

*[qubit-ulm.com]*

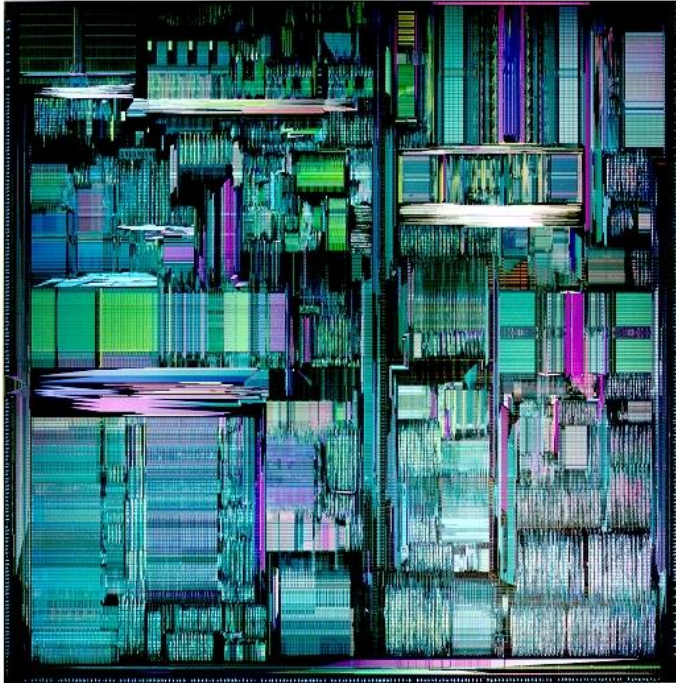
# Introduction to **Quantum Information**

letná škola FMFI UK  
Svit, 9/2014

Daniel Nagaj

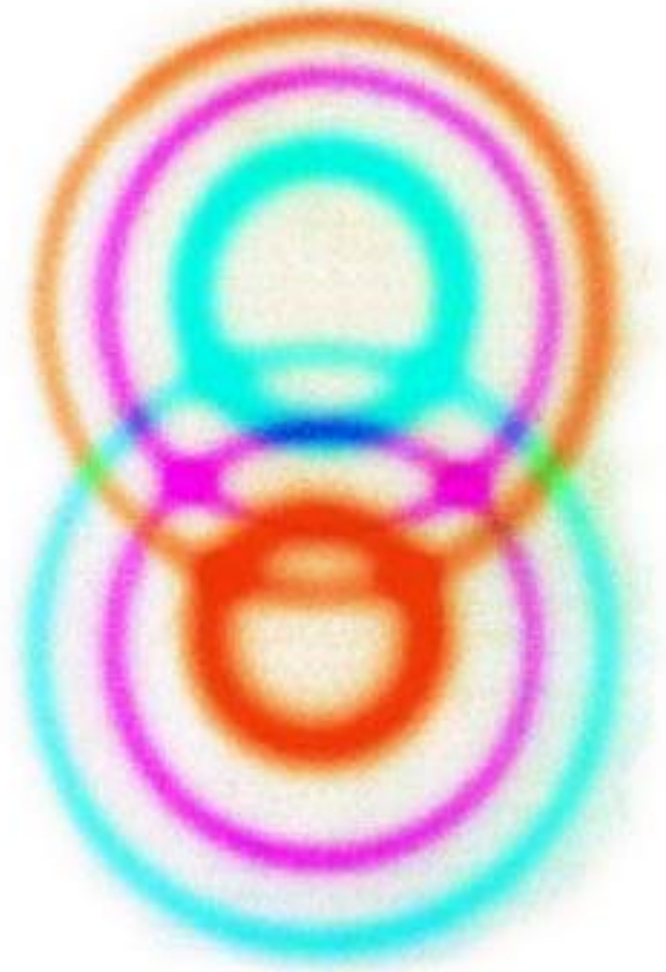






[1995 Pentium Pro, [www.tayloredge.com/museum](http://www.tayloredge.com/museum)]

What kinds of things  
does nature allow  
us to compute?



What kinds of things  
would nature allow  
us to compute  
if we could utilize  
the power of  
quantum mechanics?

*[qubit-ulm.com]*

“

Because nature is not classical, dammit, and if you want to make a simulation of nature – you’d better make it quantum mechanical!

”

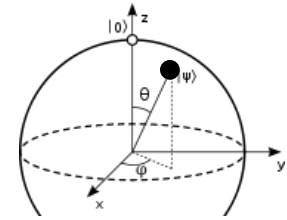
R. P. Feynman



1

# we need a qubit

what can we do with it?



2

# EPR pairs

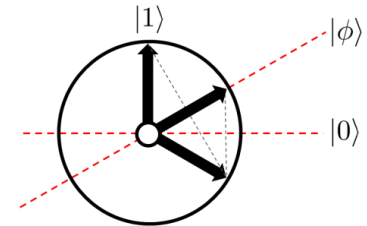
tricky 2-qubit protocols



3

# the algorithms

making quantum computing tick



4

# error correction

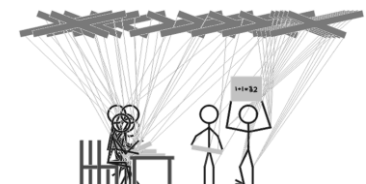
can we really scale up this stuff?



