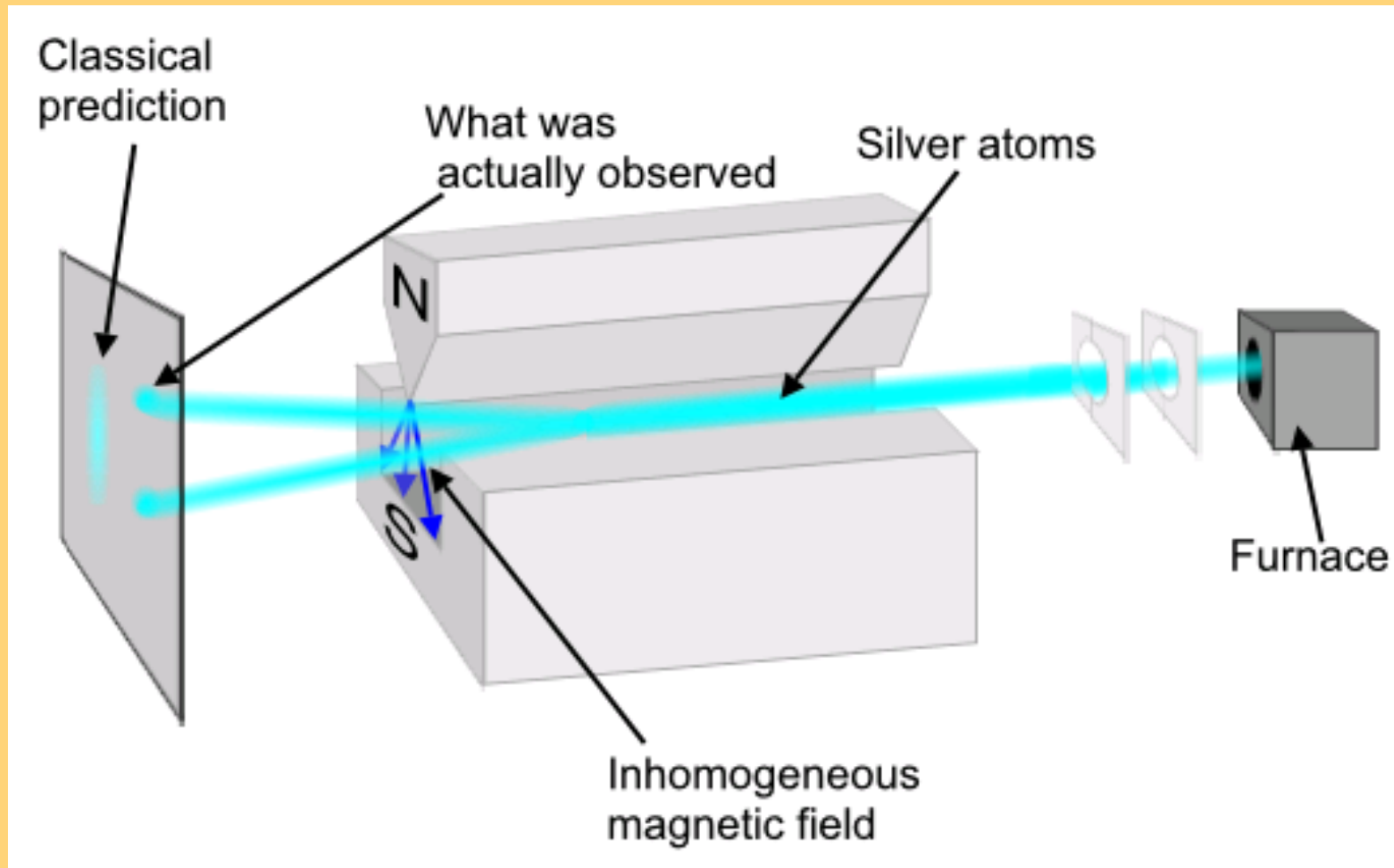
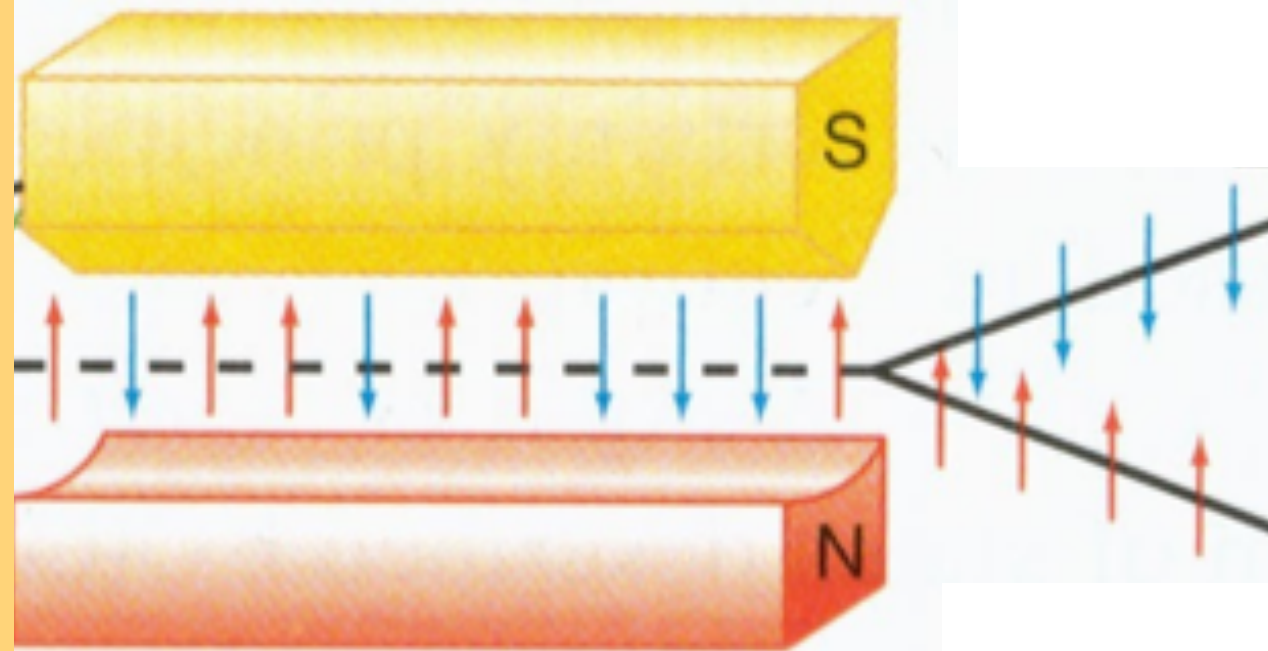
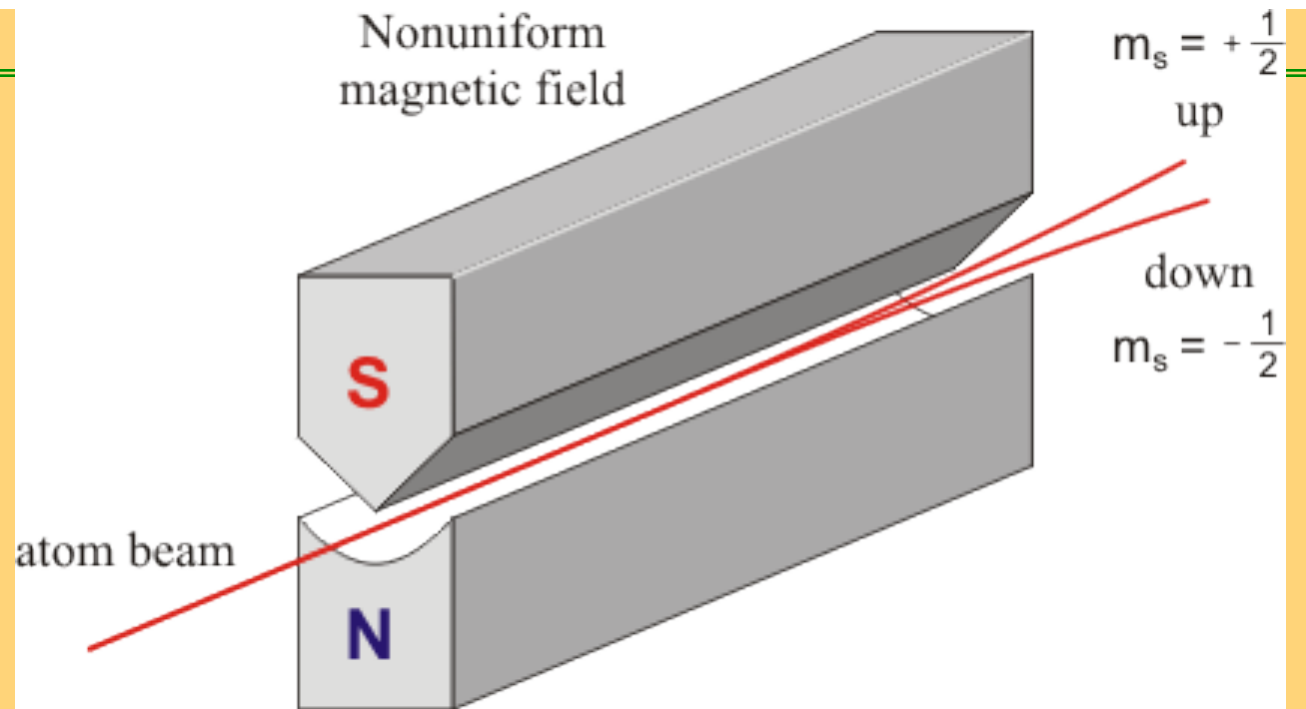


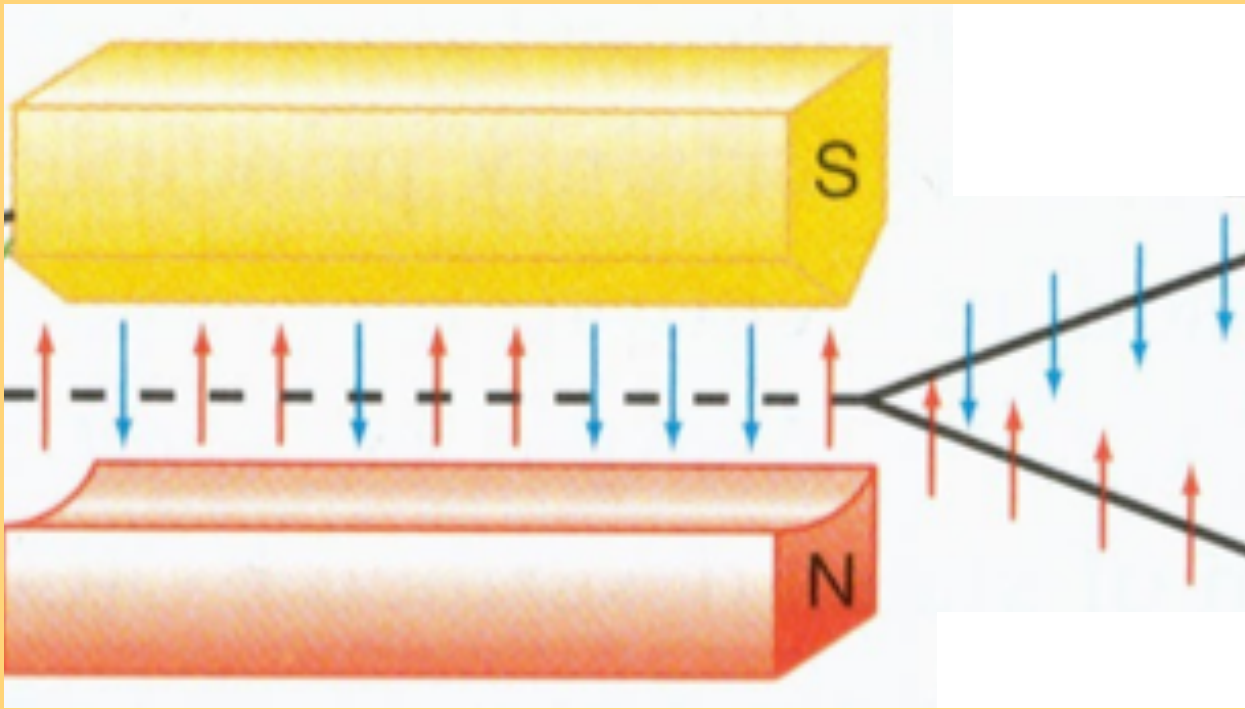
Quantum Mechanics: The Stern-Gerlach Experiment (1921)



a silver atom has an unpaired electron
(and a charged particle is deflected by a magnetic field)

