Quantum Information Processing

Harry Buhrman

CWI
&
University of Amsterdam

Physics and Computing

Computing is physical
Miniaturization → quantum effects

➔Quantum Computers

1) Enables continuing miniaturization
2) Fundamentally faster algorithms
3) New computing paradigm

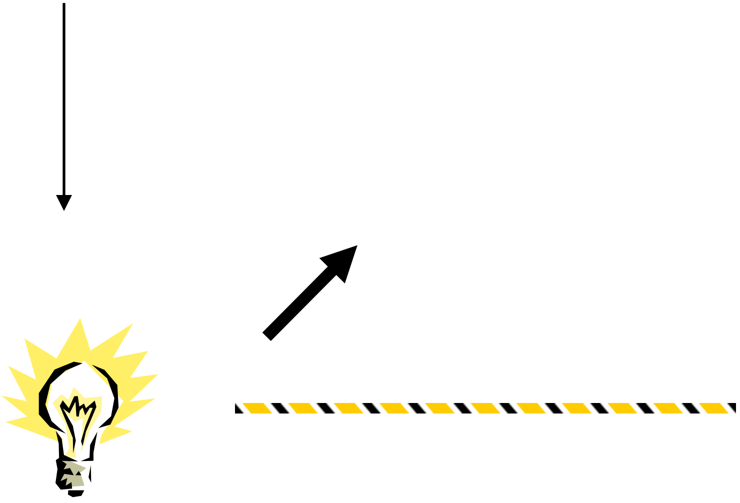
Quantum mechanics

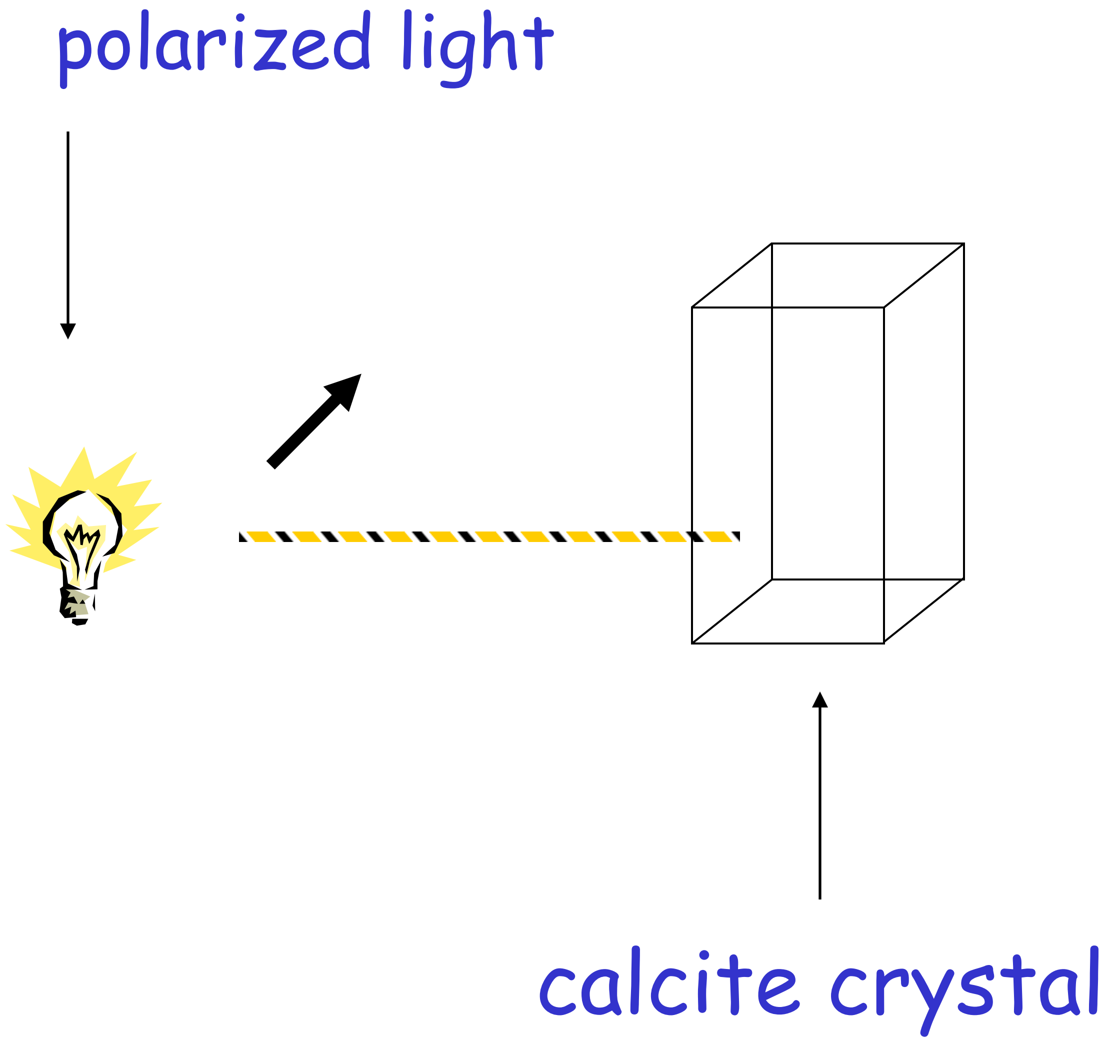
“What I am going to tell you about is what we teach our physics students in the third or fourth year of graduate school... It is my task to convince you not to turn away because you don't understand it. You see my physics students don't understand it. ... That is because I don't understand it. Nobody does. “