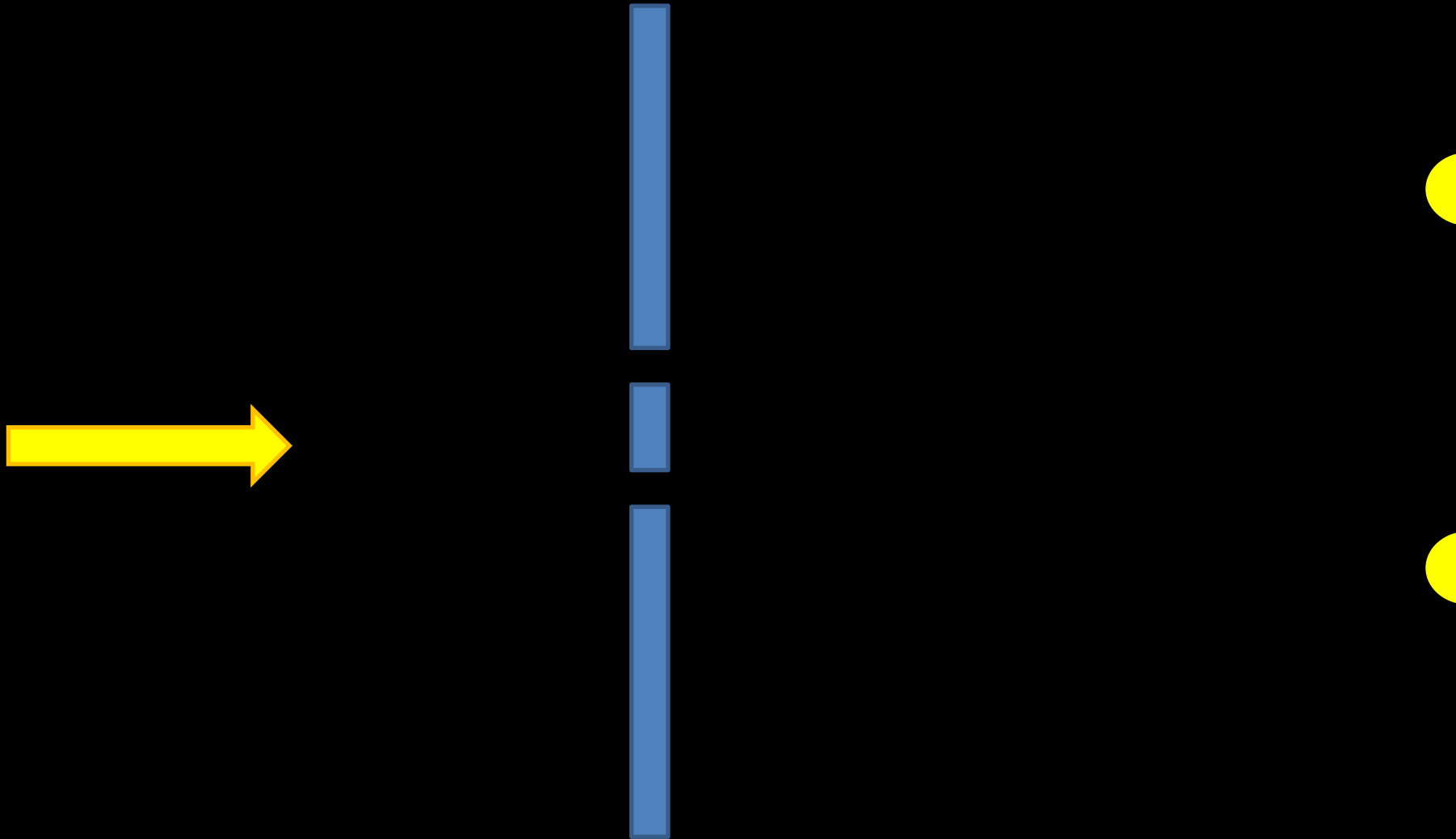
5

# the limits

complexity & limits of q. computing



two slits and light



two slits and a laser

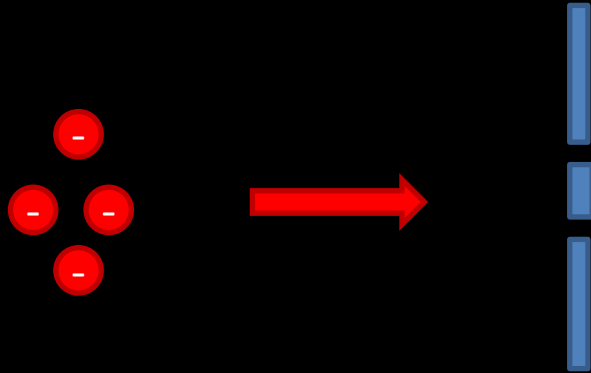
coherent  
light

interference  
superposition



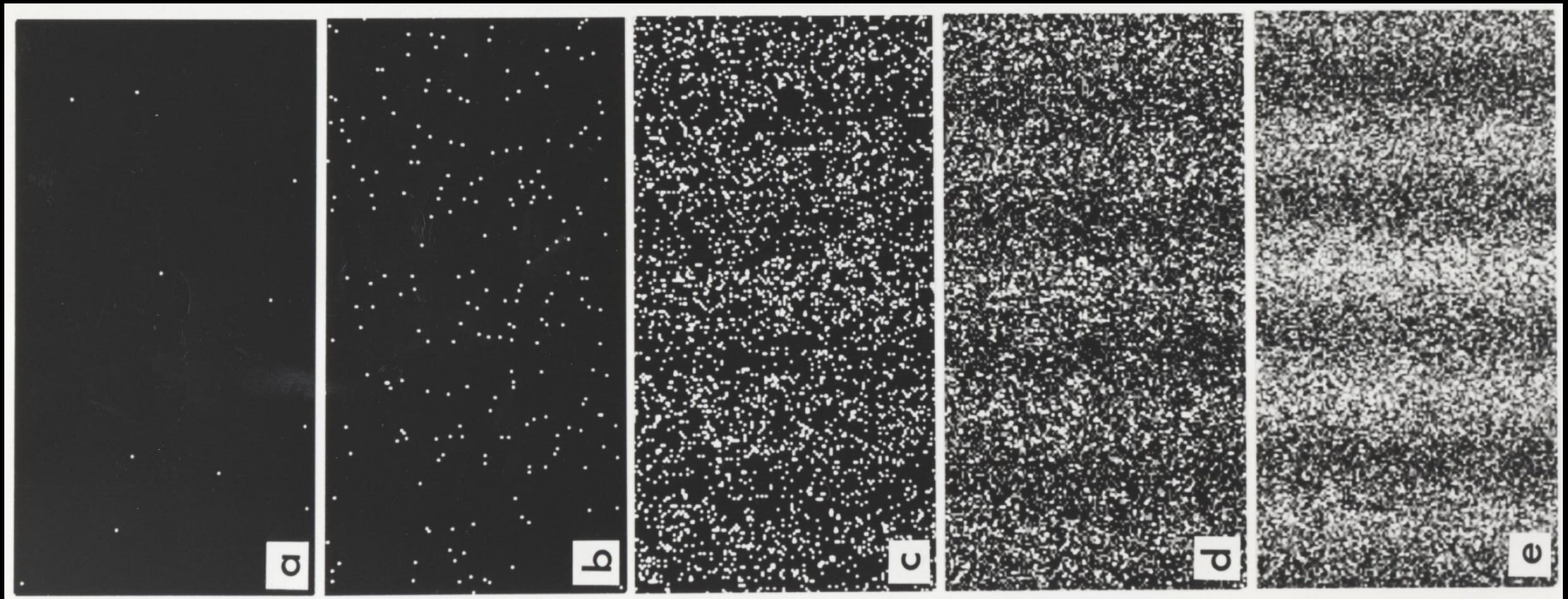
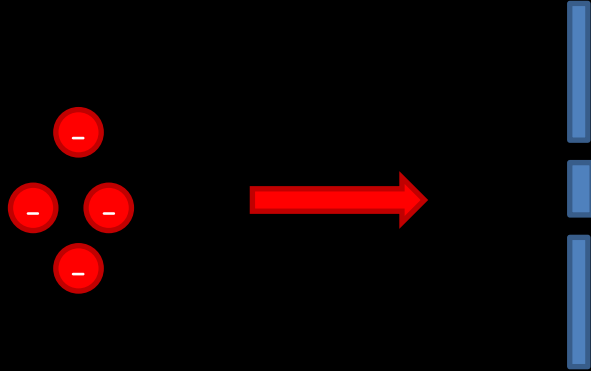


# two slits and electrons



# two slits and electrons

interference  
superposition

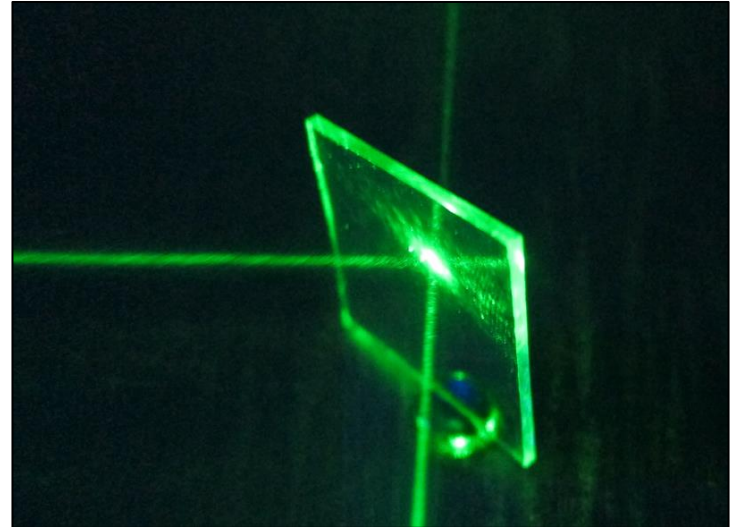
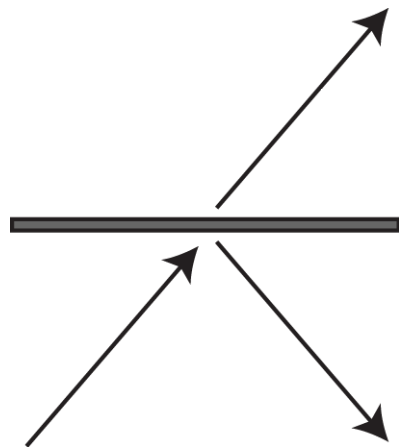
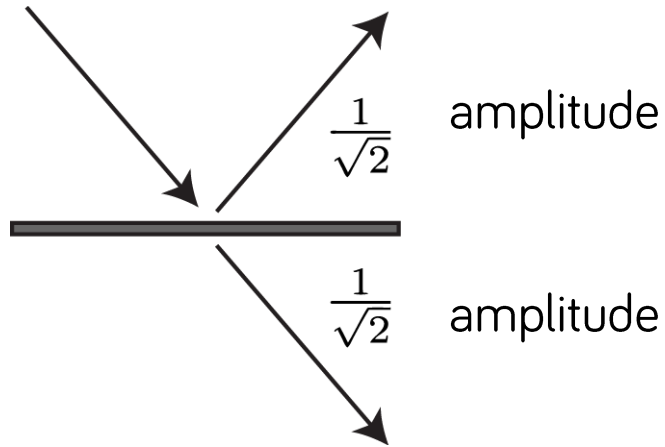


**SCHRÖDINGER'S CAT IS  
A DEADIE**

# 1

## Beamsplitters and superpositions

A single photon & a beamsplitter.



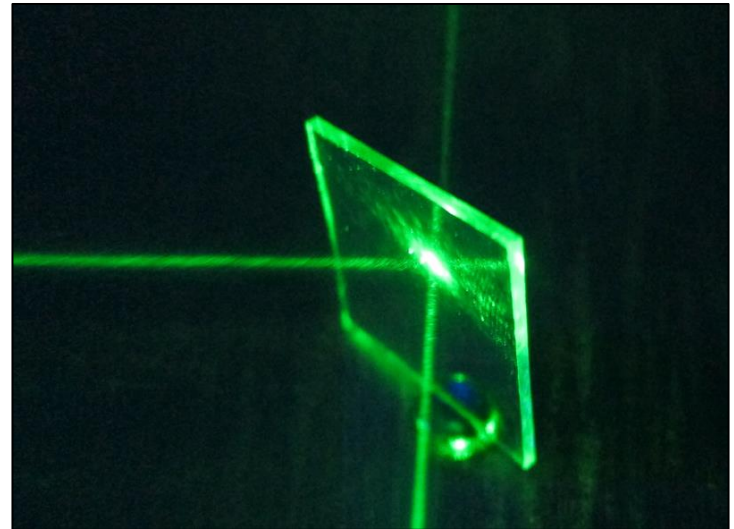
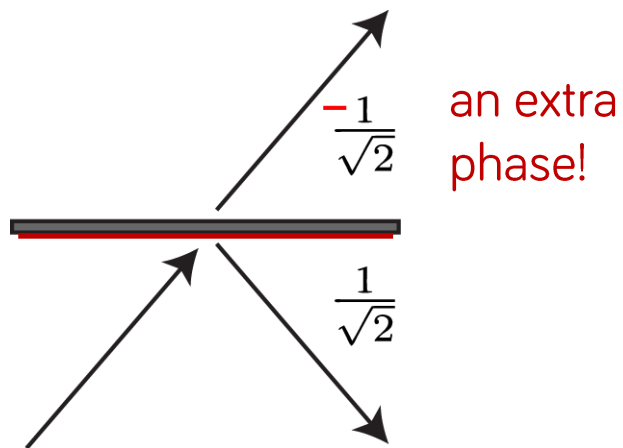
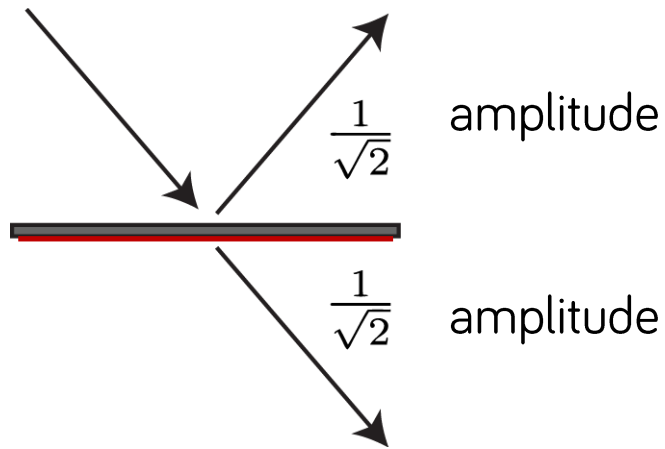
[wikipedia.org]



