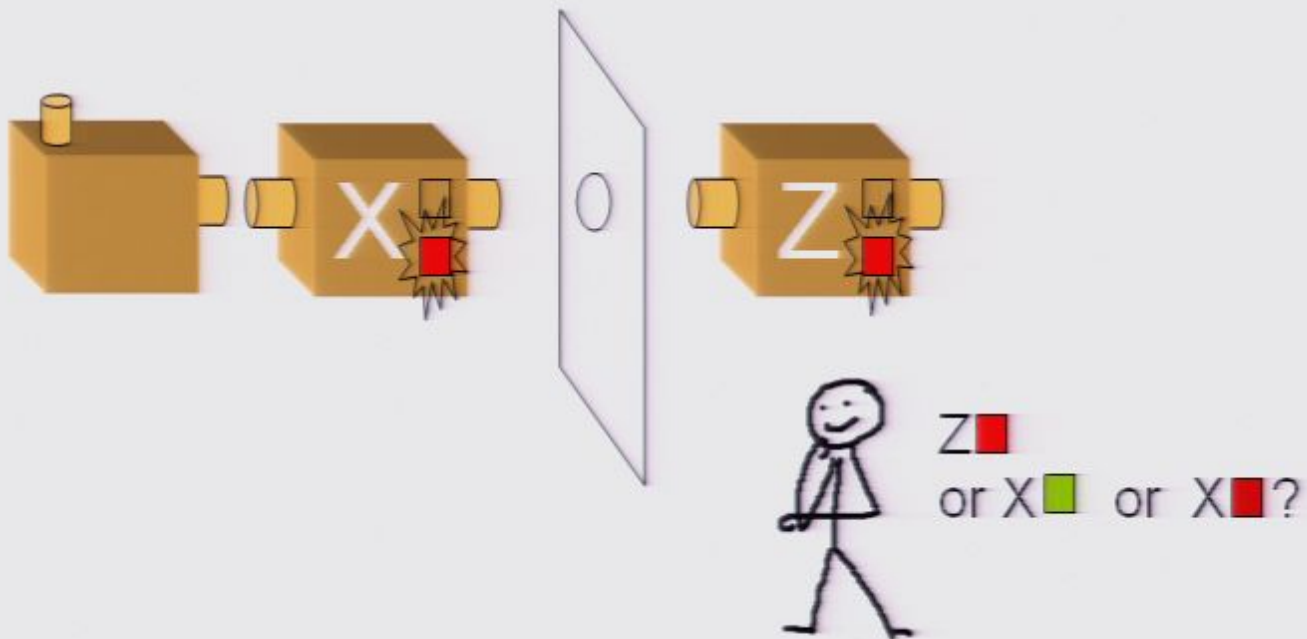


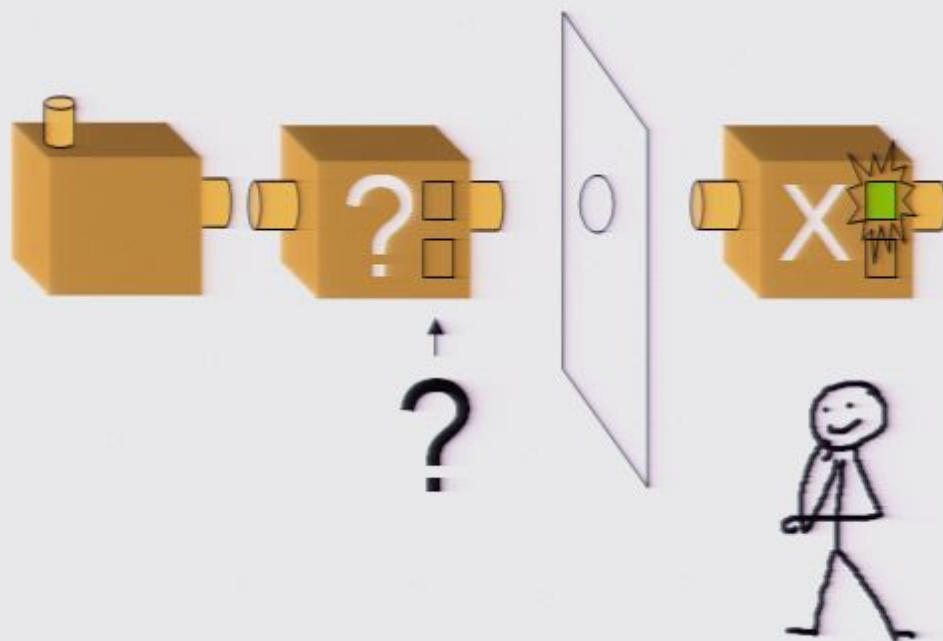


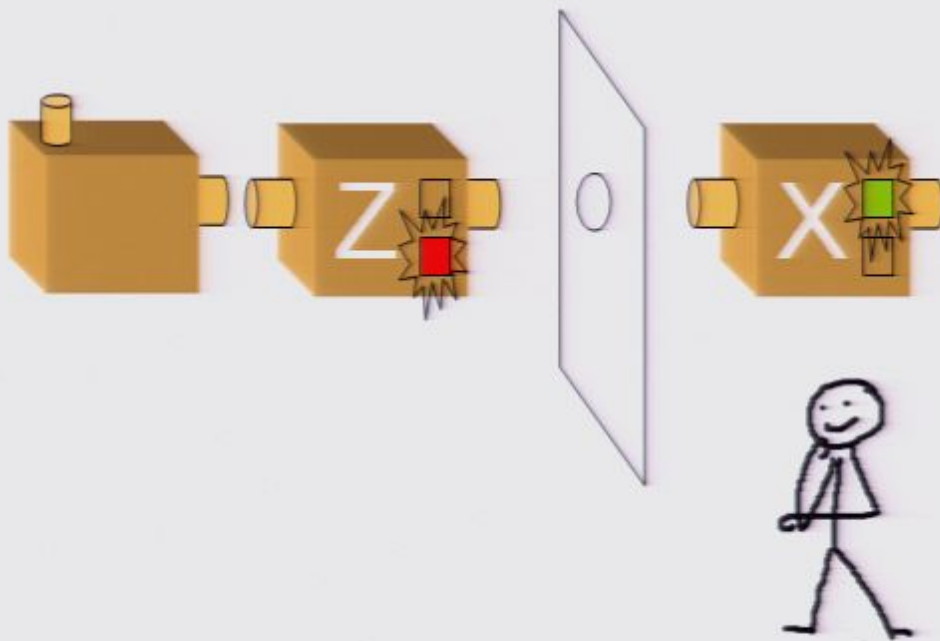


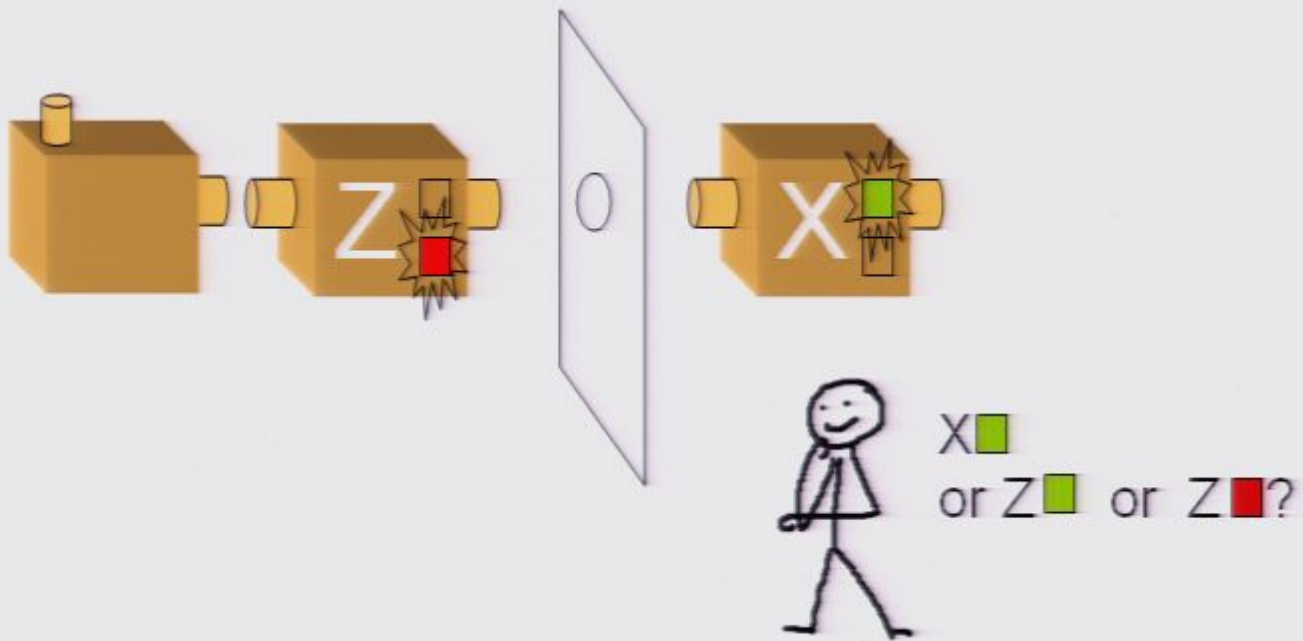


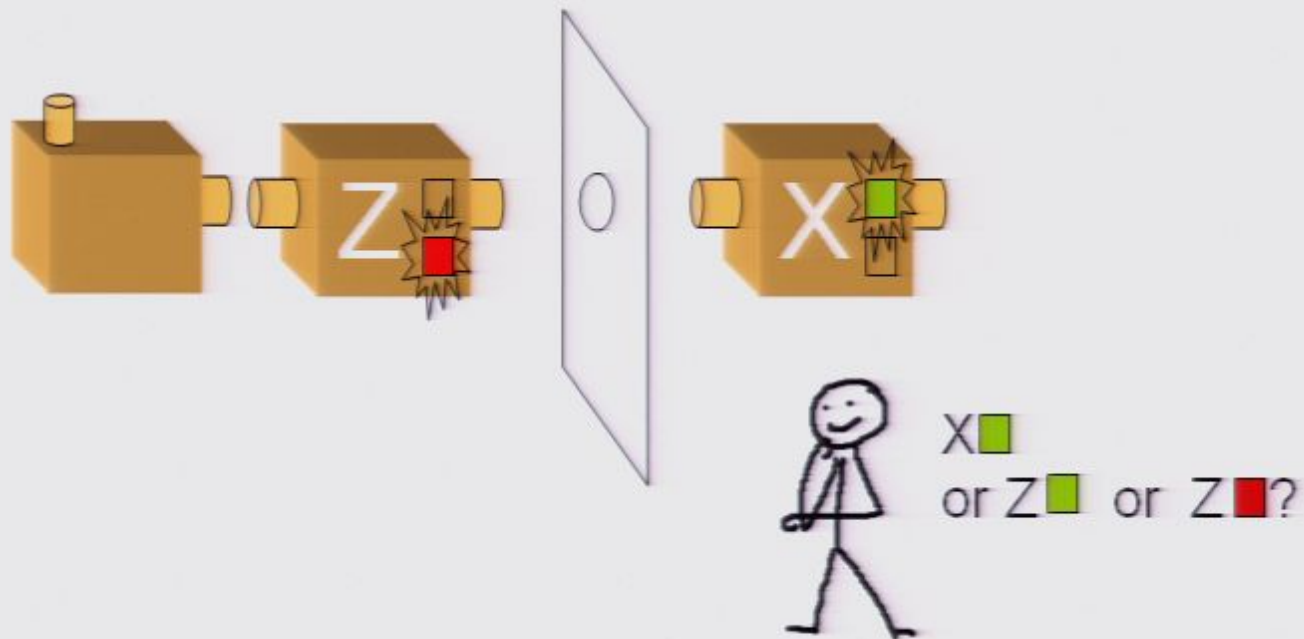




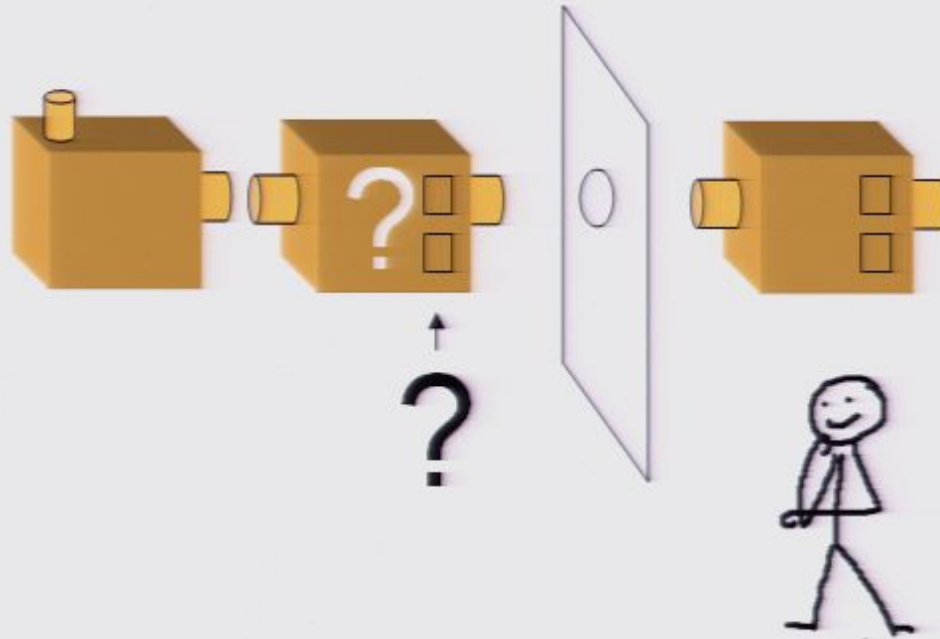








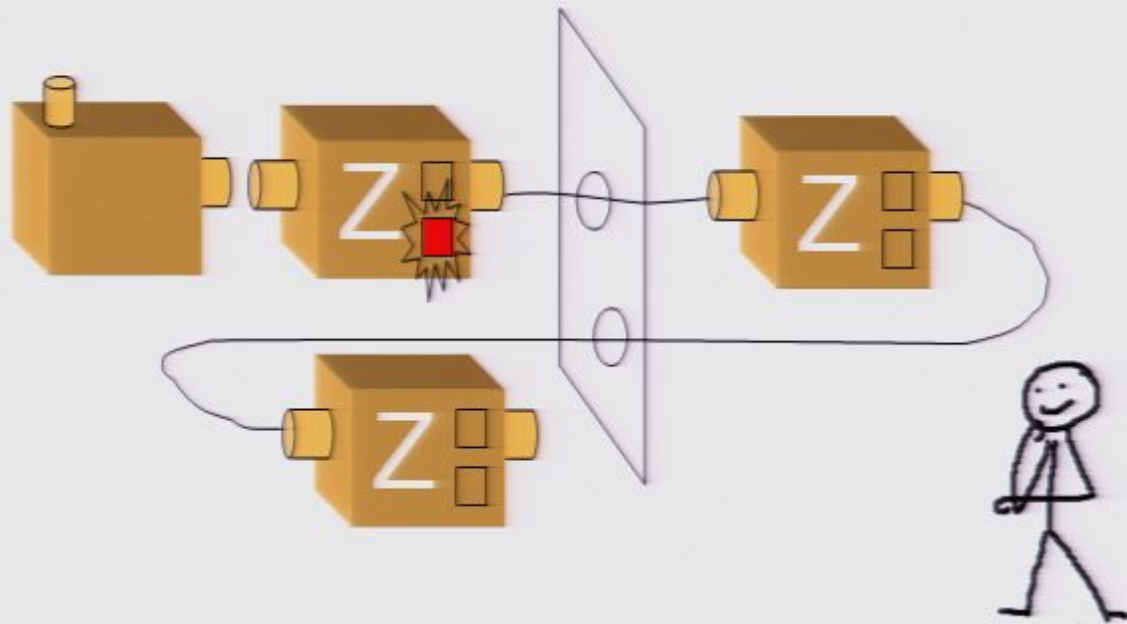
It is impossible to distinguish between  
Z Green, Z Red, X Green and X Red

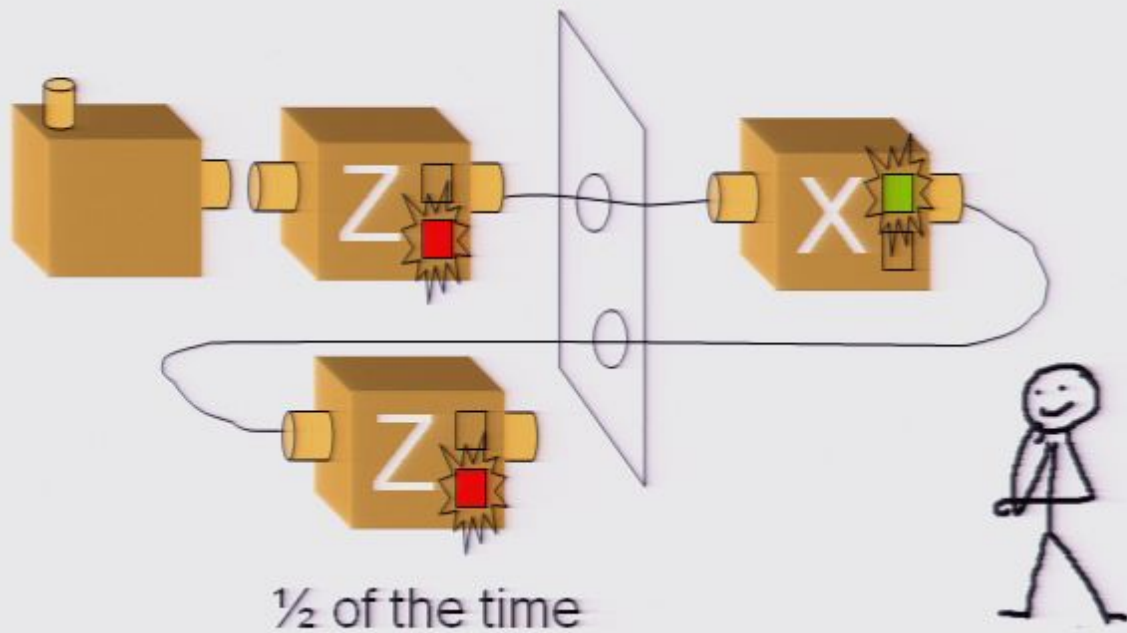


Probability of estimating correctly

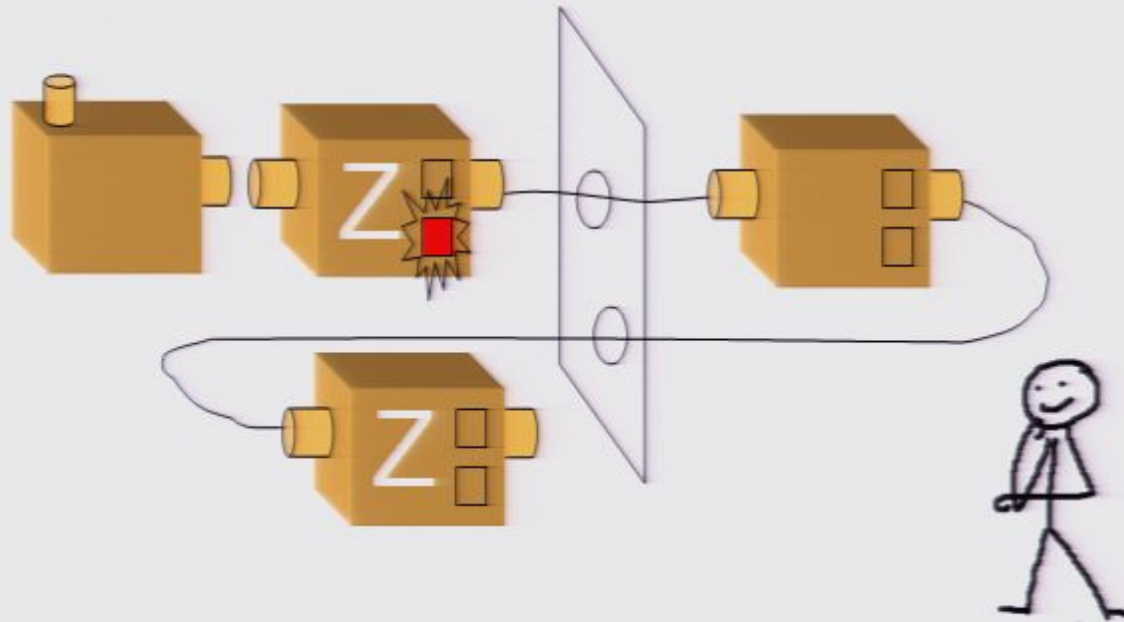
$$\begin{aligned} &= P(\text{get Z vs. X right}) \times P(\text{get Red vs. Green right} \mid \text{you got Z vs. X right}) \\ &= \frac{1}{2} \times 1 \\ &= \frac{1}{2} \end{aligned}$$

No perfect information gain



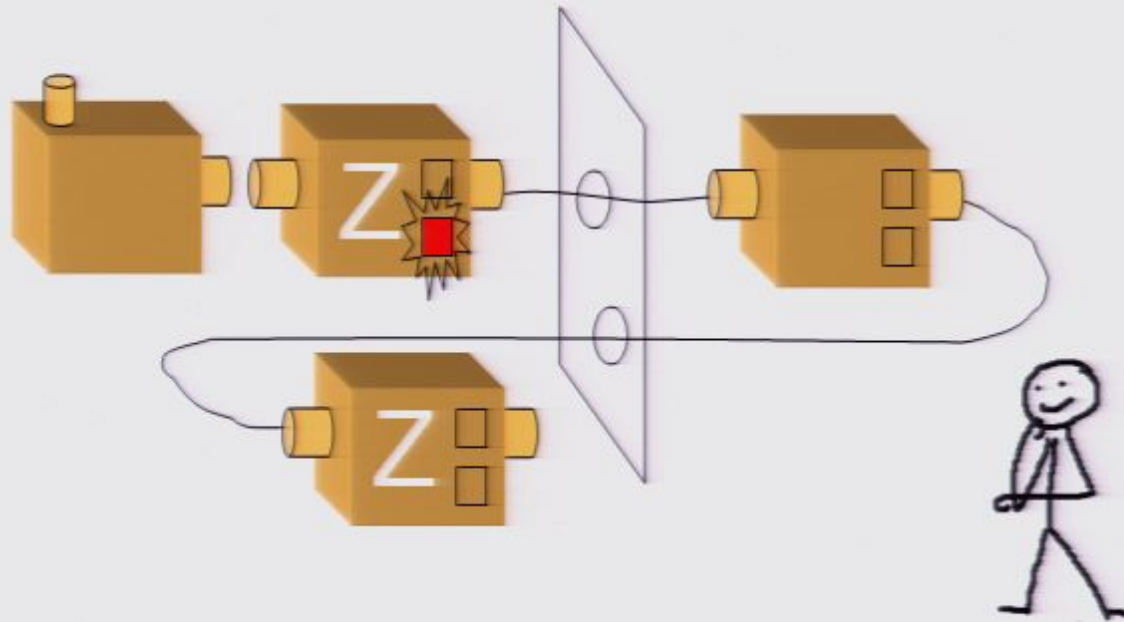






## Probability of passing test

$$\begin{aligned} &= P(\text{get Z vs. X right}) \times P(\text{pass the test} \mid \text{you got Z vs. X right}) \\ &+ P(\text{get Z vs. X wrong}) \times P(\text{pass the test} \mid \text{you got Z vs. X wrong}) \\ &= \frac{1}{2} \times 1 \\ &+ \frac{1}{2} \times \frac{1}{2} \\ &= \frac{3}{4} \end{aligned}$$



## Probability of passing test

$$\begin{aligned}
 &= P(\text{get } Z \text{ vs. } X \text{ right}) \times P(\text{pass the test} \mid \text{you got } Z \text{ vs. } X \text{ right}) \\
 &+ P(\text{get } Z \text{ vs. } X \text{ wrong}) \times P(\text{pass the test} \mid \text{you got } Z \text{ vs. } X \text{ wrong}) \\
 &= \frac{1}{2} \times 1 \\
 &+ \frac{1}{2} \times \frac{1}{2} \\
 &= \frac{3}{4}
 \end{aligned}$$