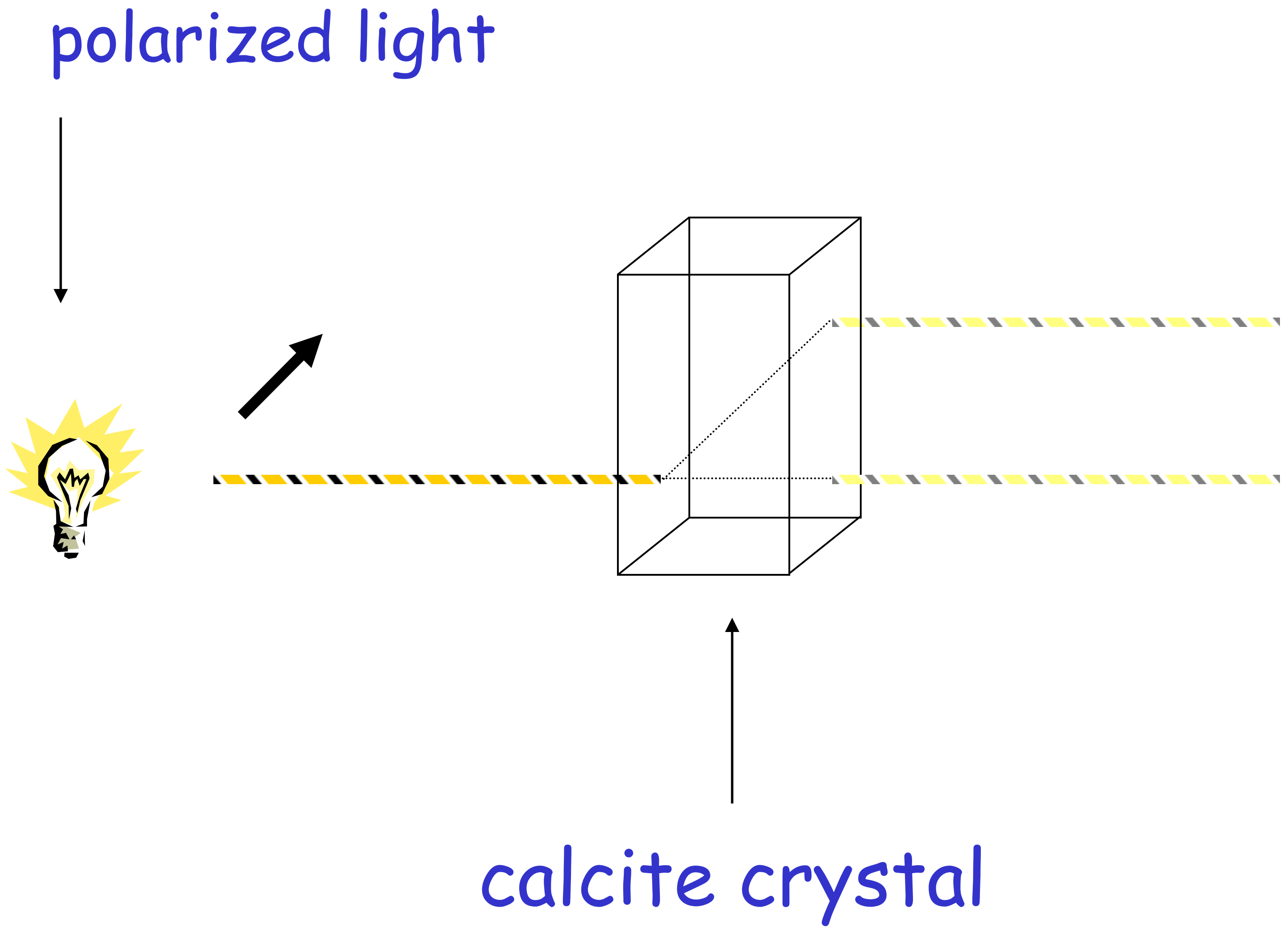
Richard Feynman, Nobel Lecture, 1966

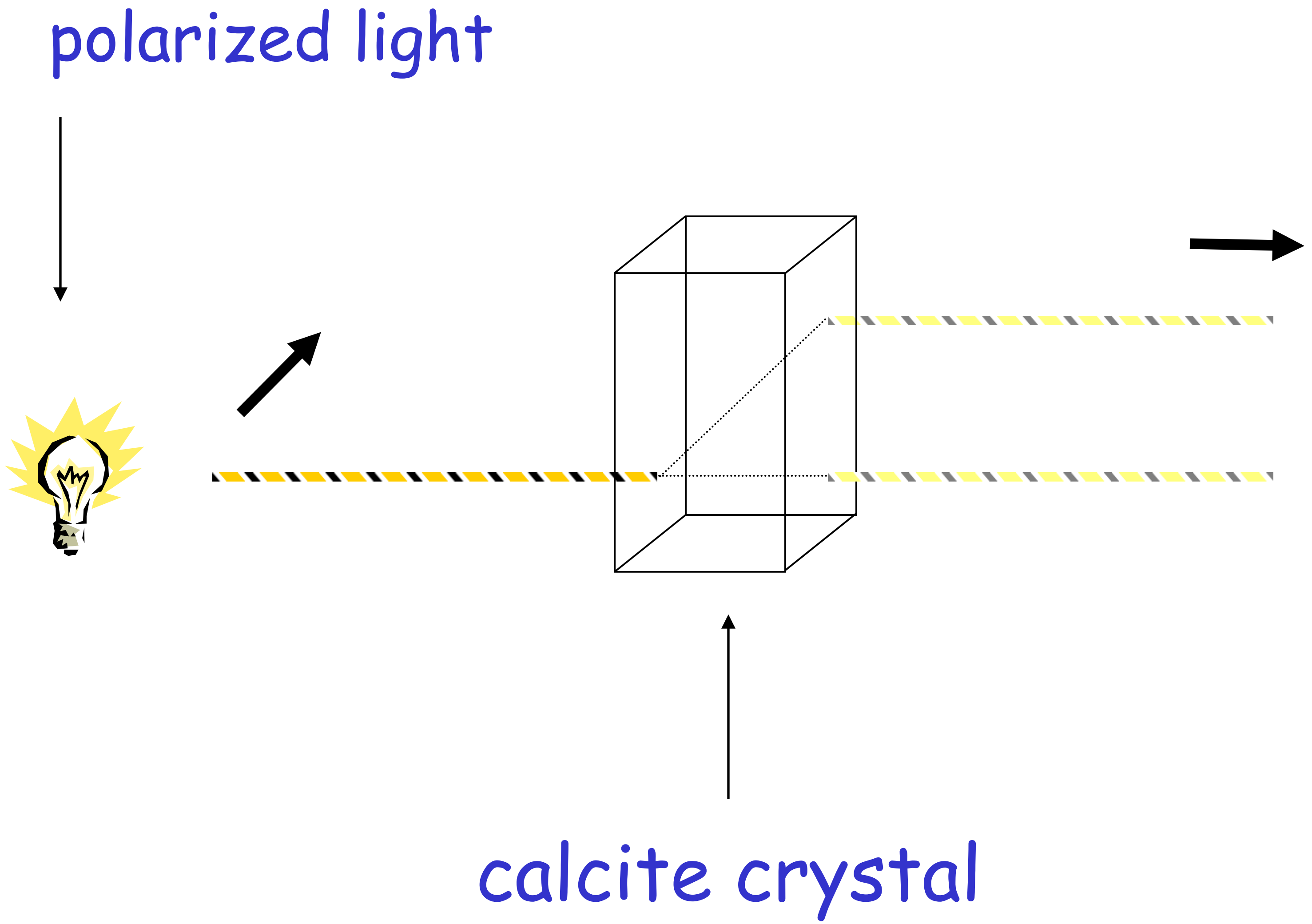
Quantum Mechanics

polarized light

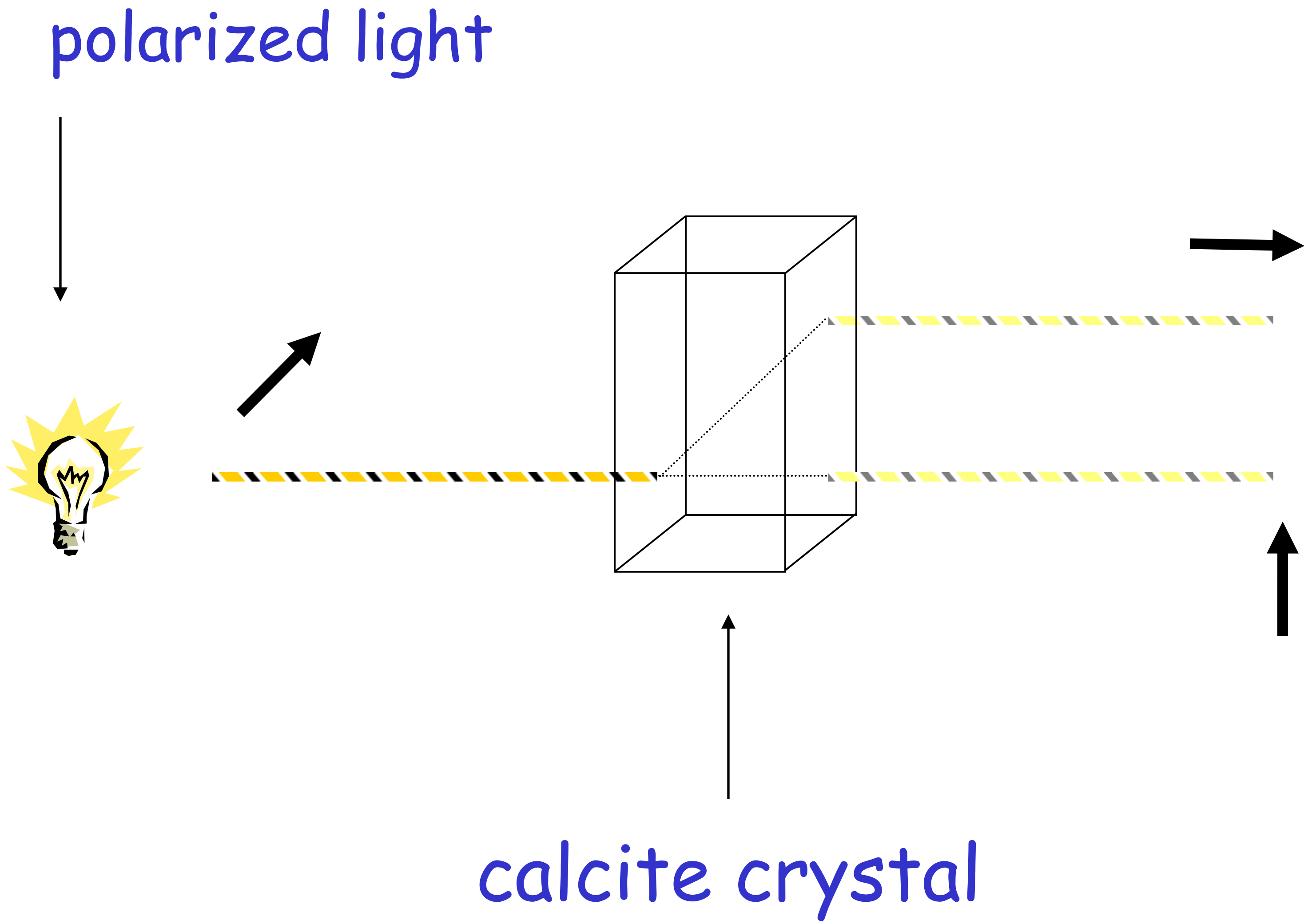


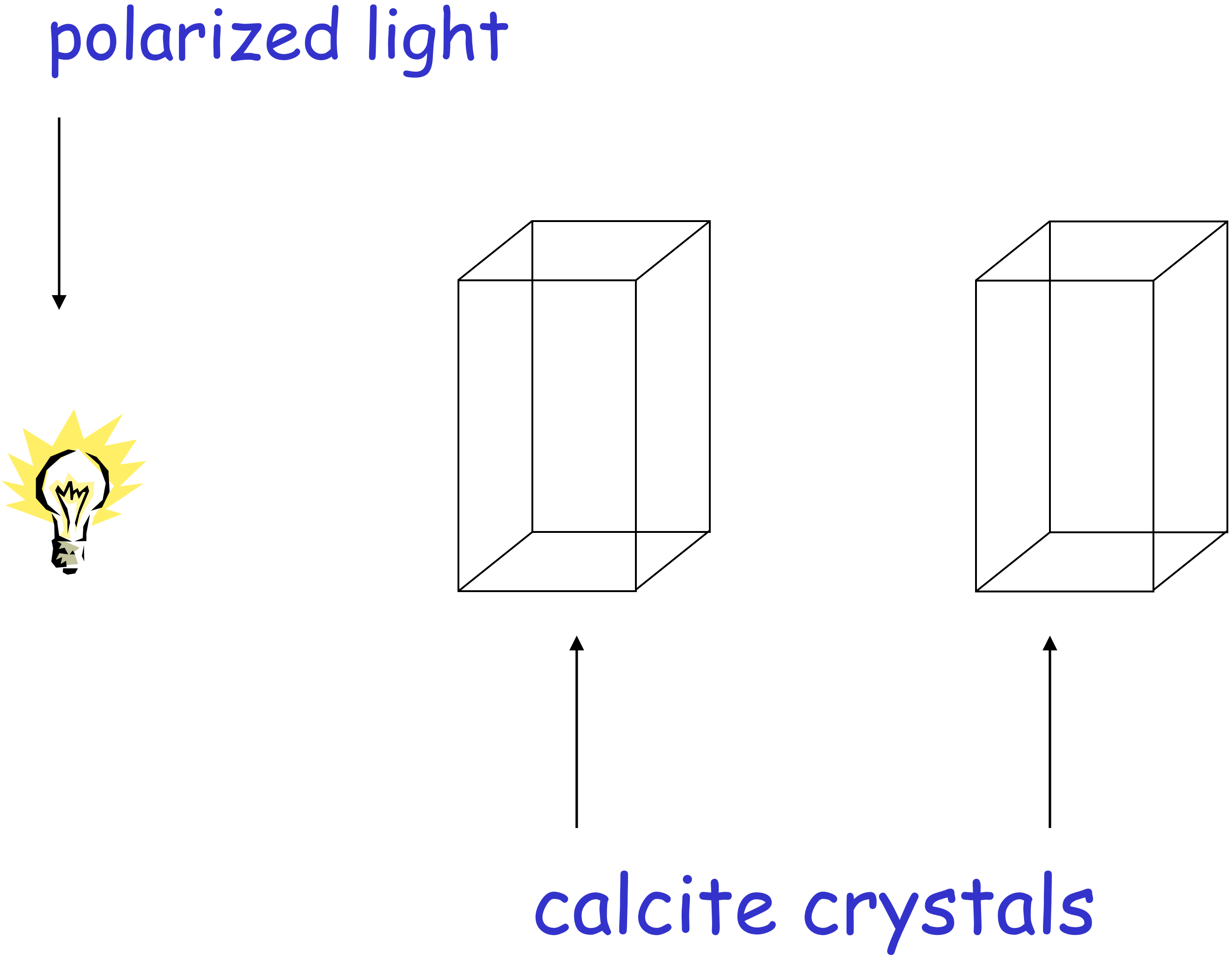

polarized light
calcite crystal

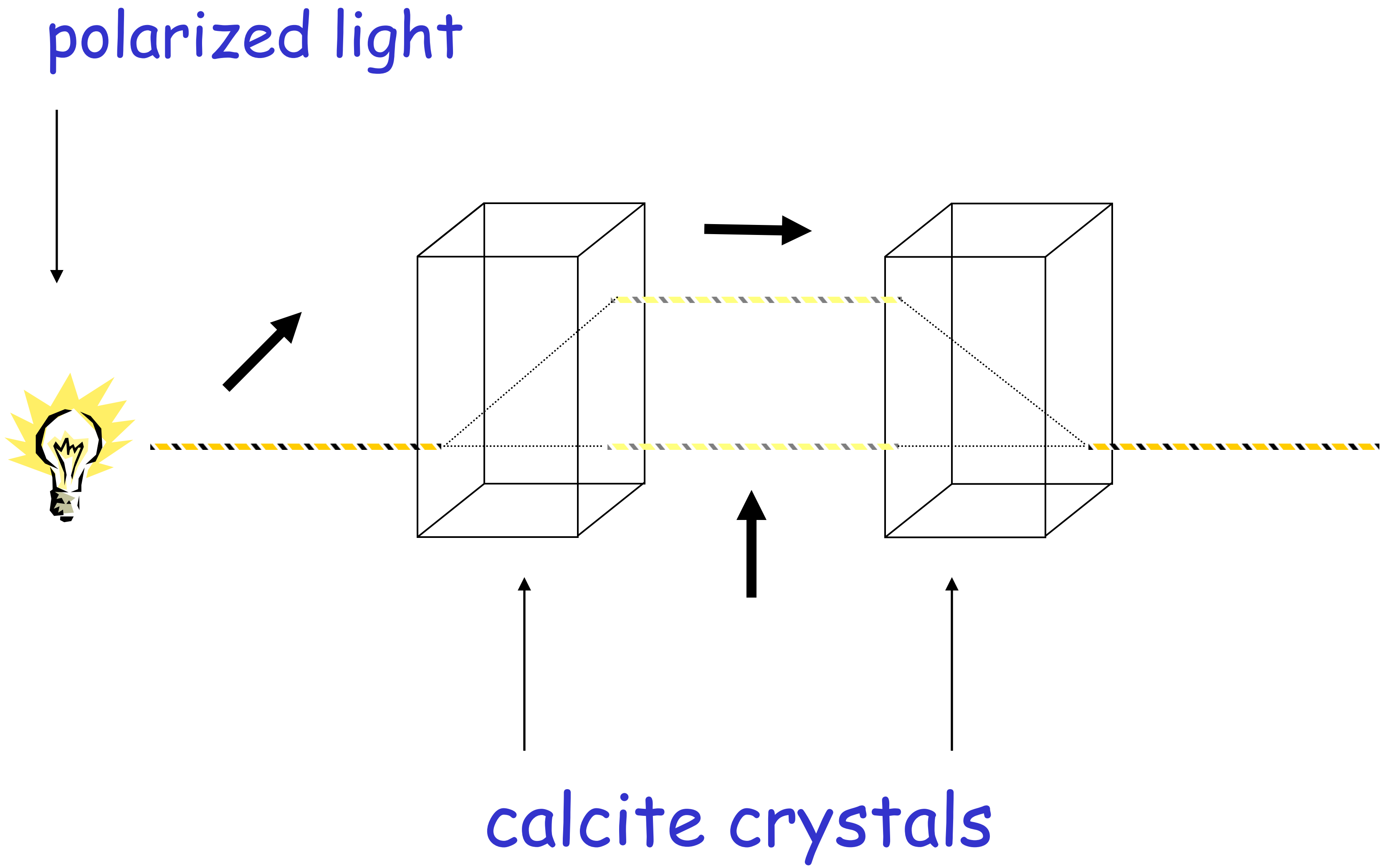

polarized light
calcite crystal



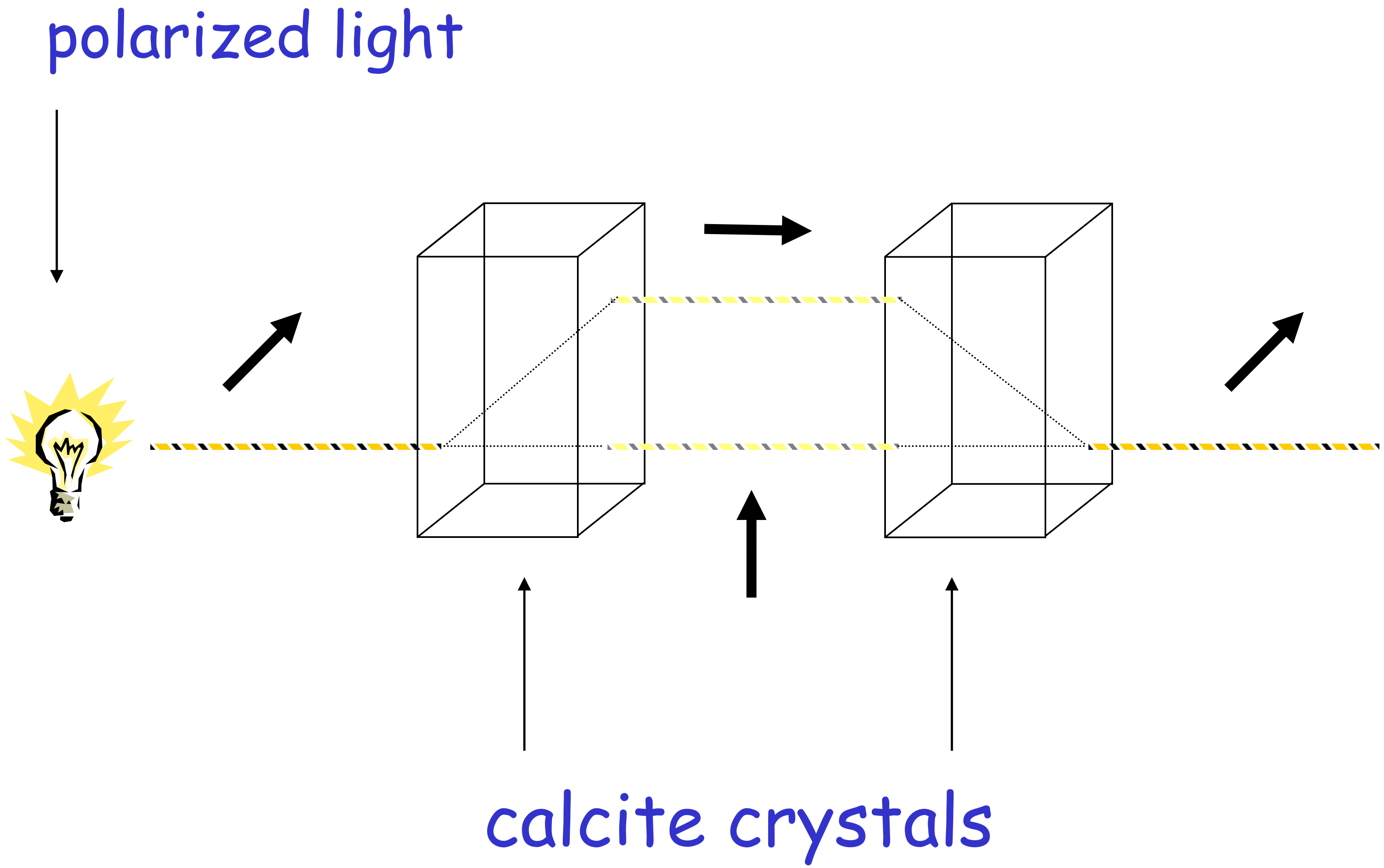
polarized light
calcite crystal

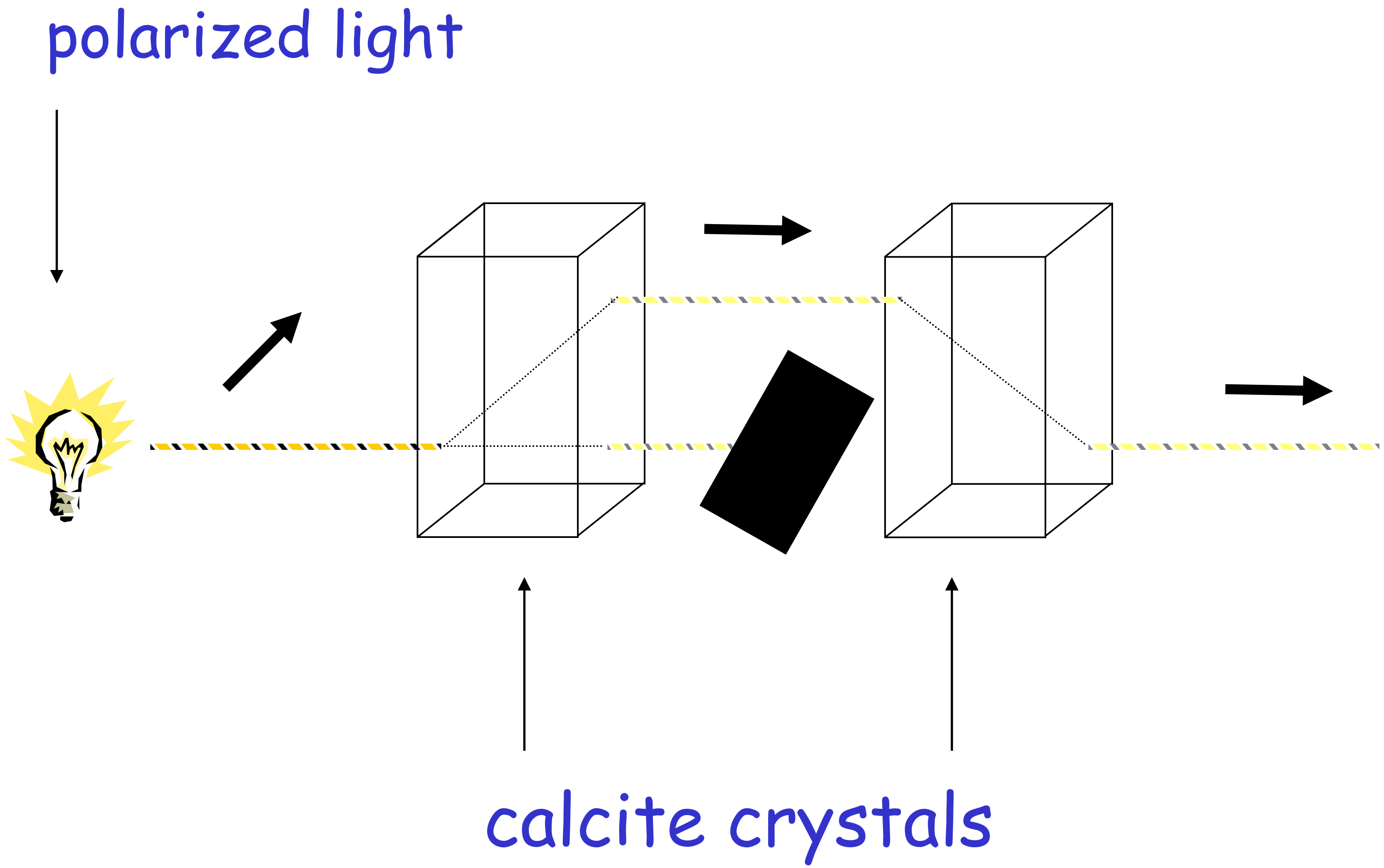

polarized light
calcite crystal

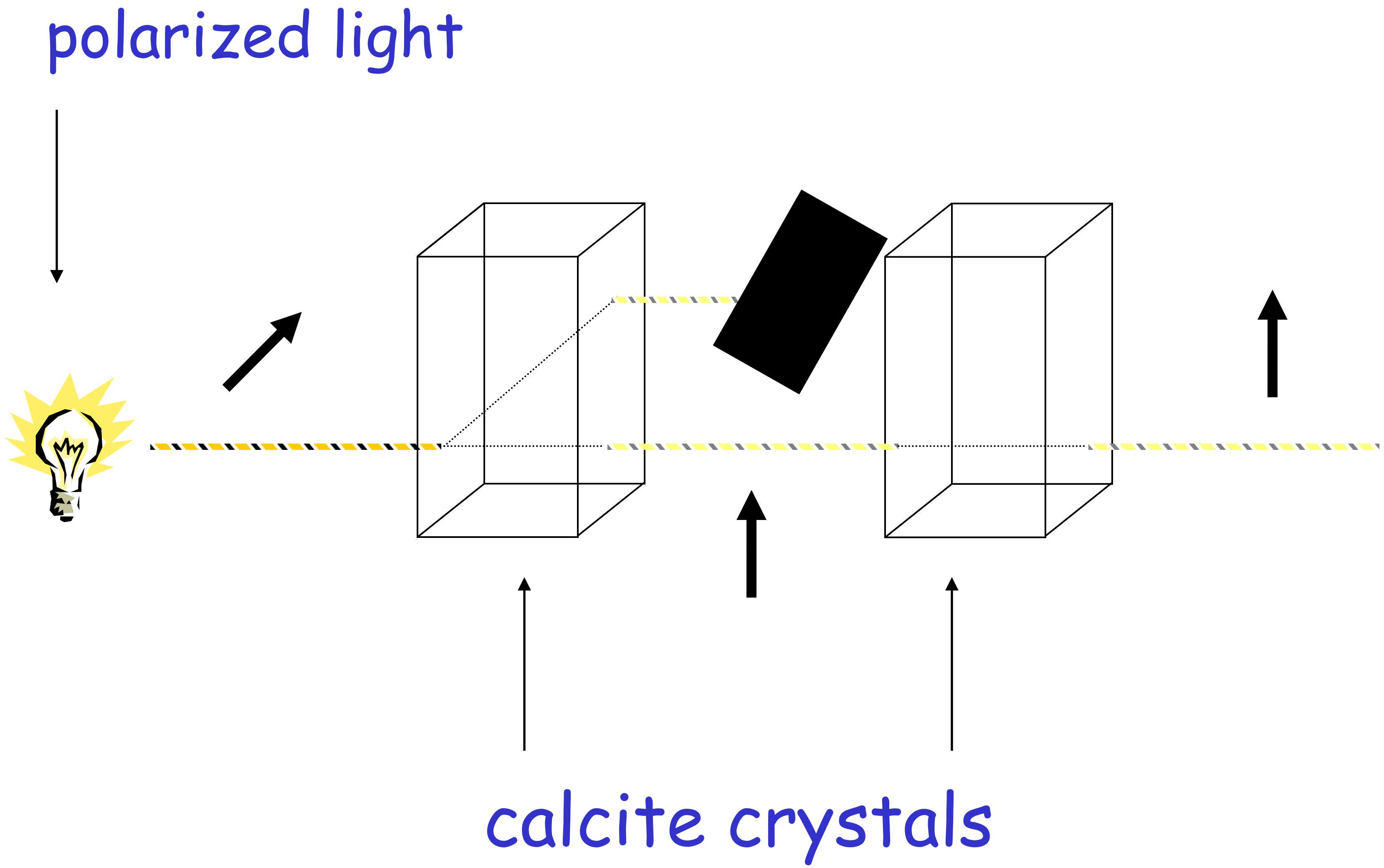

polarized light
calcite crystals

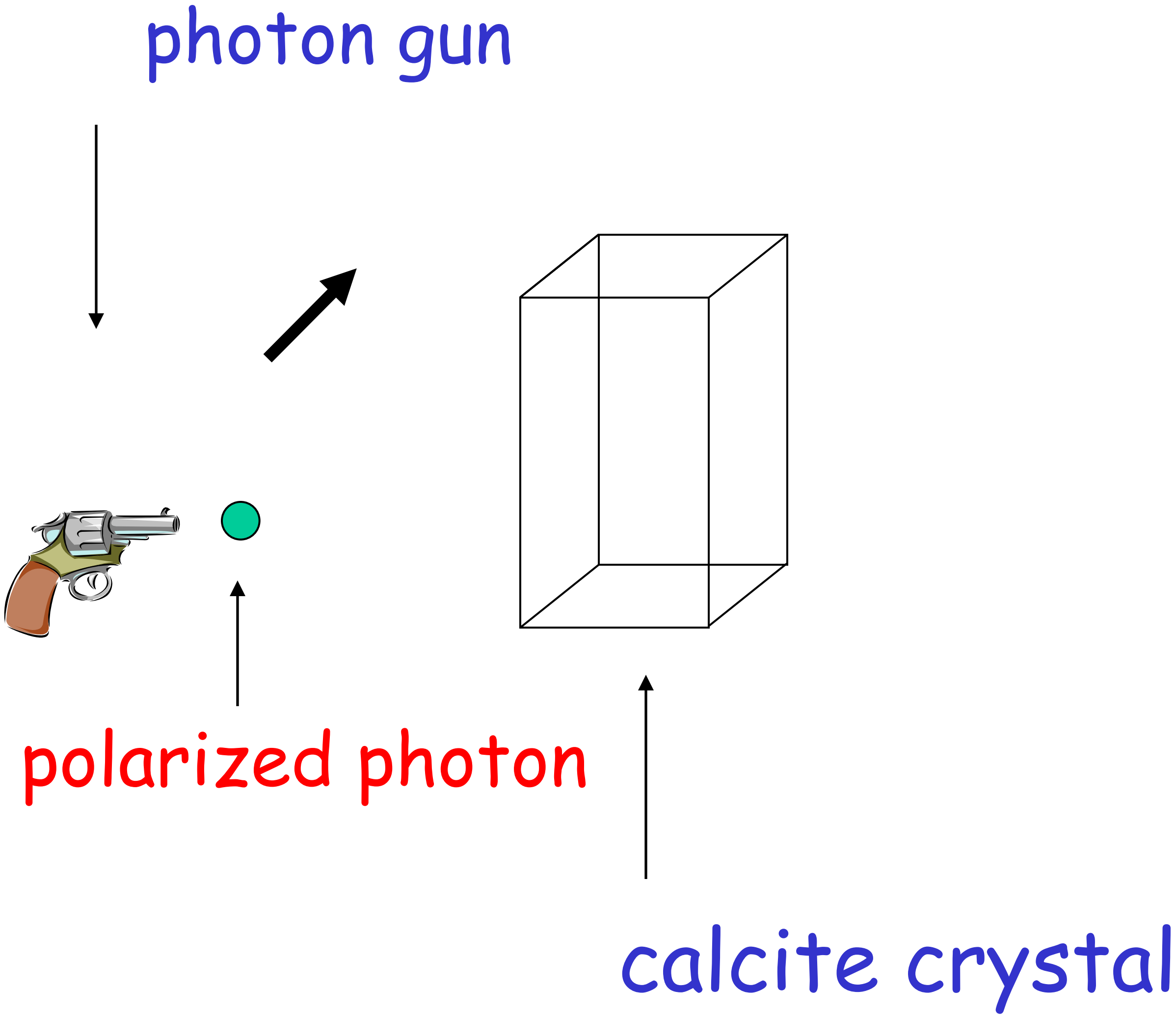