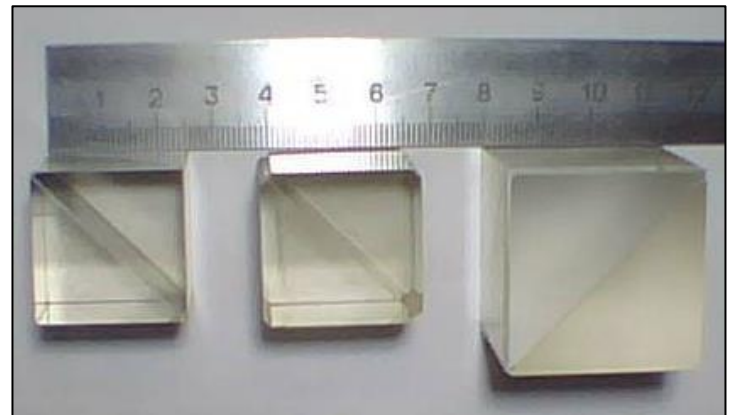
# 1

## Beamsplitters and superpositions

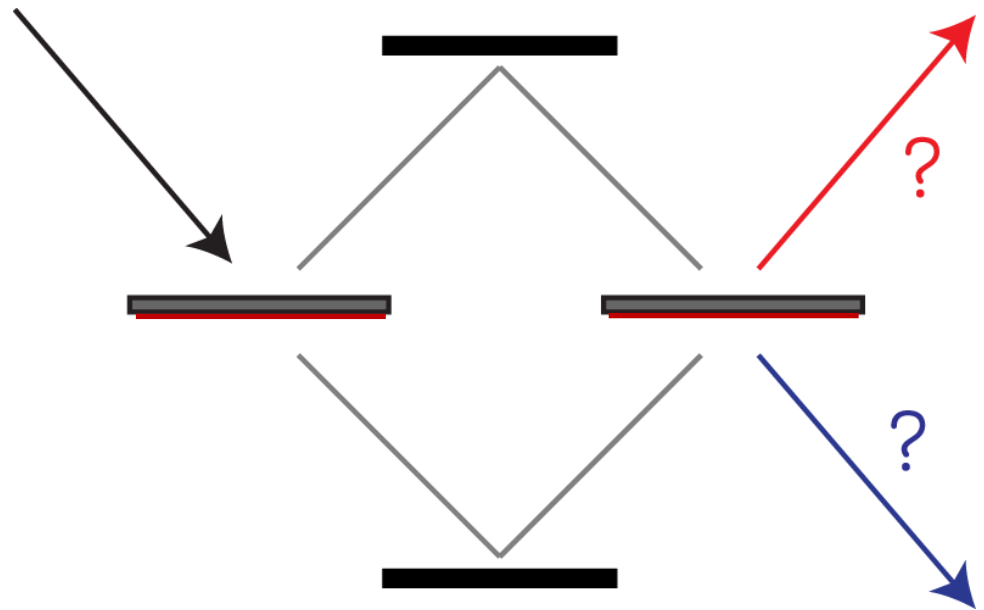
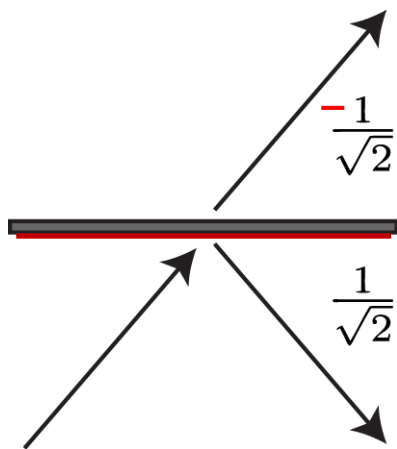
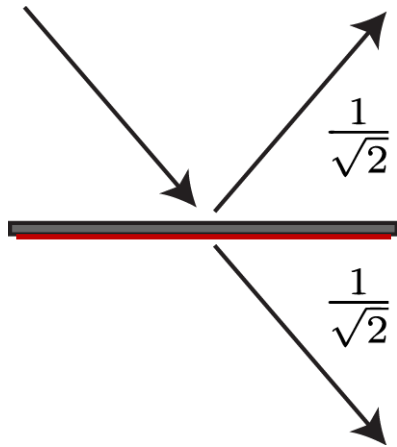
A single photon & a beamsplitter.



[wikipedia.org]