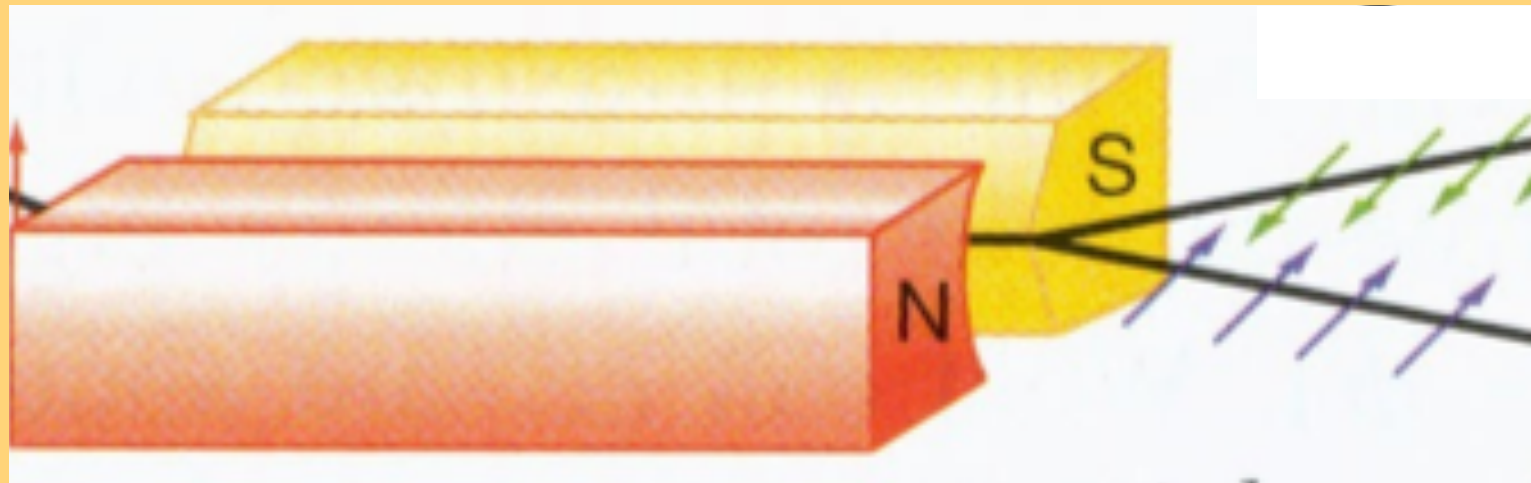
UT D





up = u

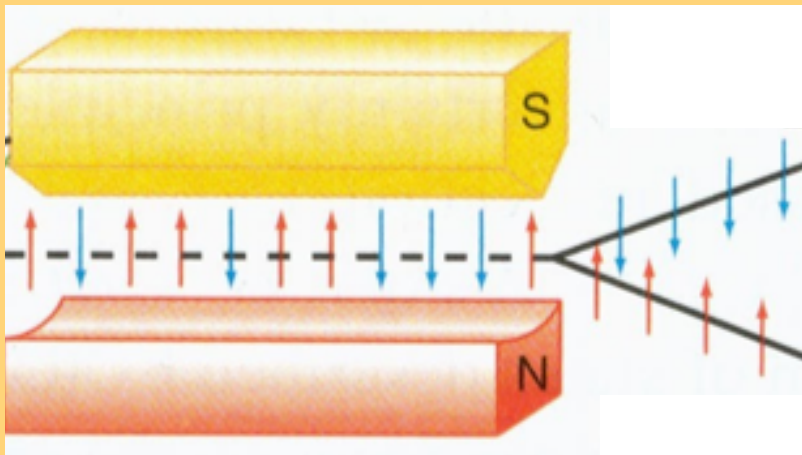
down = d



left = l

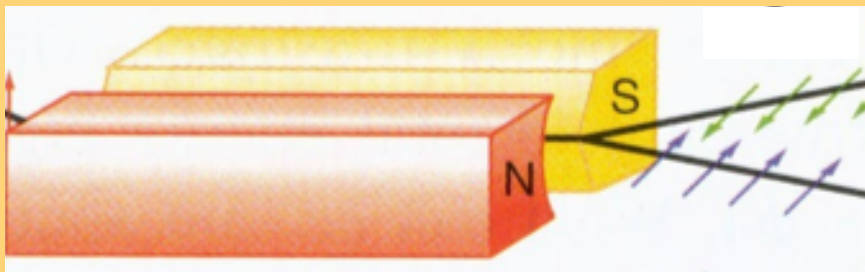
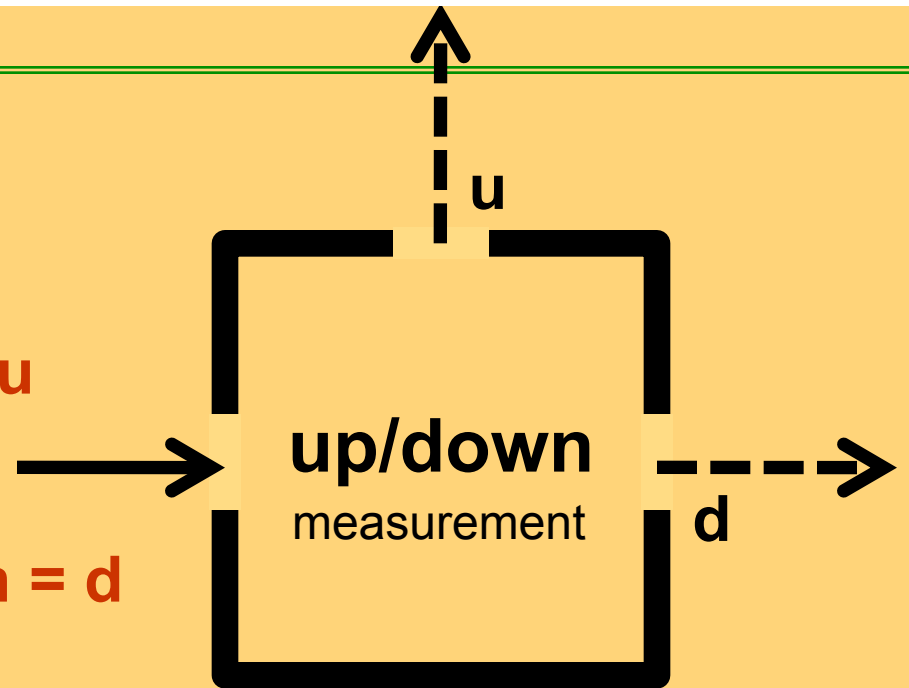
right = r