Some applications  
of these  
phenomena to  
cryptography

# Quantum counterfeit-proof money

# QUANTUM COUNTERFEIT-PROOF MONEY

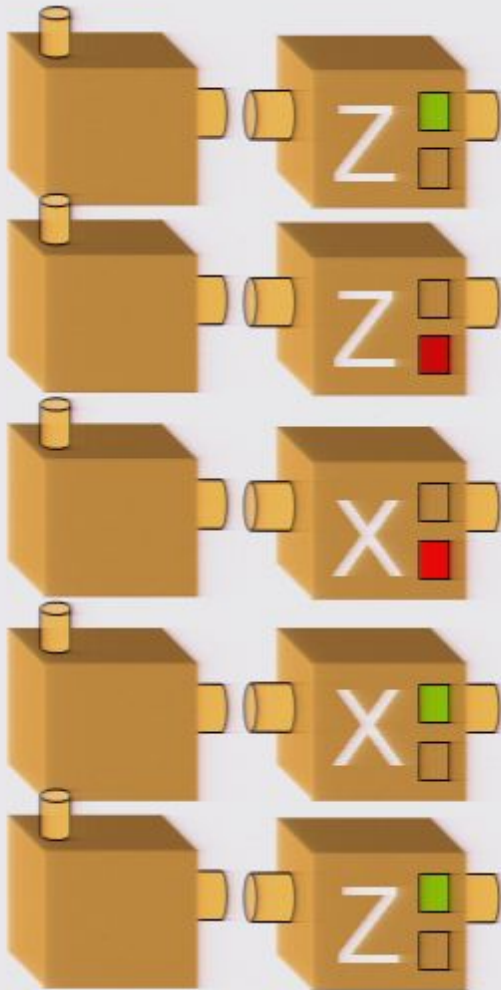




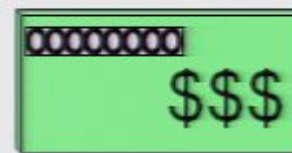
# QUANTUM COUNTERFEIT-PROOF MONEY



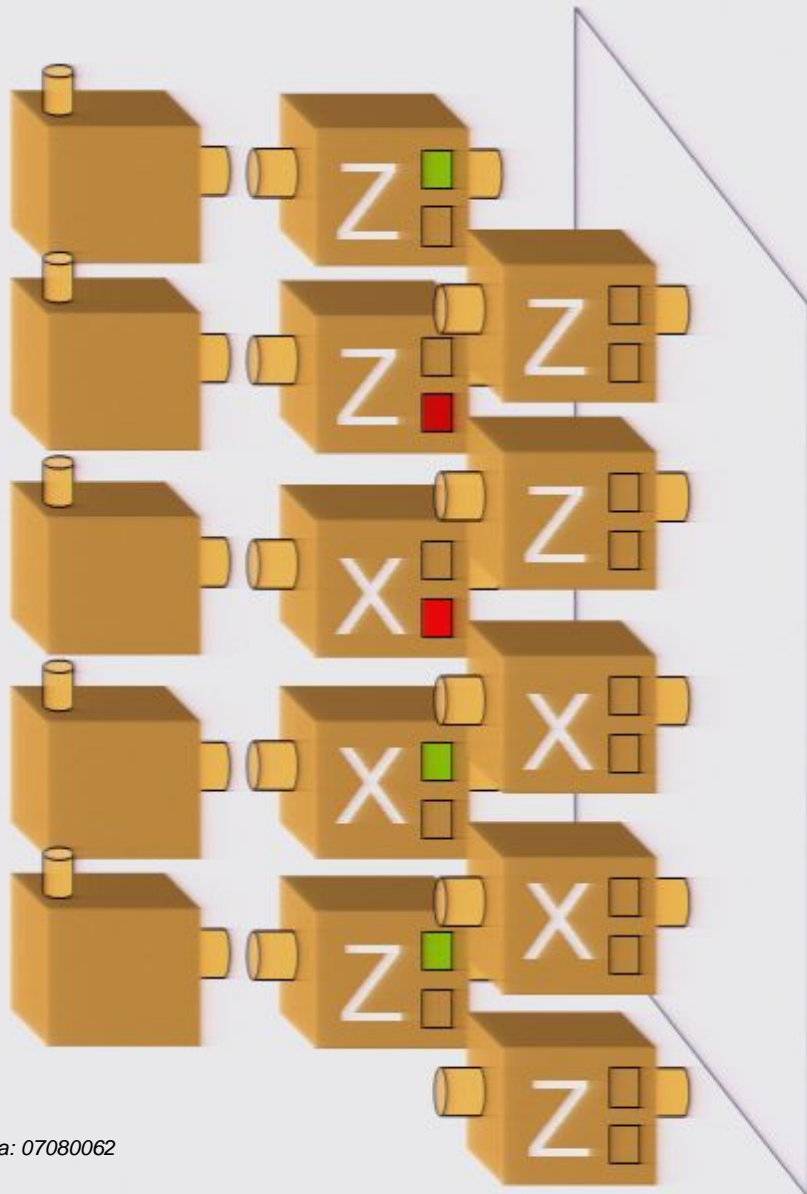
## The Mint



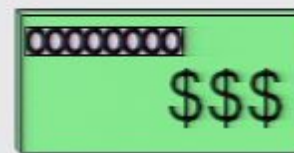
## The rest of the world



## The Mint

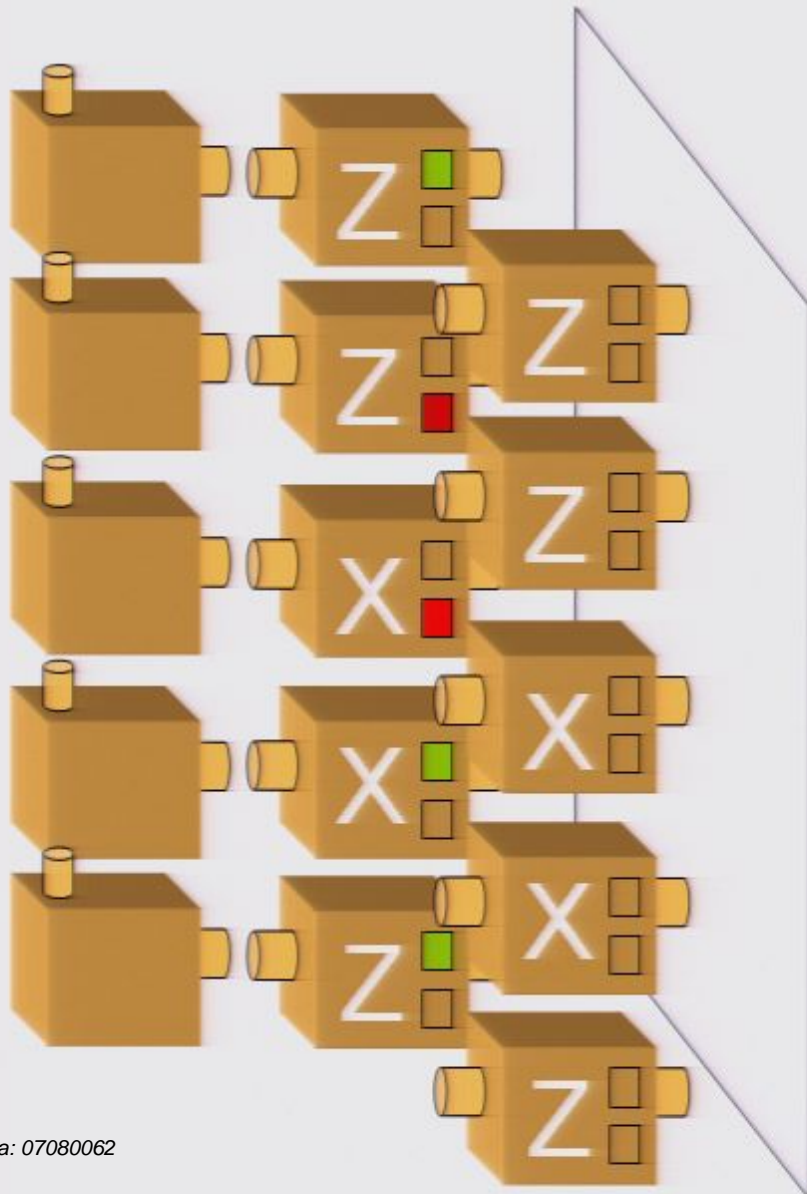


## The rest of the world

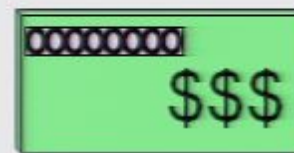




## The Mint



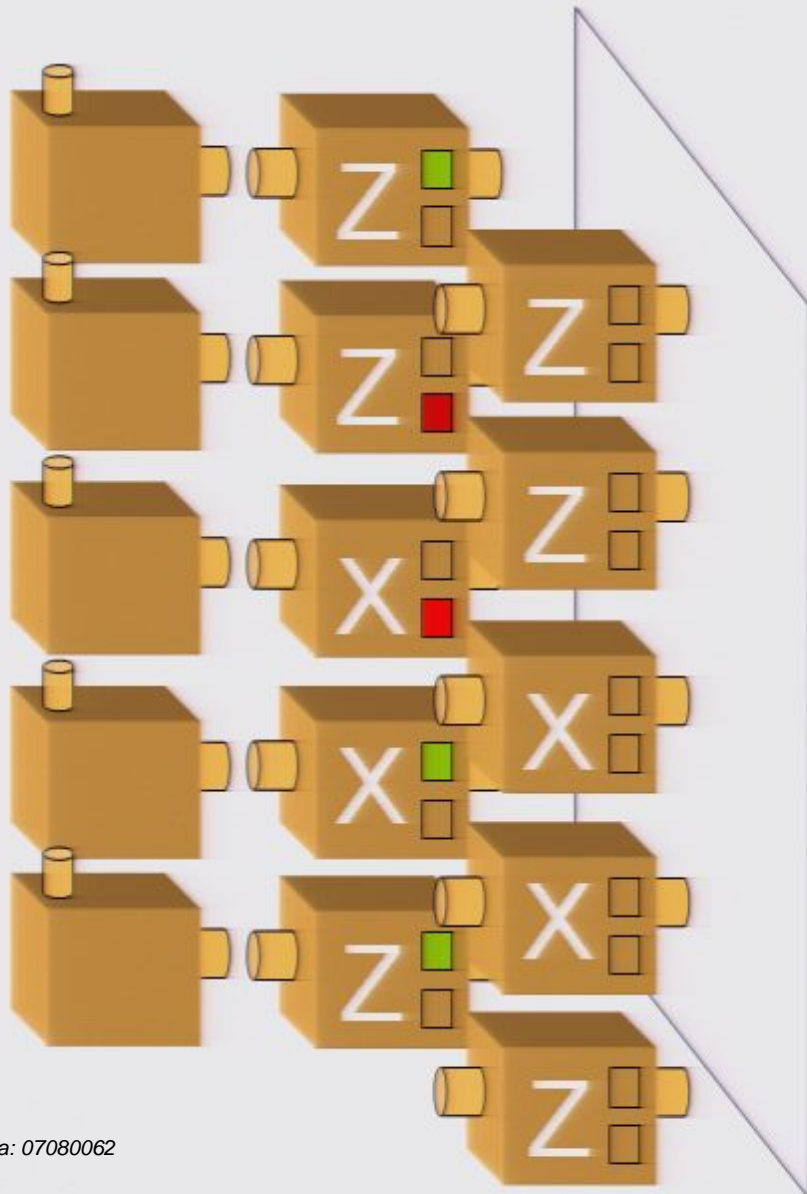
## The rest of the world



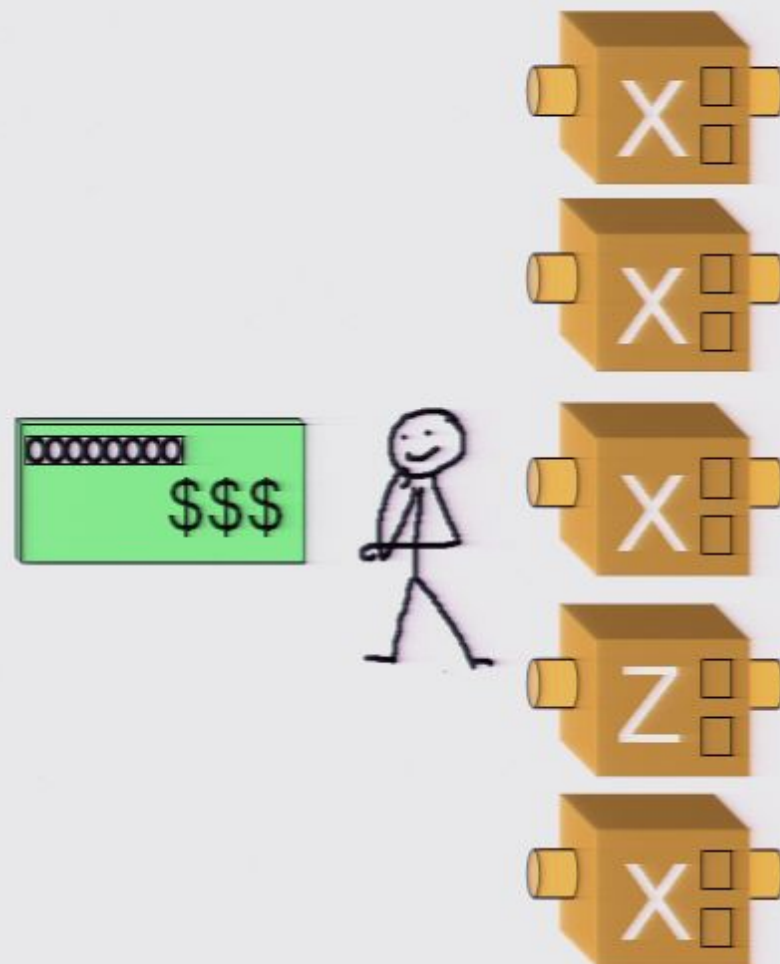
Probability every hidden measurement is estimated correctly:

$$\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \left(\frac{1}{2}\right)^8 \approx 0.0039$$