# 1 Beamsplitters and superpositions of light waves



no filter



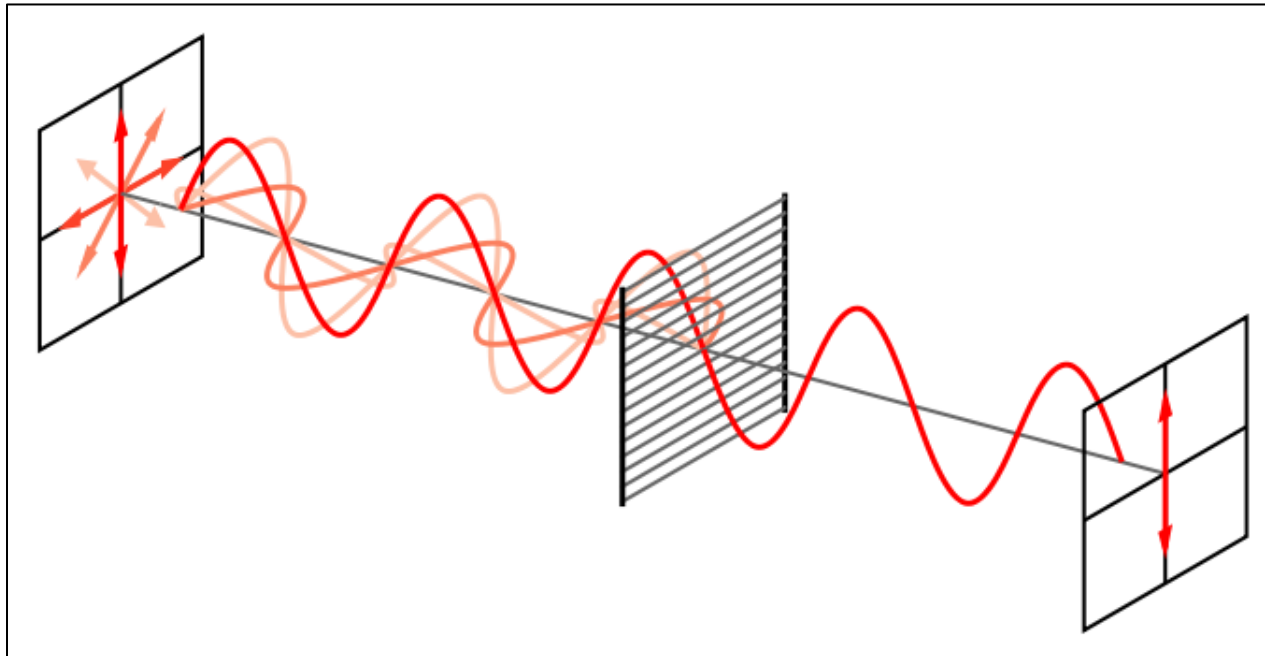
with a filter





# 1 Polarizing filters: looking through sunglasses

nonpolarized light: E in all directions

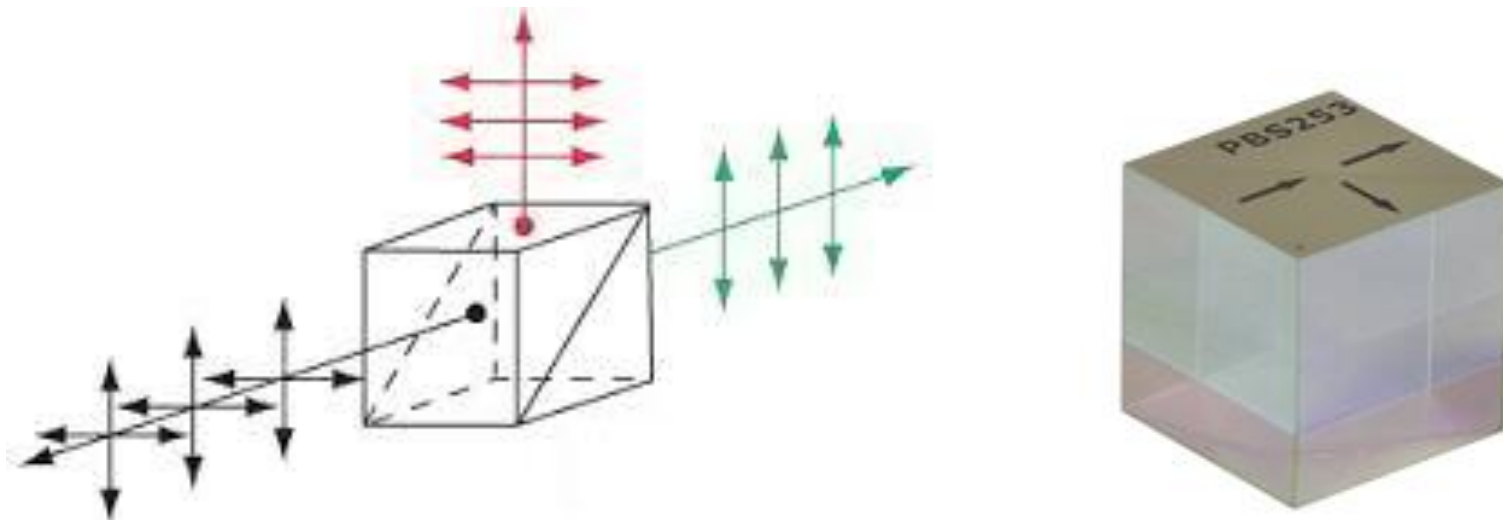


linear polarizer: let only one direction of E through

- a half-destructive measurement: pass/or not

# 1 Another option: polarizing beamsplitters

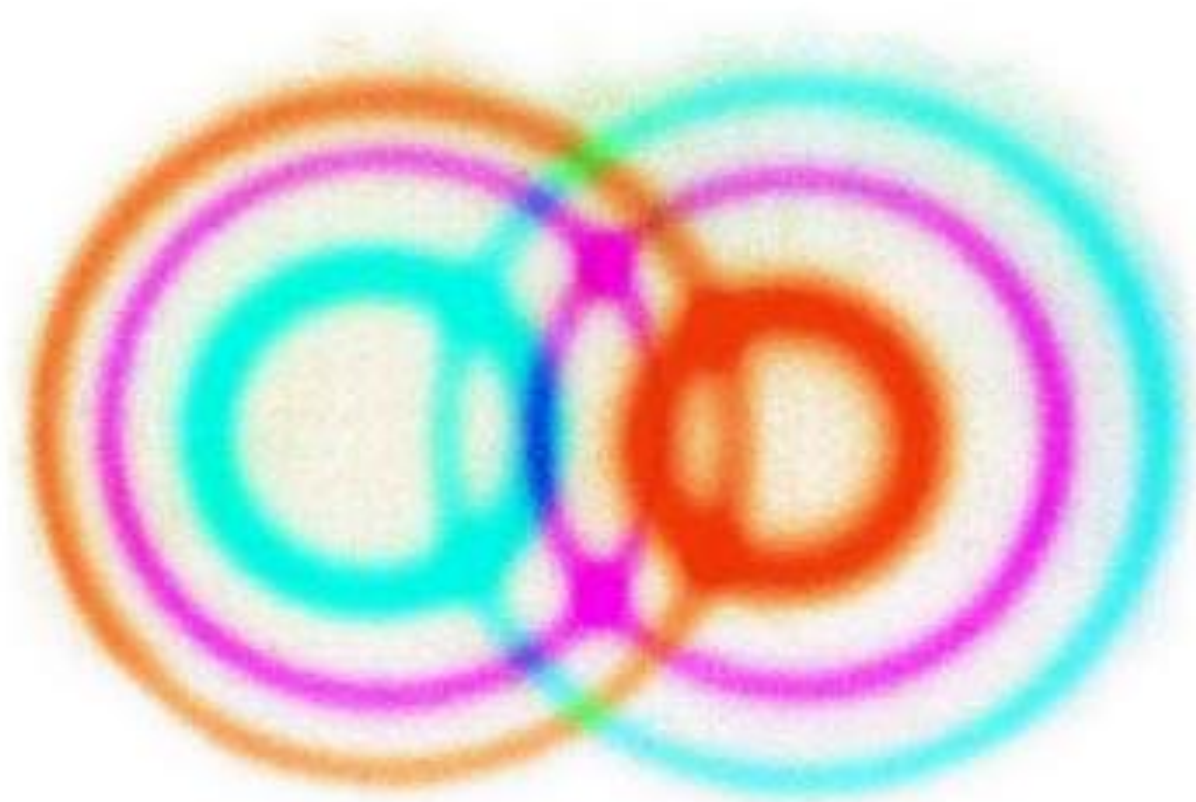
Horizontally polarized light goes one way, vertically polarized the other way.



- What if we rotate the basis?

# 1 Using a vector description (superpositions).

More than 0's and 1's.



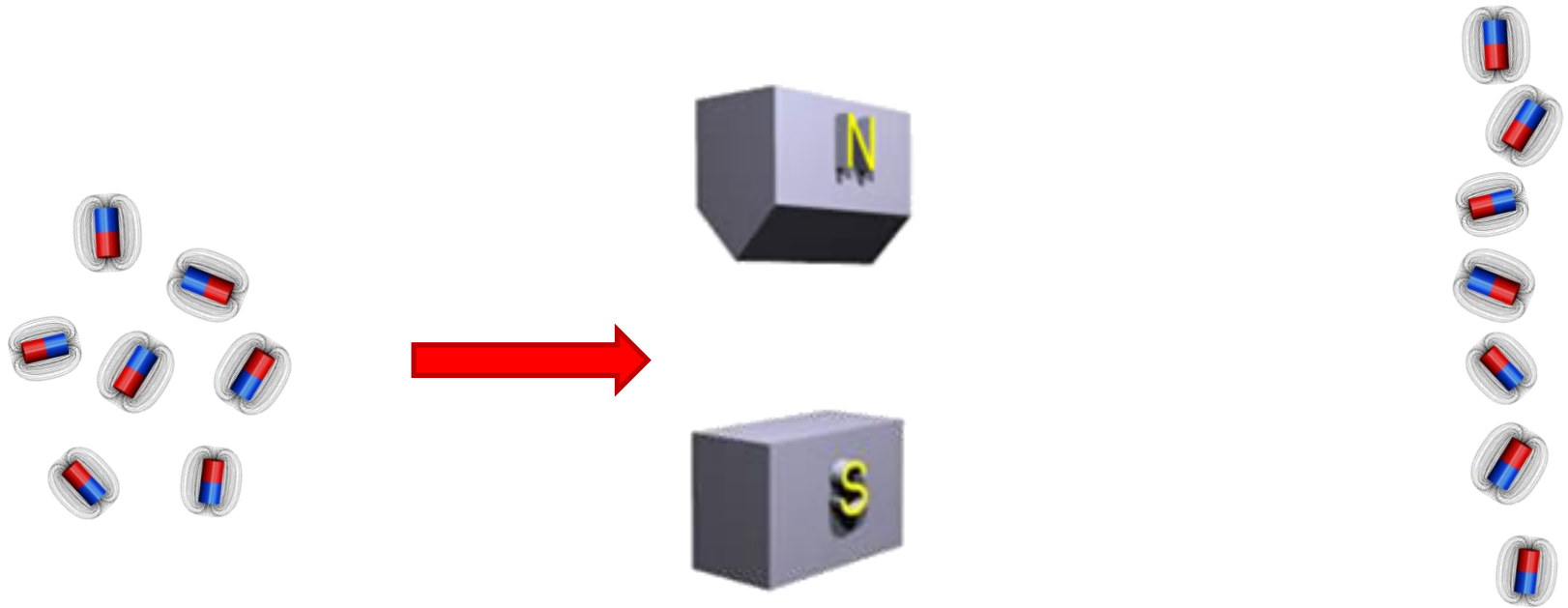
*[qubit-ulm.com]*

# 1 Do electrons contain small magnets?

Discovering the electron's spin.

inhomogeneous mag. field & magnets

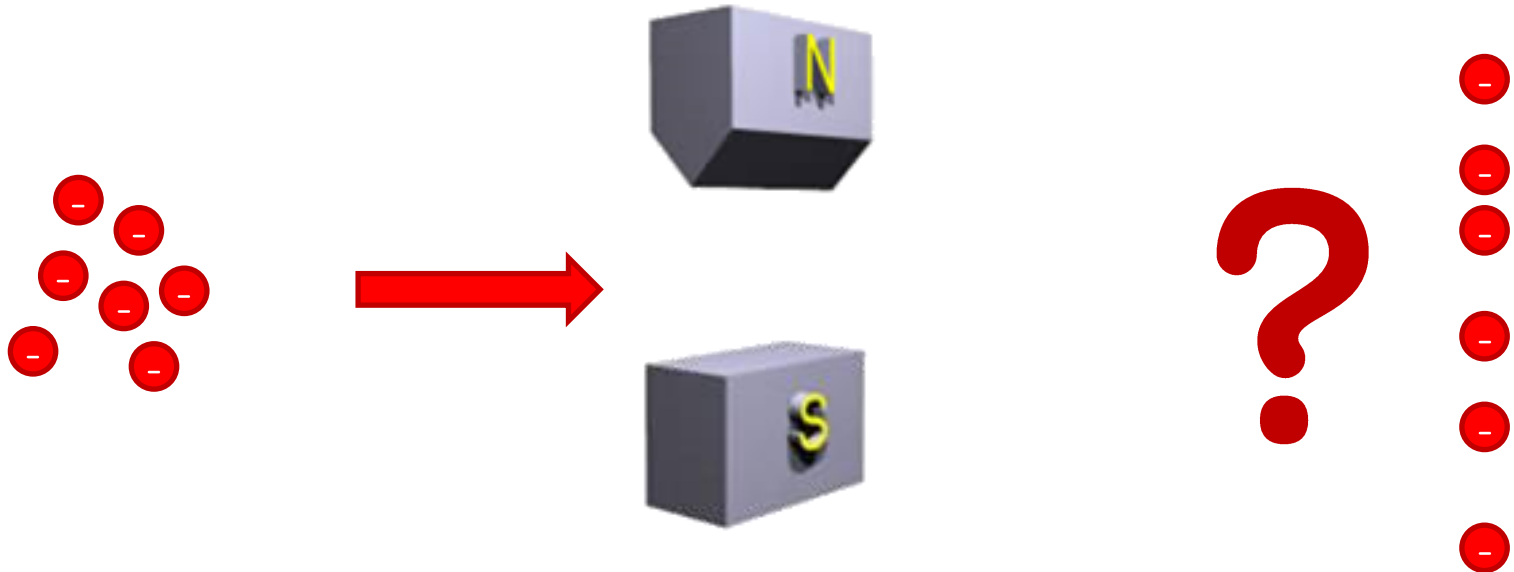
we can expect a continuous distribution



# 1 Do electrons contain small magnets?

Discovering the electron's spin.

inhomogeneous mag. field & electrons  
the Stern-Gerlach experiment (1922)

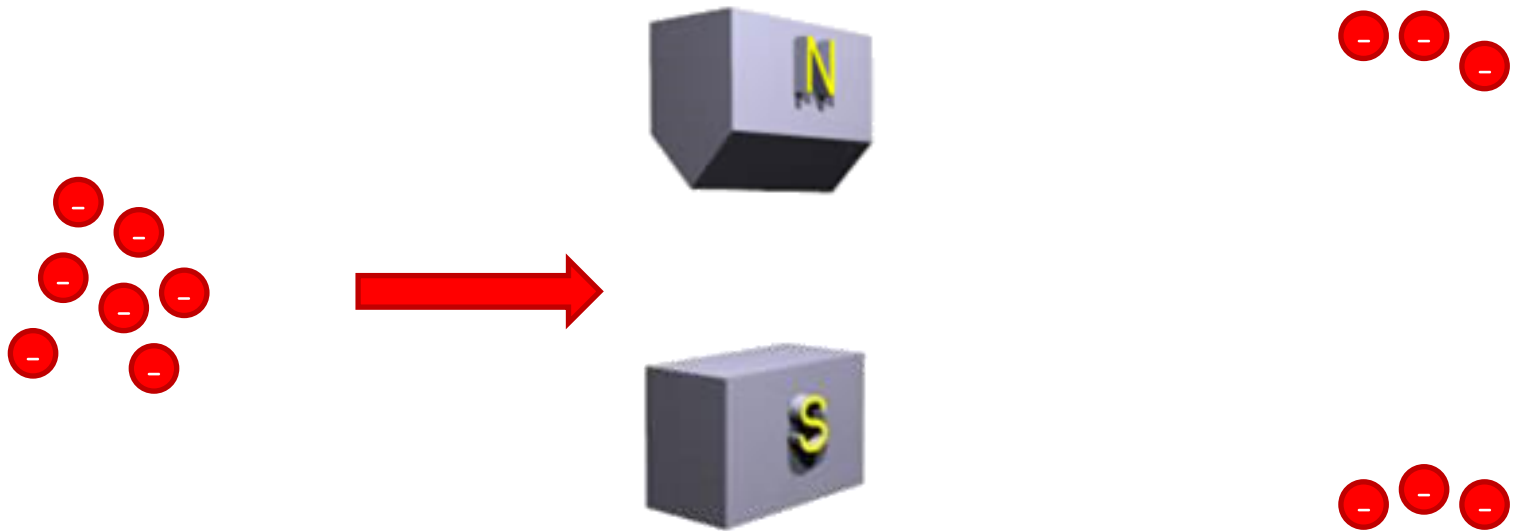


# 1 Do electrons contain small magnets?

Discovering the electron's spin.