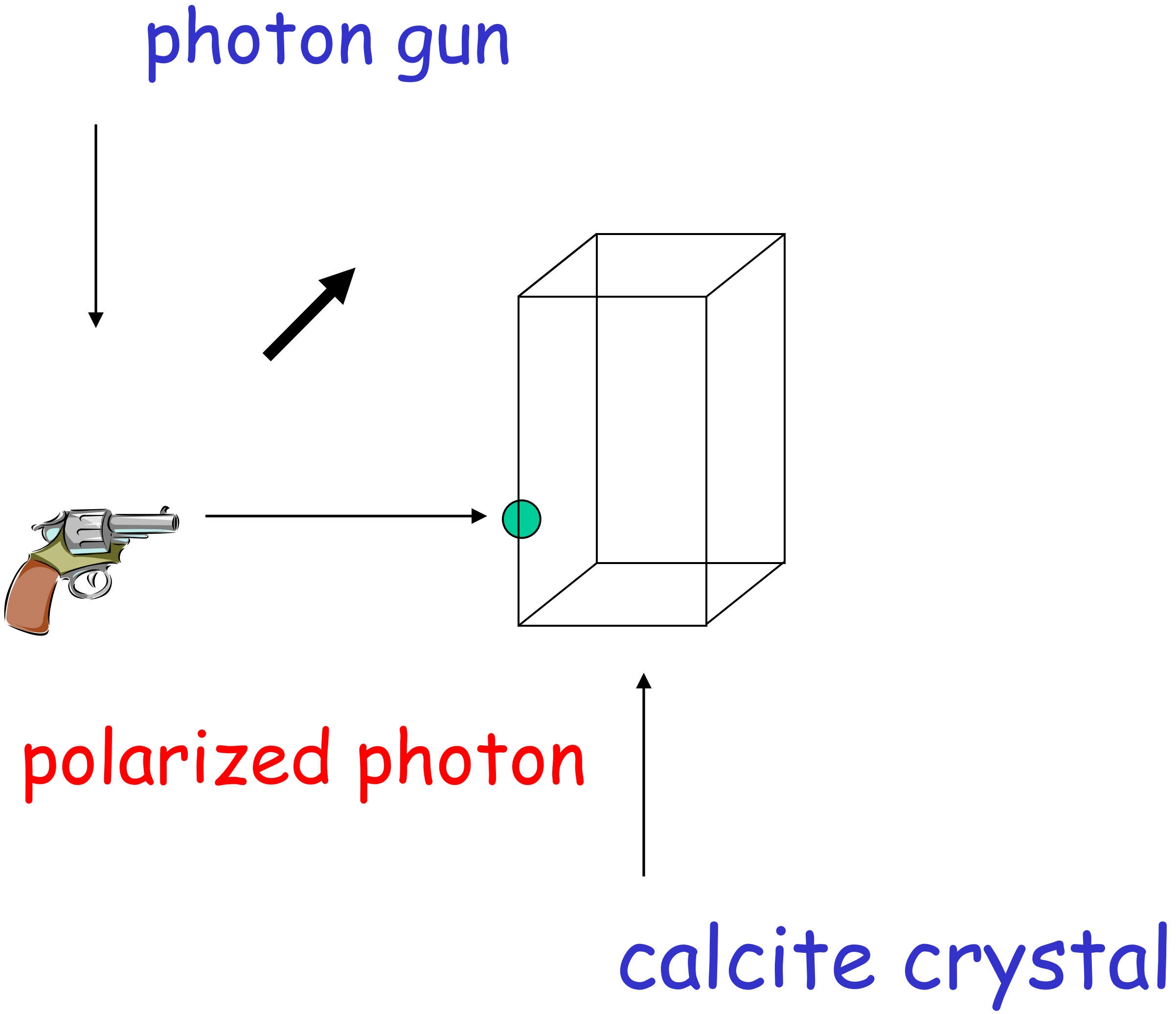
polarized light
calcite crystals

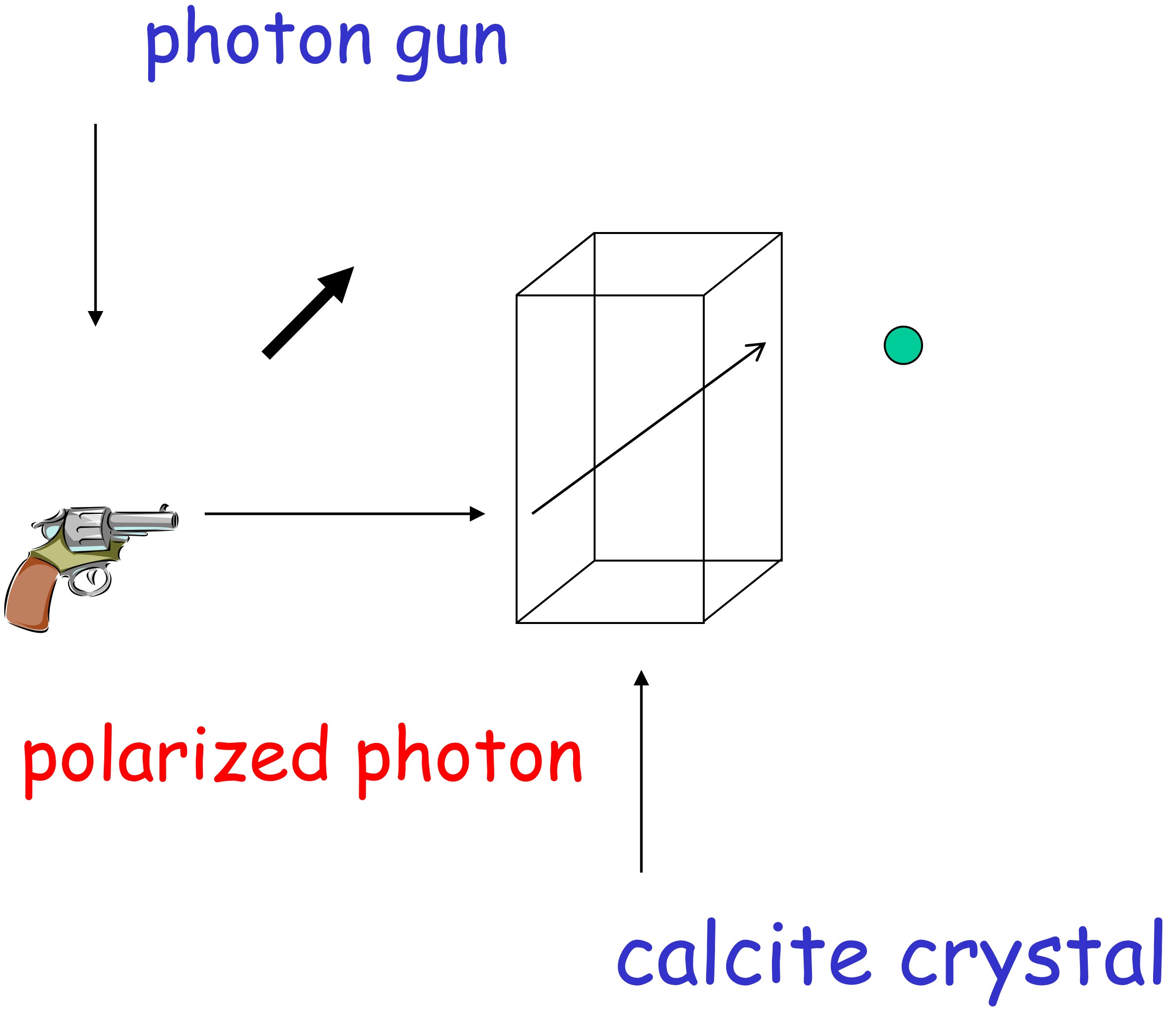

polarized light
calcite crystals


polarized light
calcite crystals

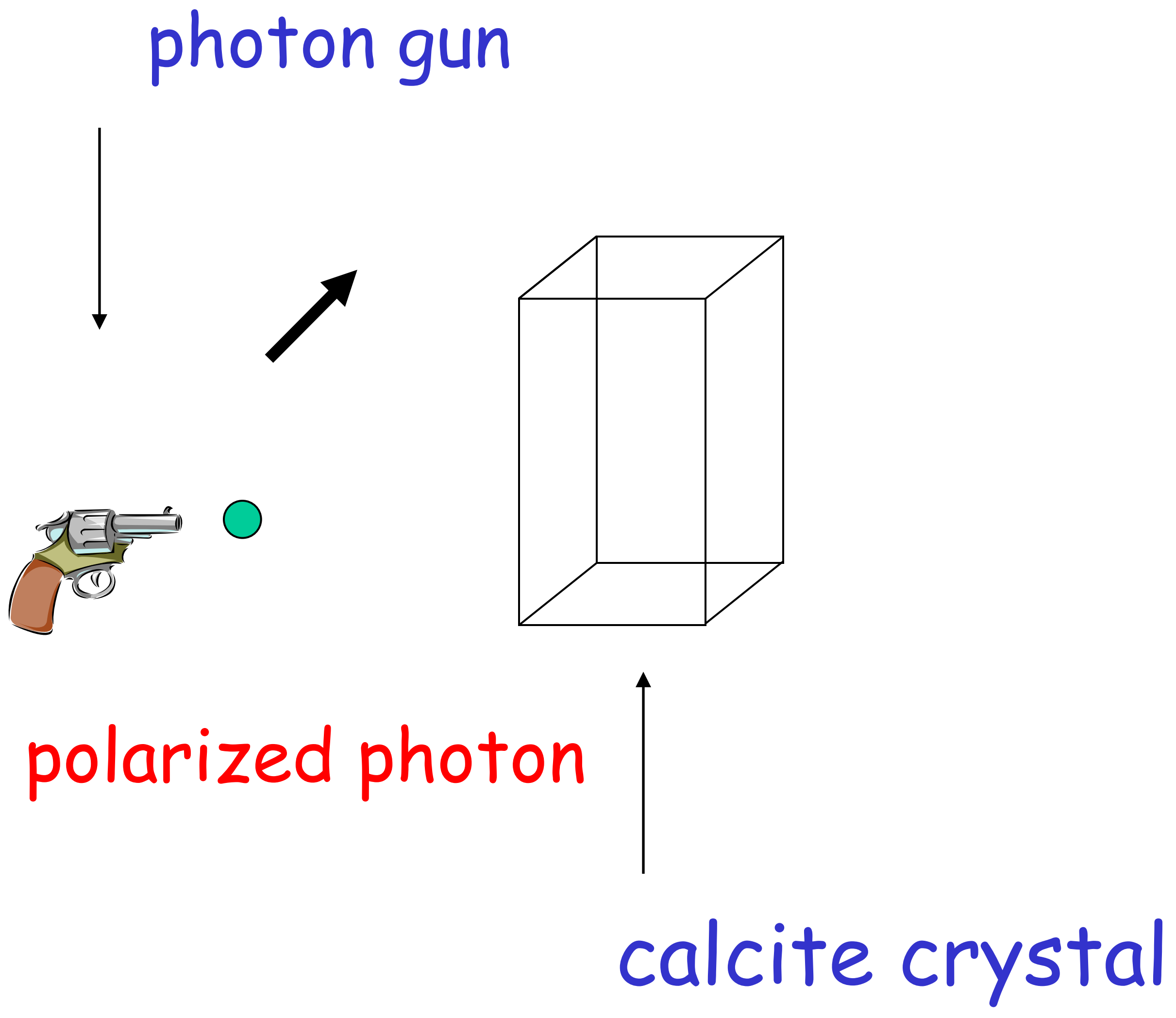

polarized light
calcite crystals


photon gun
polarized photon
calcite crystal

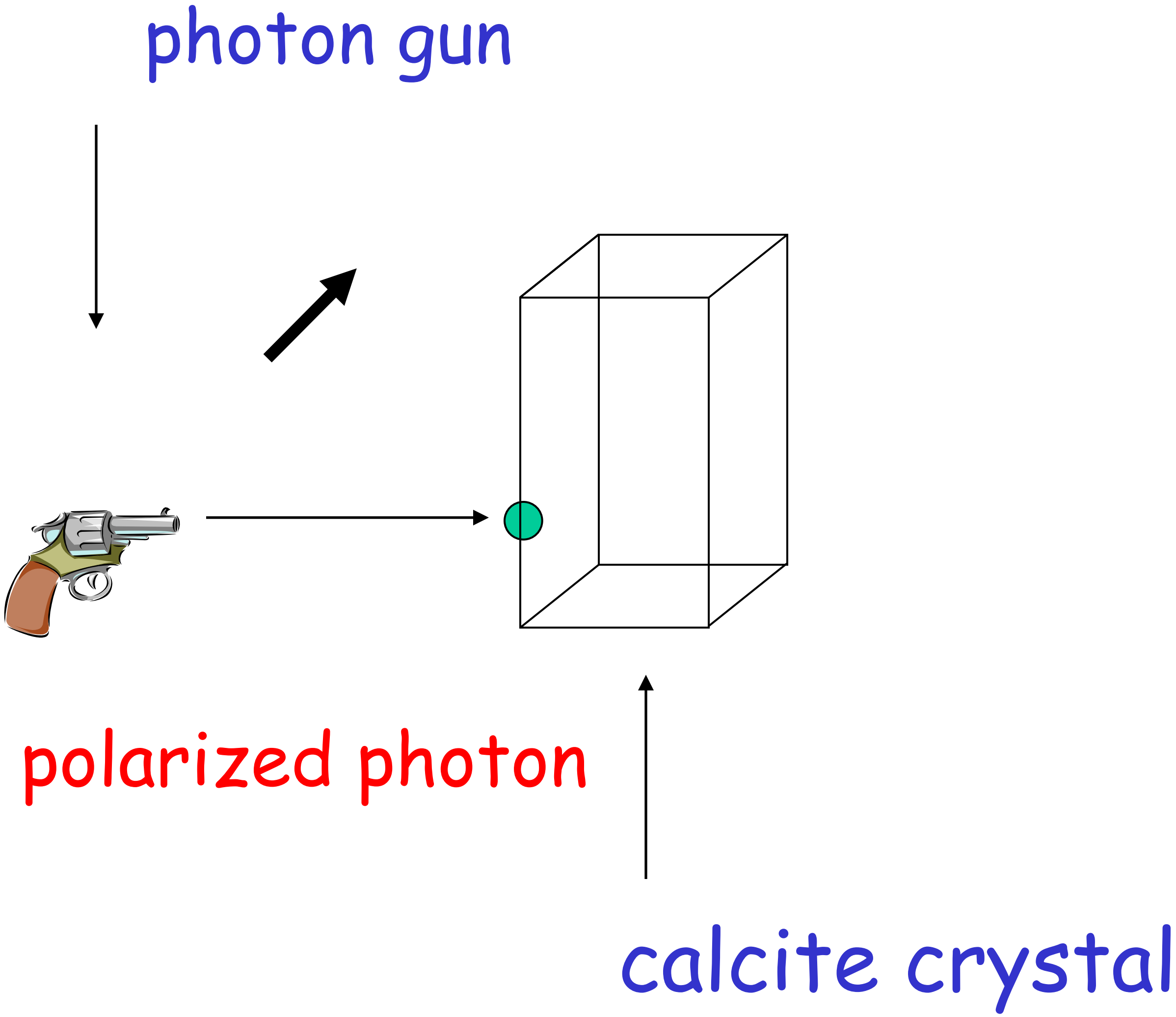

photon gun
polarized photon
calcite crystal

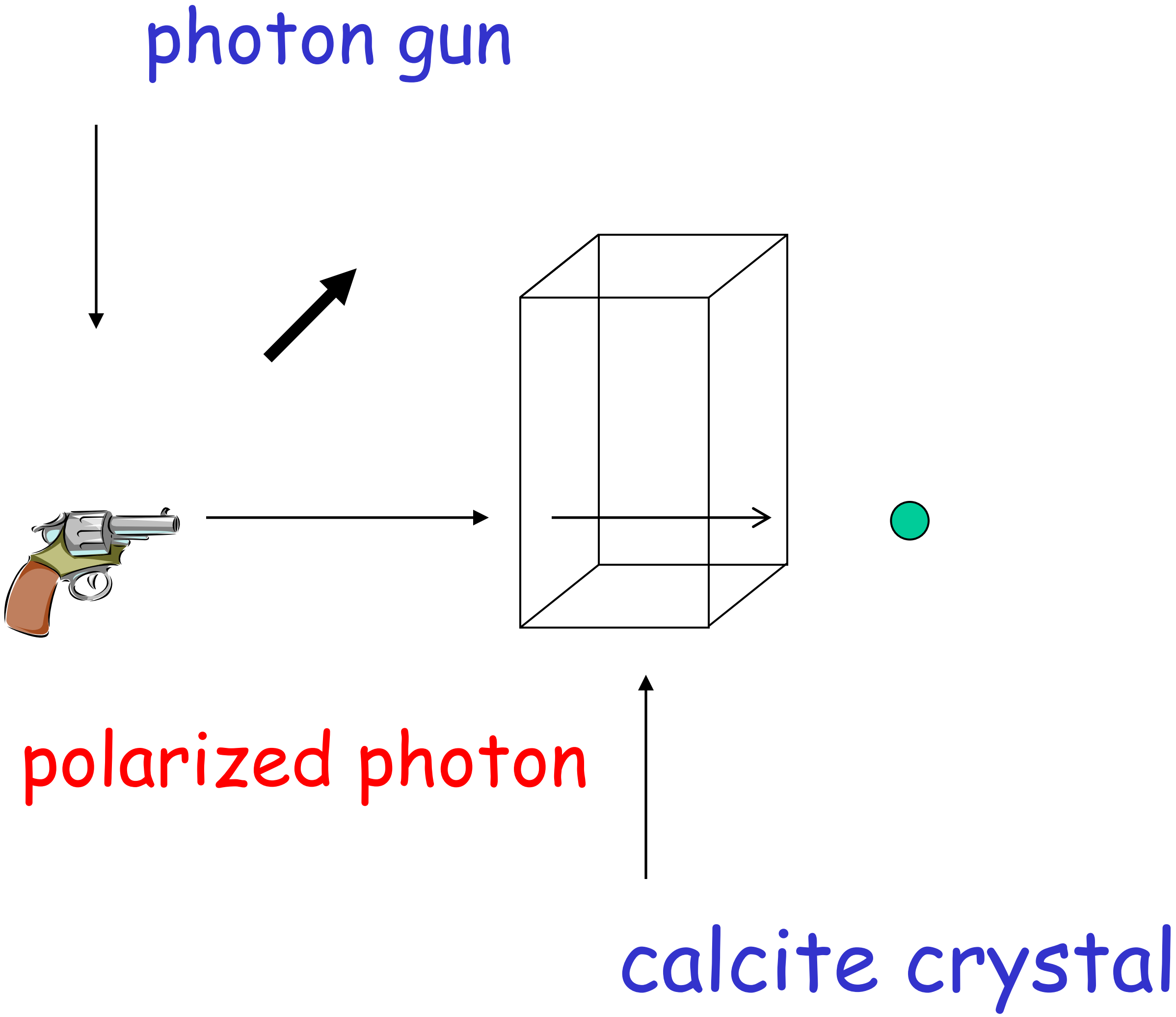


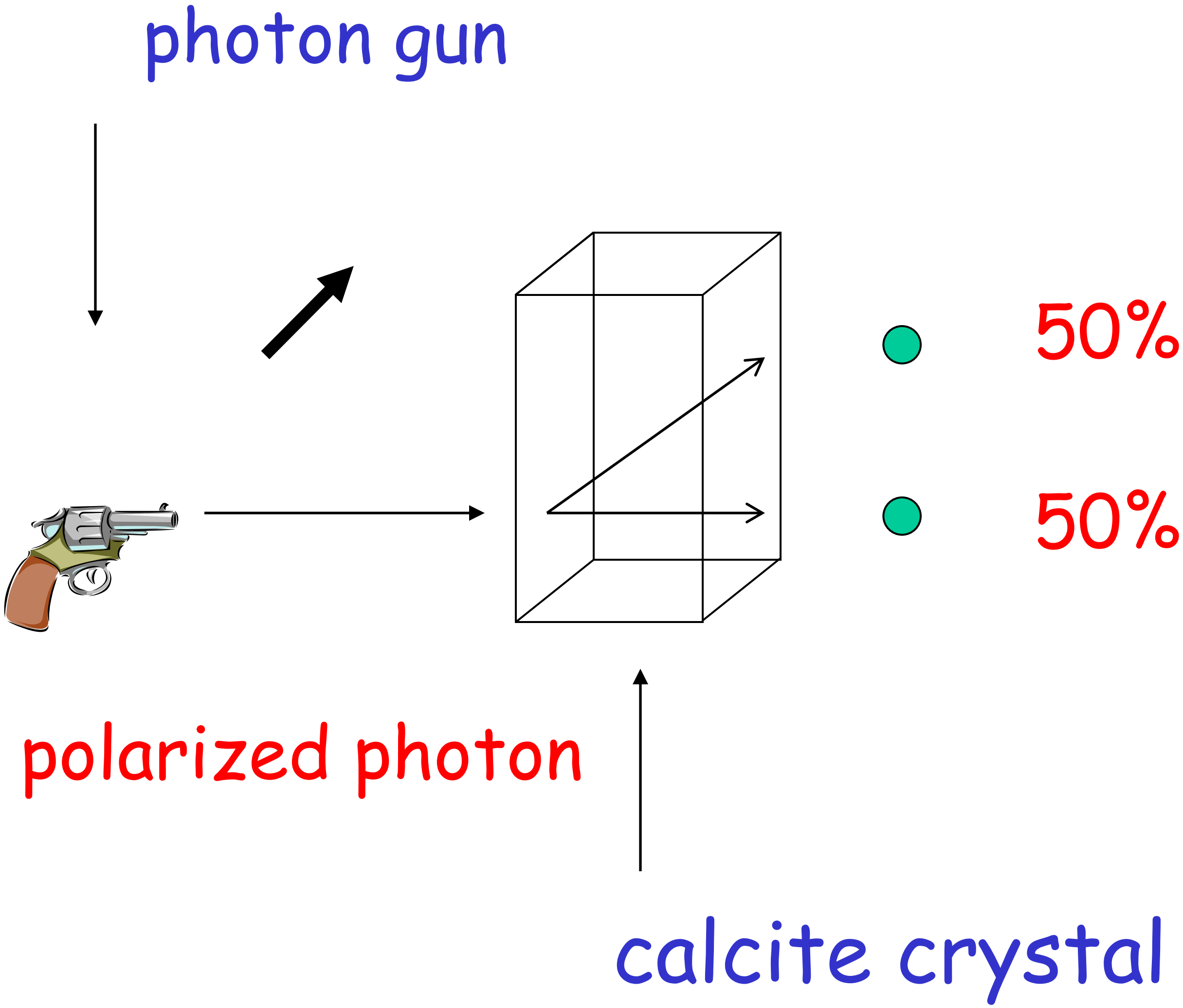
photon gun
polarized photon
calcite crystal

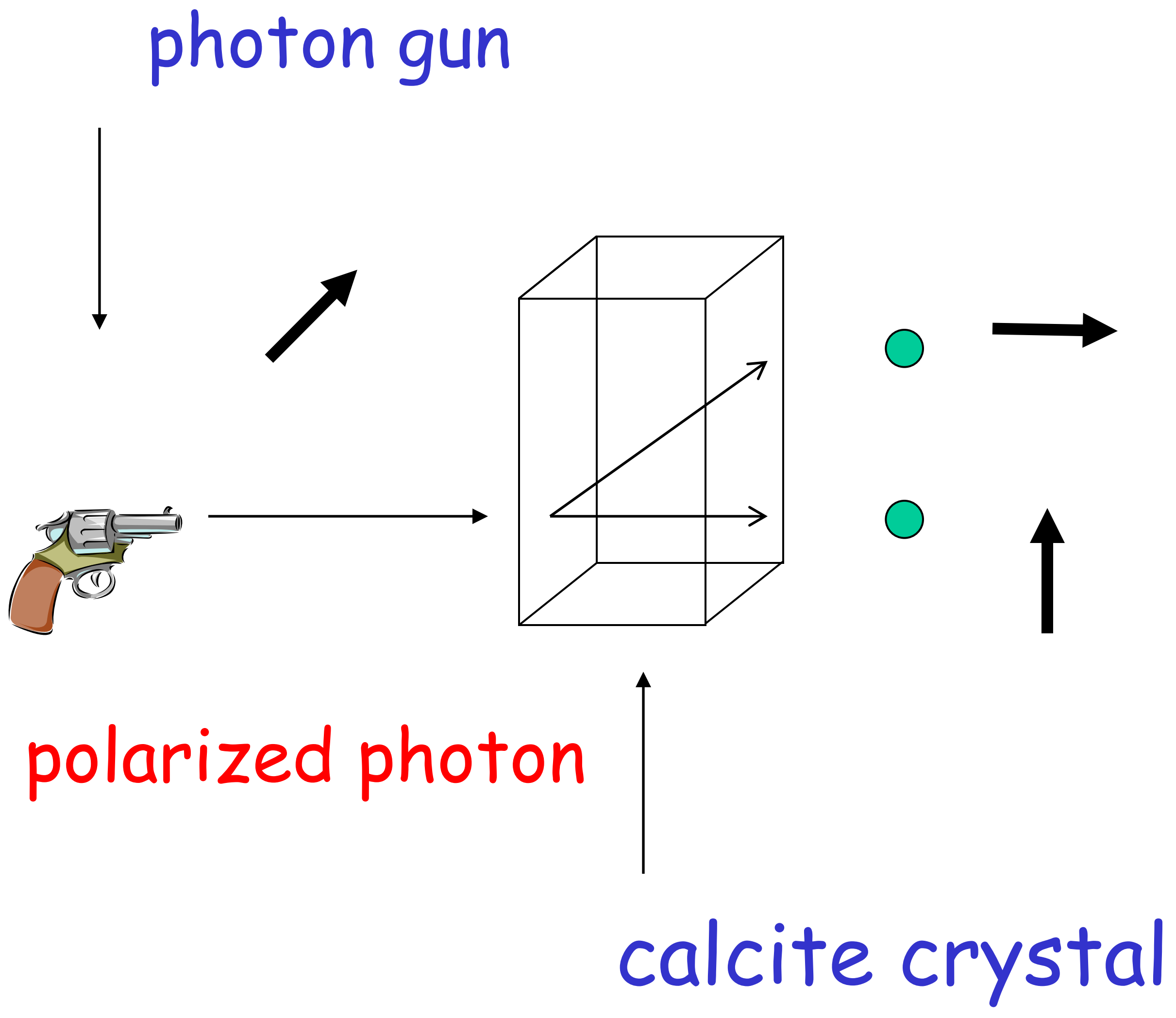


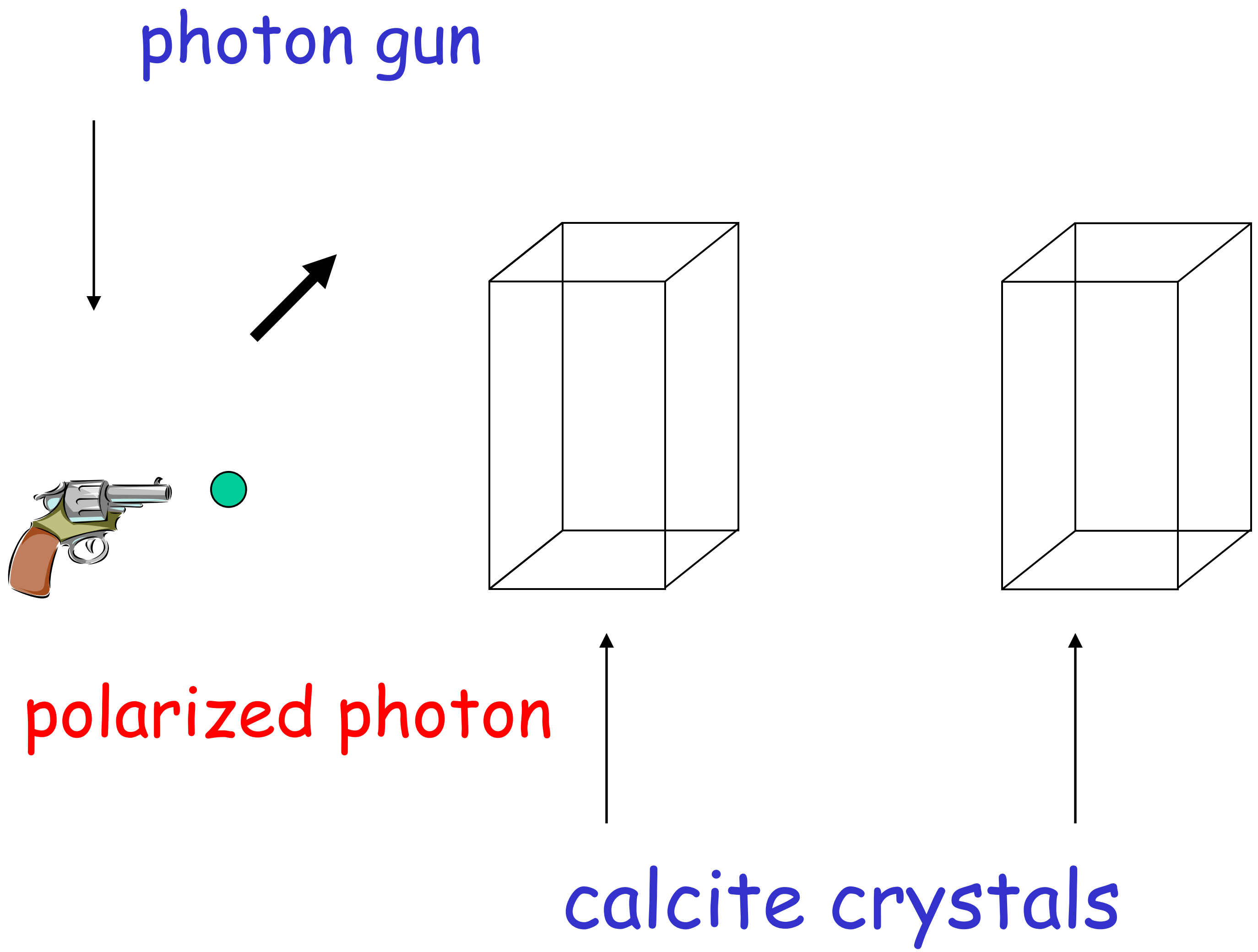
photon gun
polarized photon
calcite crystal