## The Mint



## The rest of the world



Probability every hidden measurement is estimated correctly:

$$\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \left(\frac{1}{2}\right)^8 \approx 0.0039$$

Probability every hidden measurement is estimated correctly:

$$\frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \left(\frac{1}{2}\right)^8 \simeq 0.0039$$

Probability original passes the test:

$$\frac{3}{4} \times \frac{3}{4} \times \frac{3}{4} \times \frac{3}{4} \times \frac{3}{4} \times \frac{3}{4} \times \frac{3}{4} \times \frac{3}{4} \times \frac{3}{4} = \left(\frac{3}{4}\right)^8 \simeq 0.10$$



★ MBNA®  
 Q U A N T U M ®  
 PRACTICAL. POWERFUL. INDISPENSABLE.



"Solutions for your everyday  
 and *not-so-everyday* needs."

# Quantum detection of eavesdroppers

# Private Channel





# Private Channel



# Caesar cipher

plain-text: "MEET ME AT THE RIVER"

shift each letter by  $x \in \{0, \dots, 26\}$

key: 2

cipher-text: "OGGVOGCVVJGTKXGT"

## Caesar cipher

plain-text: "MEET ME AT THE RIVER"

shift each letter by  $x \in \{0, \dots, 26\}$

key: 2

cipher-text: "OGGVOGCVVJGTKXGT"

## Vernam cipher

plain-text: "MEET ME AT THE RIVER"

shift letter  $i$  by  $x_i \in \{0, \dots, 26\}$

key: 7 20 4 12 14 23 19 8 1 2 11 19 23 ...

cipher-text: "TYIQZBWYURLCJRSE"

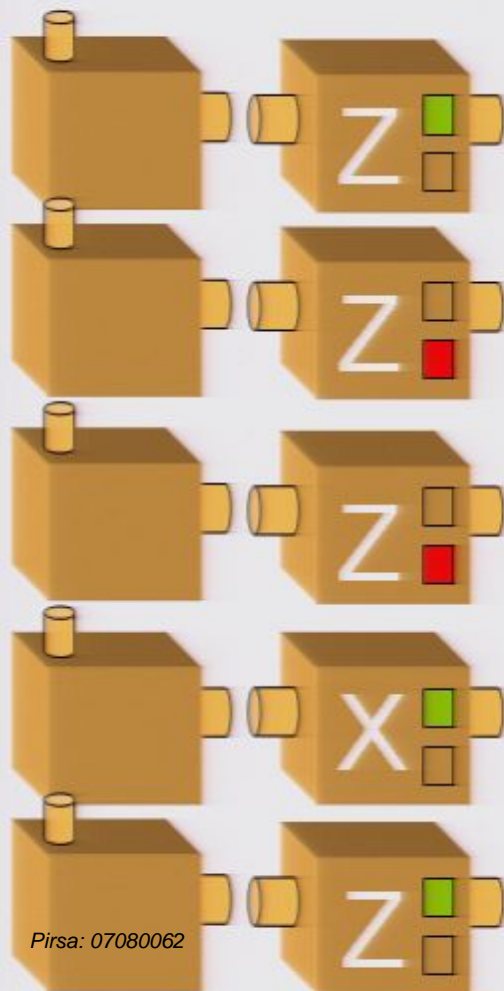
# Quantum Key distribution

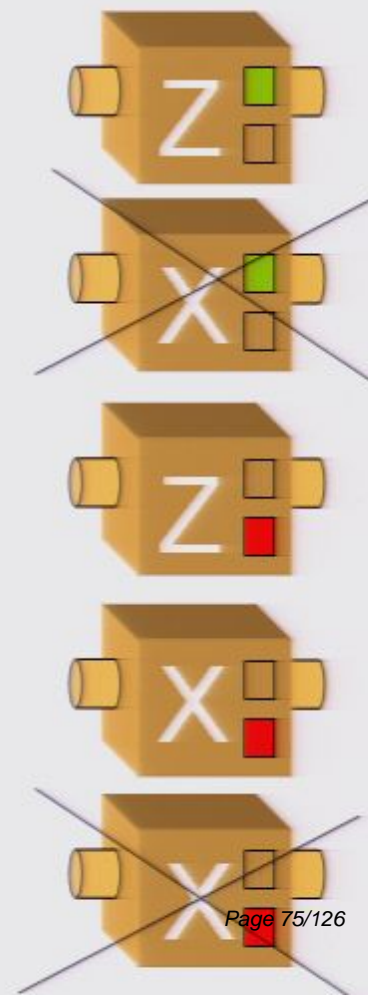
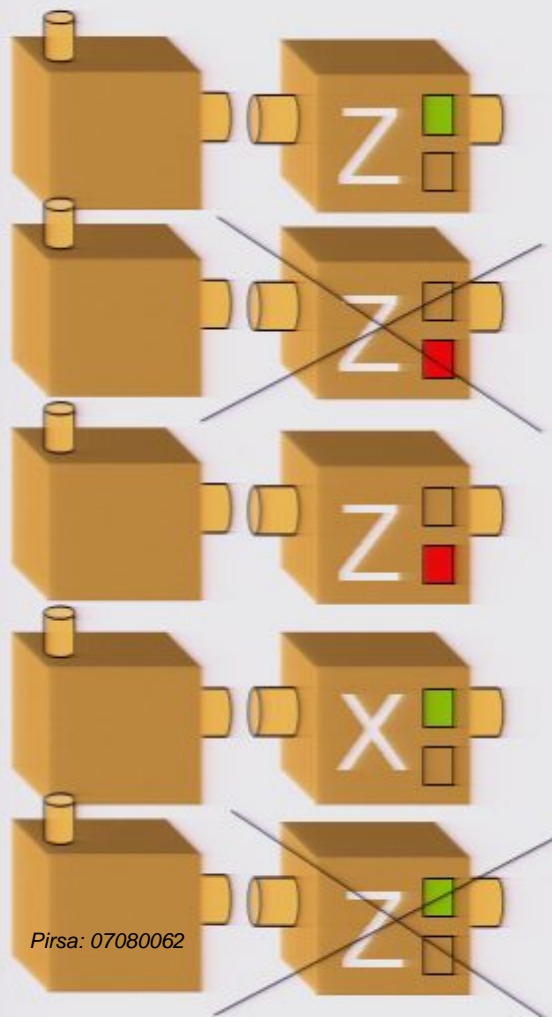


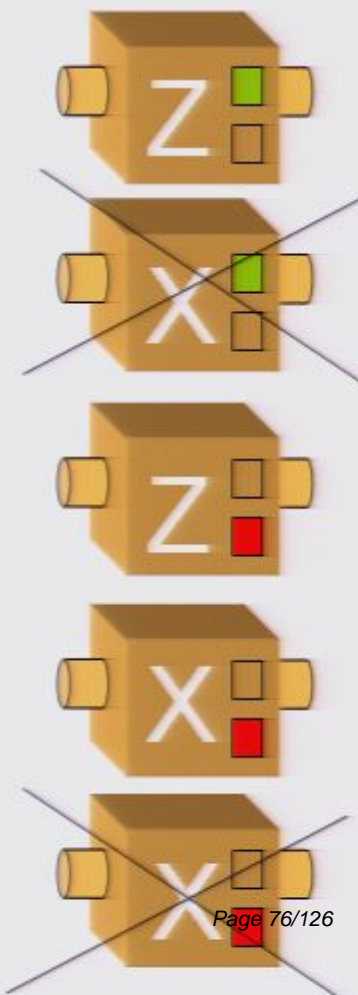
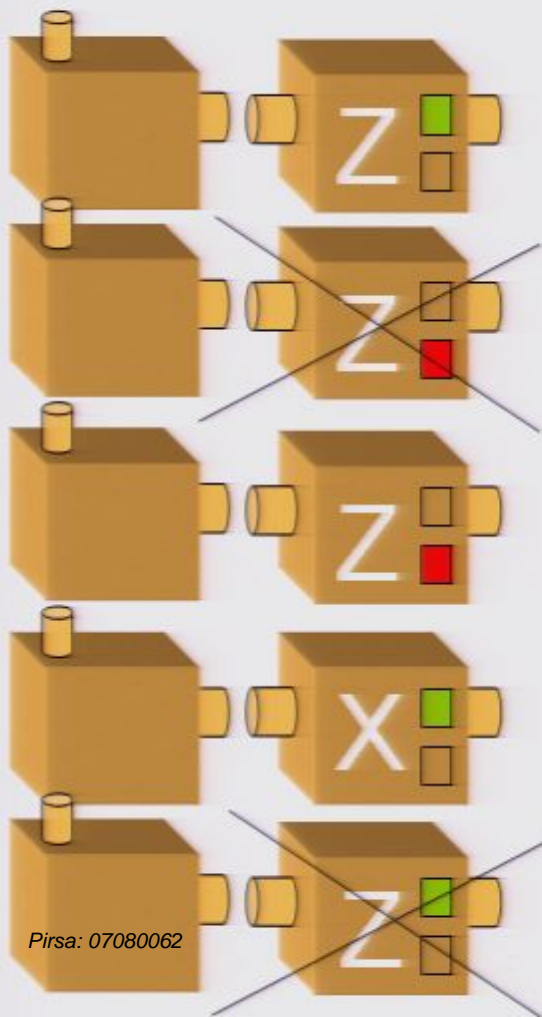
# Quantum Key distribution









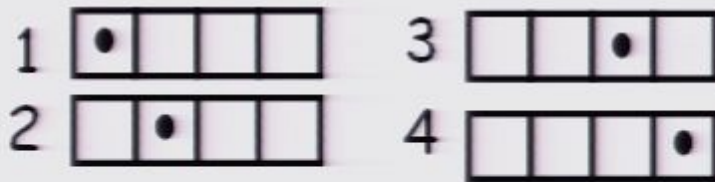




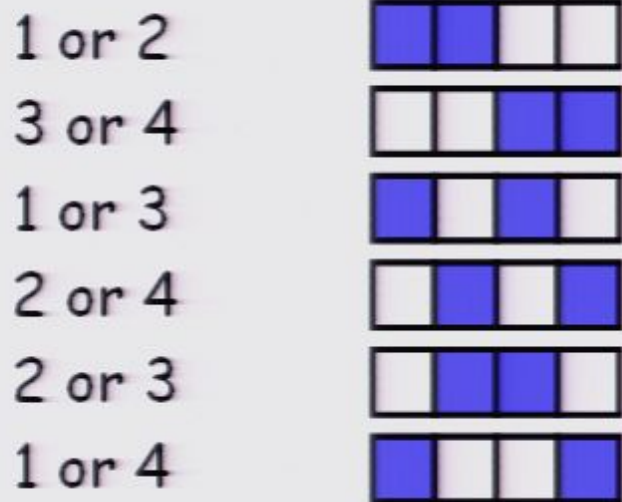
# The idea behind hidden variable models of quantum mechanics

# A toy world with a restriction on knowledge

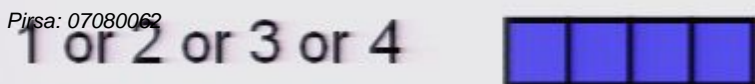
4 physical states



Probability distributions of maximal knowledge

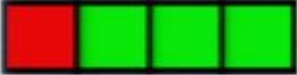


Probability distribution of non-maximal knowledge



## Reproducible measurements

must assign probability 0 to outcomes not obtained

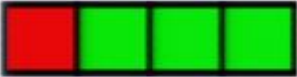
Suppose  (1) or (one of 2, 3 or 4)?  
was a valid reproducible measurement



But this is too much knowledge!