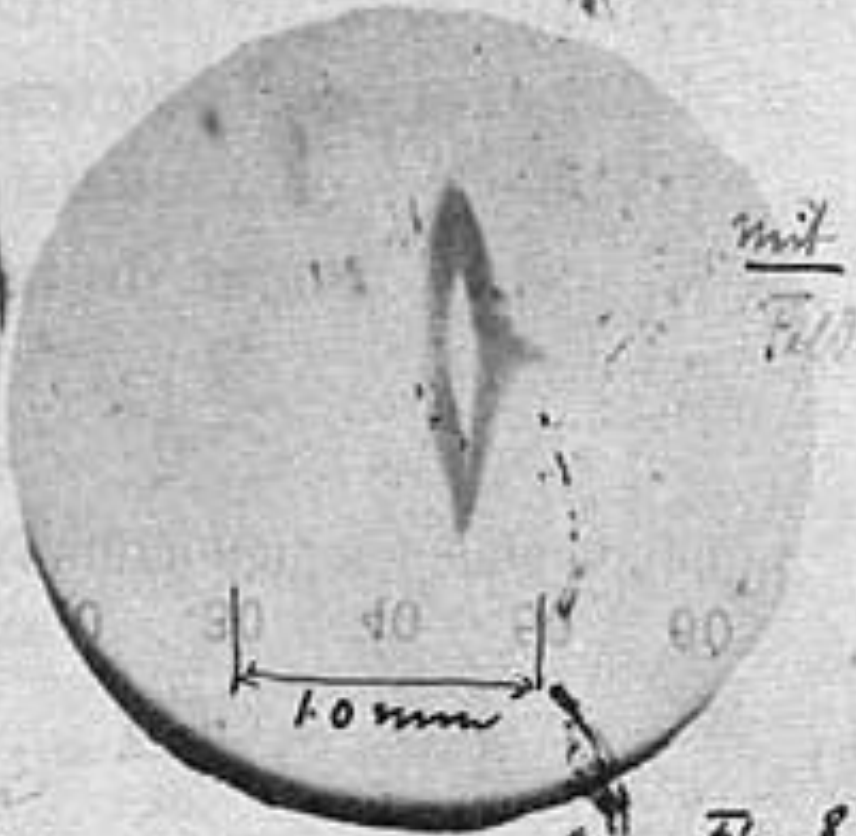
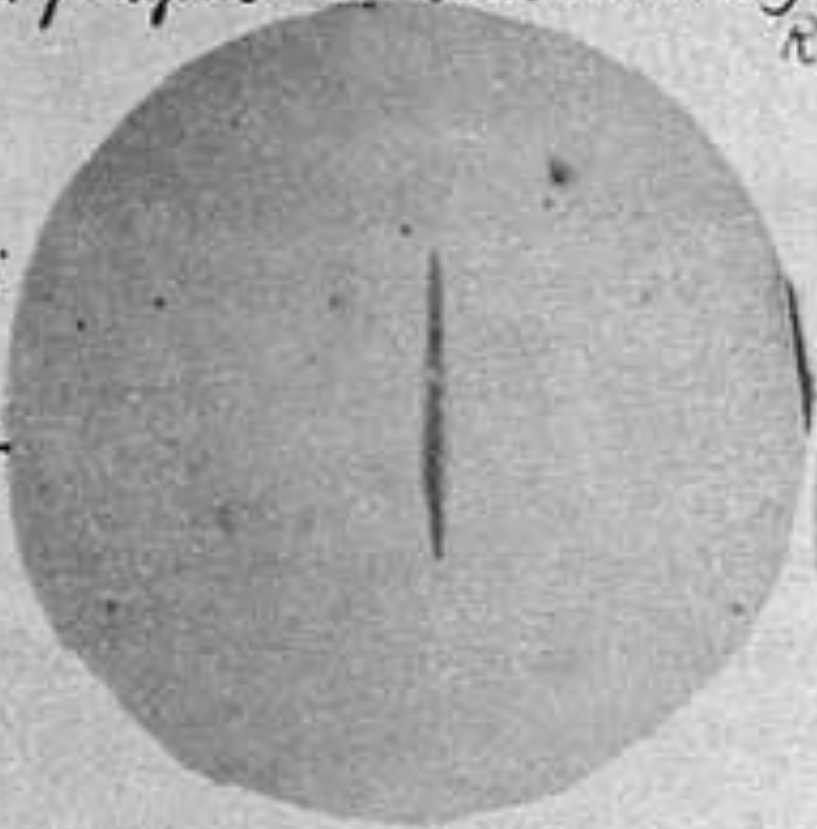
## inhomogeneous mag. field & electrons

the Stern-Gerlach experiment (1922): the actual behavior



Da verbleiben nur Bohr, auch die Fortsetzung meiner Arbeit (siehe  
 Zeitungs-f. Physik VIII. Seite 110. 1921.): Zu experimentelle Nachweis  
 Richtungsquantelung

Silber.  
ohne  
 Magnet-  
 Feld



Wir gratulieren zur Bestätigung Ihrer  
 Theorie! Mit hochachtungsvoller Grüsse  
 Ihr ergebener  
 Walter Gerlach

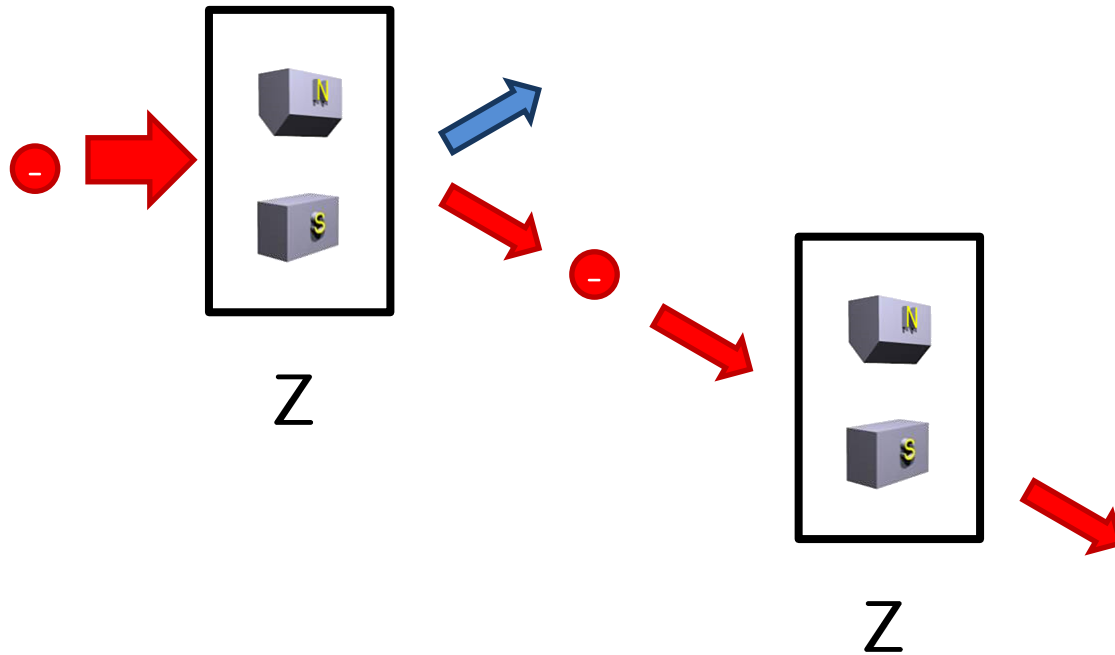
Ffm.  $\frac{8}{2}$ . 22.

Gerlach's postcard to Bohr

[Niels Bohr Archive, Copenhagen]

# 1 Electrons and their spin

Predetermined measurement results?