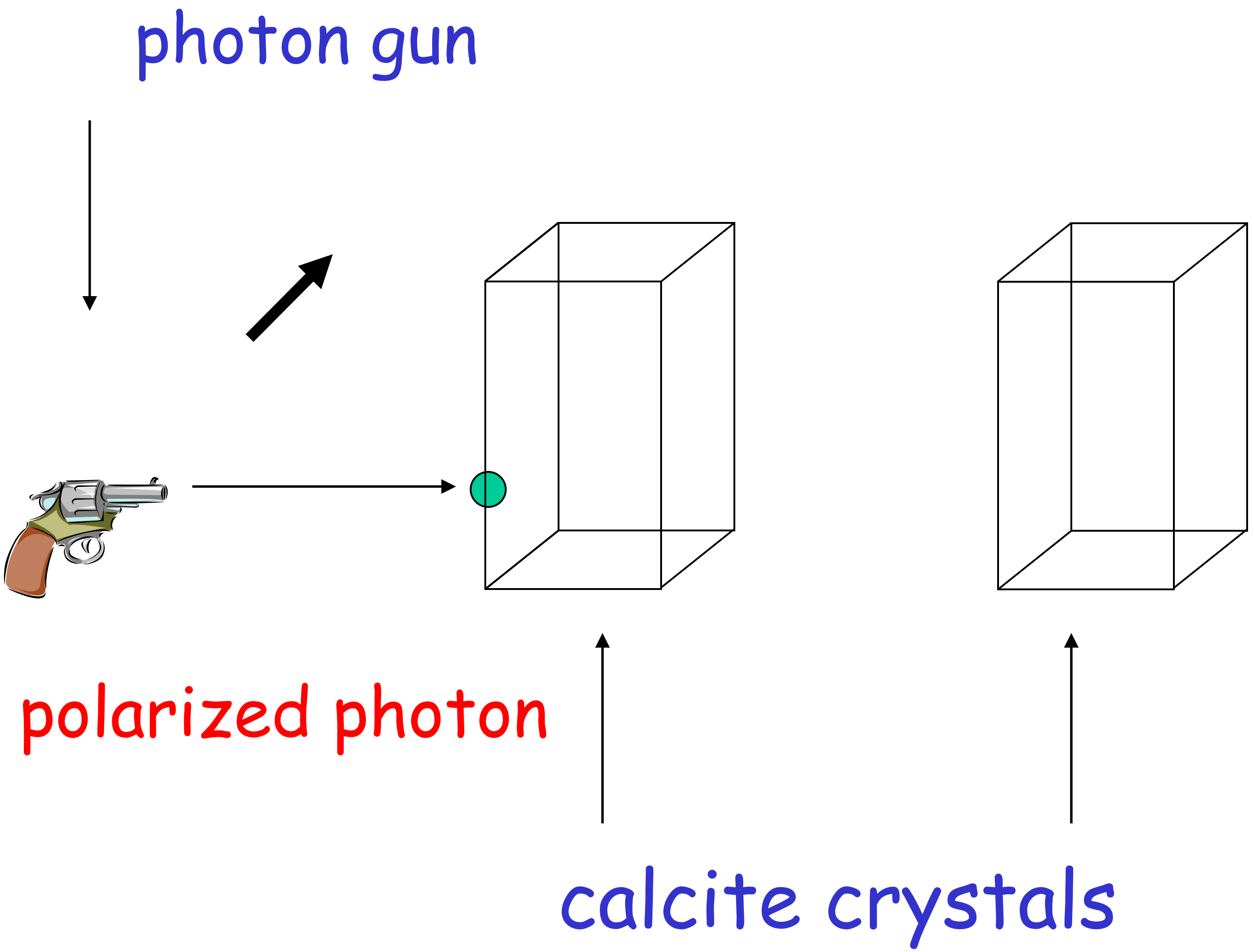

photon gun
polarized photon
calcite crystal

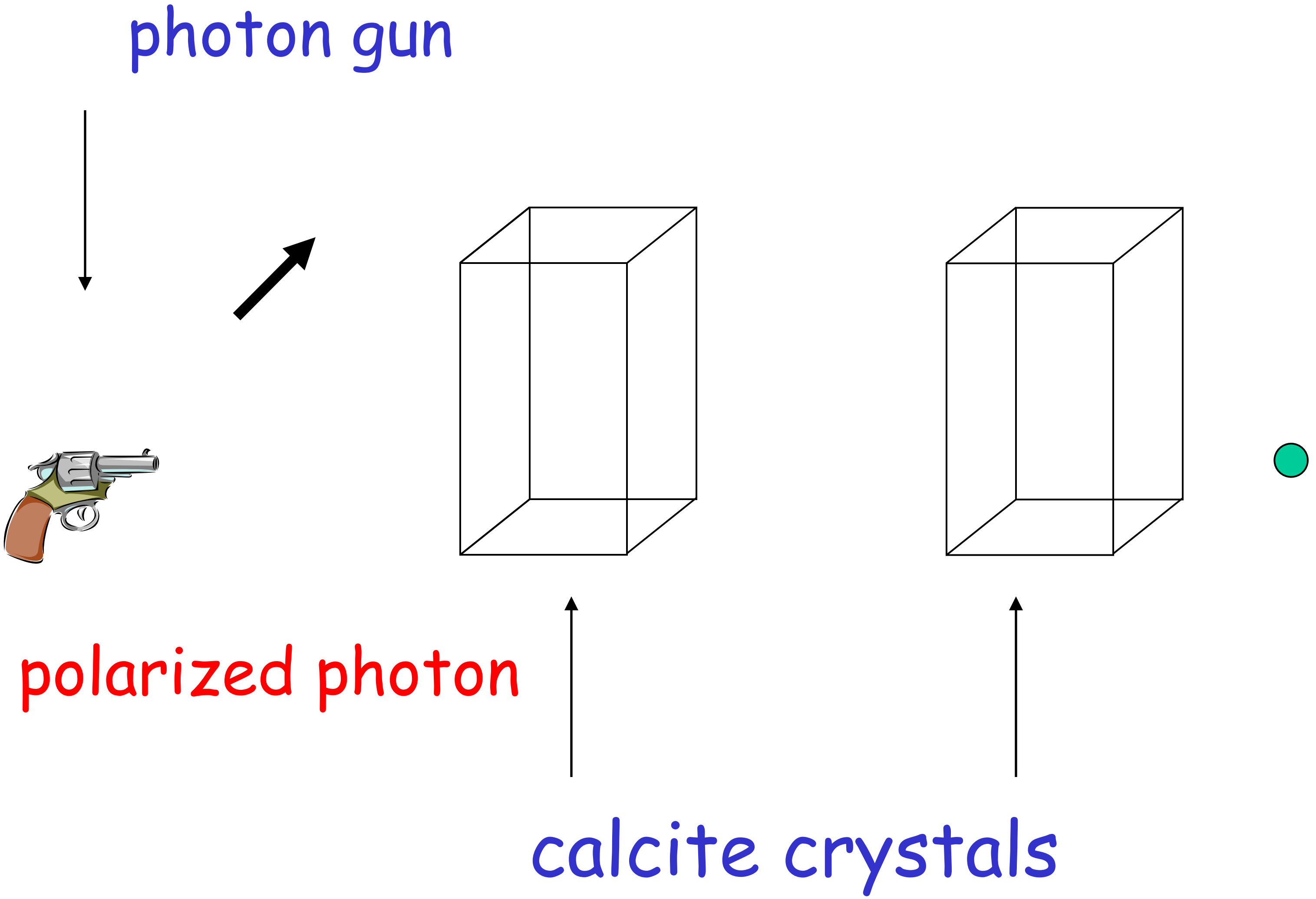

photon gun
polarized photon
calcite crystal

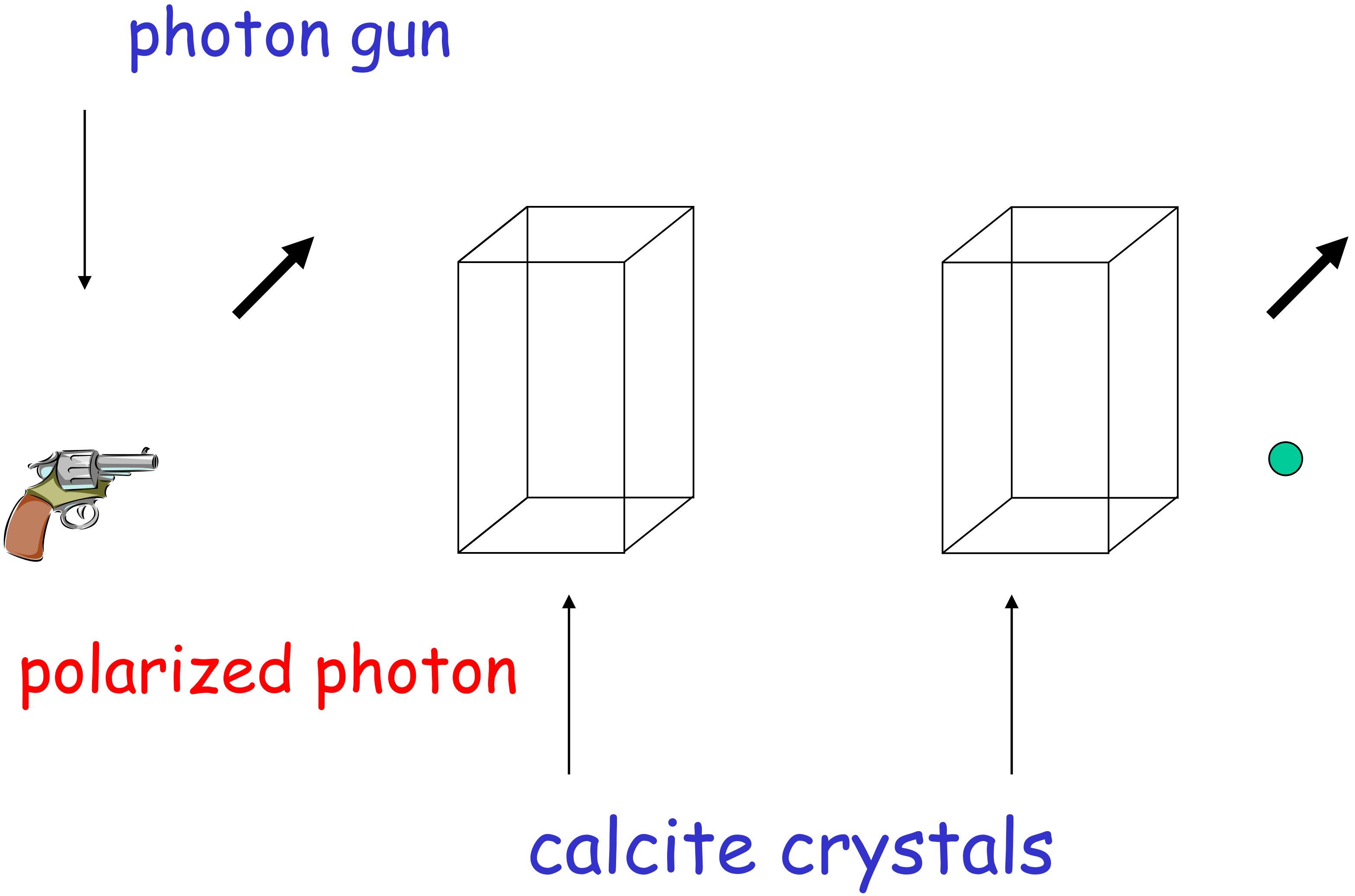

photon gun
50%
50%
polarized photon
calcite crystal

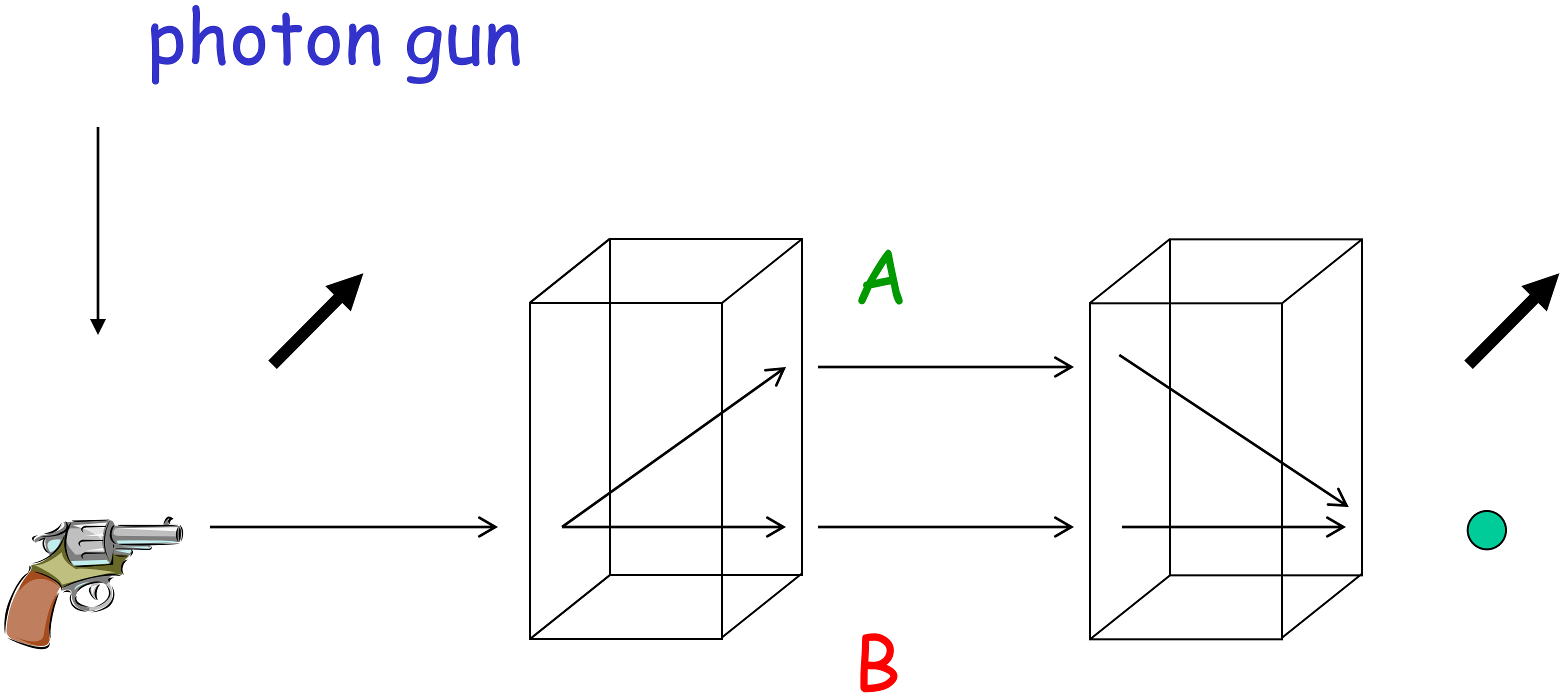

photon gun
polarized photon
calcite crystal


photon gun
polarized photon
calcite crystals

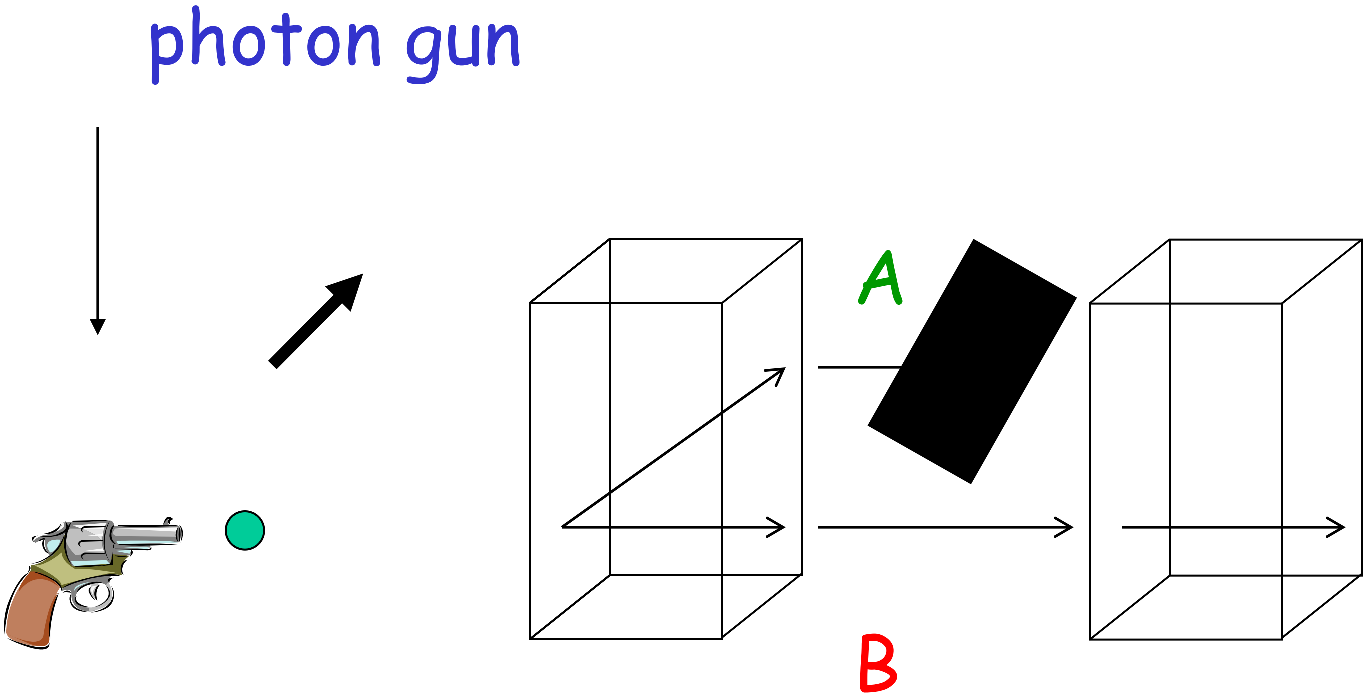

photon gun
polarized photon
calcite crystals


photon gun
polarized photon
calcite crystals

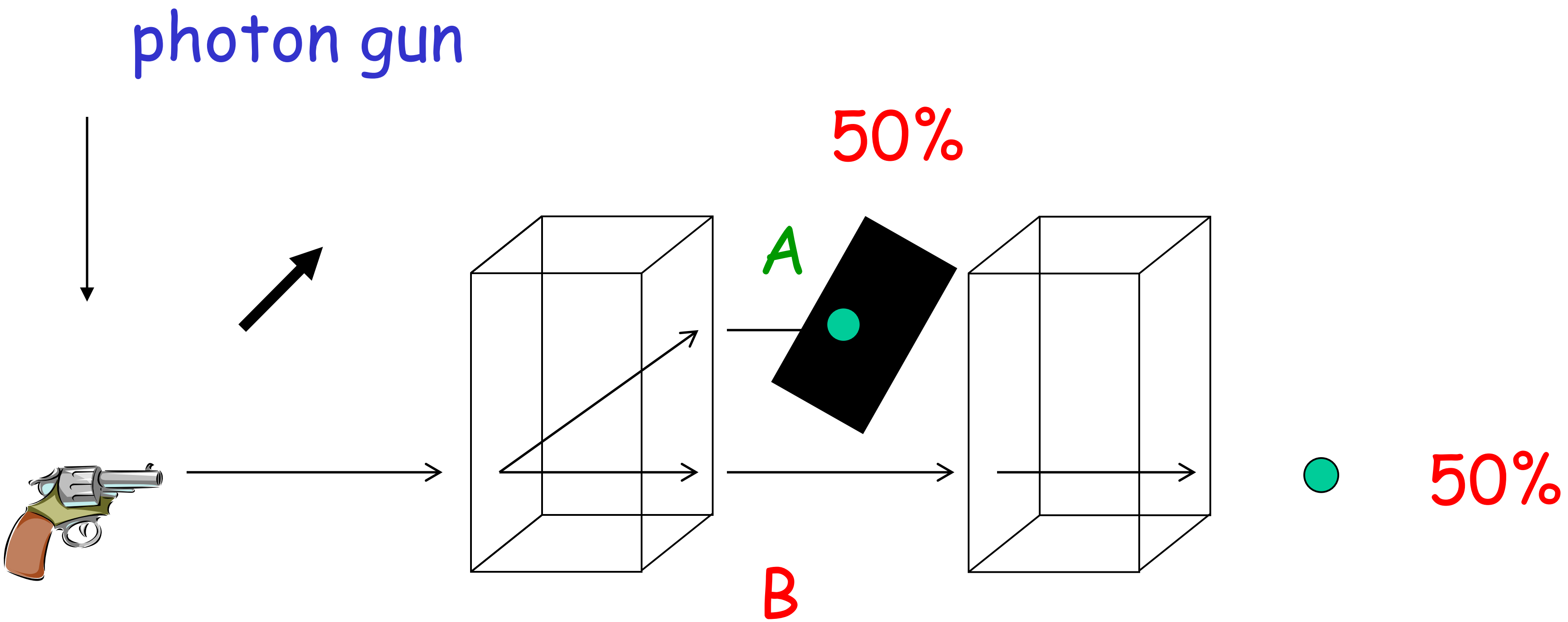

photon gun
polarized photon
calcite crystals



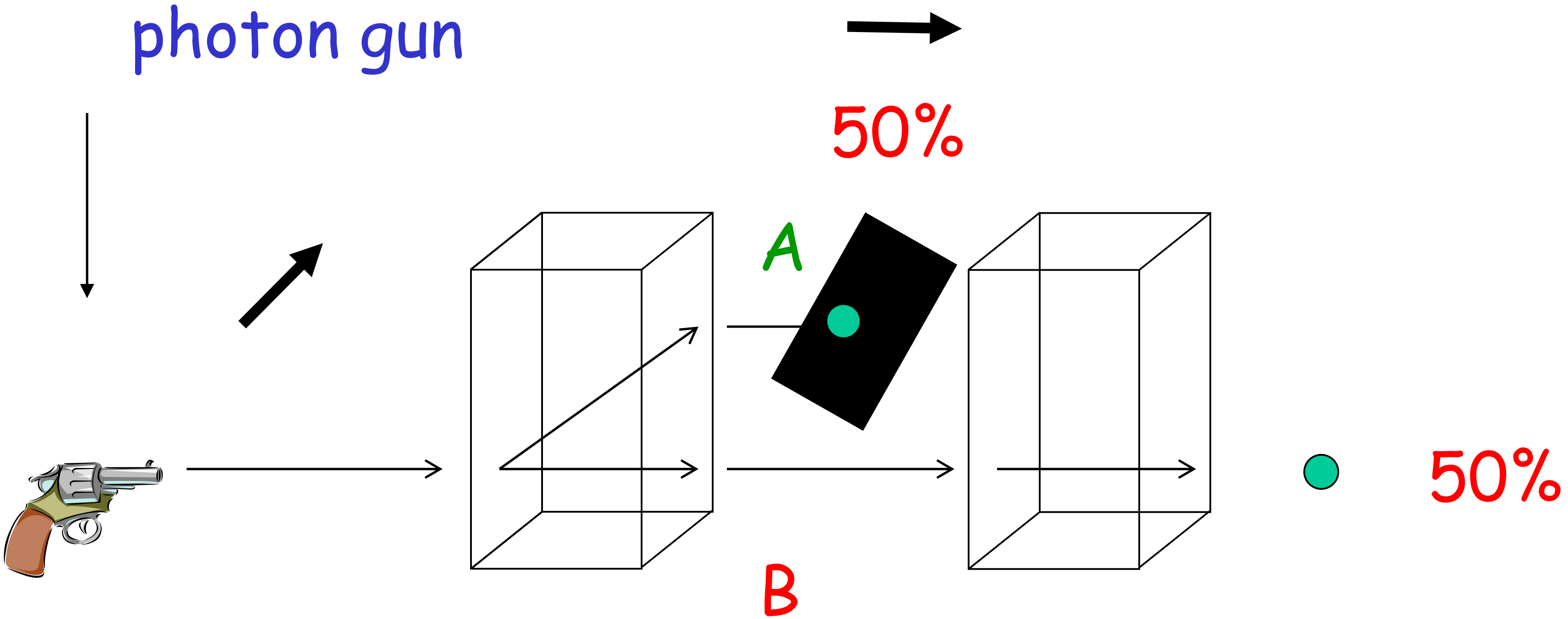
photon took either path A or B



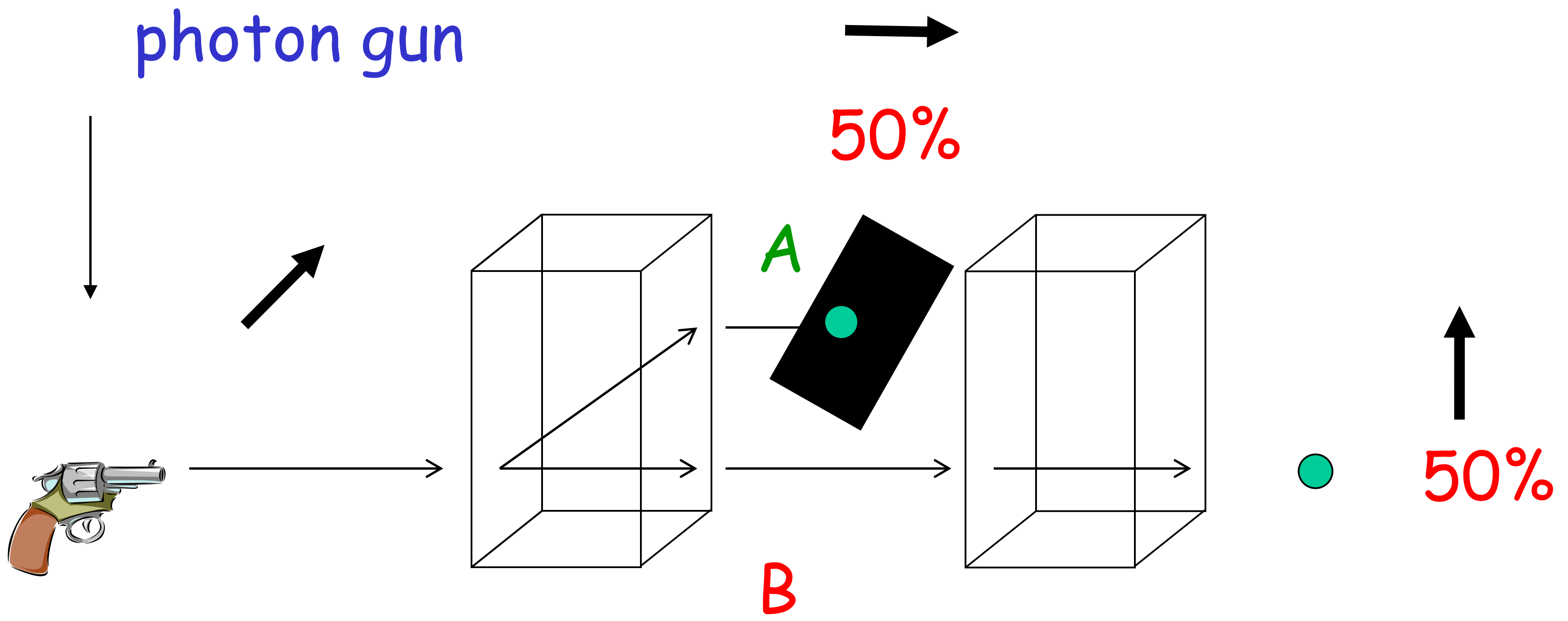
photon took either path A or B



photon took either path A or B

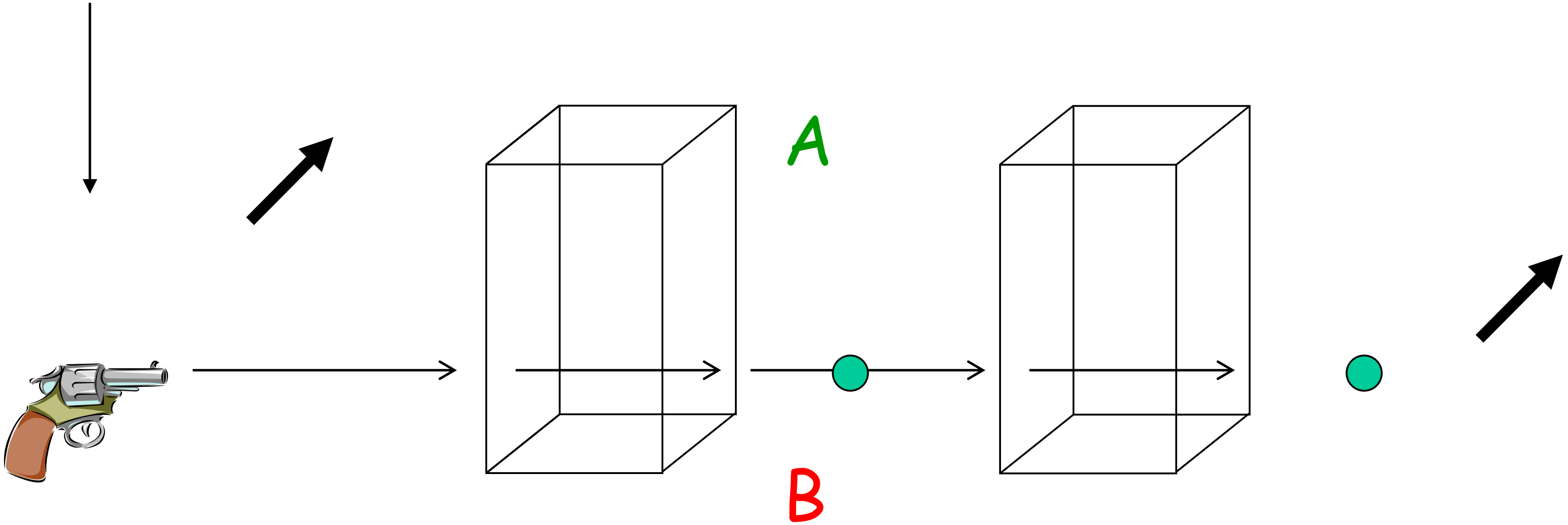


photon took either path A or B

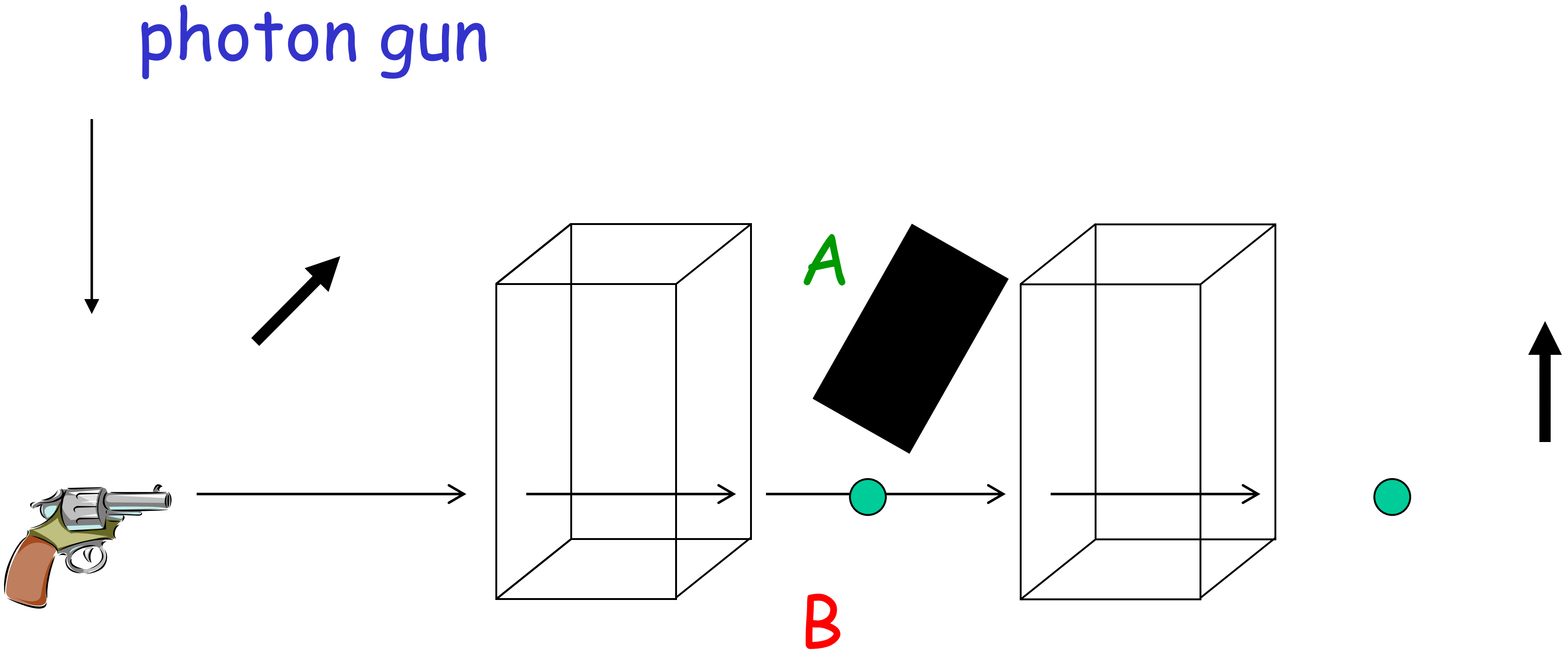