UT D



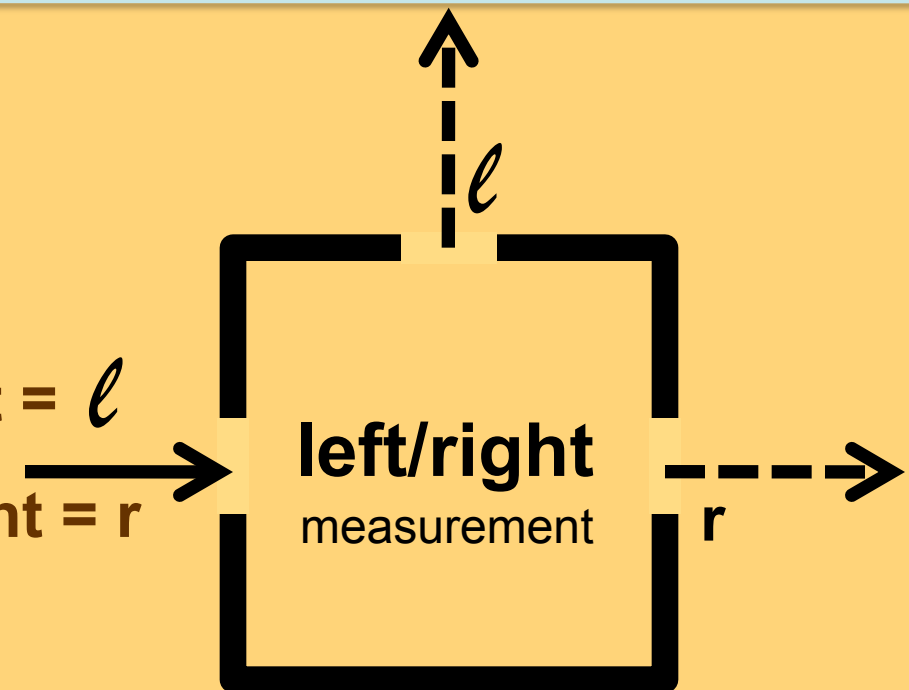
up = u

down = d



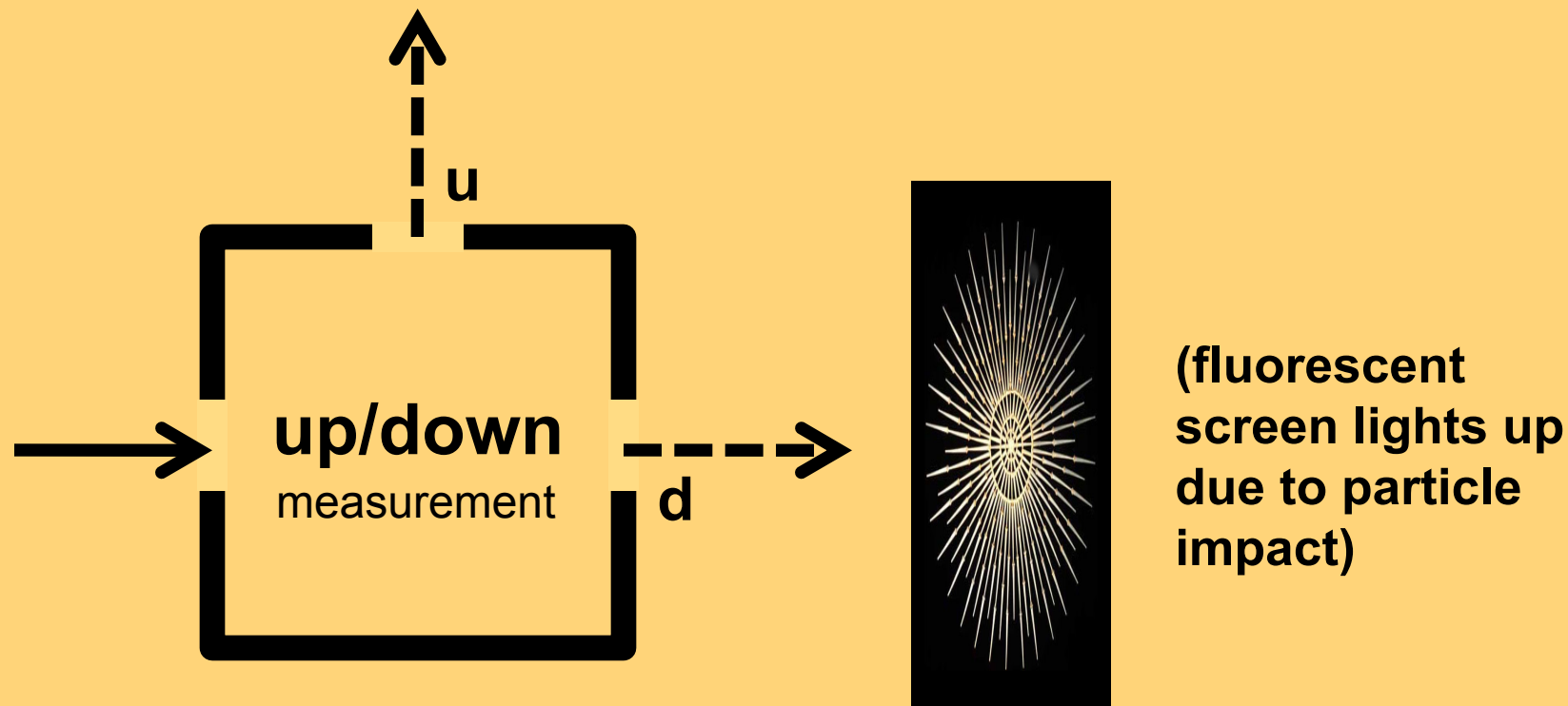
left = l

right = r



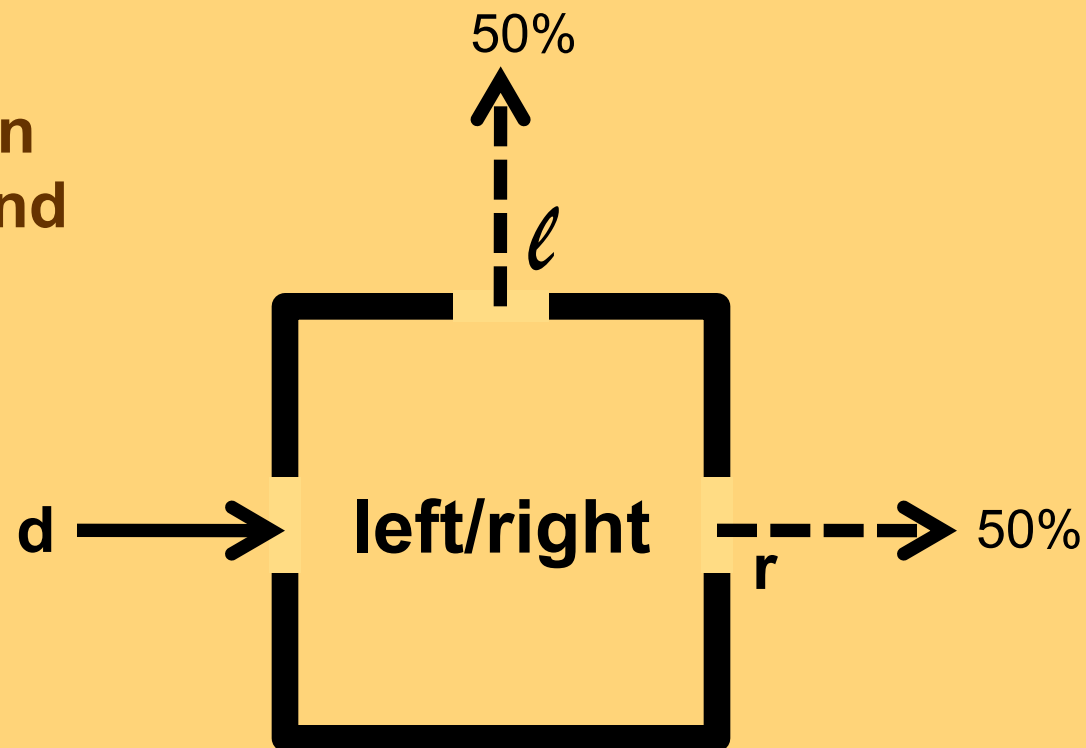
This device *measures* the up/down property by sending “up” atoms one way and “down” atoms another way.

But to learn the outcome you would have to put a fluorescent screen or something in the beam path:



Are the up/down and left/right properties of an atom correlated?

No: 50% of down atoms are left and 50% are right



knowing the up/down property of an atom tells us nothing about its left/right property
(and no additional information helps [no hidden variables])

Now assume a down atom emerges from the right aperture of a left/right box (50% will do so).

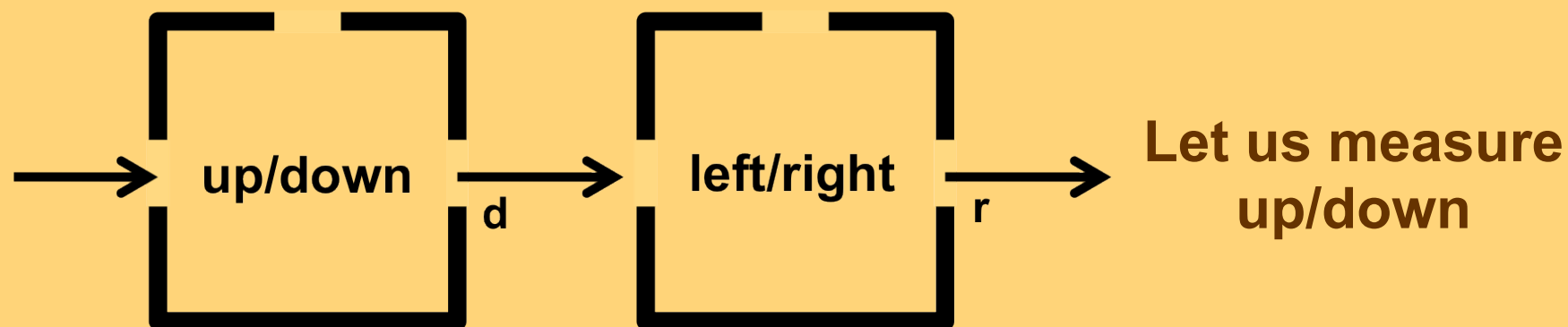
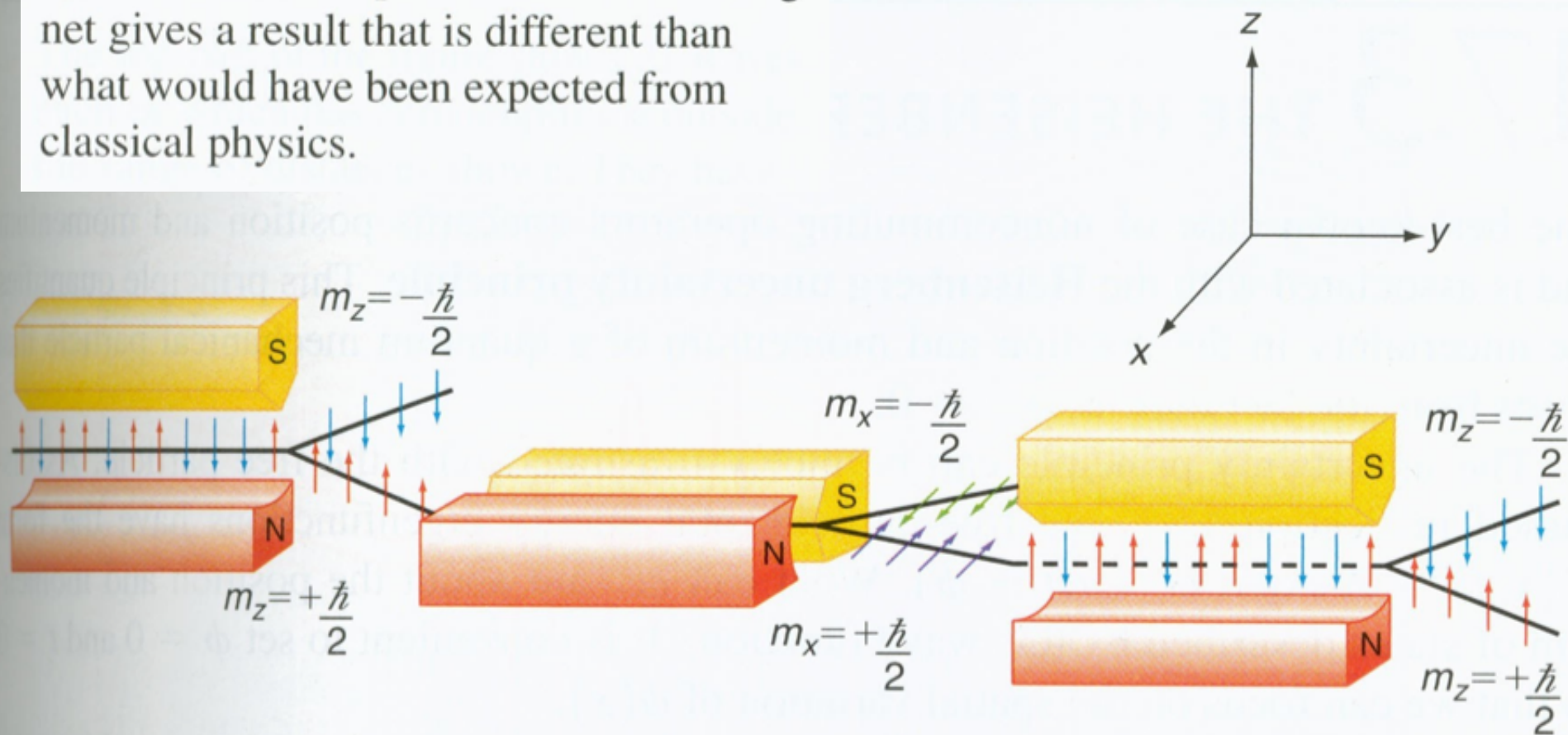
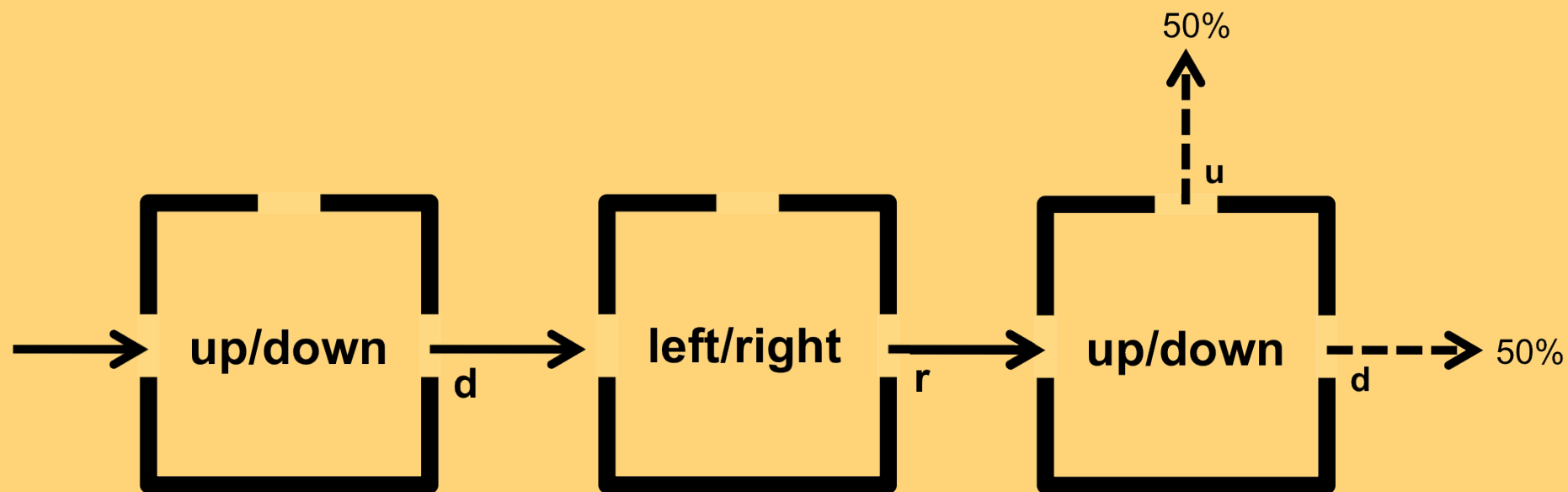