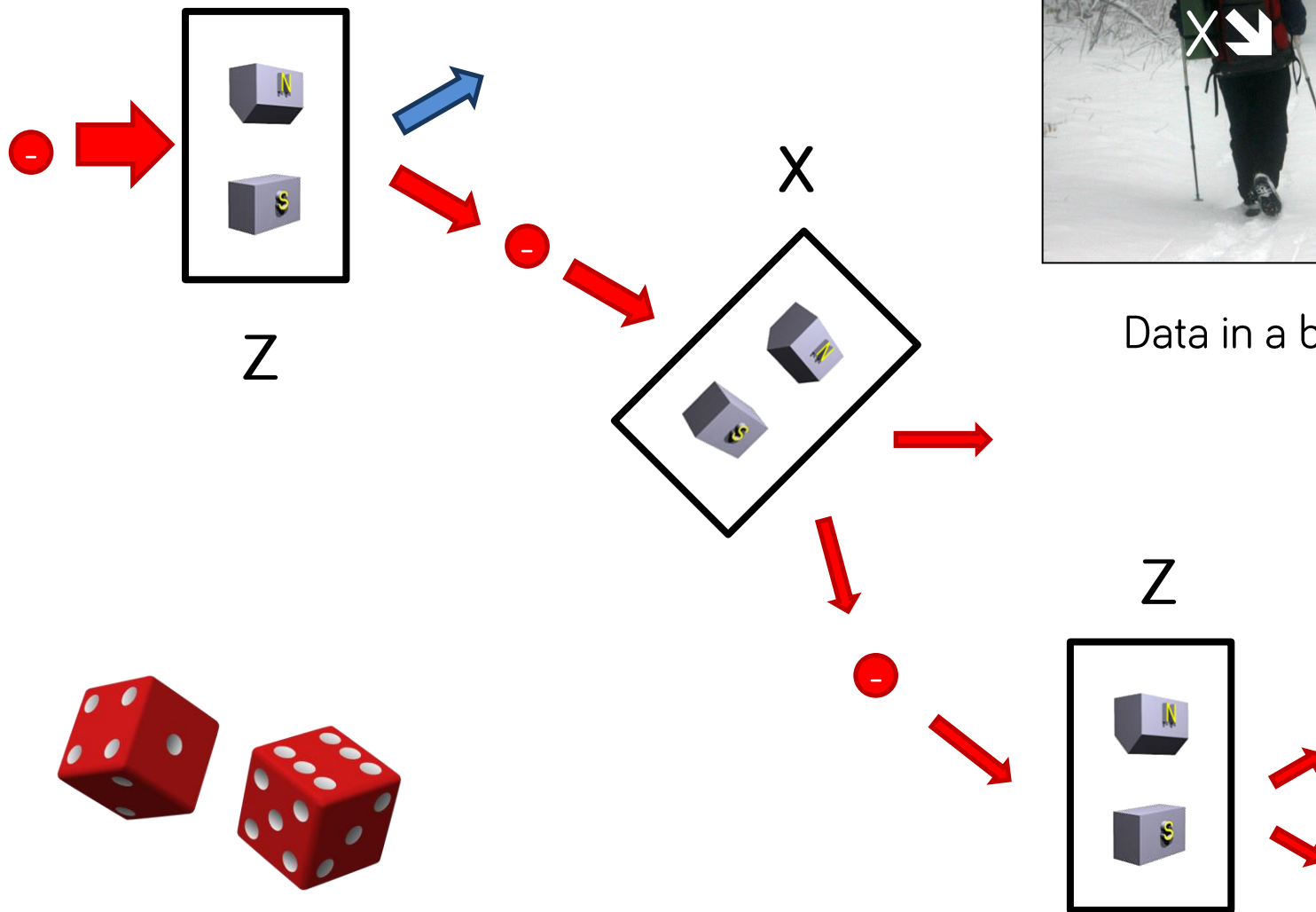


- eigenstates repeated measurements of the same type don't change the results anymore



# 1 Electrons and their spin

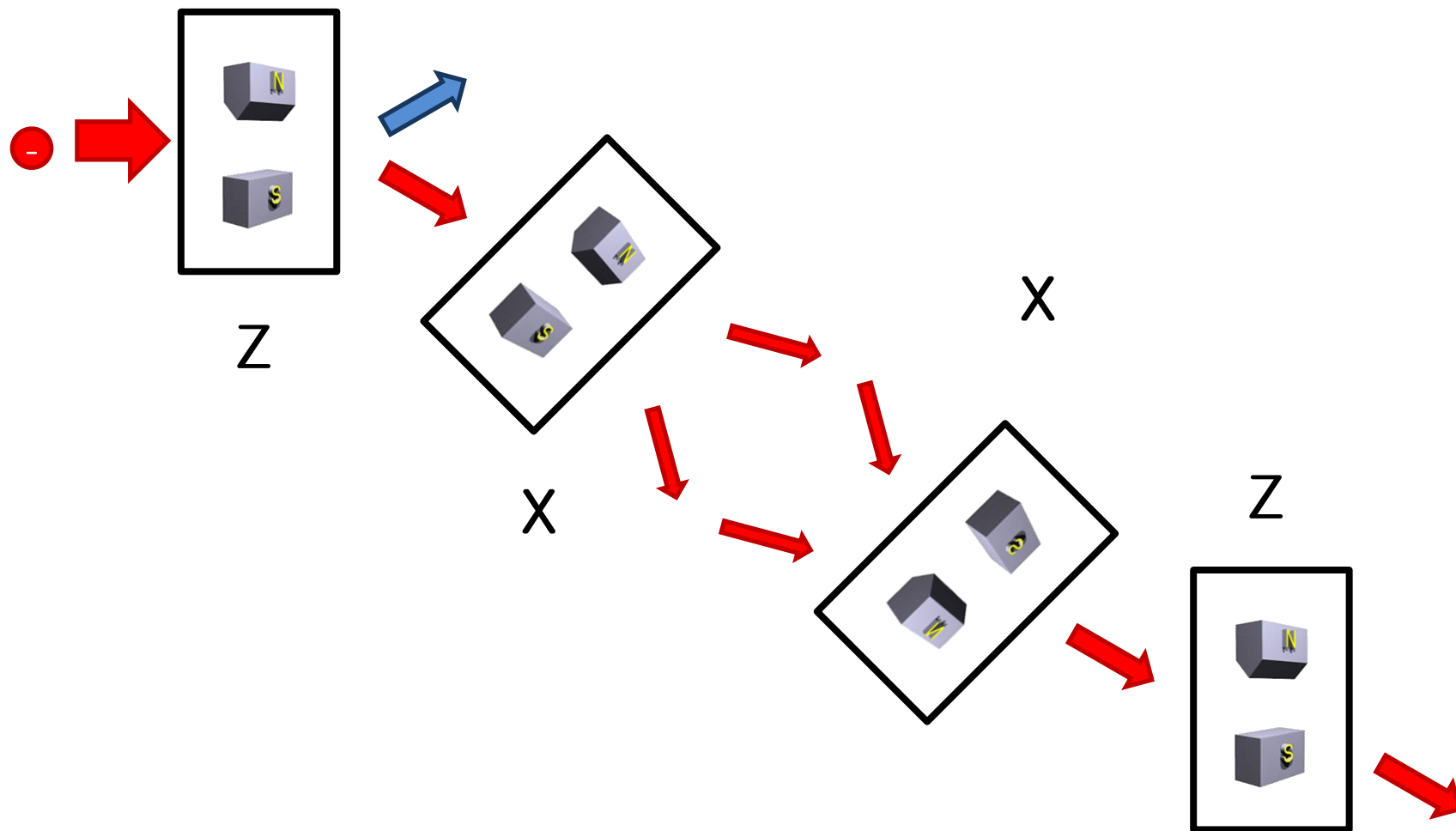
Predetermined measurement results?



Data in a backpack?

# 1 Electrons and their spin

Predetermined measurement results?



2

## The playground of QM

0 1 bits

$|0\rangle$   $|1\rangle$  qubits

$|+\rangle$   $|-\rangle$  superpositions

polarized photons

(electron) spins

ground/excited atomic states

superconducting circuits

quantum dots

MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT

MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT

MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT

MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT  
MEASUREMENT

SHUT UP

& CALCULATE

## 2 The (finite-dim) quantum-mechanical playground

The state of a single qubit.

**a bit** 0 or 1

**a qubit** a (normalized, complex) vector  
in a 2D Hilbert space

$$|\psi\rangle = a|\uparrow\rangle + b|\downarrow\rangle$$

- How many parameters?

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{matrix} |a|^2 + |b|^2 = 1 \\ \left[ \begin{array}{c} a \\ b \end{array} \right] \end{matrix}$$



## 2 A qubit: the Bloch sphere

A two-angle parametrization.

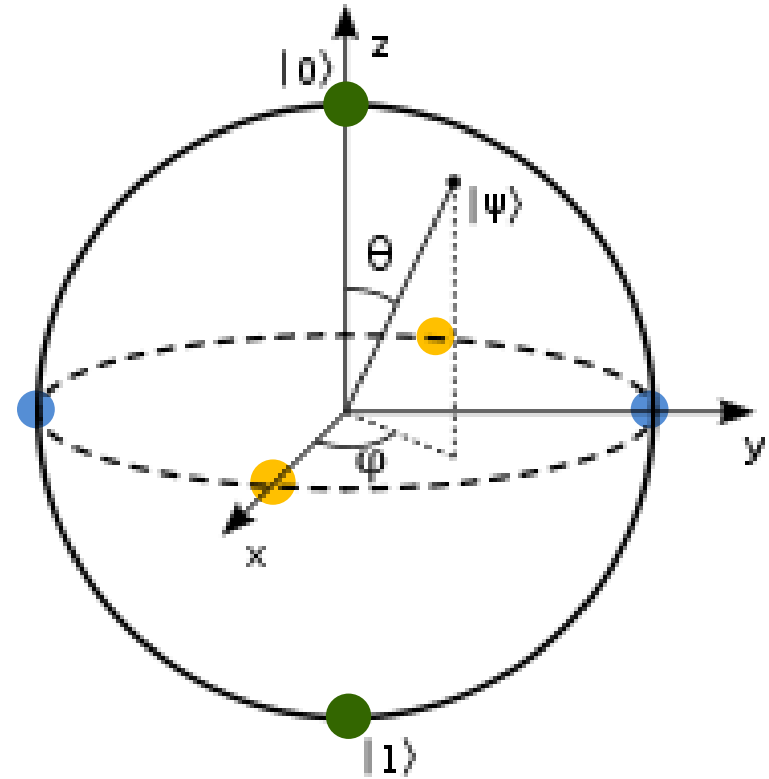
- $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

- $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

- $|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

- $|-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$

- Why are the basis states opposite in the picture?



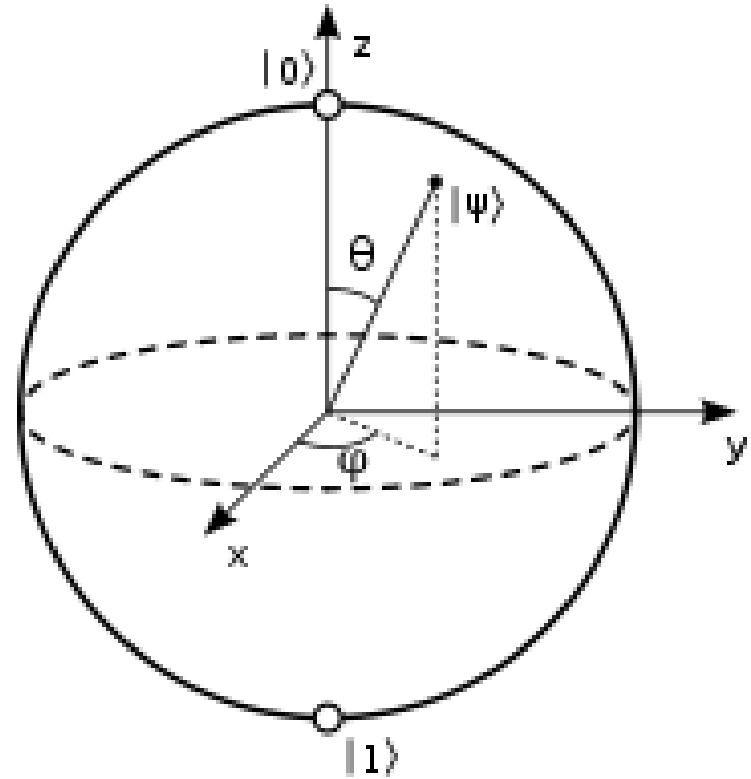
$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \quad |a|^2 + |b|^2 = 1$$

## 2 A qubit: the Bloch sphere

A two-angle parametrization.