## Reproducible measurements

must assign probability 0 to outcomes not obtained

Suppose  (1) or (one of 2, 3 or 4)?  
was a valid reproducible measurement

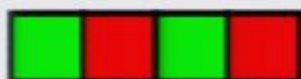


But this is too much knowledge!

The allowed reproducible measurements are:



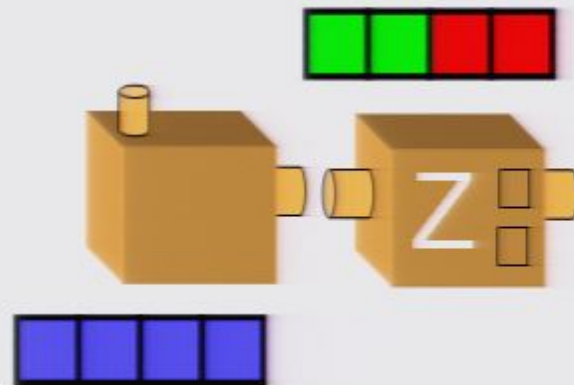
(one of 1 or 2) or (one of 3 or 4)?

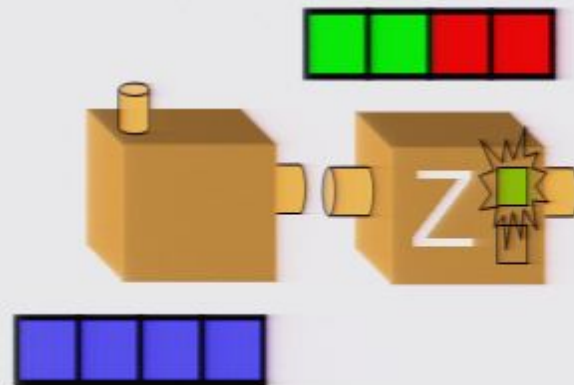


(one of 1 or 3) or (one of 2 or 4)?

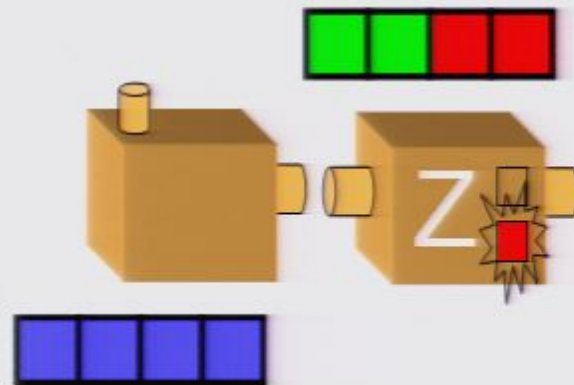


(one of 1 or 4) or (one of 2 or 3)?

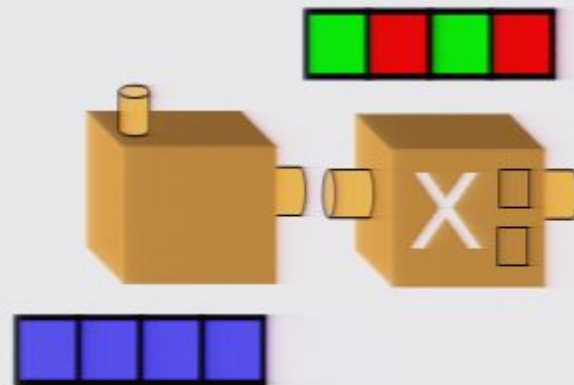




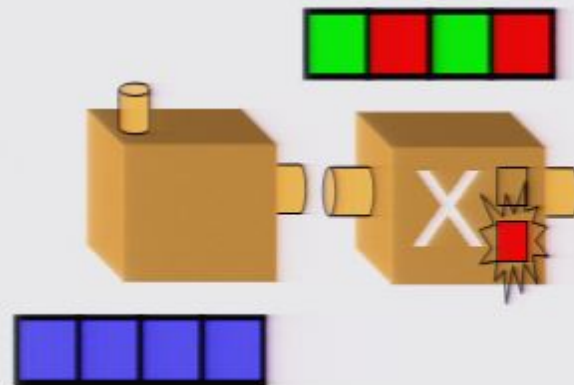
$\frac{1}{2}$  of the time



$\frac{1}{2}$  of the time

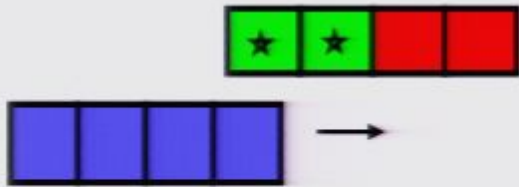






$\frac{1}{2}$  of the time

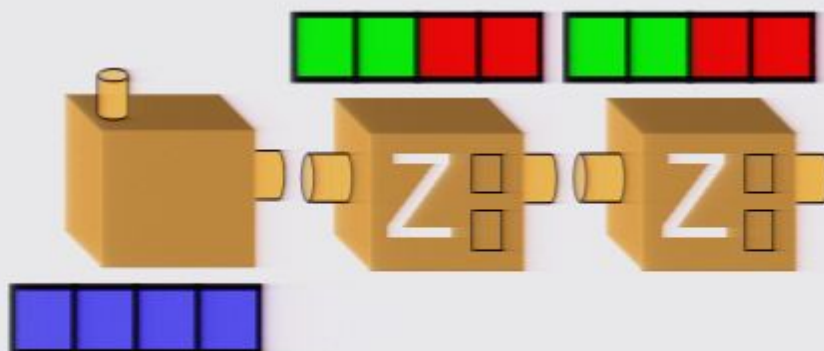
## Updating the probability distribution after a reproducible measurement

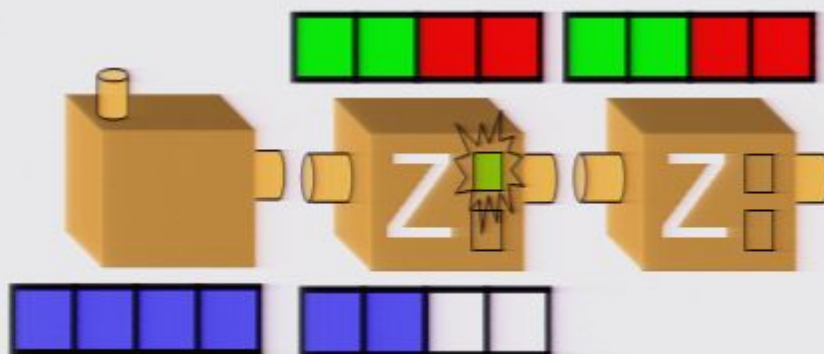


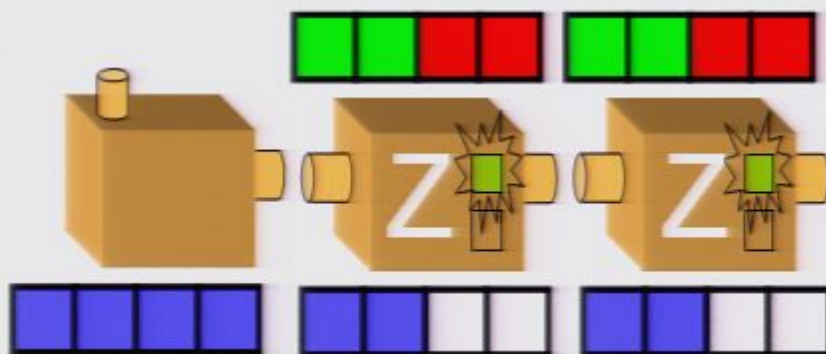
## Updating the probability distribution after a reproducible measurement

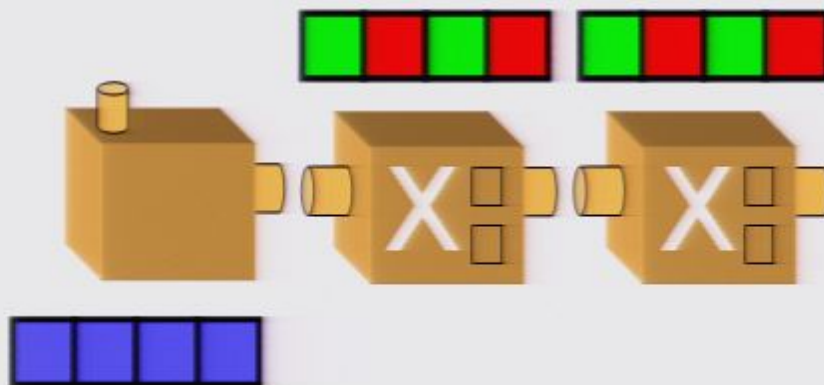


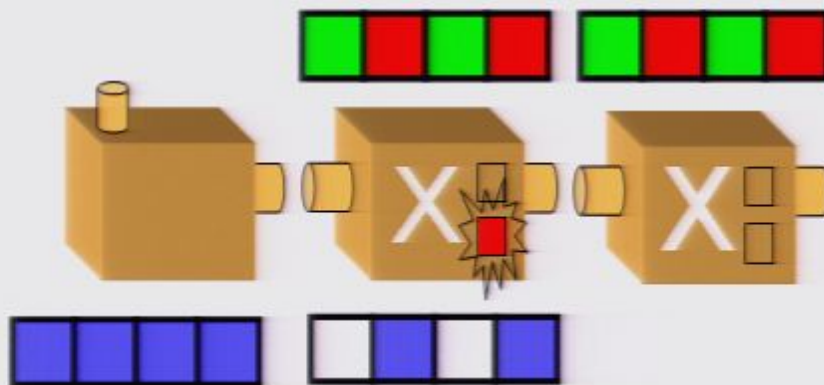
This is the only probability distribution that is sure to make this measurement reproducible is



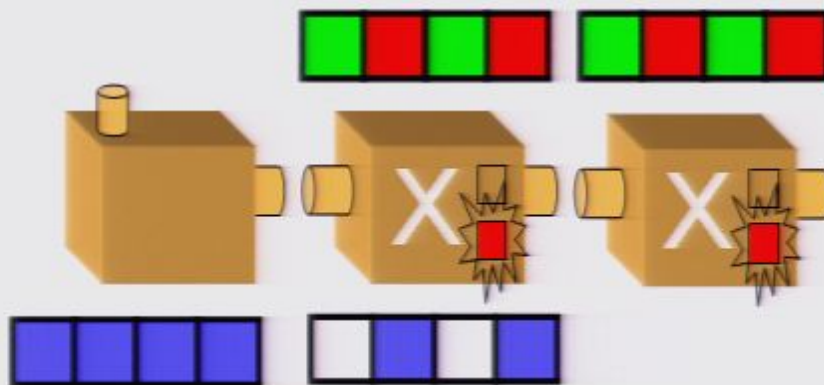


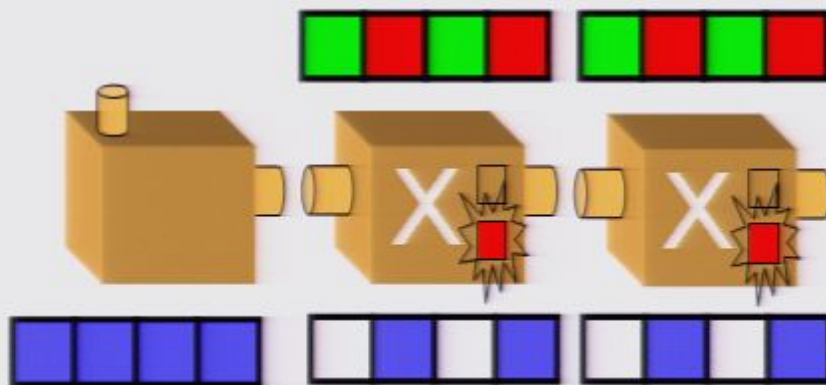




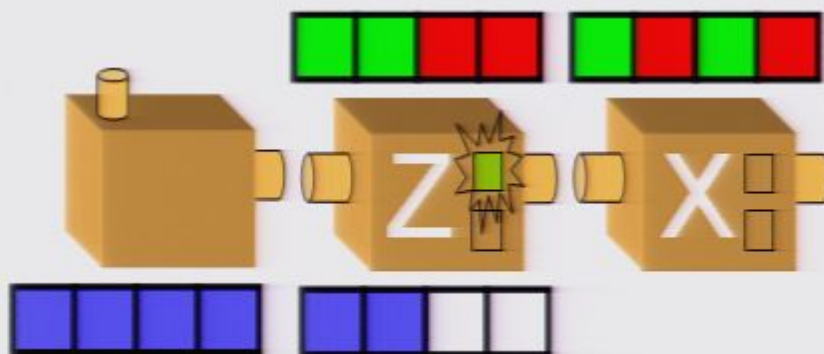






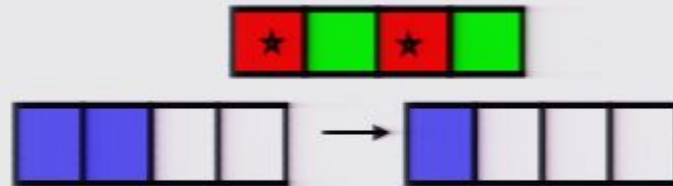






## Updating the probability distribution when the initial probability distribution is not uniform

Suppose no disturbance, then



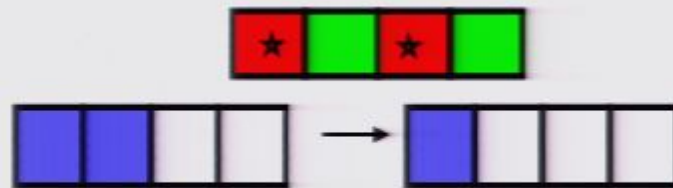
But this is too much knowledge!