FIGURE 17.3

One of the beams exiting from the first magnet has been passed through a second magnet rotated by 90° . Again the beam is split into two components. The third magnet gives a result that is different than what would have been expected from classical physics.



Now assume a down atom emerges from the right aperture of a left/right box (50% will do so).



somehow the left/right box has changed the up/down value !

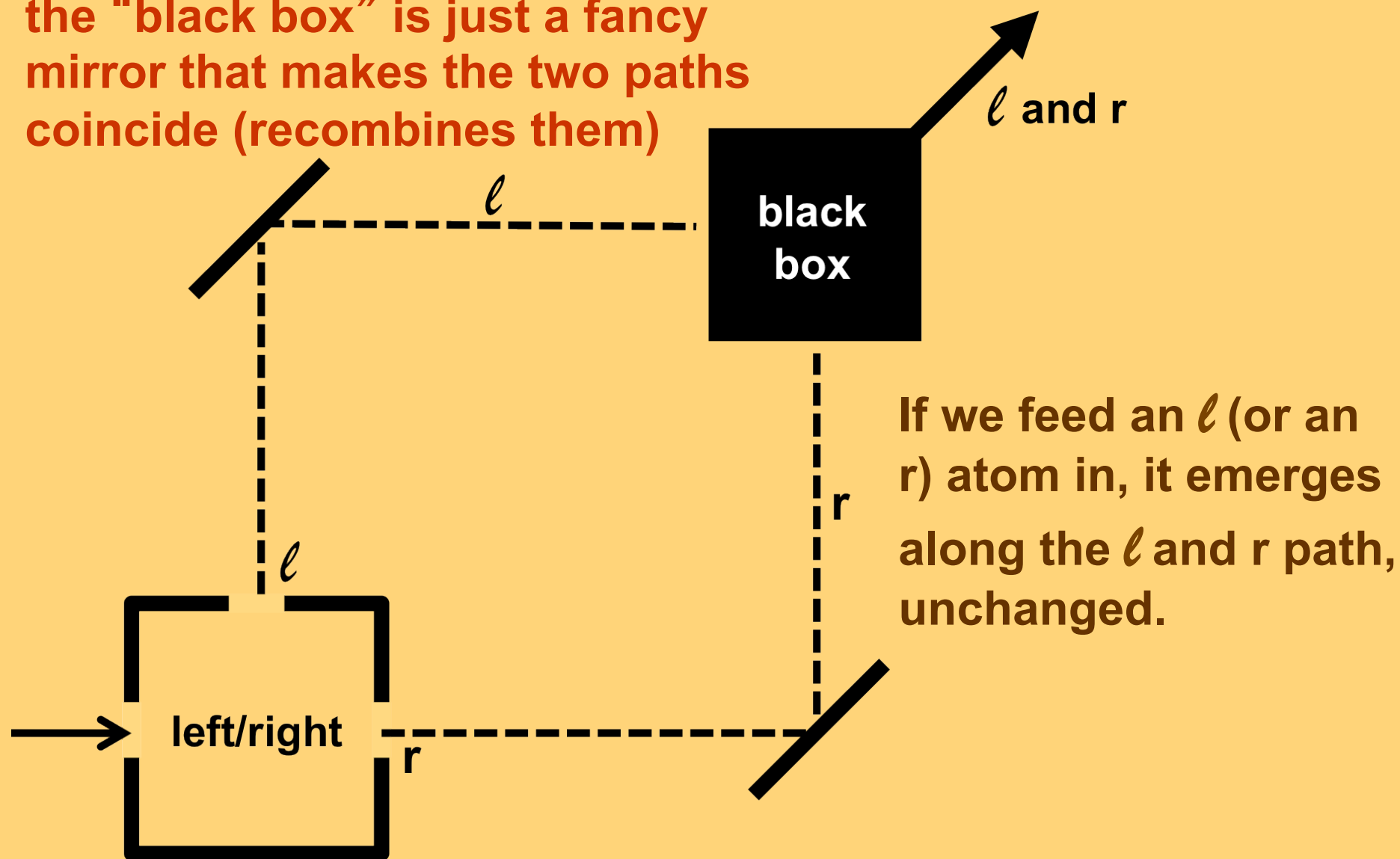
introduce vector / matrix notation for all this

when performing a measurement, we must change to the “measurement” basis to learn about the outcomes, because of how quantum mechanics works (because of the postulates)

(need to discuss the postulates including collapse)

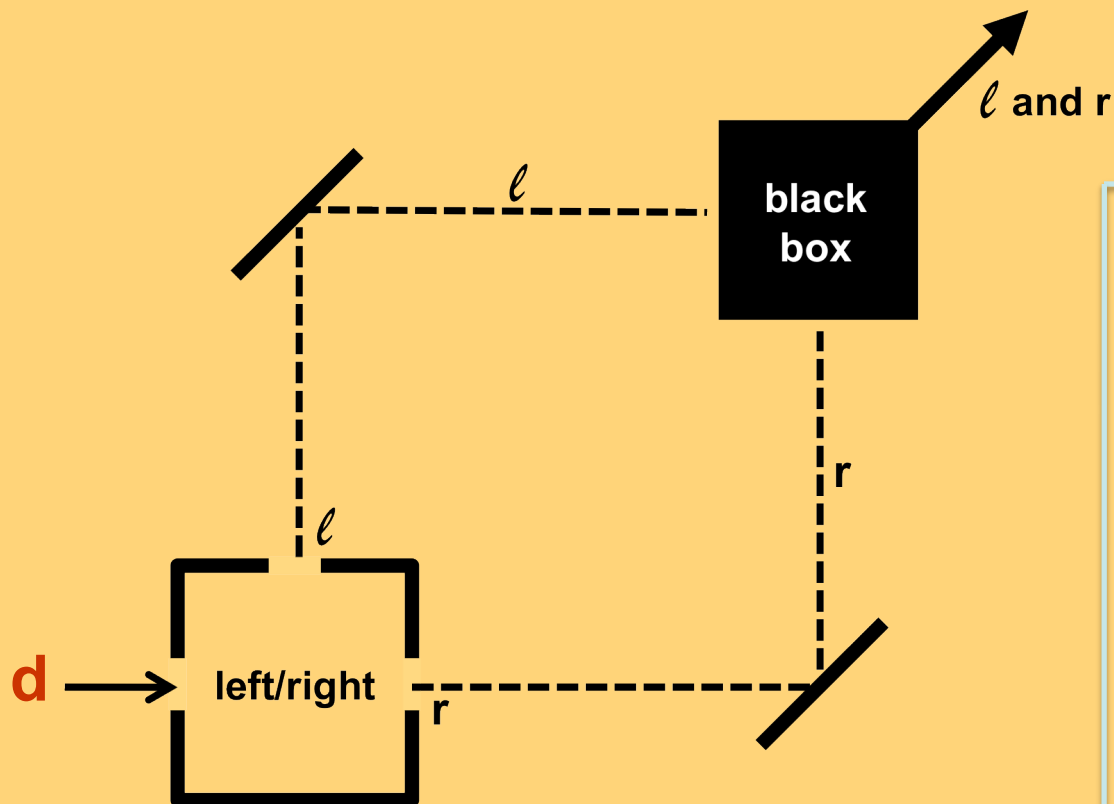
Now construct a more complicated apparatus

the “black box” is just a fancy mirror that makes the two paths coincide (recombines them)

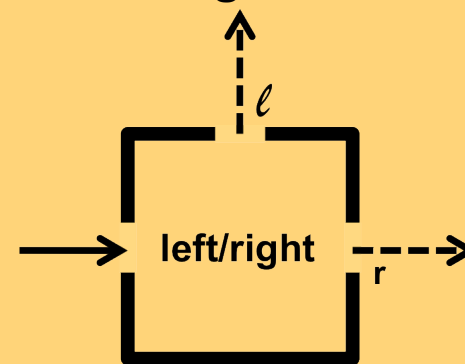


Use a down atom and measure left/right.