- How much information can we store in a qubit?
- How can we distinguish the states of a qubit?



Does an overall phase matter?

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

- **unitary transformations**
- **projective measurements**

## 2 The Dirac bra-c-ket notation for states

Pure states of a qubit, overlaps and probabilities.

**a “ket”** a vector of amplitudes

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

**the Z-basis**

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

**probability  
of finding “0”**

$$p_0 = |a|^2$$

- Which state has a 50% probability to be up or down?  $\begin{bmatrix} \phantom{a} \\ \phantom{b} \end{bmatrix}$
- How about 25%?

## 2 The Dirac bra-c-ket notation for states

Pure states of a qubit, overlaps and probabilities.

**a “ket”** a vector of amplitudes

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

**the Z-basis**

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

**probability  
of finding “ $\phi$ ”**

calculate the overlap of the states

$$p_\phi = |\langle\phi|\psi\rangle|^2$$

**a “bra”**  $\langle\phi| = [|\phi\rangle]^\dagger = [c^* \ d^*]$

eats a ket, spits out a number

## 2 The Dirac bra-c-ket notation for states

Pure states of a qubit, overlaps and probabilities.

**a “ket”** a vector of amplitudes

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

**the Z-basis**

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

**probability  
of finding “ $\phi$ ”**

calculate the overlap of the states

$$p_\phi = |\langle\phi|\psi\rangle|^2$$

**a “bra”**  $\langle\phi| = [|\phi\rangle]^\dagger = [c^* \ d^*]$

$$\langle\psi|\psi\rangle = 1$$

## 2 The players and rules of QM

States, operators, measurements and evolution.

**state** a vector of amplitudes

**operator** a Hermitian matrix  
what we observe  
real eigenvalues

spin-Z  
magnetization  
energy  
correlation

$$\bar{A} = \langle \psi | A | \psi \rangle$$

Schrödinger equation

$$i \frac{\partial}{\partial t} |\psi\rangle = H |\psi\rangle$$

the Hamiltonian

$H$

$$U(t) = e^{-iHt}$$

generates  
unitary evolution

## 2 The players and rules of QM

States, operators, measurements and evolution.

**state** a vector of amplitudes

**operator** a Hermitian matrix  
what we observe  
real eigenvalues

$$\bar{A} = \langle \psi | A | \psi \rangle$$

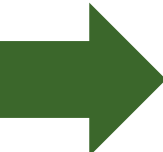
spin-Z  
magnetization  
energy  
correlation

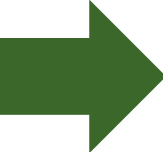
**transformation** a unitary matrix  
something we can do  
a reversible operation


$$|\psi'\rangle = U|\psi\rangle$$

a rotation  
a “gate”  
a conditional  
operation

## 2 What do you know about the Pauli operators?


$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$


$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$


$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Hermiticity? Unitarity? Trace?

Eigenvalues? Eigenvectors?

Multiplication rules?

Commutation rules?

Exponentiation?

How do they act on

the others' eigenvectors?

How can we exchange

between the X and Z bases?

$$e^{-i\varphi Z}$$

$$e^{-i\varphi X}$$

$$\vec{\sigma} = (X, Y, Z)$$

$$e^{-i\varphi(\hat{r} \cdot \vec{\sigma})}$$



### 3 A spin in a magnetic field.

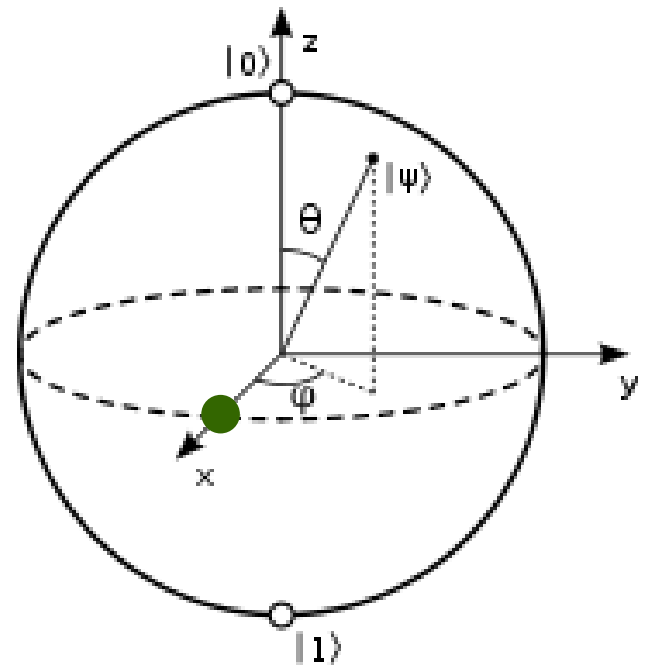
- A magnetic field in the Z-direction.

$$H = -\mu \vec{\sigma} \cdot \vec{B} = -cZ = -c \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

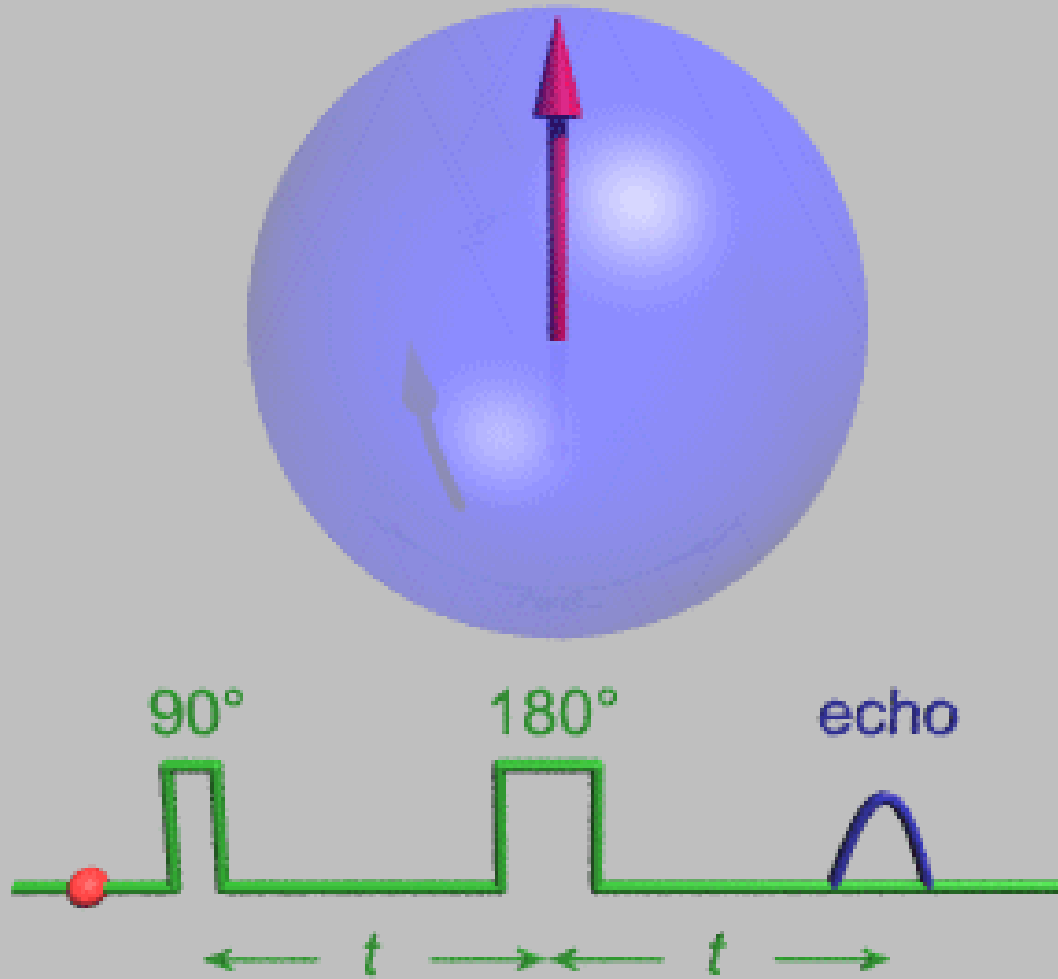
- Our initial state: spin in the x-direction.

$$|x+\rangle = |+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

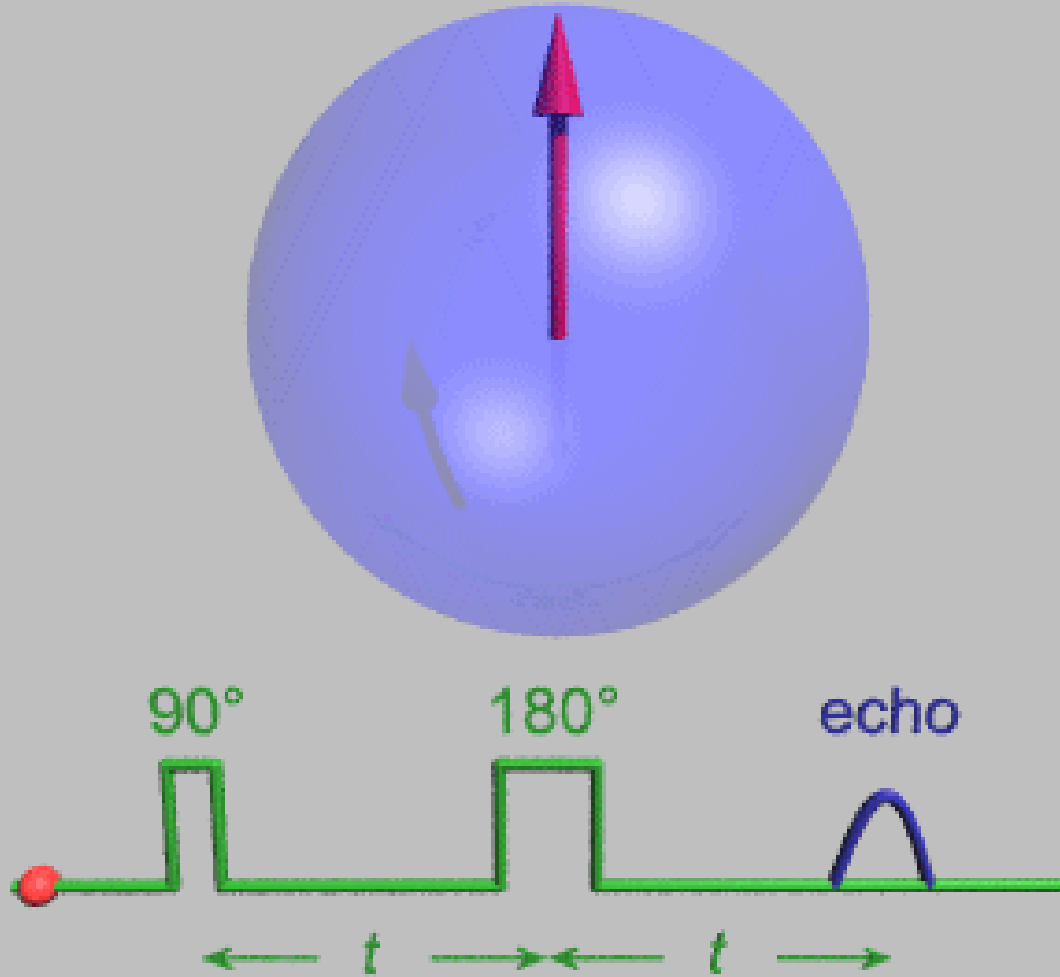
- What will happen and why?