photon took either path A or B

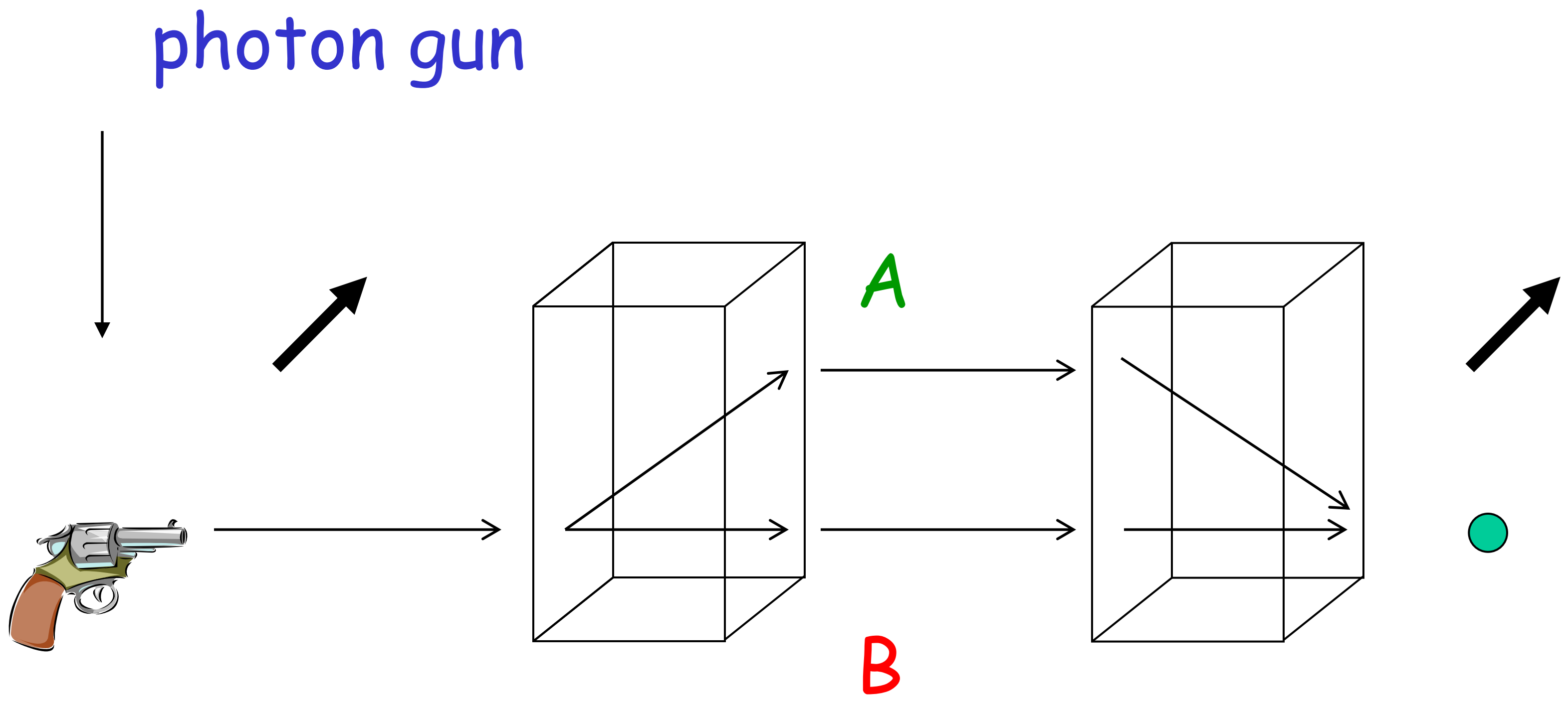
photon gun



photon took path B

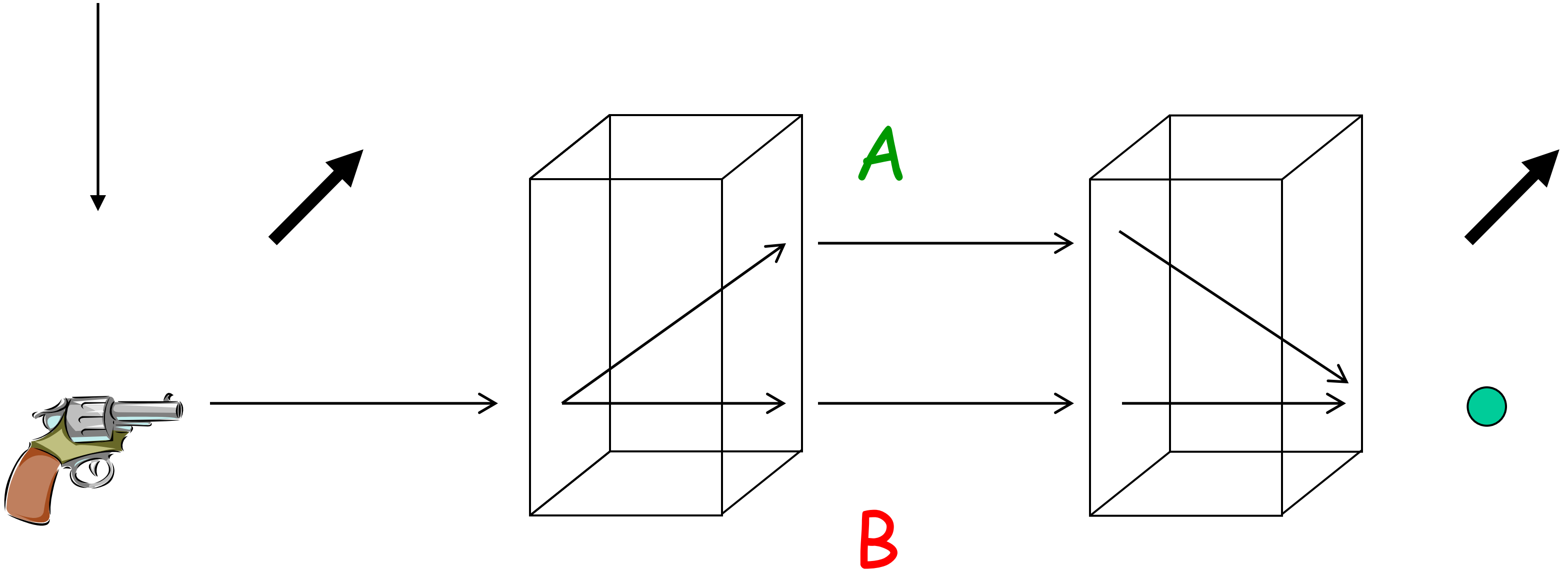


photon took path B



photon took either path A or B

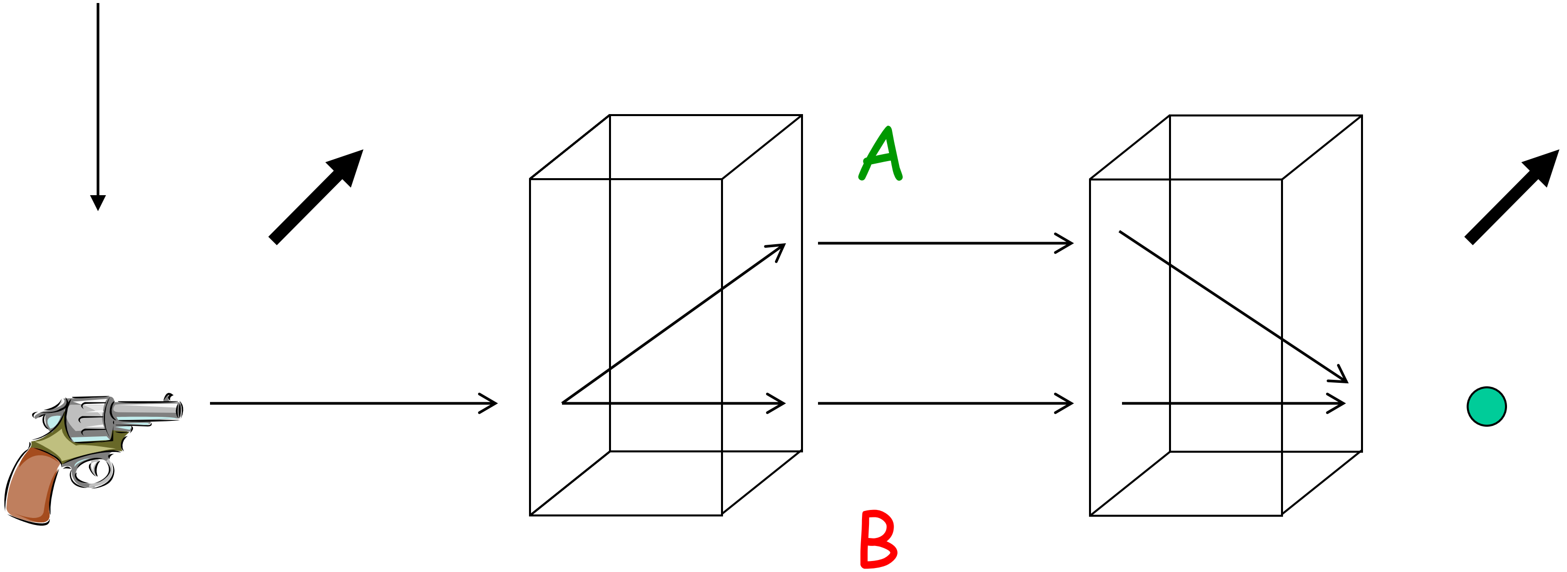
photon gun



~~photon took either path A or B~~

Quantum Mechanics

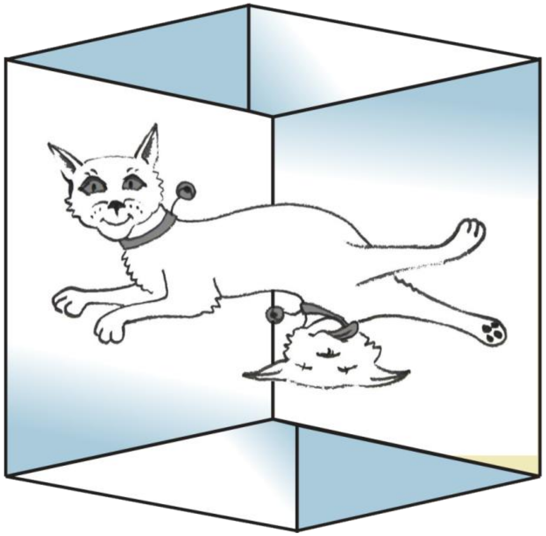
photon gun



photon was in a superposition of path A and B

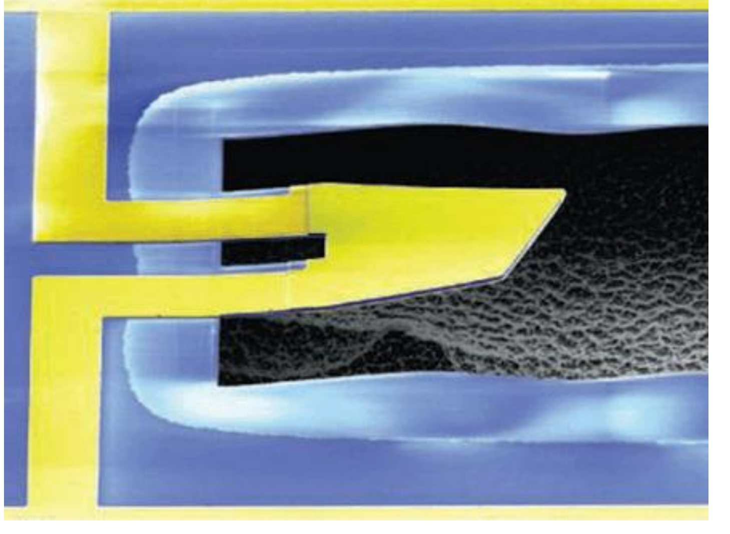
Superposition

- object in *more* states at *same* time
- Schrödinger's cat: dead *and* alive
- Experimentally verified:
  - small systems, e.g. photons
  - larger systems, molecules
- Proposed experiment:
  - virus in superposition
  - motion & stillness



Science's breakthrough of the year 2010: The first quantum machine

"Physicists [...] designed the machine—a tiny metal paddle of semiconductor, visible to the naked eye—and coaxed it into dancing with a quantum groove."