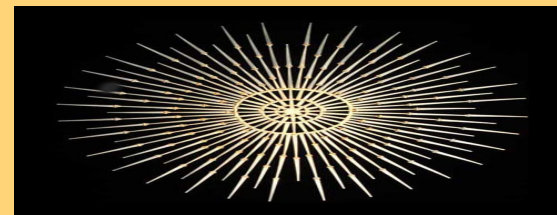
Find 50% ℓ and 50% r



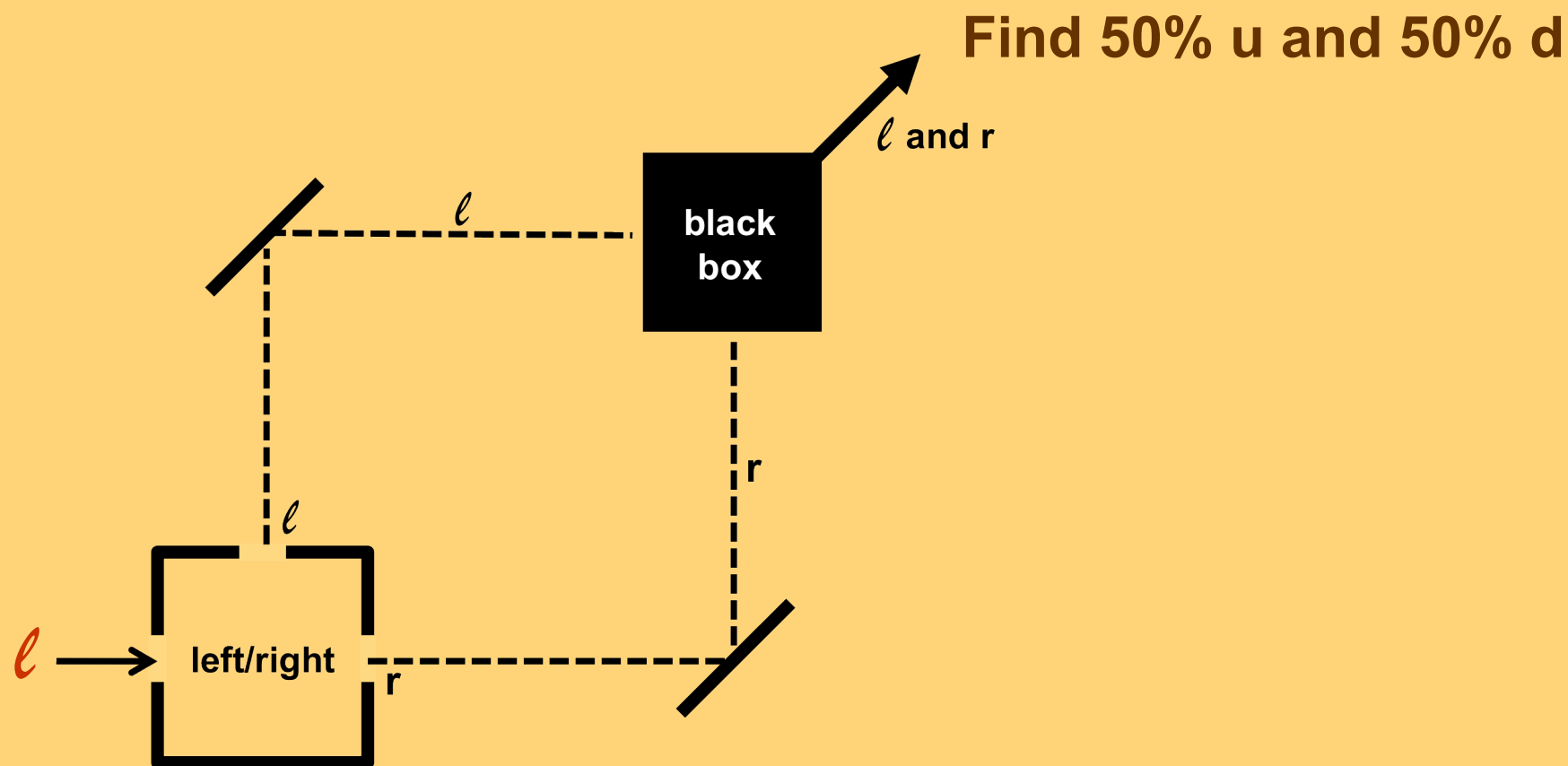
Note: "find" here means using this:



and this:

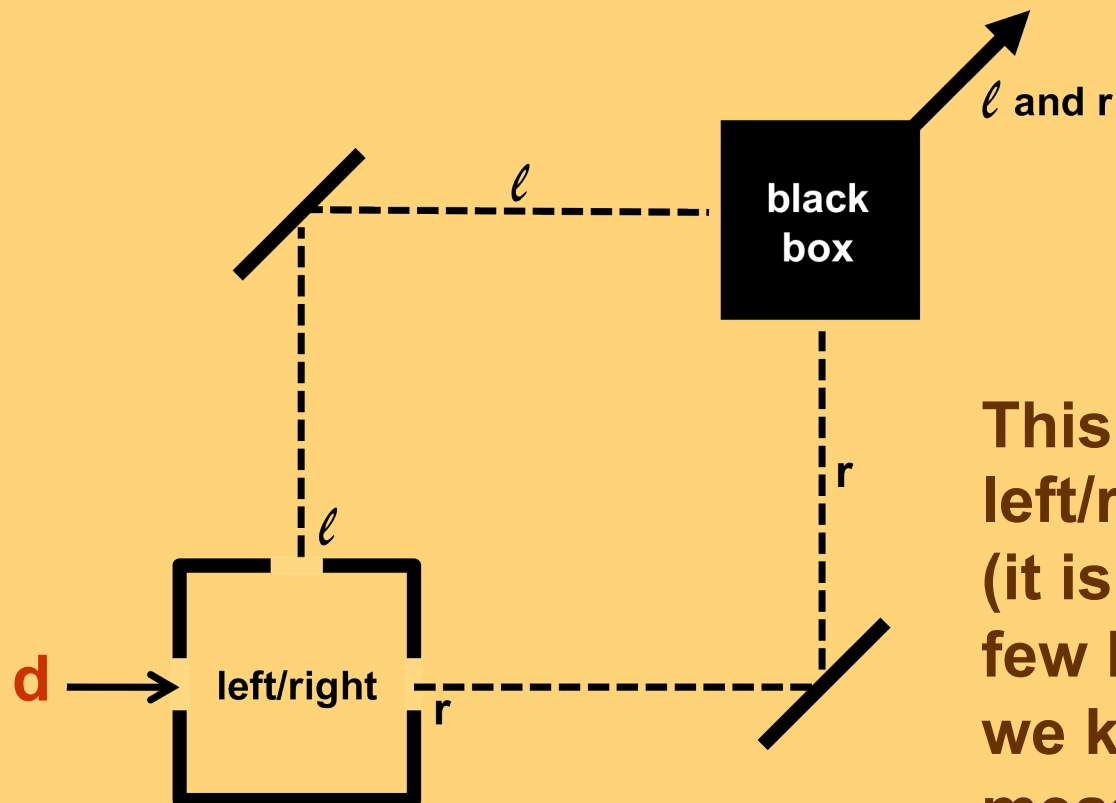


Use a left atom and measure up/down.



UTD

Use a down atom and measure up/down.

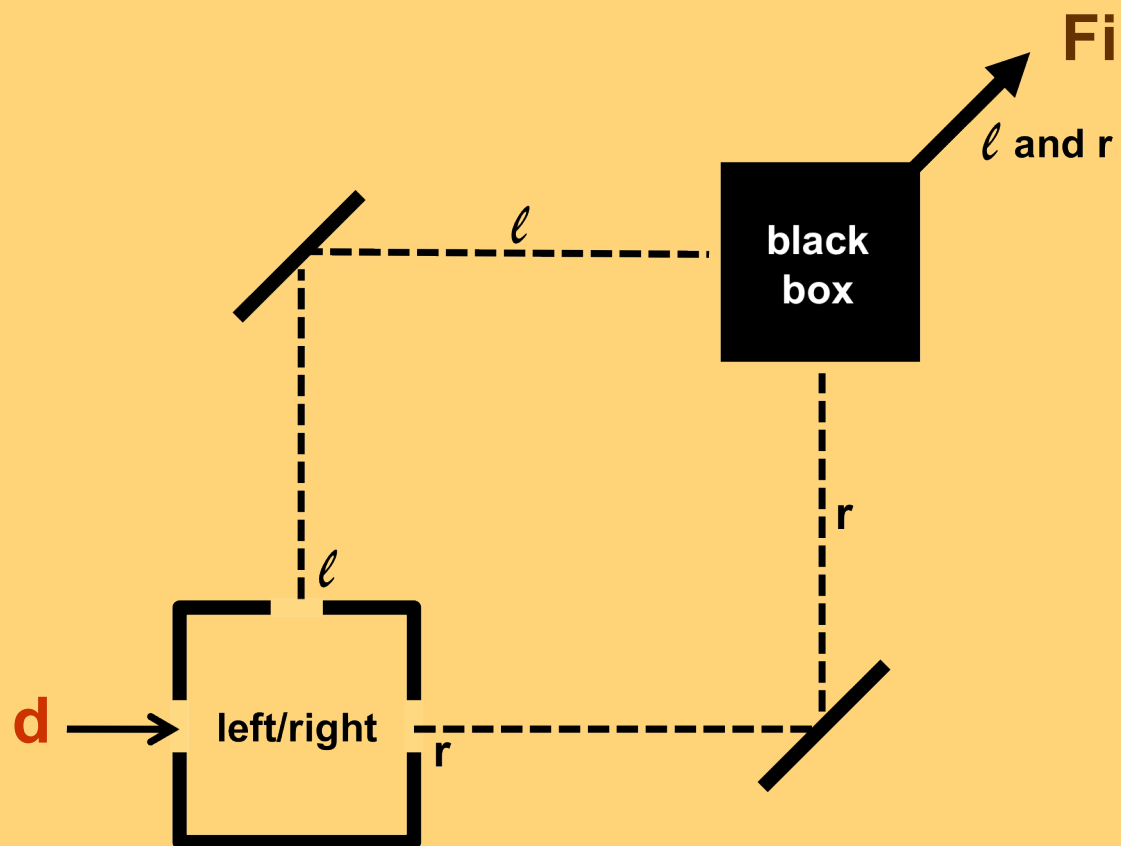


This device is just a fancy left/right box (it is a left/right box with a few harmless mirrors), and we know a left/right measurement scrambles the up/down property.

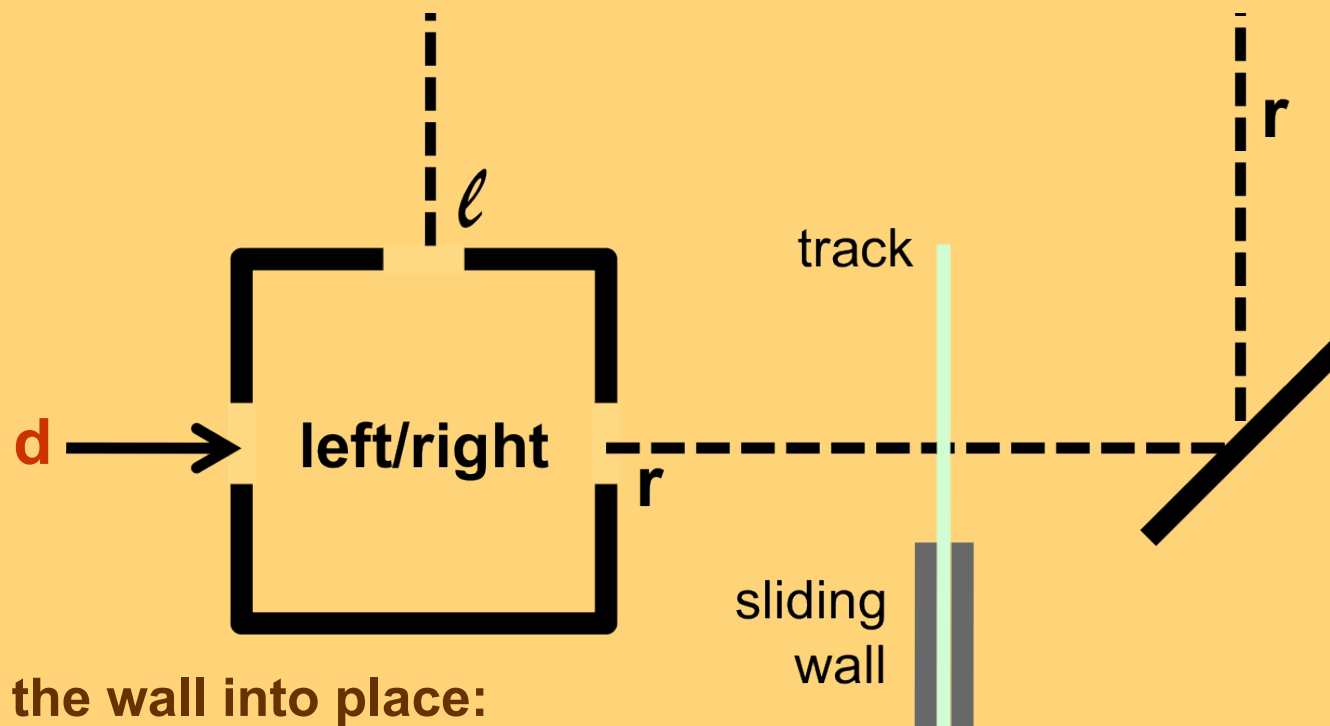
UTD

Use a down atom and measure up/down.