The only probability distribution that is sure to make this measurement reproducible is



## Updating the probability distribution when the initial probability distribution is not uniform


Suppose no disturbance, then

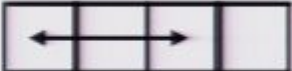


But this is too much knowledge!

The only probability distribution that is sure to make this measurement reproducible is

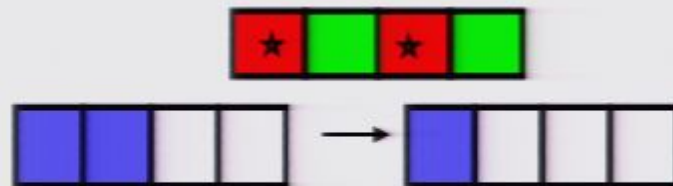


So we must assume that  occurs with prob.  $1/2$

and  occurs with prob.  $1/2$

## Updating the probability distribution when the initial probability distribution is not uniform


Suppose no disturbance, then

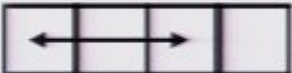


But this is too much knowledge!

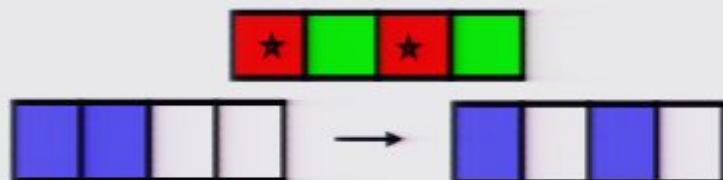
The only probability distribution that is sure to make this measurement reproducible is

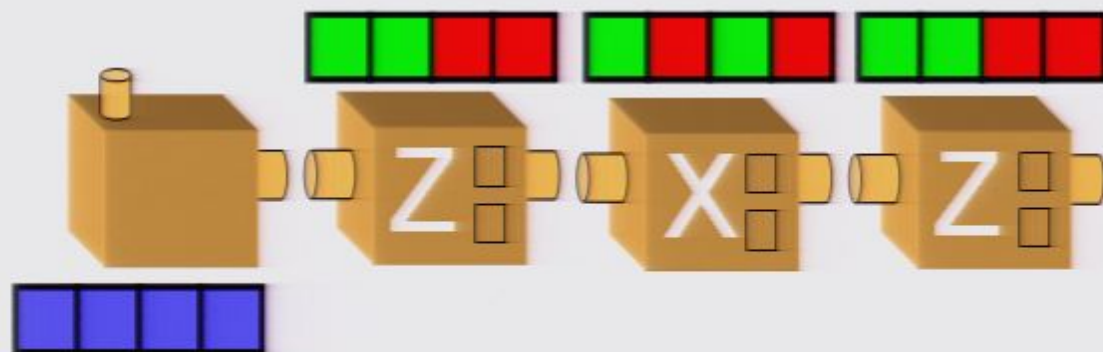


So we must assume that  occurs with prob.  $1/2$

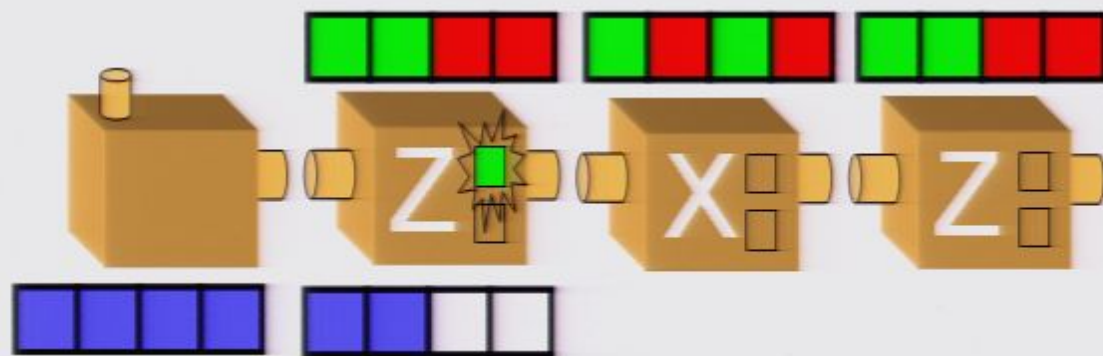
and  occurs with prob.  $1/2$

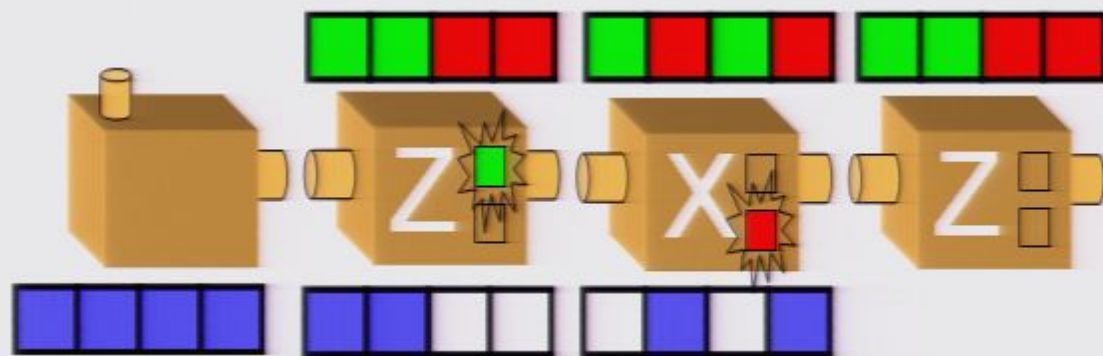
So we have

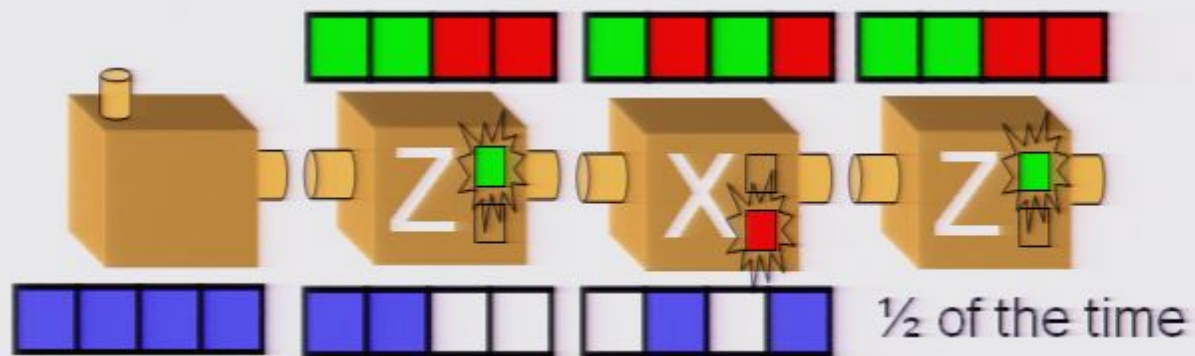




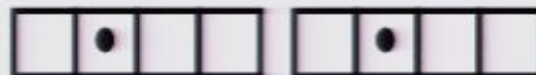


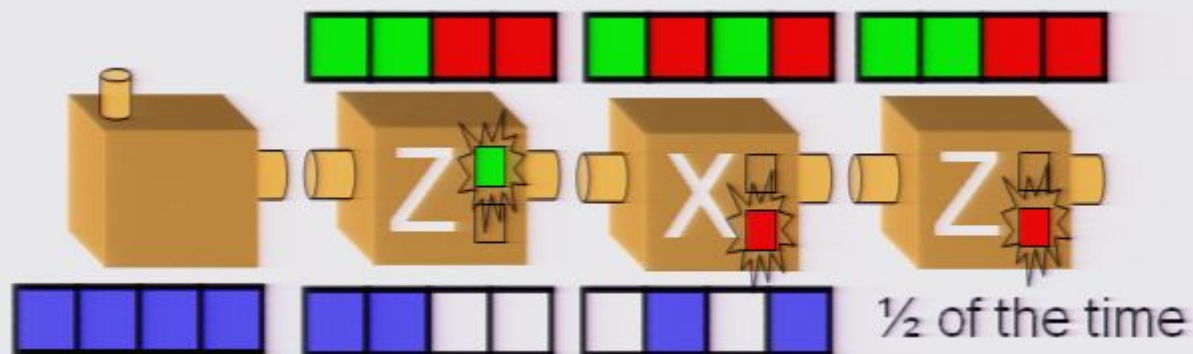




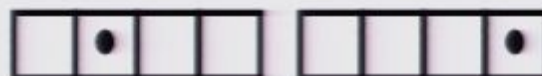


In retrospect, what must have happened:

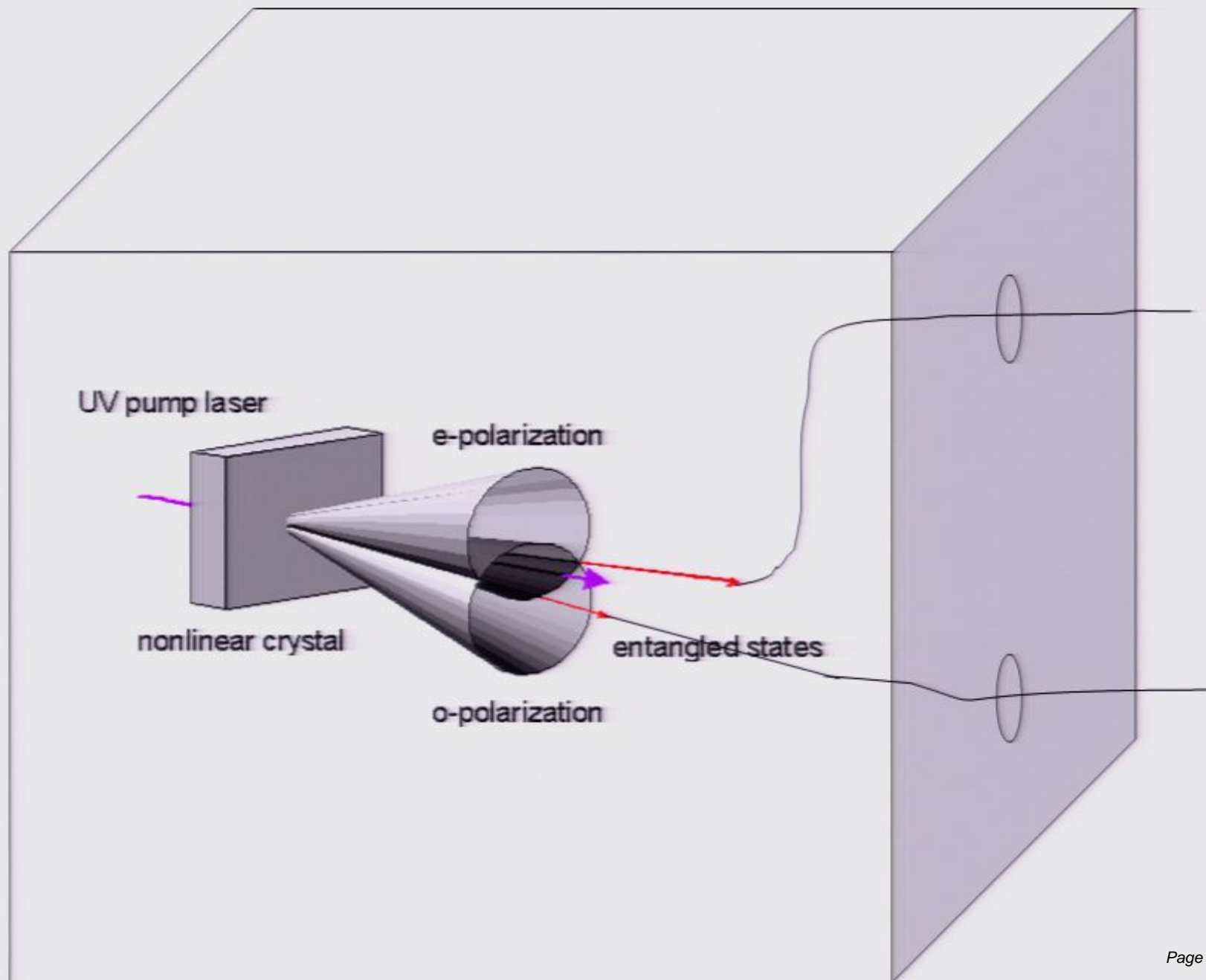


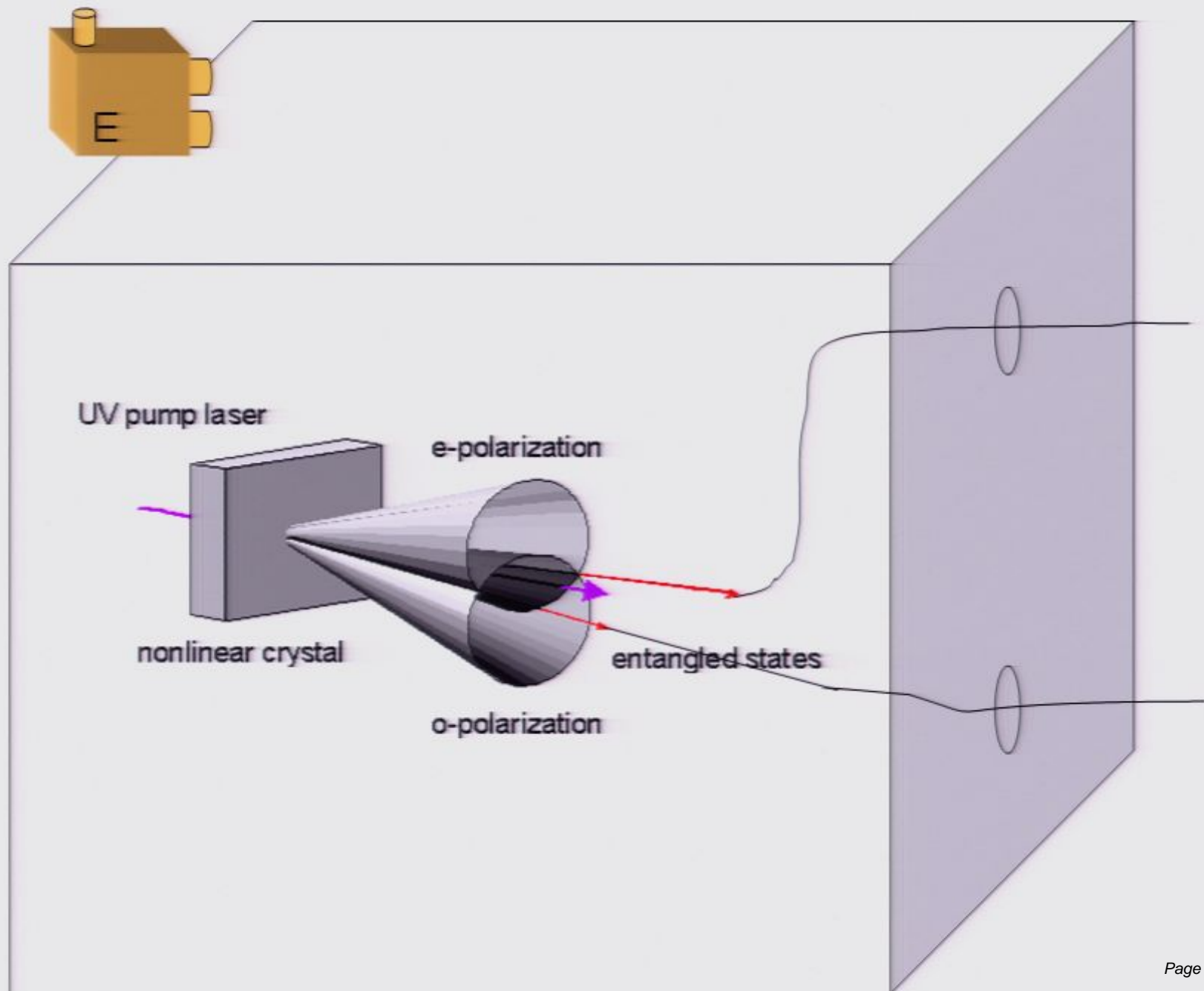


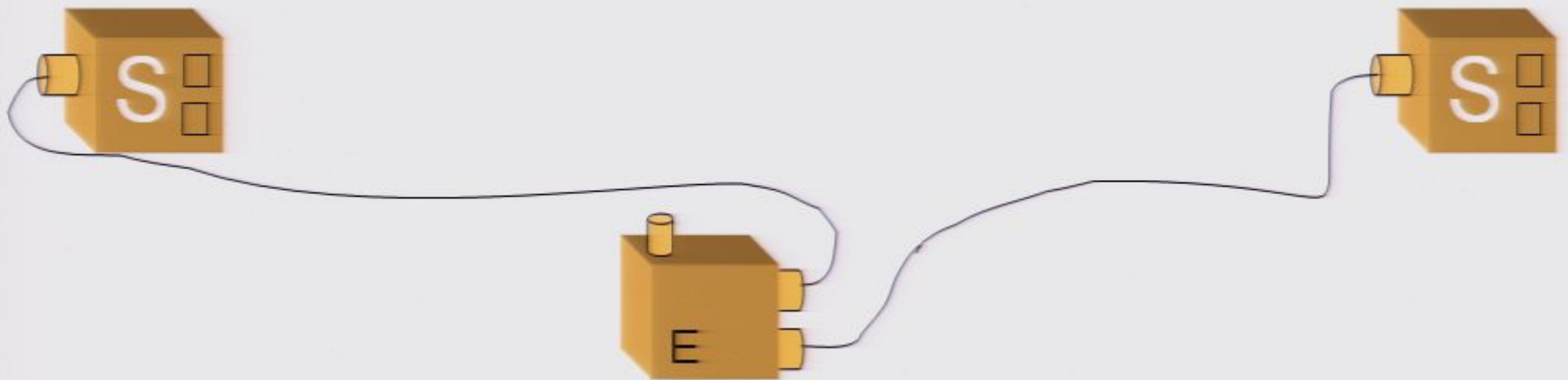
In retrospect, what must have happened:



Bell's theorem  
or  
why any realistic account  
of quantum mechanics  
must be nonlocal









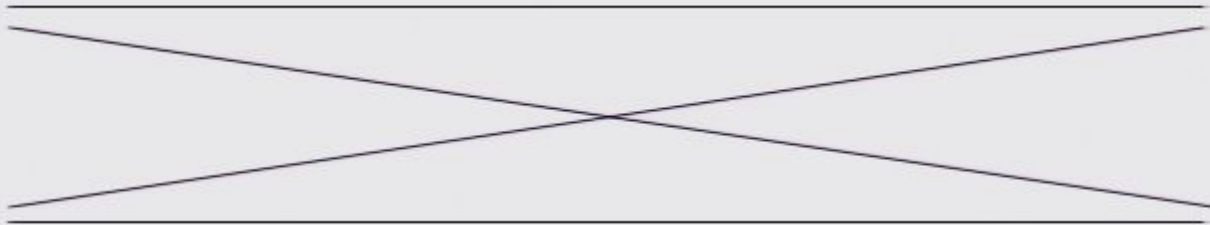
There are two possible measurements, S and T,  
with two outcomes each: green or red

Suppose which of S or T occurs at each wing is chosen at random

## Scenario 1

Features:

1. Whenever the **same** measurement is made on A and B, the outcomes always **agree**  
S and S  
or  
T and T
2. Whenever **different** measurements are made on A and B, the outcomes always **disagree**  
S and T  
or  
T and S



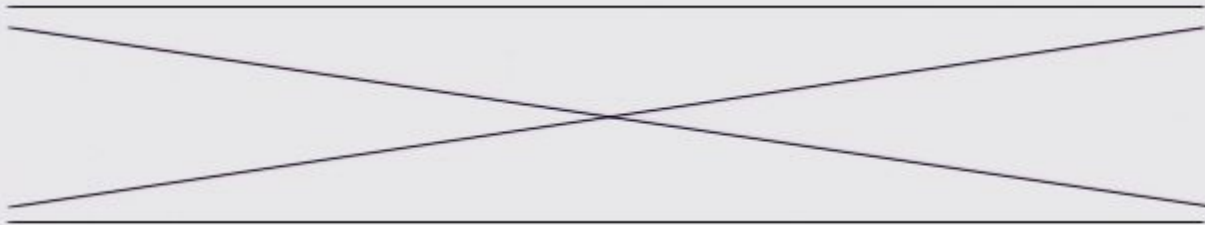
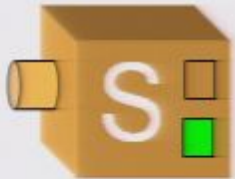
There are two possible measurements, S and T,  
with two outcomes each: green or red

Suppose which of S or T occurs at each wing is chosen at random

## Scenario 2

Features:

1. Whenever the **same** measurement is made on A and B, the outcomes always **disagree**  
S and S  
or  
T and T
2. Whenever **different** measurements are made on A and B, the outcomes always **agree**  
S and T  
or  
T and S



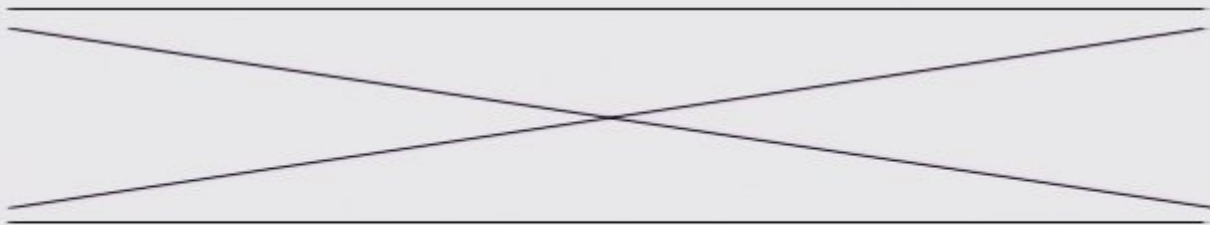
There are two possible measurements, S and T,  
with two outcomes each: green or red

Suppose which of S or T occurs at each wing is chosen at random

## Scenario 2

Features:

1. Whenever the **same** measurement is made on A and B, the outcomes always **disagree**  
S and S  
or  
T and T
2. Whenever **different** measurements are made on A and B, the outcomes always **agree**  
S and T  
or  
T and S



There are two possible "measurements", S and T,  
with two outcomes each: green or red

Suppose which of S or T occurs at each wing is chosen at random

## Scenario 3

Features:

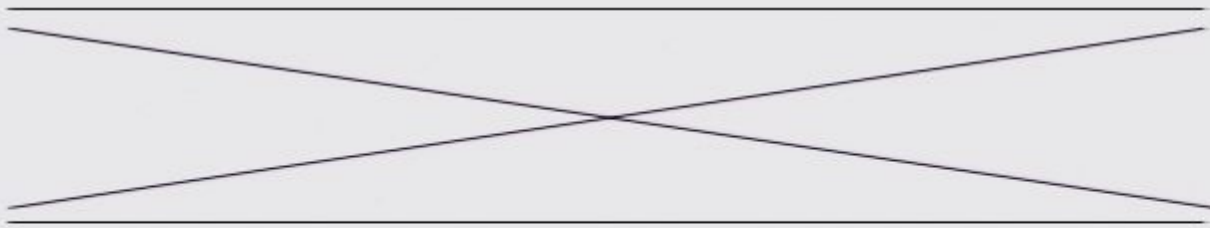
1. Whenever the measurement  
T is made on both A and B,  
the outcomes always  
disagree