Springboard. Scientists achieved the simplest quantum states of motion with this vibrating device, which is as long as a hair is wide

Quotes

- Quantum mechanics is magic. [Daniel Greenberger]
- Everything we call real is made of things that cannot be regarded as real. [Niels Bohr]
- Those who are not shocked when they first come across quantum theory cannot possibly have understood it. [Niels Bohr]
- If you are not completely confused by quantum mechanics, you do not understand it. [John Wheeler]
- It is safe to say that nobody understands quantum mechanics. [Richard Feynman]
- If [quantum theory] is correct, it signifies the end of physics as a science. [Albert Einstein]
- I do not like [quantum mechanics], and I am sorry I ever had anything to do with it. [Erwin Schrödinger]
- Quantum mechanics makes absolutely no sense. [Roger Penrose]

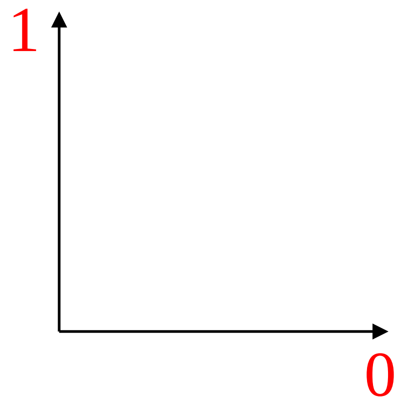
Quantum Mechanics

- Most complete description of Nature to date
- Superposition principle:
  - "particle can be at two positions at the same time"
- Interference:
  - "particle in superposition can interfere with itself"

Superposition

Classical Bit: **0** or **1**

Quantum Bit: Superposition of **0** and **1**

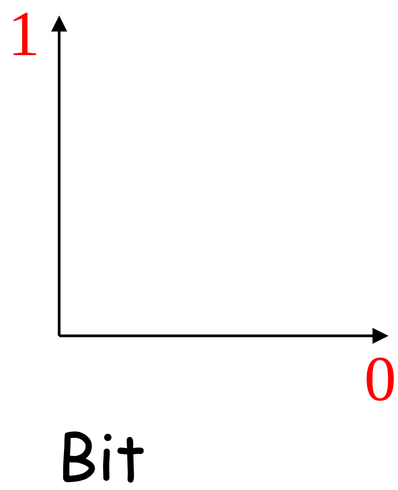


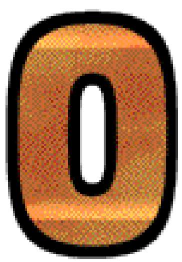
Bit

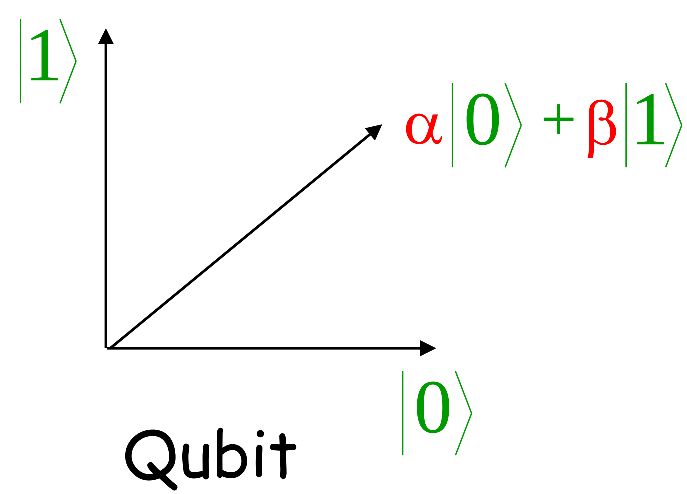
Superposition

Classical Bit: **0** or **1**

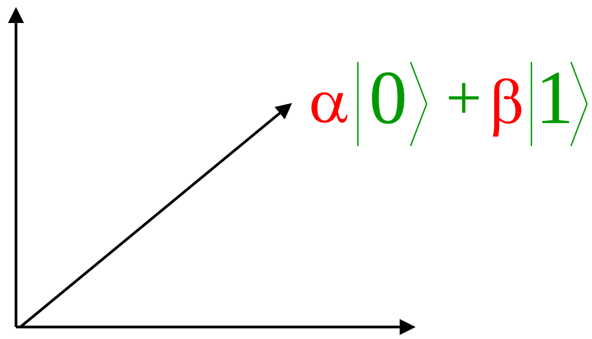
Quantum Bit: Superposition of **0** and **1**







Qubit

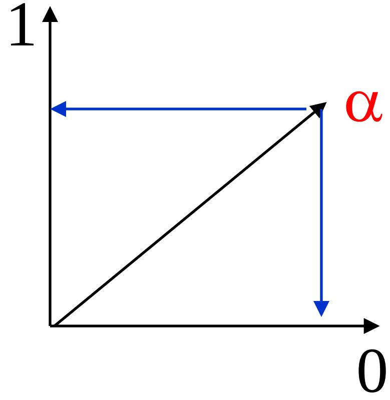


$$\alpha|0\rangle \;+\; \beta|1\rangle$$

amplitudes

Rule: $|\alpha|^2 + |\beta|^2 = 1$,
α, β are complex numbers.

Measurement

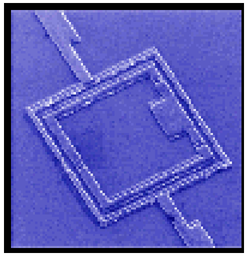


"Projection" on the 0 axis
or 1 axis.

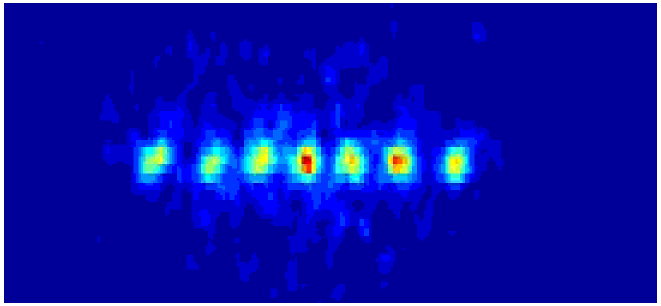
Rule:
observe 0 with probability $|\alpha|^2$
observe 1 with probability $|\beta|^2$

after measurement qubit is 0 or 1

Qubits

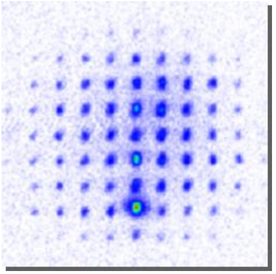


- NMR (10 qubits)
- SQUIDS (1 qubit)
- Trapped Ions (7 qubits)



- Solid state
- Bose-Einstein condensate in optical lattices (30 qubits)
- Cavity QED

  (3 qubits)



Example

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Example

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Measuring ψ: Prob [1] = 1/2
Prob [0] = 1/2

Example

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Measuring ψ: Prob [1] = 1/2
Prob [0] = 1/2

After measurement:

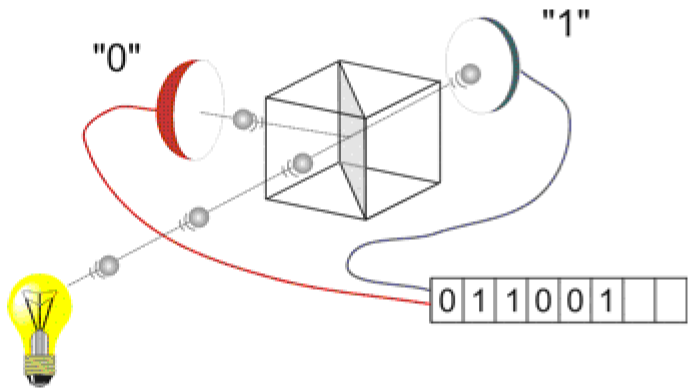
with prob 1/2 $|\psi\rangle = |0\rangle$

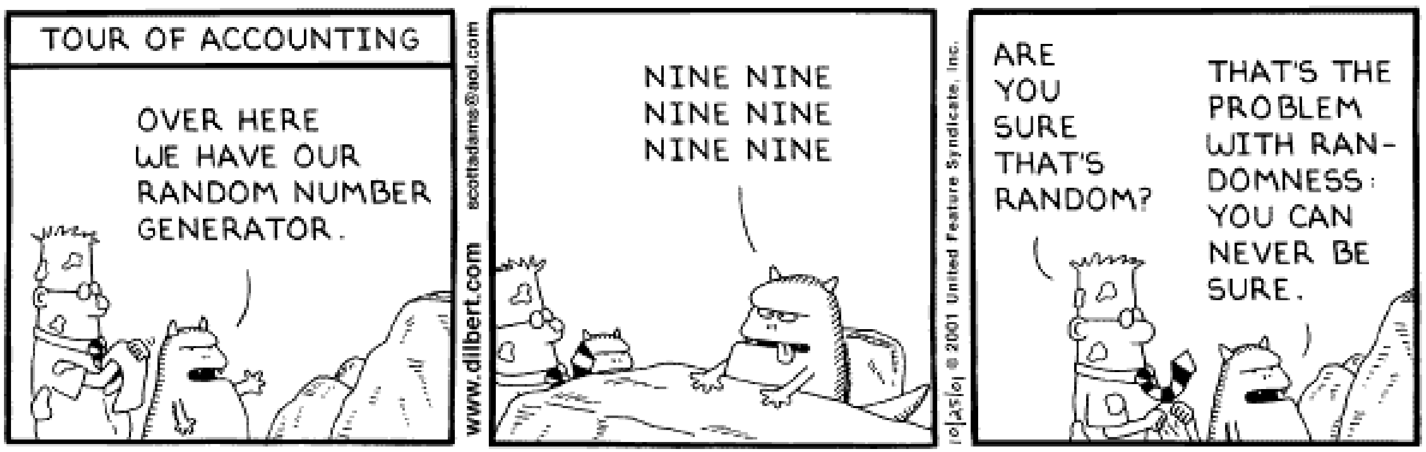
with prob 1/2 $|\psi\rangle = |1\rangle$

Quantis – QUANTUM RANDOM NUMBER GENERATOR

Although random numbers are required in many applications, their generation is often overlooked. Being deterministic, computers are not capable of producing random numbers. A physical source of randomness is necessary. Quantum physics being intrinsically random, it is natural to exploit a quantum process for such a source. Quantum random number generators have the advantage over conventional randomness sources of being invulnerable to environmental perturbations and of allowing live status verification.

Quantis is a physical random number generator exploiting an elementary quantum optics process. Photons - light particles - are sent one by one onto a semi-transparent mirror and detected. The exclusive events (reflection - transmission) are associated to "0" - "1" bit values.




TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
scottadams@aol.com
www.dilbert.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.

Qubit

$$\alpha|0\rangle + \beta|1\rangle$$

$$\alpha, \beta \in \mathbb{C}$$

$$|\alpha|^2 + |\beta|^2 = 1$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad \begin{bmatrix} 0 \\ 1 \end{bmatrix} \qquad \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Measurement:

observe 0 with probability $|\alpha|^2$

observe 1 with probability $|\beta|^2$

Tensor Products

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \quad \otimes \quad (\alpha_2|0\rangle + \beta_2|1\rangle)$$

$$\begin{bmatrix}\alpha_1\\ \beta_1\end{bmatrix} \otimes \begin{bmatrix}\alpha_2\\ \beta_2\end{bmatrix} = \begin{bmatrix}\alpha_1\alpha_2\\ \alpha_1\beta_2\\ \beta_1\alpha_2\\ \beta_1\beta_2\end{bmatrix}$$

$$|\alpha_1\alpha_2|^2 + |\alpha_1\beta_2|^2 + |\beta_1\alpha_2|^2 + |\beta_1\beta_2|^2 = 1$$

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \quad B = \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} a_{1,1}\cdot B & a_{1,2}\cdot B \\ a_{2,1}\cdot B & a_{2,2}\cdot B \end{bmatrix}$$

basis states

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

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

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

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

$$\boxed{|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle}$$

Two Qubits

$$\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$$

$$|\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 + |\alpha_4|^2 = 1$$

Prob[00] = $|\alpha_1|^2$, Prob[01] = $|\alpha_2|^2$,

Prob[10] = $|\alpha_3|^2$, Prob[11] = $|\alpha_4|^2$,

n Qubits

$$\sum_{x=0}^{2^n-1} \alpha_x |x\rangle \qquad \sum_{x=0}^{2^n-1} |\alpha_x|^2 = 1$$

$x = x_1 \ldots x_n$

Prob[observing y] = $|\alpha_y|^2$

Dirac Notation

- $$|a\rangle = \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$ norm 1 vector

- $$\langle a| =_{def} |a\rangle^*$$ complex conjugate transpose

- $$\langle a| = [\overline{a_1} \cdots \overline{a_n}]$$

inner product

$$\langle a| = [\overline{a_1} \cdots \overline{a_n}]$$

$$|b\rangle = \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

$$\langle a \mid b\rangle = [\overline{a_1} \cdots \overline{a_n}] \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$

inner product
between
$|a\rangle$ and $|b\rangle$

inner product(2)

$$\langle a \mid a \rangle = [\overline{a_1} \cdots \overline{a_n}] \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix} =$$

$$\sum_{i=1}^{n} \overline{a_i} a_i = \sum_{i=1}^{n} |a_i|^2 = 1$$

Evolution

Evolution

1. Postulate: the evolution is a linear operation
2. quantum states maped to quantum states
   - 1 & 2 implies that operation is Unitary

- length preserving
- rotations.
- $U U^* = I$.   (U* : complex conjugate, transpose)

Hadamard Transform

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$H^* = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

$$H \times H^* = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Hadamard on 0

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \times \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2}+\frac{1}{2} \\ \frac{1}{2}-\frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

interference

$$\psi = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{H} |0\rangle$$

Hadamard on 0

$$\boldsymbol{H} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \times \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2}+\frac{1}{2} \\ \frac{1}{2}-\frac{1}{2} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

interference

$$\psi = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \overset{H}{\longleftrightarrow} \quad |0\rangle$$

Hadamard on 1

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \times \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} - \frac{1}{2} \\ \frac{1}{2} + \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\psi = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{\quad H \quad} |1\rangle$$

Hadamard on 1

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \times \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} - \frac{1}{2} \\ \frac{1}{2} + \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$\psi = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \overset{H}{\longleftrightarrow} |1\rangle$$

Hadamard on n qubits

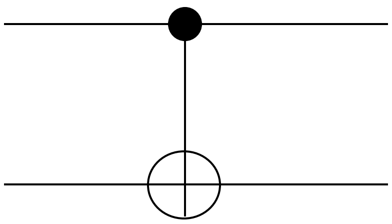
$$|y\rangle \overset{H^{\otimes n}}{\longleftrightarrow} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x \cdot y} |x\rangle$$

$y = y_1 \cdots y_n$

inner product modulo 2

$$|0^n\rangle \overset{H^{\otimes n}}{\longleftrightarrow} \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

C-not Gate



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

$$|00\rangle \mapsto |00\rangle$$
$$|01\rangle \mapsto |01\rangle$$
$$|10\rangle \mapsto |11\rangle$$
$$|11\rangle \mapsto |10\rangle$$

defined on basis states

$\Rightarrow$

defined on superpositions

No Cloning

no cloning

it is not possible to copy an unknown qubit [Wooters & Zurek'82, Dieks'82]

$$U_c[(\alpha|0\rangle + \beta 1) \otimes |0\rangle] \quad = \quad (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

$$\| \qquad\qquad\qquad\qquad \|$$

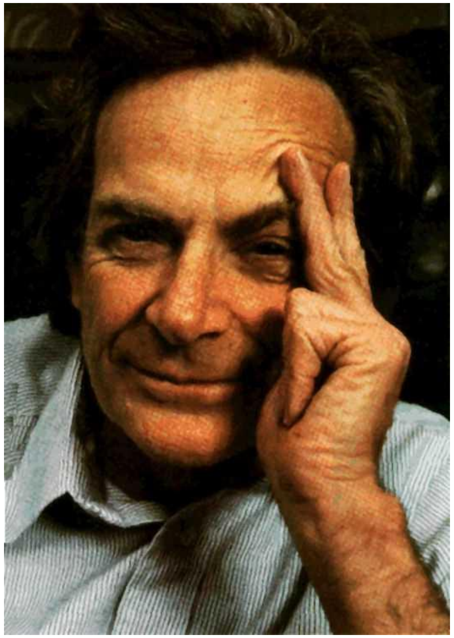
$$U_c[\alpha|00\rangle + \beta|10\rangle] \qquad \boxed{\begin{array}{c}\alpha\alpha|00\rangle + \alpha\beta|01\rangle + \\ \beta\alpha|10\rangle + \beta\beta|11\rangle\end{array}}$$

$$\| \qquad\qquad\qquad\qquad \nparallel$$

$$U_c\alpha|00\rangle + U_c\beta|10\rangle \quad = \quad \boxed{\alpha|00\rangle + \beta|11\rangle}$$

equal only if: α = 0 & β =1 or
α = 1 & β =0

Quantum Algorithms



Feynman

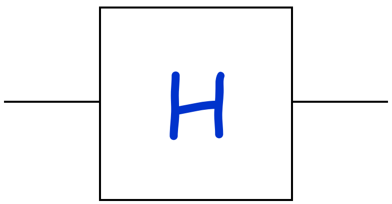
Deutsch '85

Quantum Algorithms

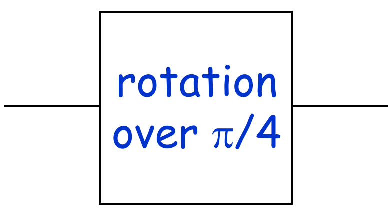
- Quantum Program:
  - unitary operation
  - measurement

Feynman
Deutsch '85

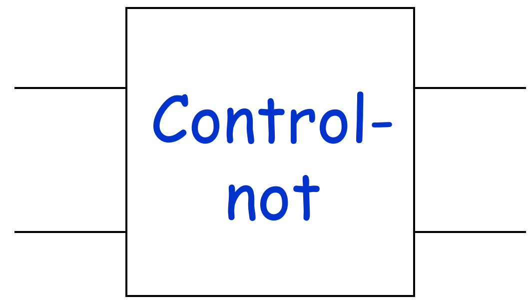
Universal set of Gates



$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$



$$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$



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

can implement ***any*** Unitary operation

Quantum Algorithms

- Quantum Program:
  - unitary operation
  - measurement
- Fast:
  - unitary implemented by polynomially many "H", "$\pi/4$", and "C-not"
  - Efficient Quantum Computation: BQP

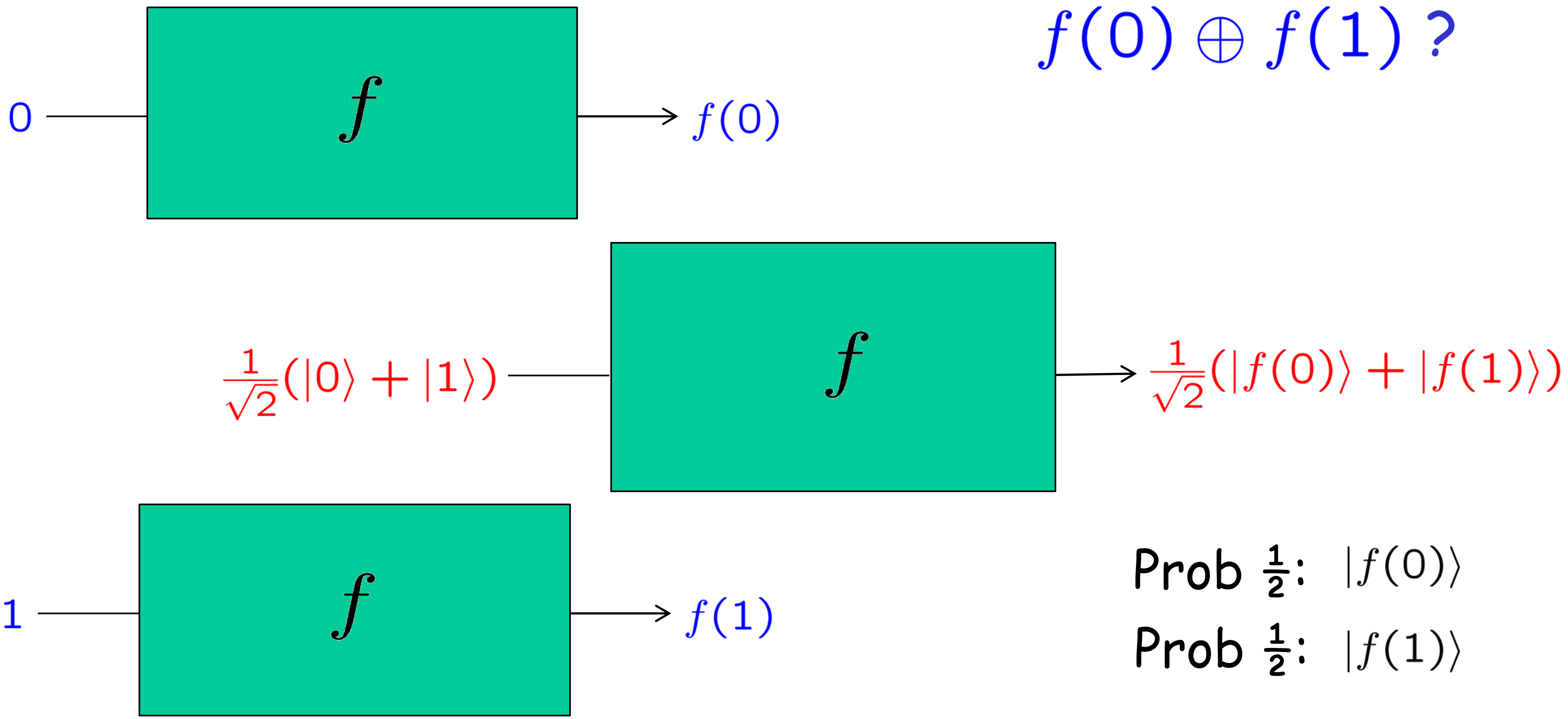
Early Quantum Algorithms

Deutsch's Problem

$f : \{0,1\} \to \{0,1\}$

compute

$f(0) \oplus f(1)$?