Find 100% down !!!



Let us add a movable wall that absorbs atoms



Slide the wall into place:

- 1.) 50% reduction in the number of atoms emerging from the apparatus
- 2.) Of the atoms that emerge, their up/down property is now scrambled: 50% u and 50% d.

What can possibly be going on ?

Consider an atom which passes through the apparatus when the sliding wall is out.

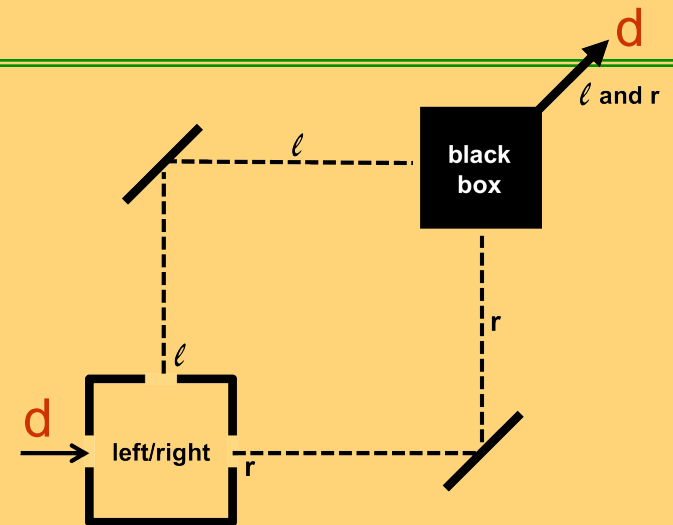
Does it take route ℓ ? No, because ℓ atoms have 50/50 u/d statistics.

Does it take route r ? No, same reason.

Can it somehow have taken both routes ? No: if we look (use a fluorescent screen) to see where the atom is inside the apparatus, we find that 50% of the time it is on route ℓ , and 50% of the time it is on route r . We never find two atoms inside, or two halves of a single, split atom, or anything like that. There isn't any sense in which the atom seems to be taking both routes.

Can it have taken neither route? No: if we put sliding walls in place to block both routes, nothing gets through at all.

But these are all the logical possibilities !



What can these atoms be doing?

We use the word (which is just a name for something we don't understand) *superposition*.

What we say about an initially down atom which is now passing through our apparatus (with the wall out) is that it's not on path ℓ and not on r and not on both and not on neither, but, rather, that it's in a *superposition* of being on ℓ and being on r . And what this means (other than "none of the above") we don't know.

We know, by experiment, that atoms emerge from the left aperture of a left/right box if and only if they're left atoms when they enter that box.

When a *down* atom is fed into a left/right box, it emerges neither through the left aperture nor through the right one nor through both nor through neither. So, it follows that a down atom can't be a left one, or a right one, or (somehow) both, or neither. To say that an atom is down must be just the same as to say that it's in a *superposition* of being left and right.

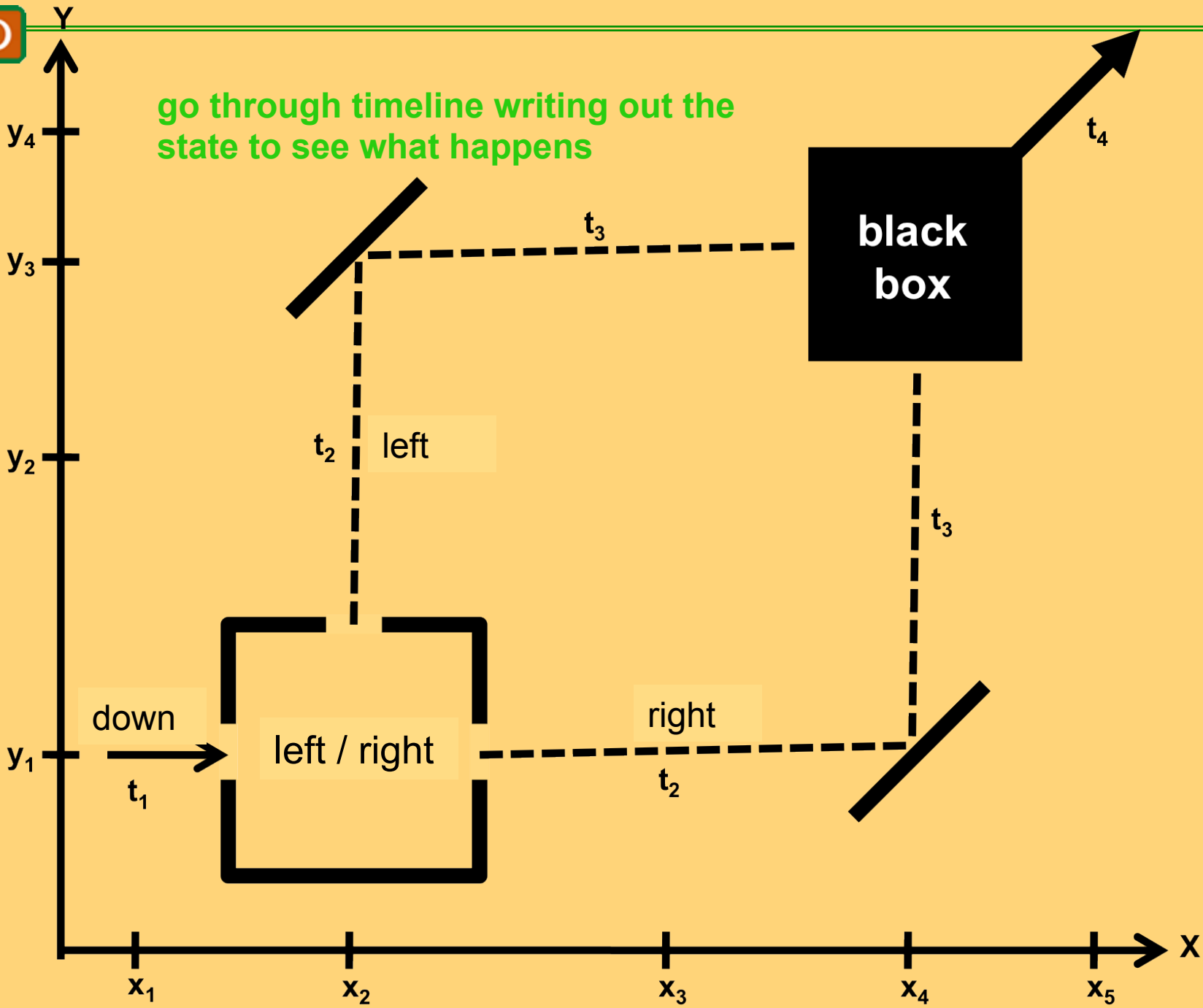
So what outcome can we expect of a left/right measurement?

Quantum mechanics must be a probabilistic theory !!

in Richard Feynman's words
(Lectures on Physics, Vol. III, Page 1-1)

We choose to examine a phenomenon which is impossible, *absolutely* impossible, to explain in any classical way, and which has in it the heart of quantum mechanics. In reality, it contains the *only* mystery. We cannot make the mystery go away by "explaining" how it works. We will just tell you how it works.

UT D



assign the Scientific American article “The Duality in Matter and Light” for reading, which among other things shows that the double-slit interference pattern emerges *even* if the photons are sent one at a time!

Quantum Cryptography: how to communicate without eavesdropping

(from S.J. Lomonaco, Jr., <http://www/csee.ubmc.edu/~lomonaco>)

Key idea: How to determine if Eve is listening to Alice and Bob's conversation?

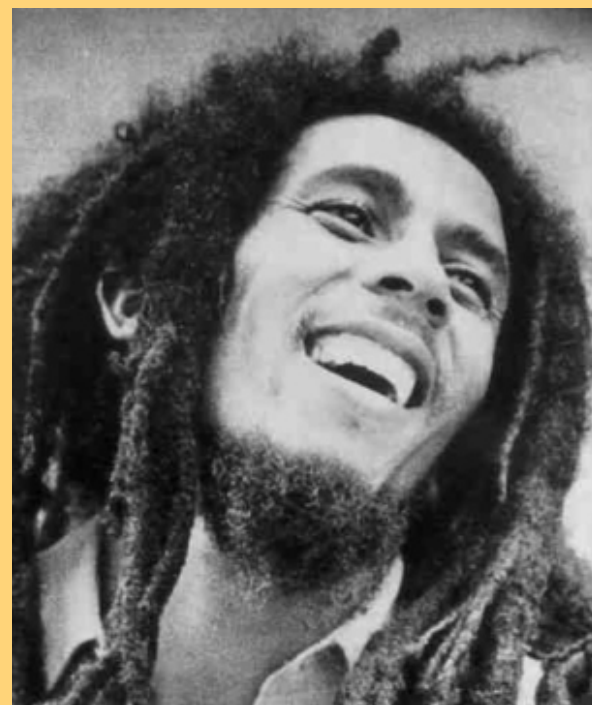
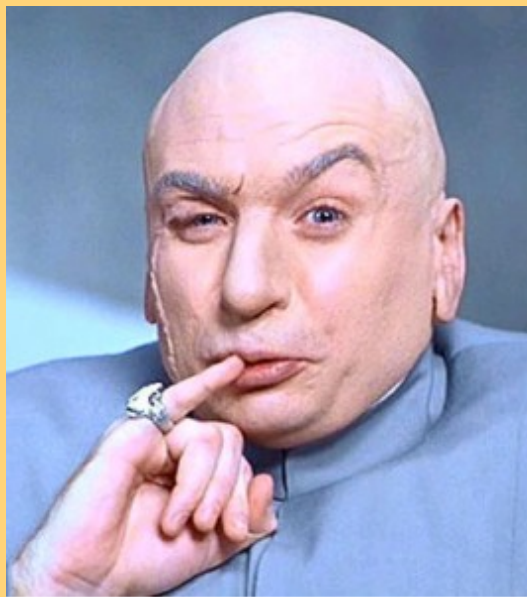
Quantum Cryptography: how to communicate without eavesdropping

(from S.J. Lomonaco, Jr., <http://www/csee.ubmc.edu/~lomonaco>)



Alice

Eve



Bob

Key idea: How to determine if Eve is listening to Alice and Bob's conversation?

The Dilemma

How do I prevent
Eve from
eavesdropping ???