T and T

2. Otherwise, the outcomes  
always agree

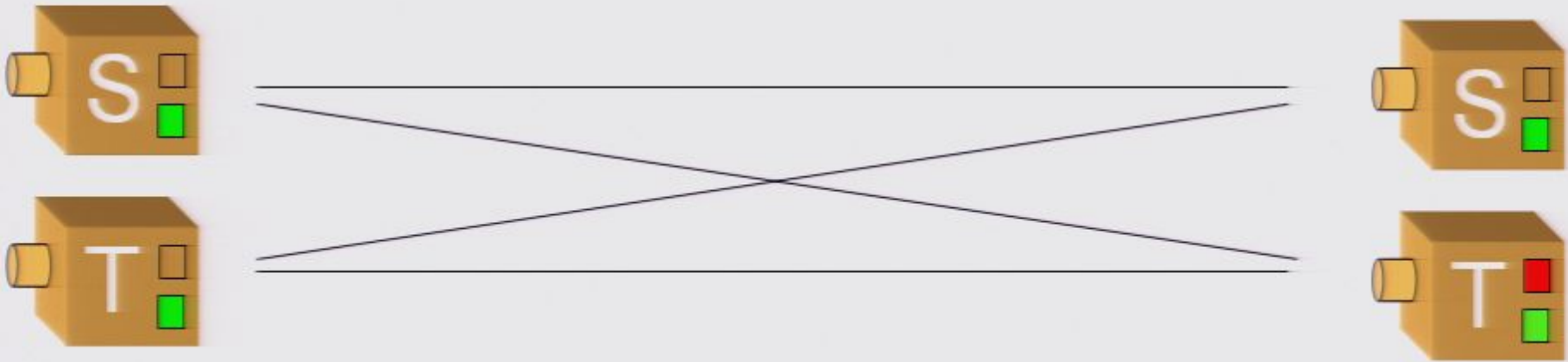
S and S  
or  
S and T  
or  
T and S





Q: What's the best probability of winning?

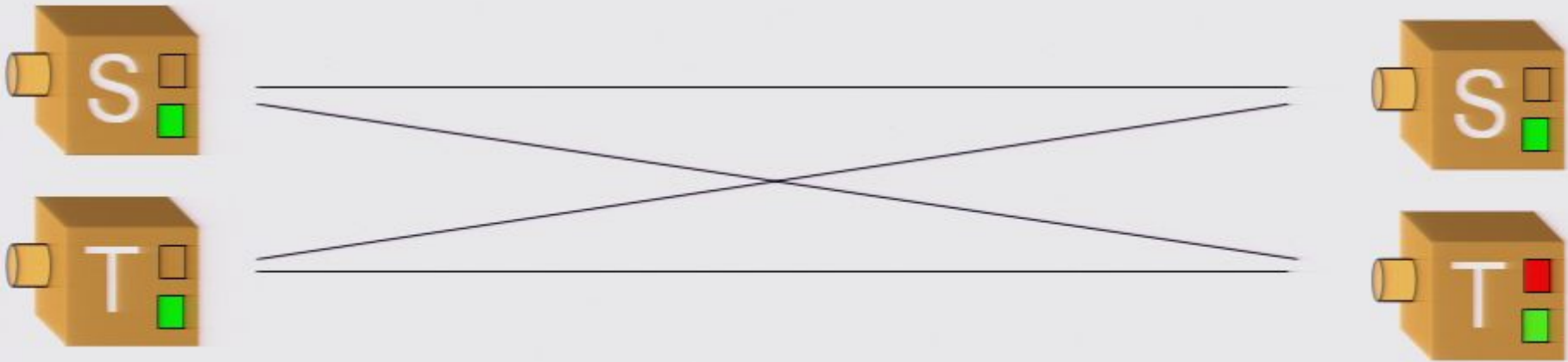




Q: What's the best probability of winning?

The best local strategies "win the game" only 75% of the time  
Using quantum systems, one can win 85% of the time!

Q: How could you cheat and win the game all the time?



Q: What's the best probability of winning?

The best local strategies "win the game" only 75% of the time  
Using quantum systems, one can win 85% of the time!

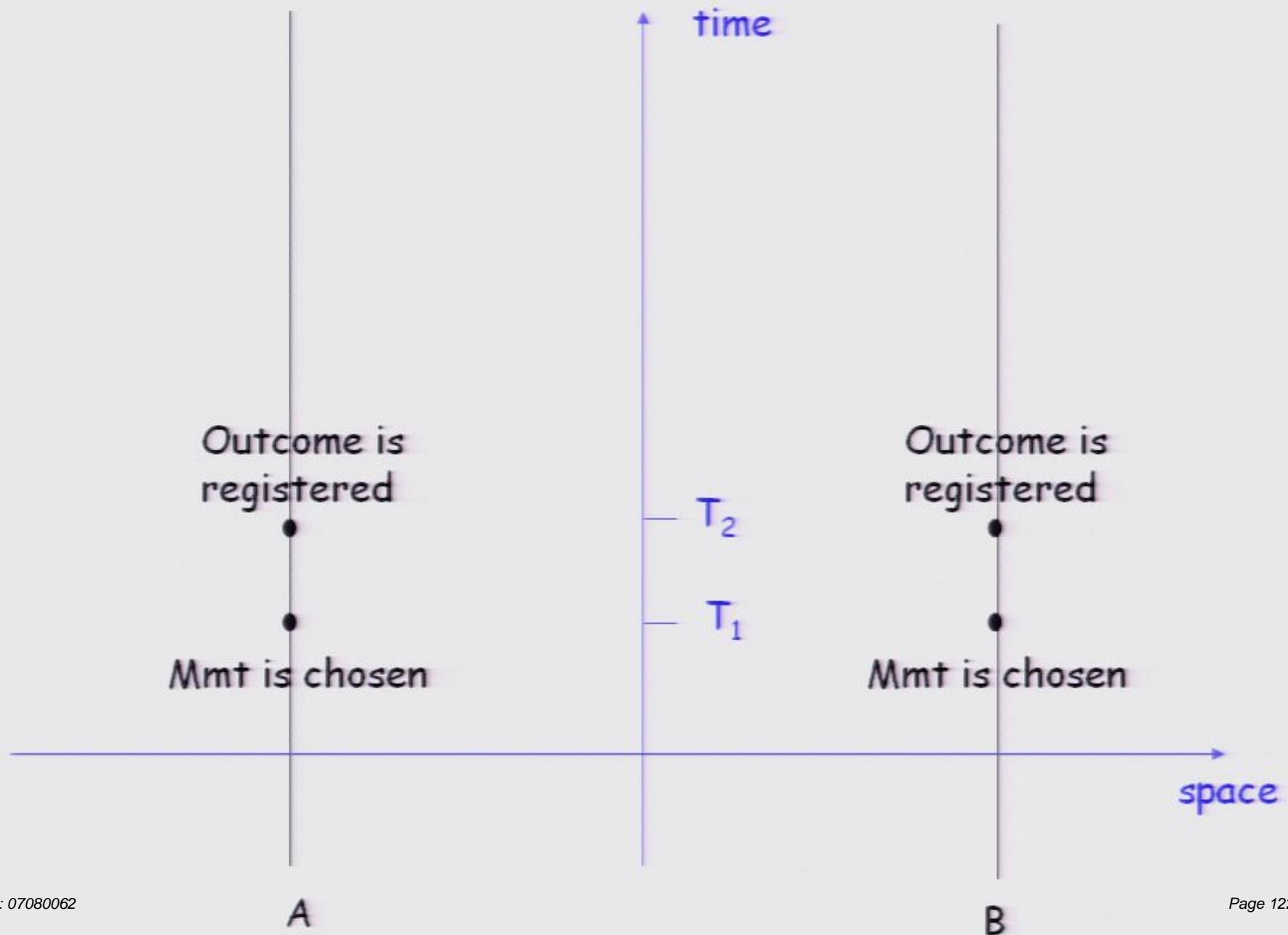
Q: How could you cheat and win the game all the time?

Q: How could you cheat and win the game all the time?

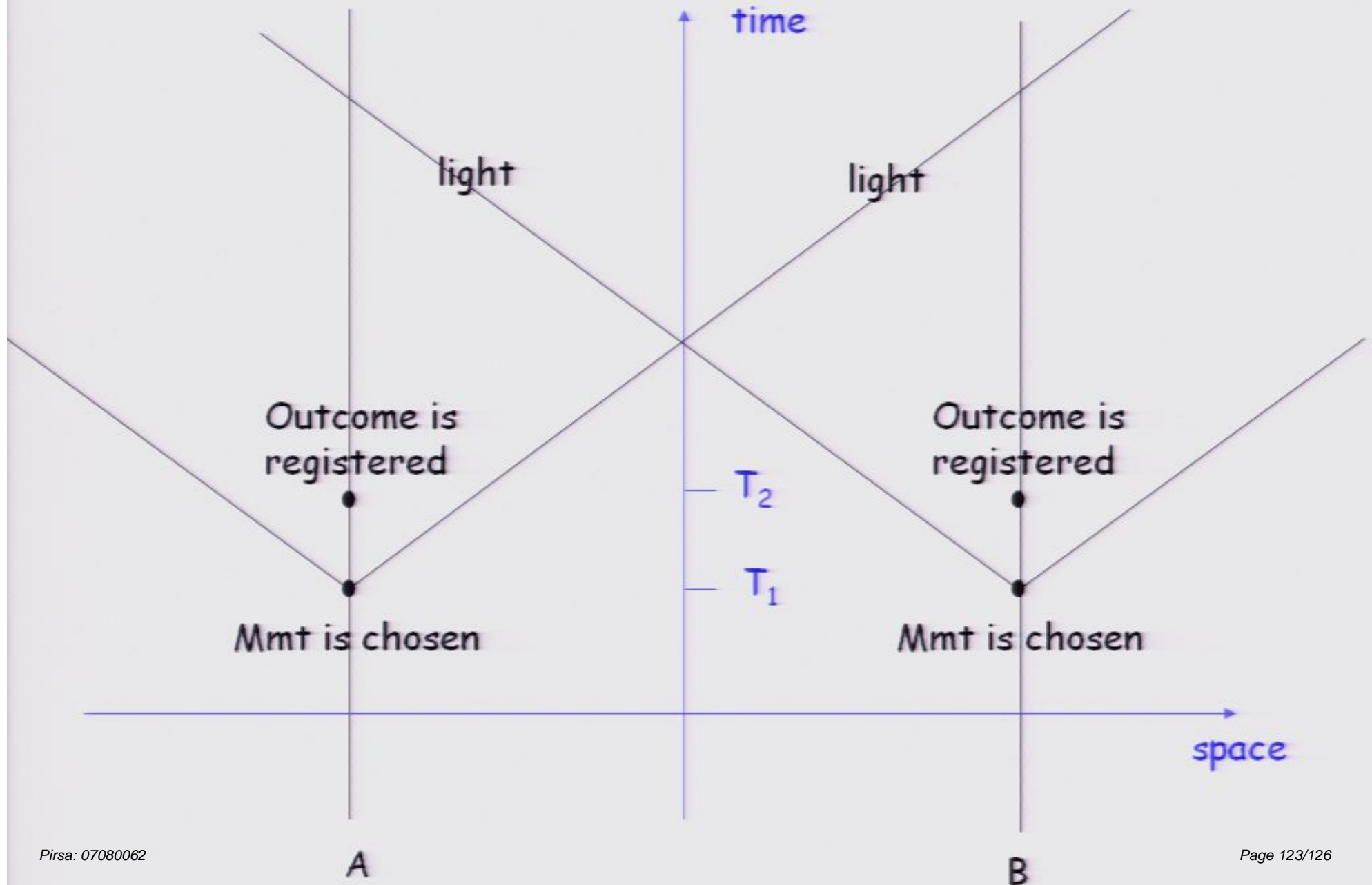
A: Communication of the choice of measurement in one wing to the system in the opposite wing

But there's a problem...

## Tension with the theory of relativity



## Tension with the theory of relativity



Experiment can distinguish:

- 1) the quantum predictions
- 2) the predictions of any locally causal theory



Experiment can distinguish:

- 1) the quantum predictions
- 2) the predictions of any locally causal theory

Quantum theory wins!

When seeking a realist explanation of Bell's theorem, the mystery is the tension between:

- 1) No superluminal signalling (independence of statistics at one wing on choice of measurement at the other)
- 2) The necessity of superluminal influences (dependence of particular outcomes at one wing on choice of measurement at the other)