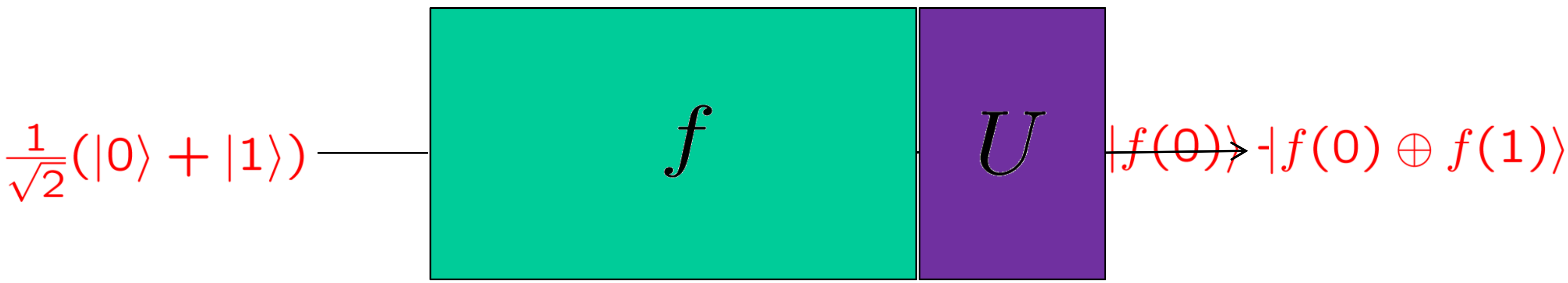


Prob $\frac{1}{2}$: $|f(0)\rangle$

Prob $\frac{1}{2}$: $|f(1)\rangle$

Deutsch's Algorithm

$f : \{0,1\} \rightarrow \{0,1\}$ $\qquad$ $f(0) \oplus f(1)$



Additional quantum operation

Prob $\frac{1}{2}$: $|f(0)\rangle$

Prob $\frac{1}{2}$: $|f(1)\rangle$

once computation time of f

More detail

Parity Problem

X_0 and X_1

- compute $X_0 \oplus X_1$

- Classically 2 queries
- Quantum 1 query!

Quantum query

- Querying X_0 $\quad |0\rangle \longrightarrow (-1)^{X_0}|0\rangle$
- Querying X_1 $\quad |1\rangle \longrightarrow (-1)^{X_1}|1\rangle$

- General query:

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow$$

$$\alpha(-1)^{X_0}|1\rangle + \beta(-1)^{X_1}|1\rangle$$

$$|\alpha|^2 + |\beta|^2 = 1$$

Deutsch's Algorithm for Parity

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$$

$$\xrightarrow{\text{Query}} \frac{1}{\sqrt{2}}[(-1)^{X_0}|0\rangle + (-1)^{X_1}|1\rangle]$$

$$\xrightarrow{H} \frac{1}{2}[(-1)^{X_0}(|0\rangle + |1\rangle) + (-1)^{X_1}(|0\rangle - |1\rangle)]$$

cont.

$$\frac{1}{2}[(-1)^{X_0}(|0\rangle + |1\rangle) + (-1)^{X_1}(|0\rangle - |1\rangle)]$$

cont.

$$\frac{1}{2}[(-1)^{X_0}(|0\rangle + |1\rangle) + (-1)^{X_1}(|0\rangle - |1\rangle)]$$

$$\frac{1}{2}[(-1)^{X_0} + (-1)^{X_1}|0\rangle +$$

cont.

$$\frac{1}{2}[(-1)^{X_0}(|0\rangle + |1\rangle) + (-1)^{X_1}(|0\rangle - |1\rangle)]$$

$$\frac{1}{2}[((-1)^{X_0} + (-1)^{X_1})|0\rangle +$$

$$((-1)^{X_0} - (-1)^{X_1})|1\rangle]$$

cont.

$$\frac{1}{2}[(-1)^{X_0}(|0\rangle + |1\rangle) + (-1)^{X_1}(|0\rangle - |1\rangle)]$$

$$\frac{1}{2}[(-1)^{X_0} + (-1)^{X_1}|0\rangle +$$

$$(-1)^{X_0} - (-1)^{X_1}|1\rangle]$$

$X_0 \oplus X_1 = 0$

$X_0 = 0$ & $X_1 = 0$ or

$X_0 = 1$ & $X_1 = 1$

See only $|0\rangle$

cont.

$$\frac{1}{2}[(-1)^{X_0}(|0\rangle + |1\rangle) + (-1)^{X_1}(|0\rangle - |1\rangle)]$$

$$\frac{1}{2}[(-1)^{X_0} + (-1)^{X_1}|0\rangle +$$

$$(-1)^{X_0} - (-1)^{X_1}|1\rangle]$$

$X_0 \oplus X_1 = 1$

$X_0 = 0$ & $X_1 = 1$ or

$X_0 = 1$ & $X_1 = 0$

See only $|1\rangle$

cont.

$$\frac{1}{2}[(-1)^{X_0}(|0\rangle + |1\rangle) + (-1)^{X_1}(|0\rangle - |1\rangle)]$$

$$\boxed{\frac{1}{2}[(-1)^{X_0} + (-1)^{X_1}|0\rangle + (-1)^{X_0} - (-1)^{X_1}|1\rangle]}$$

$X_0 \oplus X_1 = 0$ See only $|0\rangle$

$X_0 \oplus X_1 = 1$ See only $|1\rangle$

Extension:
Constant or Balanced

Deutsch-Jozsa Problem

- Promise on X:
  - (1) For all i: $X_i = 1$ (0) or (constant)
  - (2) $|\{i \mid X_i = 1\}| = |\{j \mid X_j = 0\}|$ (balanced)
- Goal: determine case (1) or (2)
- Classical: N/2 + 1 probes.
- Quantum: 1 probe.

Quantum query

- Querying X_i $$|i\rangle \longrightarrow (-1)^{X_i}|i\rangle$$

- General query:

$$\sum_i \alpha_i|i\rangle \longrightarrow \sum_i (-1)^{X_i}\alpha_i|i\rangle$$

$$\sum_i |\alpha_i|^2 = 1$$

Deutsch-Jozsa Algorithm

(1) $$|0^n\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

(2) $$\xrightarrow{\text{Query}} \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{X_i} |i\rangle$$

(3) $$\xrightarrow{H^{\otimes n}} \frac{1}{2^n} \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} (-1)^{X_i \oplus (i \cdot j)} |j\rangle$$

Deutsch-Jozsa cont.

$$\frac{1}{2^n}\sum_{i=0}^{2^n-1}\sum_{j=0}^{2^n-1}(-1)^{X_i\oplus(i\cdot j)}|j\rangle$$

measure state $|0^n\rangle$

$$\frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{X_i}|0^n\rangle$$

Constant:
see $|0^n\rangle$ with prob. 1

Balanced:
see $|0^n\rangle$ with prob. 0

Quantum Algorithms

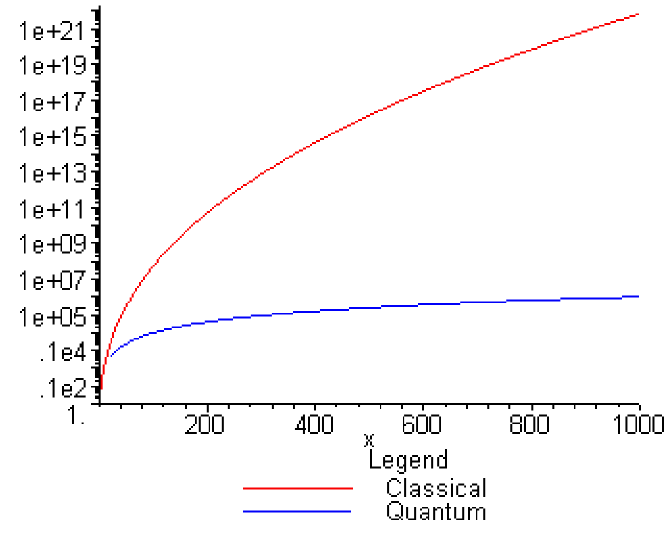
- Deutsch-Jozsa
- Simon's algorithm
- Shor's factoring algorithm
- Grover's search algorithm
- Quantum Random Walk

factorization

- Factor number in prime factors
  87 = 3 * 29
- Classical Computer : Exponential time
- Quantum Computer : Poly-time: n^2

[Shor'94]

- For a 300 digit number
  - Classical: >100 years
  - Quantum: 1 minute



impact

- Safety of modern cryptography based on exponential slowness of factorization
- RSA, electronic commerce, internet…

$\Rightarrow$ Quantum computer destroys this!

Shor's Algorithm

- factoring a number N reduces to period finding problem: x find smallest r such that $x^r \bmod N = 1$
- fast quantum algorithm for period finding
- classical post processing to obtain factor of N

Fourier transform

- Fourier transform F over Z_{2^m}

$$|y_1 \ldots y_m\rangle = \sum_{x=0}^{2^m-1} e^{\frac{2\pi i x y}{2^m}} |x\rangle$$

- Fourier transform over Z_{2^m} can be efficiently implemented

period finding for x

(1) $$|0^m\rangle|0^l\rangle \xrightarrow{F_{2^m}} \frac{1}{\sqrt{2^m}}\sum_{j=0}^{2^m-1}|j\rangle|0^l\rangle$$

(2) query

not black box!

$$\frac{1}{\sqrt{2^m}}\sum_{j=0}^{2^m-1}|j\rangle|x^j mod N\rangle$$

(3) $$\xrightarrow{F_{2^m}} \frac{1}{2^n}\sum_{j=0}^{2^m-1}\sum_{k=0}^{2^m-1} e^{\frac{2\pi ijk}{2^m}}|k\rangle|x^j mod N\rangle$$

Grover's Search Algorithm

search problem

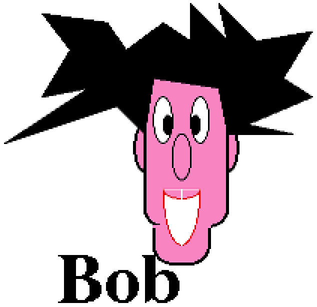
- Input N (=2^n) bits (variables):

  $X = X_1 \quad X_2 \quad X_3 \quad \ldots \quad X_N$

- exists/find i such that $X_i = 1$
- Classically $\Omega(N)$ queries (bounded error)
- Quantum $O(\sqrt{N})$ queries

Quantum Random Walk

- Speedup for different search problems:
  - Element Distinctness
  - AND-OR trees
  - pruning of game trees
  - local search algorithms

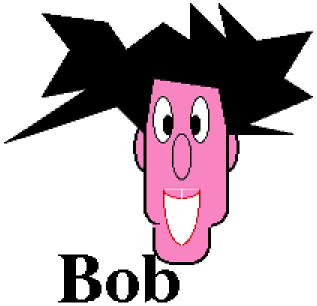


Alice and Bob


OH ALICE... YOU'RE THE ONE FOR ME
BUT BOB... IN A QUANTUM WORLD HOW CAN WE BE SURE?
ψ+ or ψ- ?

Communication?

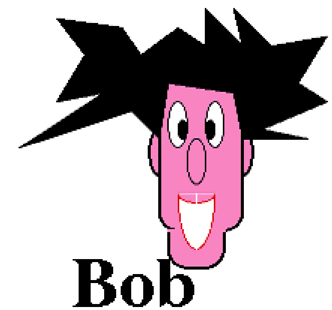
qubits



Communication?

qubits

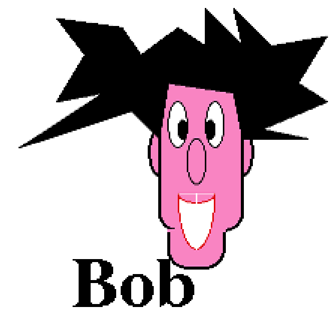
→



Theorem [Holevo'73]
Can not compress k classical bits into k-1 qubits

Communication Complexity

Classical bits

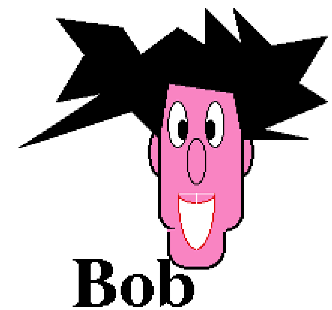


$X = x_1 \, x_2 \, \ldots \, x_N$

$Y = y_1 \, y_2 \, \ldots \, y_N$

Goal: Compute some function $F(X,Y) \longrightarrow \{0,1\}$
minimizing communication bits.

Communication Complexity



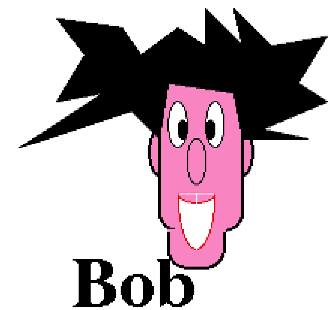
Classical bits

$X = x_1\, x_2 \ldots x_N$

$Y = y_1\, y_2 \ldots y_N$

Goal: Compute some function $F(X,Y) \longrightarrow \{0,1\}$ minimizing communication bits.

Equality



Classical bits

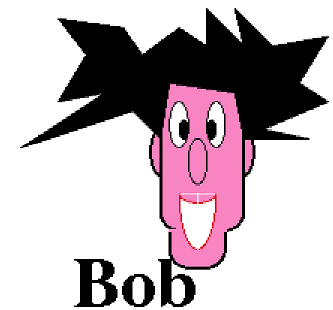
$X = x_1\, x_2 \ldots x_N$

$Y = y_1\, y_2 \ldots y_N$

$F(X,Y) = 1$ iff $X=Y$

Equality

Classical bits



$X = x_1 x_2 \ldots x_N$

$Y = y_1 y_2 \ldots y_N$

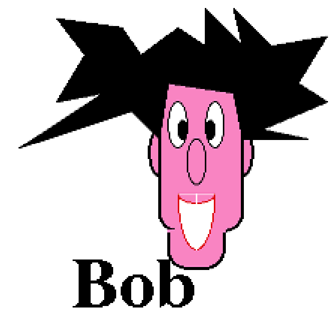
$F(X,Y) = 1$ iff $X=Y$

N bits necessary and sufficient:

$C(EQ) = N$

Quantum Communication Complexity

$F(X,Y) \rightarrow \{0,1\}$



qubits

$\longleftarrow$

$\longrightarrow$

$X = x_1\, x_2 \ldots x_N$ $\qquad$ $Y = y_1\, y_2 \ldots y_N$

$F(X,Y) = 1$ iff $X=Y$

Question: Can qubits reduce communication for certain F's?

Qubits Can Reduce Cost

Theorem [B-Cleve-Wigderson'98]

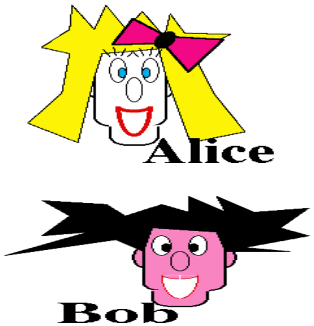
$$EQ'(X,Y) = 1 \text{ iff } X=Y$$

Promise $\Delta(X,Y) = N/2$ or 0

Hamming Distance

- Need $\Omega(N)$ classical bits.
- Can be done with $O(\log(N))$ qubits.

Reduction to D-J



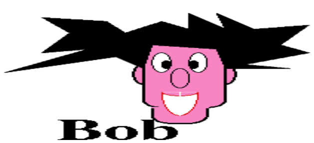
$$
\begin{array}{l}
X_1\ X_2\ \dots\ \dots\ X_N \\
Y_1\ Y_2\ \dots\ \dots\ Y_N \quad \oplus \\
\hline
Z_1\ Z_2\ \dots\ \dots\ Z_N
\end{array}
$$

$\Delta(X,Y) = N/2$
Z
is balanced

$\Delta(X,Y) = 0$
Z
is constant

The quantum protocol

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{X_i} |i\rangle$$



$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{X_i \oplus Y_i} |i\rangle =$$

$$\frac{1}{\sqrt{2^n}} \sum_{i \in \{0,1\}^n} (-1)^{Z_i} |i\rangle$$

Finishes Deutsch-Josza Algorithm

Cost

- Alice sends n= log(N) qubits to Bob
- Bob sends n= log(N) qubits to Alice
- Total cost is 2*log(N)

Classical Lower Bound

Lower Bound

Theorem [Frankl-Rödl'87]*

S,T families of N/2 size sets $\subseteq \{1,\dots,N\}$

for all s,t in S,T : $|s \cap t| \neq N/4$ then:

$$|S| * |T| \leq 4^{0.96N}$$

*$250 problem of Erdös

Lower Bound

Theorem [Frankl-Rödl'87]

S,T families of N/2 size sets $\subseteq \{1,\dots,N\}$

for all s,t in S,T : $|s \cap t| \neq N/4$ then:

$$|S|*|T| \leq 4^{0.96N}$$

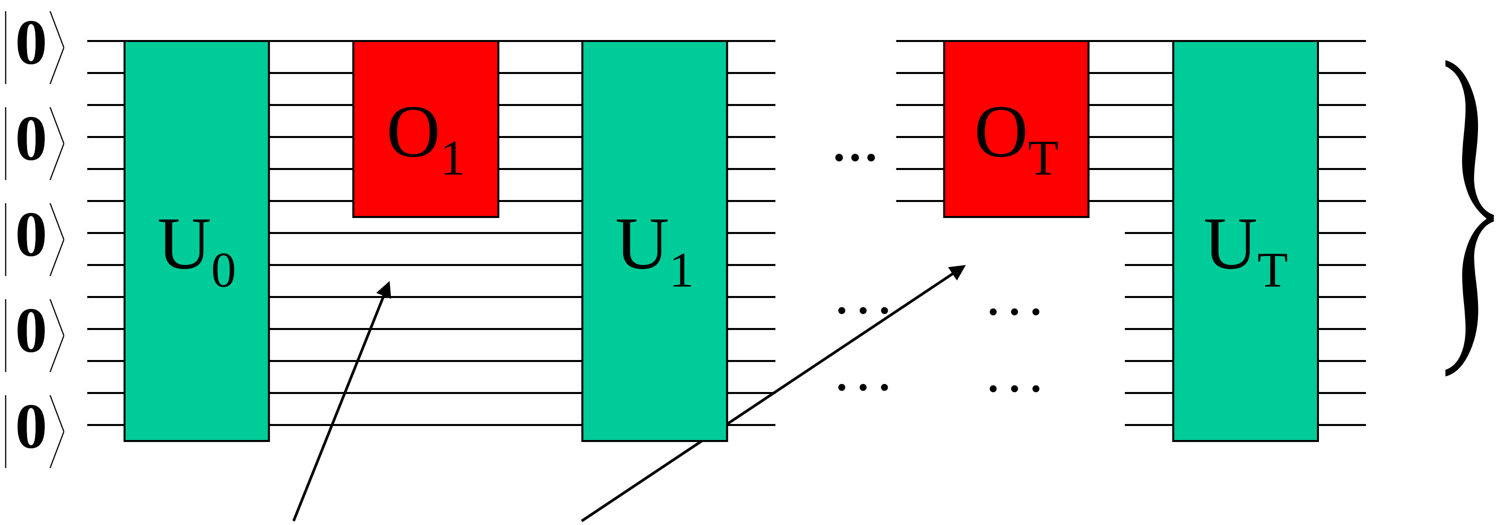
protocol solving EQ' in $\leq N/100$ bits

induces S and T satisfying:

$$|S|*|T| \geq 4^{0.99N}$$

other quantum algorithms…

Quantum Algorithm

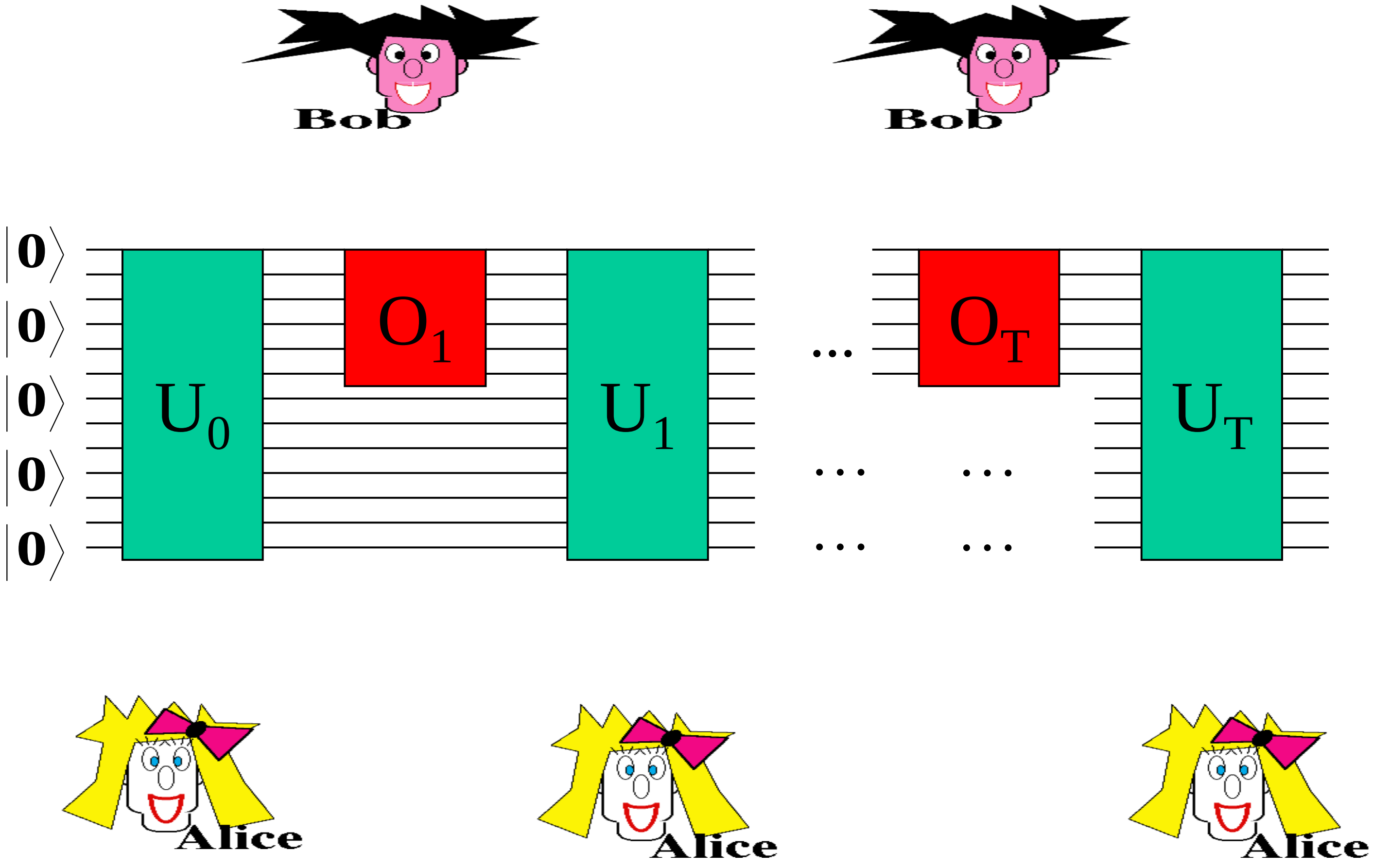


$$\sum_{i=1}^{2^k} \alpha_i |i\rangle$$

Prob [output = 1] $= \sum_{\text{all } i \text{ that end in } 1} |\alpha_i|^2 \begin{cases} >2/3 \\ <1/3 \end{cases}$

Prob [output = 0] = 1 - Prob [output = 1]

Generalization



Grover's Algorithm

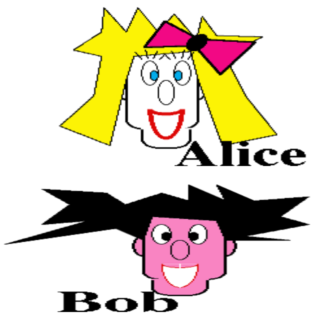
- Find i such that $X_i = 1$

  $OR(X_1,\ldots,X_N)$

- Classical Probabilistic: N/2 queries
- Quantum: $O(\sqrt{N})$ queries
- No promise!