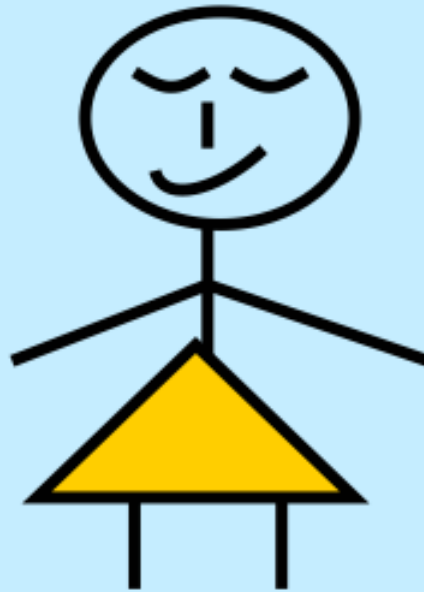
How can I
outwit Eve
???



Alice

Alice Takes a Quantum Mechanics Course

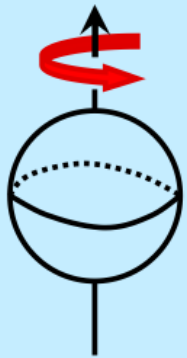
$$i\hbar \frac{\partial \psi}{\partial t} = \hat{H}\psi$$



Alice

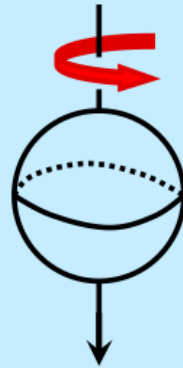
Introducing the Quantum Bit ... The Qubit

Example 1. A spin- $\frac{1}{2}$ particle



Spin Up

1



Spin Down

0

Example 2. The polarization state of a photon

Vertical
Polarization

Horizontal
Polarization

$$1 = |\updownarrow\rangle$$

$$0 = |\leftrightarrow\rangle$$

Can be both **0** & **1**
at the same time !

Alice Daydreams

How do I prevent
Eve from
eavesdropping ???

How can I
outwit Eve
???



Alice

Alice Has an Idea

But How ???

Idea: Couldn't I somehow
use Heisenberg's
Uncertainty Principle to
detect Eve's eavesdropping
???



Alice

Alice Invents the BB84 Quantum Crypto Protocol

BB84 = Bennett-Brasard 1984




Two Bases of 2-D Hilbert Space H

- The vertical and horizontal polarization states




This is our left/right value

form a basis of H which we will call the **vertical/horizontal (V/H) basis** 

- The slanted polarization states



This is our up/down value

also form a basis of H which we will call the **oblique basis** 

Quantum Channel Encoding Conventions





- For the **V/H** basis , Alice & Bob agree to communicate via the following **quantum alphabet**

$$\begin{cases} \text{"1"} = |\updownarrow\rangle \\ \text{"0"} = |\leftrightarrow\rangle \end{cases}$$

- For the **oblique** basis , Alice & Bob agree to communicate via the following **quantum alphabet**

$$\begin{cases} \text{"1"} = |\nearrow\rangle \\ \text{"0"} = |\searrow\rangle \end{cases}$$

Using Heisenberg's Uncertainty Principle

- Because of Heisenberg's uncertainty principle, Alice & Bob know that observations with respect to the  basis are incompatible with observations with respect to the  basis.
- So Alice communicates to Bob by randomly choosing between the two quantum alphabets  and .

The BB84 Protocol Step by Step

No Noise





















- Over the quantum channel, Alice sends her message to Bob, randomly choosing between the quantum alphabets
- Over the public channel, Bob communicates to Alice which quantum alphabets he used for each measurement.
- Over the public channel, Alice responds by telling Bob which of his measurements were made with the correct alphabet.
- Alice & Bob then delete all bits for which they used incompatible quantum alphabets to produce their resulting **RAW KEYS**.
- If Eve has not eavesdropped, their their two **RAW KEYS** will be the same.

The BB84 Protocol Step by Step (Cont.)

No Noise

- Over the public channel, Alice & Bob compare small portions of their **RAW KEYS**, and then delete the disclosed bits from their RAW Key to produce their **FINAL KEY**.
- If Alice & Bob find through their public disclosure that no errors were revealed, then they know Eve was not present, and now share a common **secret FINAL KEY**.

BB84: Eve Not Present (No Noise is Assumed)

Alice										
										
	1	0	0	1	1	0	0	1	0	1

W C W C C C C W C W

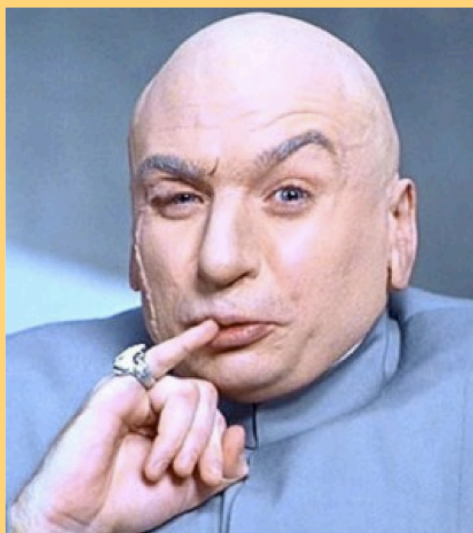
Bob										
	1	0	1	1	1	0	0	0	0	0

	0		1	1	0	0		0	
--	----------	--	----------	----------	----------	----------	--	----------	--

Raw Key

What Happens if Eve Listens In ?

Eve



BB84: Eve Is Present (No Noise is Assumed)

If Eve is eavesdropping, then she will create (because of Heisenberg's uncertainty principle) an **error rate** between Alice's & Bob's **RAW KEY**.

Thus, Alice and Bob can determine Eve's presence by publicly comparing a small portion of their respective **RAW KEYS**. If there are errors, they know Eve is present, discard their **RAW KEYS**, and start all over again. If there are no errors, they will then discard the publically disclosed portion. Then the undisclosed portion of their **RAW KEYS** agree, and is now an uncompromised secret **FINAL KEY** shared by Alice and Bob.

BB84: Eve Is Present (No Noise is Assumed)

Alice's Raw Key

- 0 - 1 1 0 0 - 0 -

Alice										
	↕	↘	↘	↗	↕	↘	↔	↗	↔	↗
	1	0	0	1	1	0	0	1	0	1

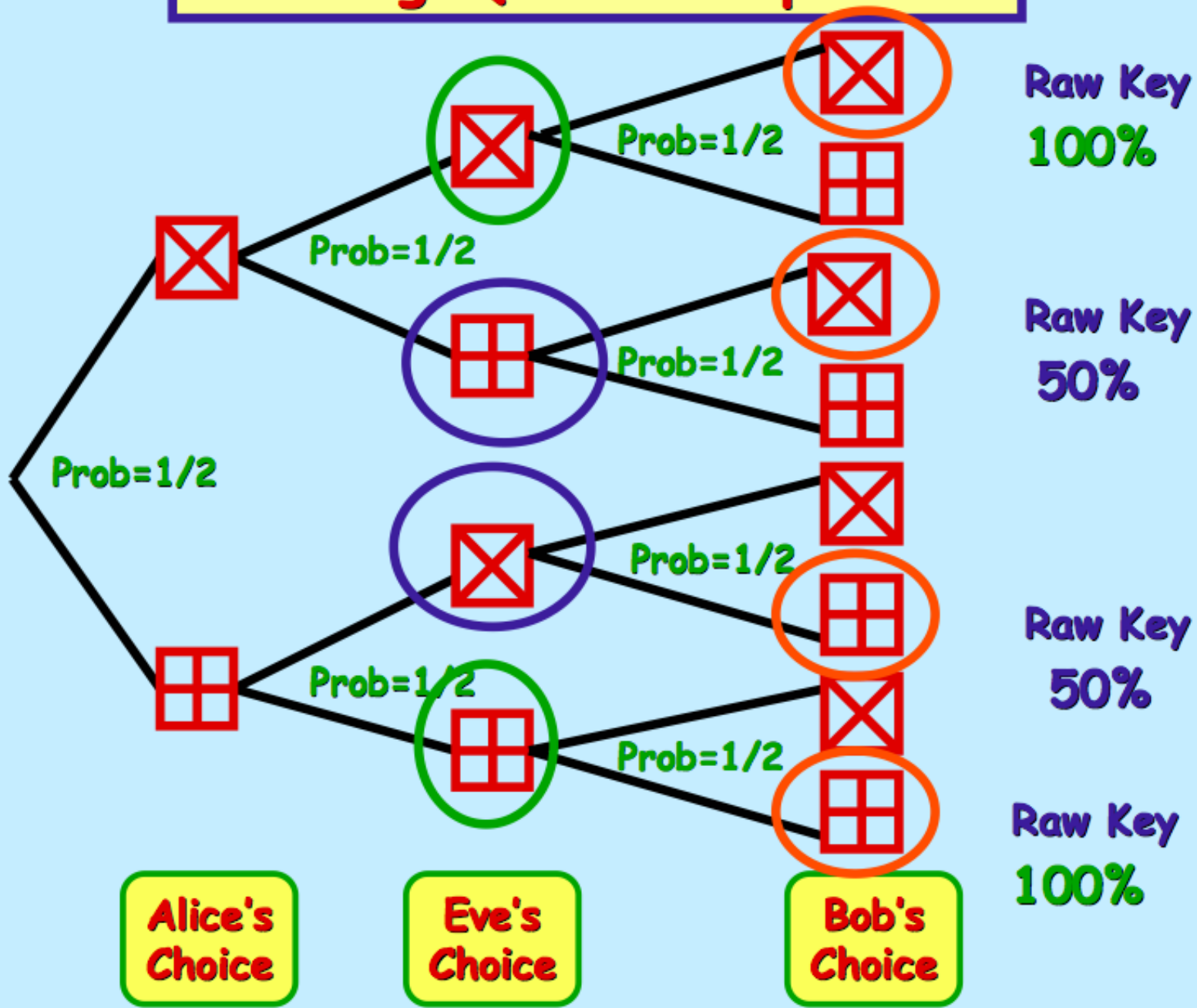
Eve										
	1	0	1	1	1	1	0	1	0	0

Bob										
	1	0	1	1	1	1	1	0	0	0

Bob's Raw Key

- 0 - 1 1 1 1 - 0 -

Choosing Quantum Alphabets



BB84: Eve Is Present (No Noise is Assumed)

Hence, if Eve eavesdrops, then Alice & Bob's Raw Keys disagree by 25%.