### 3 Spin echo.



### 3 Spin echo.



## 4 Detecting a bomb without detonating it [Elitzur-Vaidman].

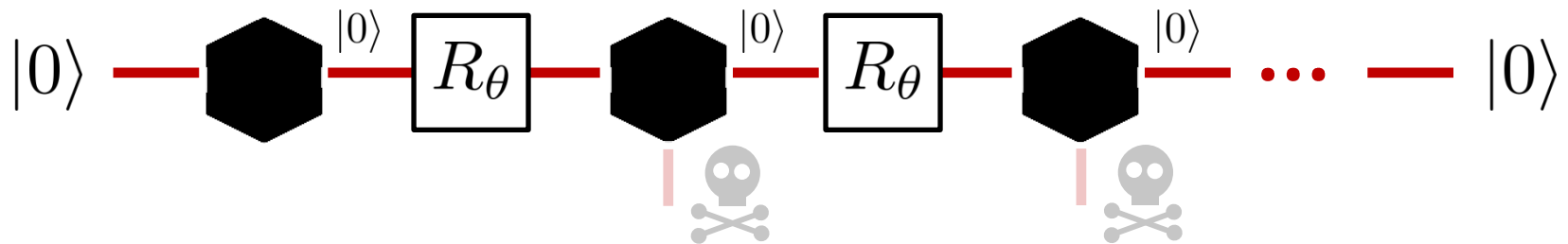
- A bomb explodes we decide to look at it.
- If we could use a qubit as our “control”...

$|0\rangle$  don't look

$|1\rangle$  let's test our luck



Rotate the qubit a little and test again...



- What if there was no bomb?



OH ALICE... YOU'RE THE ONE FOR ME

BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE

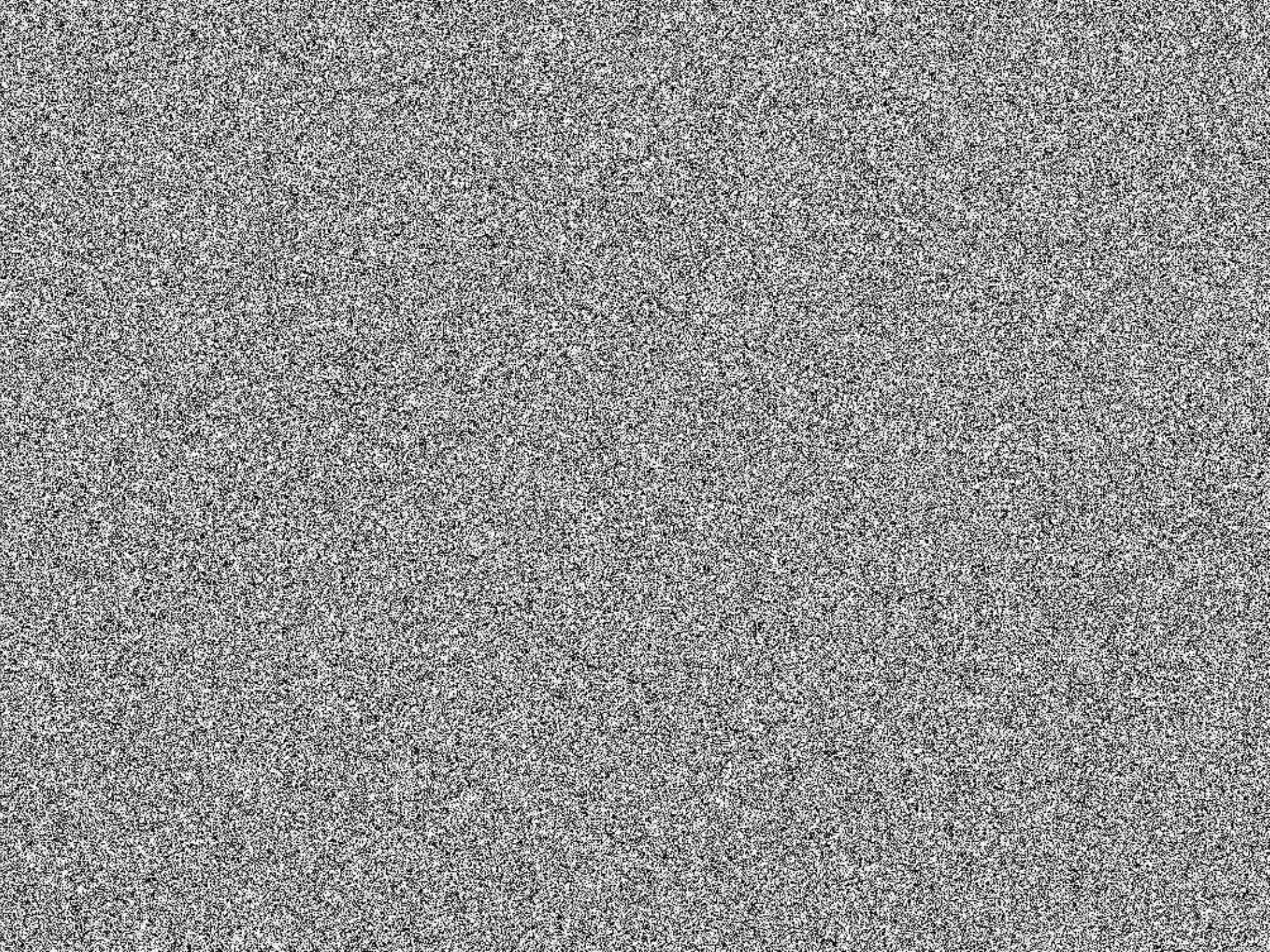
$\psi^+$  or  $\psi^-$ ?



## 5 Unconditional security: one-time pad

$$P \xrightarrow{\quad} C = P \oplus x$$

plaintext                      ciphertext                      key



## 5 Unconditional security: one-time pad

$$P \longrightarrow C = P \oplus x$$

plaintext                      ciphertext                      key

$$P = C \oplus x \oplus x$$

- the key can be safely used only once!

$$D = Q \oplus x$$

$$C \oplus D = P \oplus Q$$

- a different option: **computational security**  
 $C = F(P)$ , and computing  $F^{-1}$  is hard



[wiki]



## 5 Sharing a password: photons & a public channel

- Prepare *photons*  
Send *photons*  
Detect *photons*
- Announce the results!
- Do some checking.
- Get a **secret key** (one-time pad).



# 5 Making up a password using a public channel

The BB84 protocol (no entanglement).

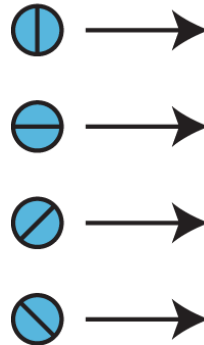
## Alice

choose a basis  
prepare a photon  
send it



## Bob

choose a basis  
measure the photon



**1**  
**0**  
random  
random

## 5 Making up a password using a public channel

The BB84 protocol (no entanglement).

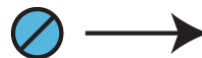
### Alice

choose a basis  
prepare a photon  
send it



### Bob

choose a basis  
measure the photon



random

random

**1**

**0**

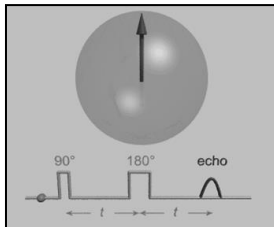
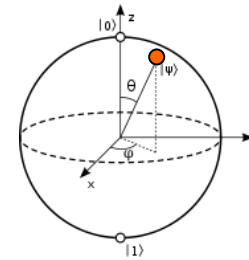
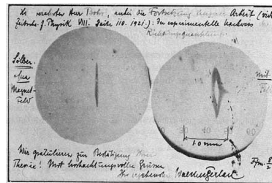
compare the basis choices (publicly)  
correlated results wherever the bases match  
those results make up the **secret key**

*[Bennett & Brassard]*

1

# we need & use a qubit

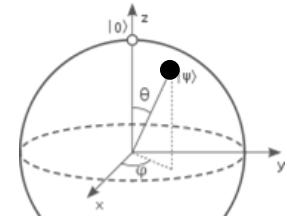
spin- $\frac{1}{2}$ , superpositions, transforming & measuring



1

# we need a qubit

well, what can we do with it?



2

# EPR pairs

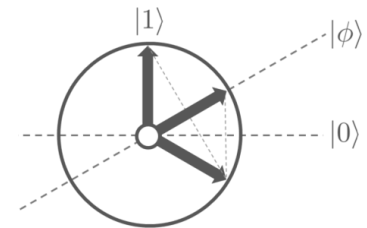
and tricky 2-qubit protocols



3

# the algorithms

that make quantum computing tick



4

# error correction

can we really scale up this stuff?



5

# the limits

complexity & limits of q. computing



19:00