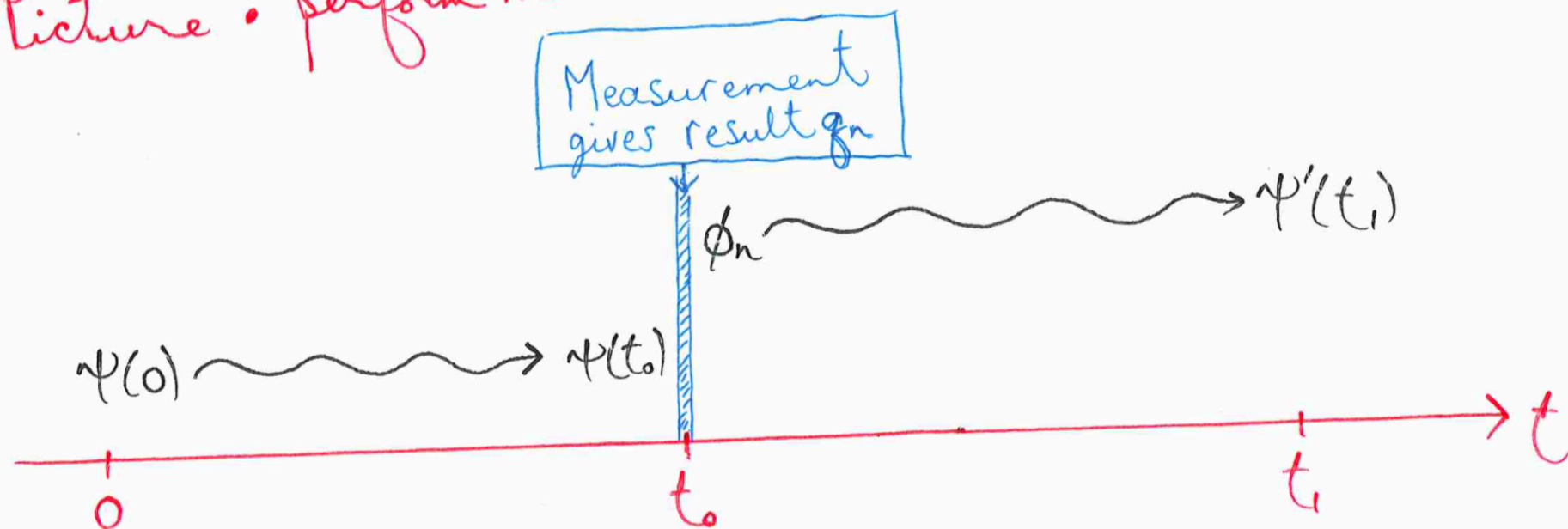
Quantum Computing

use quantum bits (qubits) to store information

use logic gates to manipulate the bits
(just like classical computing):

NOT, AND, NAND, OR, NOR, XOR, ...

- Picture: perform measurement at time t_0 .



wavefunction of the system undergoes an abrupt modification.

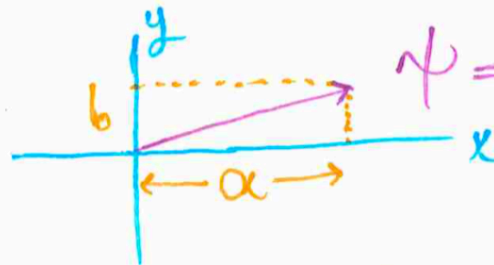
Collapse

1
+
2

- Perform a measurement of the physical quantity \hat{Q} on the system in state ψ .
- Say we obtain the result q_n .
- The state of the system is ~~is~~ now ϕ_n where $\hat{Q}\phi_n = q_n\phi_n$.

We learned that a "down" silver atom is in a superposition of being "left" and "right".

Let us express this using a mathematical formalism in which we express the wavefunctions as vectors in a 2d spin space.

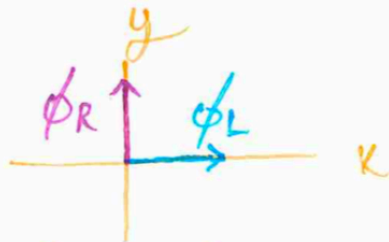

$$\psi = \alpha \hat{x} + b \hat{y} = \begin{bmatrix} \alpha \\ b \end{bmatrix}$$

Left/right operator = $\hat{L}R = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

This operator has 2 eigenvalues/eigenvectors.

Eigenvalue 1 ("left"), eigenvector $\phi_L = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

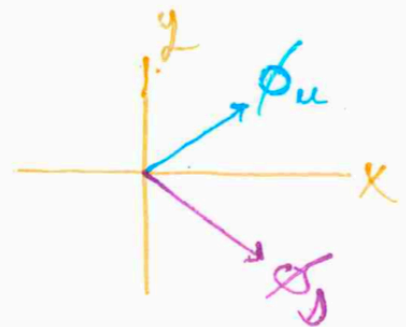
Eigenvalue -1 ("right"), eigenvector $\phi_R = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$



Up/down operator = $\hat{U}D = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Eigenvalue 1 ("up"), eigenvector $\phi_U = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$

Eigenvalue -1 ("down"), eigenvector $\phi_D = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$



Superposition is expressed as :

$$\phi_u = \frac{1}{\sqrt{2}} \phi_L + \frac{1}{2} \phi_R$$

$$\phi_L = \frac{1}{\sqrt{2}} \phi_u + \frac{1}{\sqrt{2}} \phi_D$$

$$\phi_D = \frac{1}{\sqrt{2}} \phi_L - \frac{1}{\sqrt{2}} \phi_R$$

$$\phi_R = \frac{1}{\sqrt{2}} \phi_u - \frac{1}{\sqrt{2}} \phi_D$$

Heisenberg and Von Neumann Interpretation

A physical system's observable properties always have definite values between measurement, but we can never know what those values are since the values can only be determined by measurement, which indeterministically disturbs the system.

This implies that the system was in a definite state before measurement, and that the quantum mechanical formalism gives an incomplete description of physical systems.

Bohr Interpretation (The Copenhagen Interpretation)

(the received view among physicists) (the orthodox interpretation)

It does not make sense to attribute definite values to a physical system's observable properties except relative to a particular kind of measurement procedure, and then it only makes sense when that measurement is actually being performed.

Famously, Bohr proposed an interpretation that denies that the description given by the quantum mechanical formalism is incomplete.

On Bohr's view, the world is divided into two realms of existence, that of quantum systems, which behave according to the formalism of quantum mechanics and do not have definite observable values outside the context of measurement, and of "classical" measuring devices, which always have definite values but are not described within quantum mechanics itself. The line between the two realms is arbitrary.

There are several difficulties with this view, which together constitute the **"measurement problem"**.

To begin with, the orthodox interpretation gives no principled reason why physics should not be able to give a complete description of the measurement process. Indeed, the orthodox interpretation claims that whether a certain physical interaction is a "measurement" is arbitrary, *i.e.*, a matter of choice on the part of the theorist modeling the interaction.

Schrödinger's Cat

Schrödinger pointed out that the orthodox interpretation allows for inconsistent descriptions of the state of macroscopic systems, depending on whether we consider them measuring devices.

Put a cat in an enclosed box along with a device that will release poisonous gas if (and only if) a Geiger counter measures that a certain radium atom has decayed.

The radium atom is in a superposition of decaying and not decaying, and hence the Geiger counter and the cat should also be in a superposition (cat = dead + alive) if we do *not* consider the cat to be a measuring device.

On the other hand, if we consider the cat to be a measuring device, then according to the orthodox interpretation, the cat will either be definitely alive or definitely dead.

When does collapse occur?

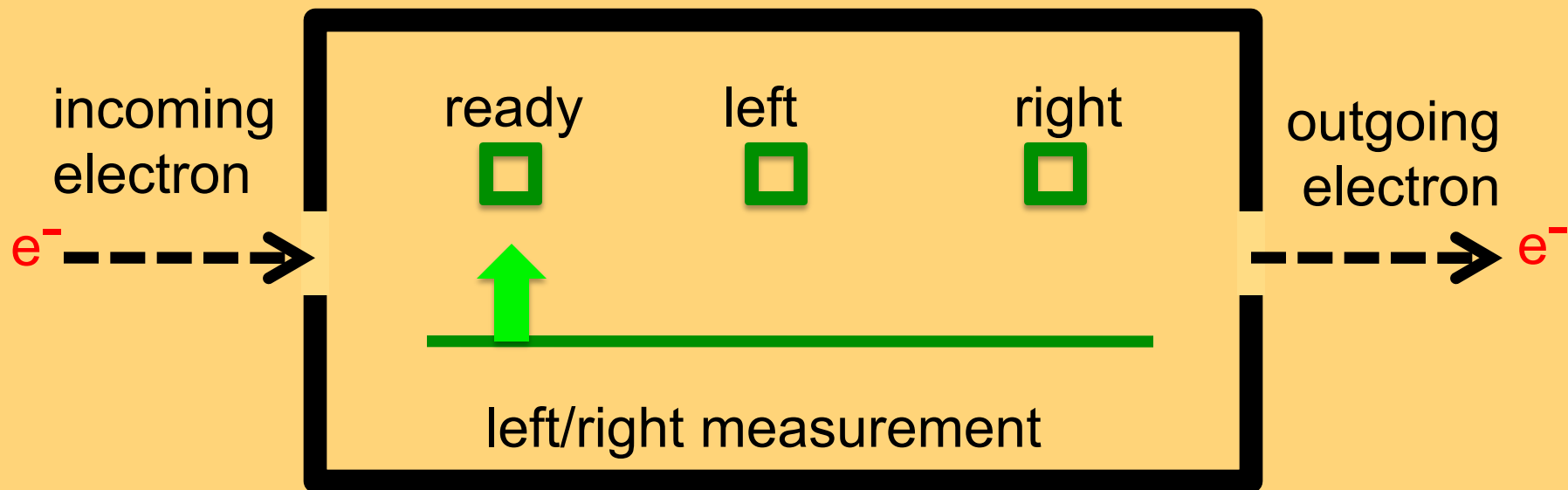
Suppose that Alice has a theory about collapse:

collapse happens immediately after the electron exits the measurement box.

And suppose that Bob has another theory about collapse:

collapse happens later, for example when a human retina or optic nerve or brain gets involved.

Can we decide who is right empirically, that is, by performing some experiment?



Can we decide who is right empirically, that is, by performing some experiment?

Here's how to start: Feed a up electron into a left/right device and give it enough time to pass through. If Alice is right, the state of the system is now

either $left^m \phi_l^e$ (with 50% prob.)
or $right^m \phi_r^e$ (with 50% prob.)

whereas if Bob is right, the state of the system is currently

$$\frac{1}{\sqrt{2}} left^m \phi_l^e + \frac{1}{\sqrt{2}} right^m \phi_r^e$$

so all we need to do is to figure out a way to distinguish, by means of a measurement, these two cases: In one case the pointer points in a particular (but as yet unknown) direction, and in the other case the pointer *isn't* pointing in any particular direction *at all*.

What if we measure the position of the tip of the pointer? That is, let's measure where the pointer is pointing. **This won't work.**

If Alice is right, of course we will find a 50/50 chance of finding the pointer “pointing-at-left” vs. “pointing-at-right”. This is because, according to Alice, the pointer is already in one of those two states.

But if Bob is right, then a measurement of the position of the tip of the pointer will have a 50% change of *collapsing* the wavefunction of the pointer onto the “pointing-at-left” state, and 50% change of collapsing it to “pointing-at-right”.

Therefore the probability of any given outcome of a measurement of the position of the pointer will be the *same* for both these theories; and so this isn't the sort of measurement we are looking for.

What if we measure the up/down property of the atom?
This won't work.

What if we measure the left/right property of the atom?
This won't work.

These arguments establish that different conjectures about precisely where and precisely when collapse occurs cannot be empirically distinguished from one another.

And so the best we can do at present is to try to think of precisely where and precisely when collapses might *possibly* occur (that is, without contradicting what we *do* know to be true by experiment). But it turns out to be hard to do even that.