Non-Disjointness

Goal: exists i such that $X_i=1$ and $Y_i=1$?



Grover

$$X_1\ X_2\ \ldots.\ \ldots.\ X_N$$

$$Y_1\ Y_2\ \ldots.\ \ldots.\ Y_N \qquad \wedge$$

$$\overline{\hspace{10em}}$$

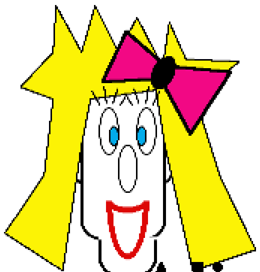
$$Z_1\ Z_2\ \ldots.\ \ldots.\ Z_N$$

Disjointness

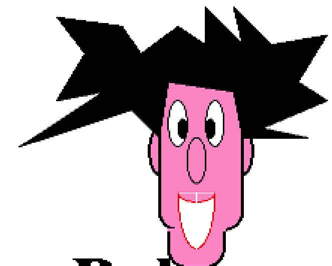
- Bounded Error probabilistic $\Omega(N)$ bits [Kalyanasundaram-Schnitger'87]
- Grover's algorithm + reduction
  $O(\log(N)*\sqrt{N})$ qubits [BCW'98]
  $O(\sqrt{N})$ qubits [AA'04]
  $\Omega(\sqrt{N})$ lower bound [Razborov'03]

CWI

Apointment Scheduling



Alice



Bob

qubits

Quantum: √n qubits communication

Classical: n bits communication

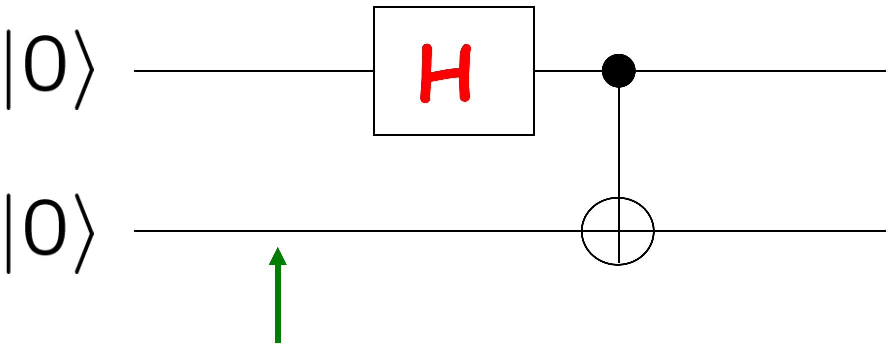
Other Functions

- Exponential gap [Raz'99]
  - $O(\log(N))$ with qubits, $\Omega(N^{1/4})$ bits classically.
  - partial Domain, bounded error
- Exponential gap for other models of communication complexity:
  - limited rounds, SMP etc.
- Quantum Fingerprinting
- Streaming, Learning Theory…

back to physics

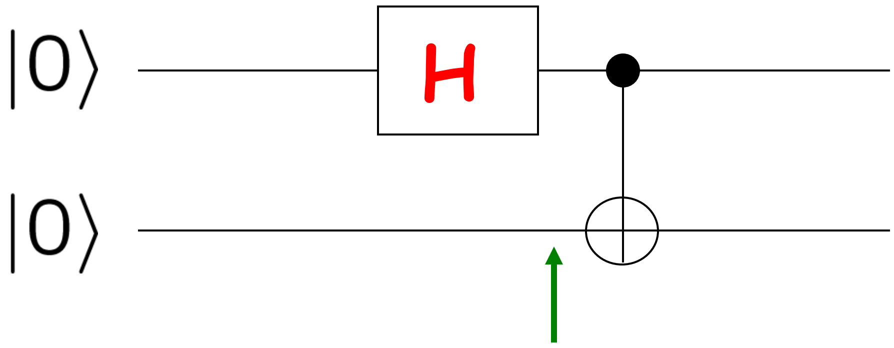
Einstein Podolsky Rosen paradox

simple quantum circuit



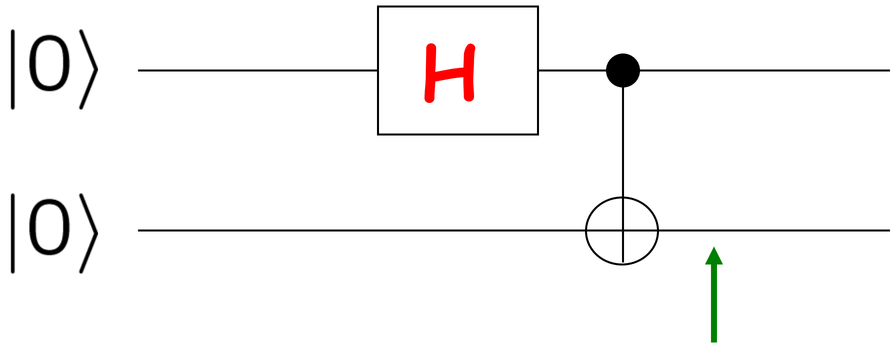
$|00\rangle$

simple quantum circuit



$$|00\rangle \longrightarrow \frac{1}{\sqrt{2}}[|00\rangle + |10\rangle]$$

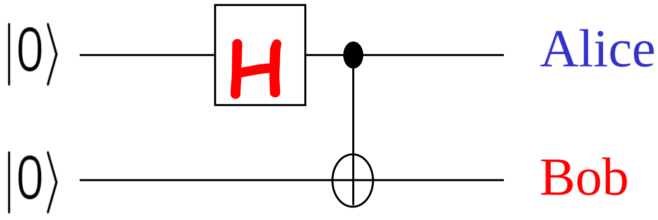
simple quantum circuit



$$|00\rangle \longrightarrow \frac{1}{\sqrt{2}}[|00\rangle + |10\rangle]$$

$$\longrightarrow \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$$

EPR Pair



Bob

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Alice

Entangled:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \neq (\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$$

EPR Pair

Bob

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Alice

if Bob measures: 0/1 with prob. $\frac{1}{2}$

if Alice measures: 0/1 with prob. $\frac{1}{2}$

EPR Pair

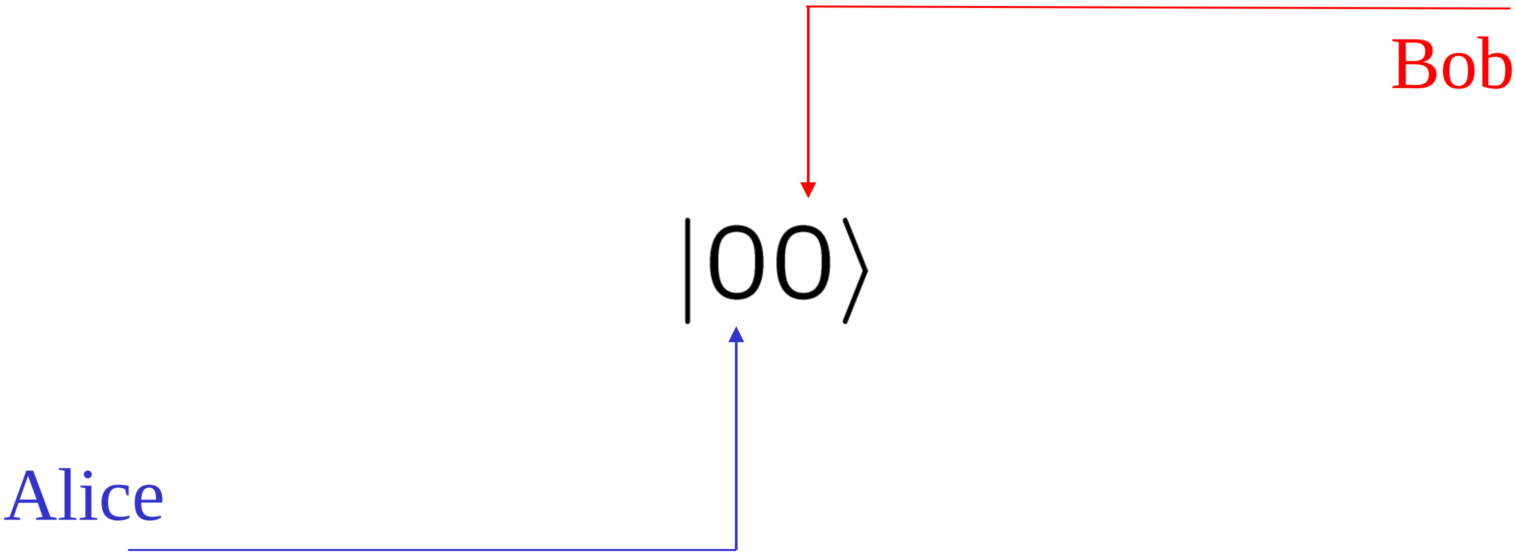
Bob

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Alice

Alice measures: 0
state will collapse!

EPR Pair



Alice measures: 0
state will collapse!

Bob's state has changed!
he will also measure 0

EPR Pair

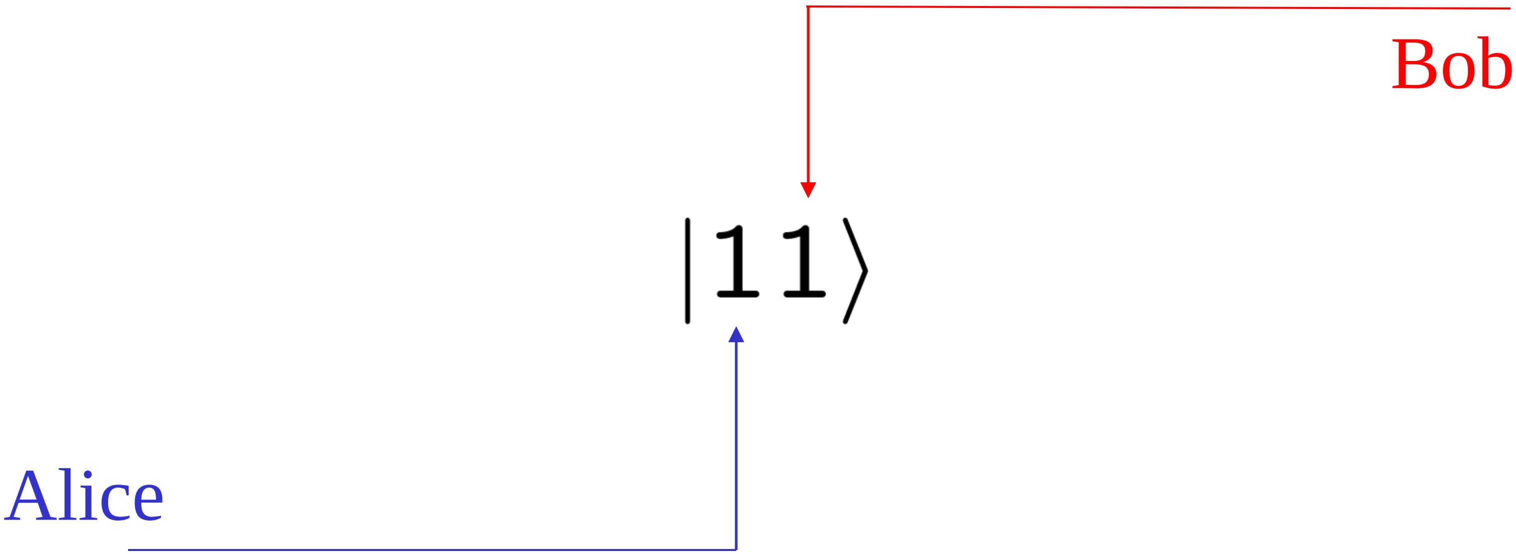
Bob

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Alice

Alice measures: 1
state will collapse!

EPR Pair

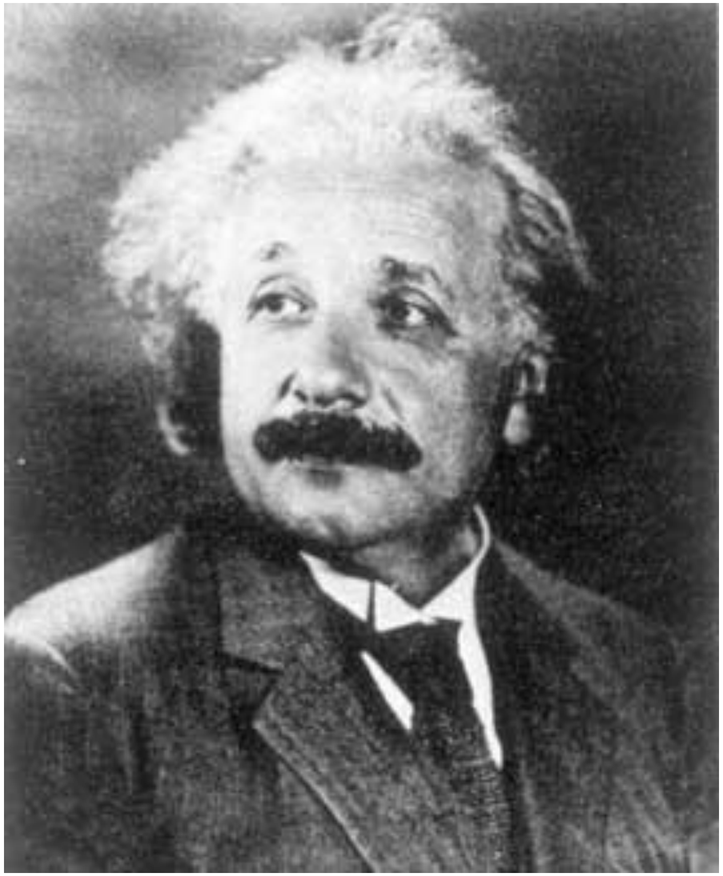


Alice measures: 1
state will collapse!

Bob's state has changed!
he will also measure 1

1) At time of measurement a random outcome is produced
   - instantaneous information transfer
2) Outcome was already present at time of creation of EPR-pair
   - quantum mechanics is incomplete

1935

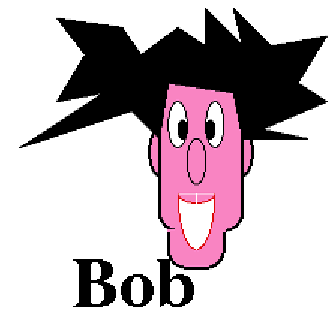


Einstein: nothing, including information, can go faster than the speed of light, hence quantum mechanics is incomplete

Communication

Communication?

bits →



$|0 \cdots\cdots 0\rangle$

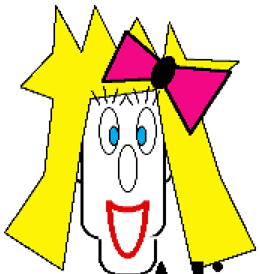
with EPR pairs $+$

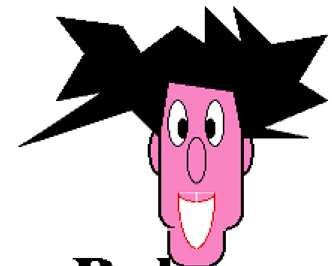
$|1 \cdots\cdots 1\rangle$

Can not compress k bits into k-1 bits

Teleportation

Teleportation


Alice


Bob

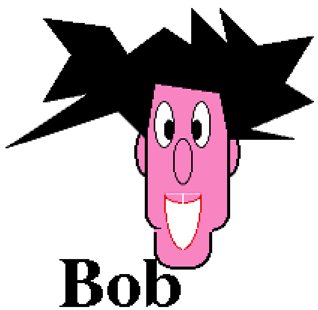
$$\alpha|0\rangle + \beta|1\rangle \longrightarrow$$

$|0$ $0\rangle$

$+$

$|1$ $1\rangle$

Teleportation



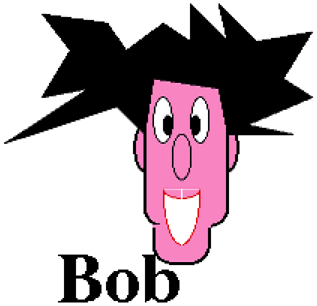
$\left|\Phi_1\right\rangle$

$\left|\Phi_2\right\rangle$

Classical bits:
$b_1\ b_2$

Teleportation

$b_1\ b_2$ →

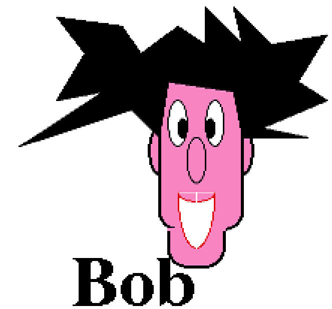


$$|\Phi_1\rangle$$

$$|\Phi_2\rangle$$

Classical bits:
$b_1\ b_2$

Teleportation

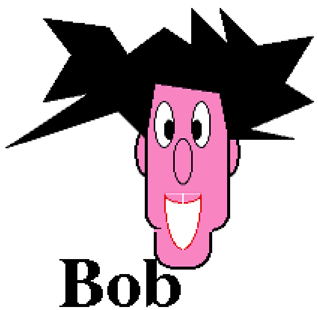


$|\Phi_1\rangle$ → $|\Phi_2\rangle$

Classical bits:
$b_1\ b_2$

$b_1\ b_2$

Teleportation



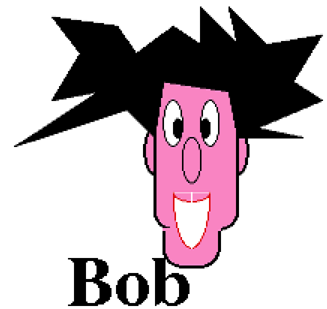
$|\Phi_1\rangle$ → $U_{b_1 b_2}|\Phi_2\rangle$

Classical bits:

$b_1\, b_2$

$b_1\, b_2$

Teleportation



$$|\mathbf{\Phi}_1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle$$

Classical bits:

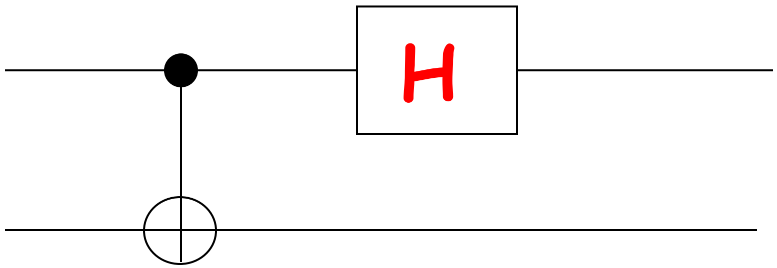
b_1 b_2

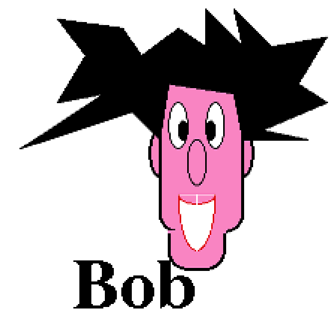
b_1 b_2

Alice's protocol

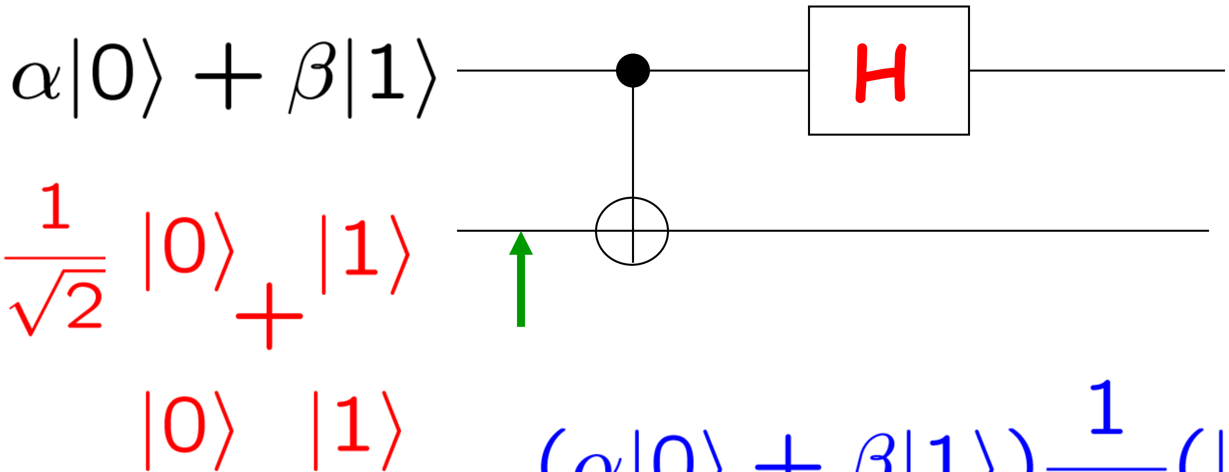
$\alpha|0\rangle + \beta|1\rangle$

$\frac{1}{\sqrt{2}} \left(|0\rangle|0\rangle + |1\rangle|1\rangle \right)$





Alice's protocol



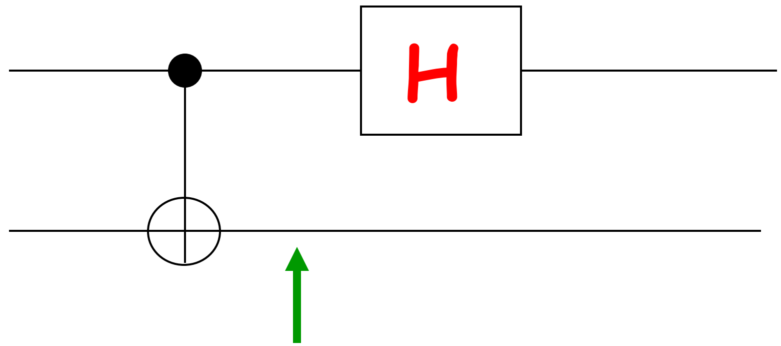
$$(\alpha|0\rangle + \beta|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) =$$

$$\frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |111\rangle)$$

Alice's protocol

$\alpha|0\rangle + \beta|1\rangle$

$\frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right)$



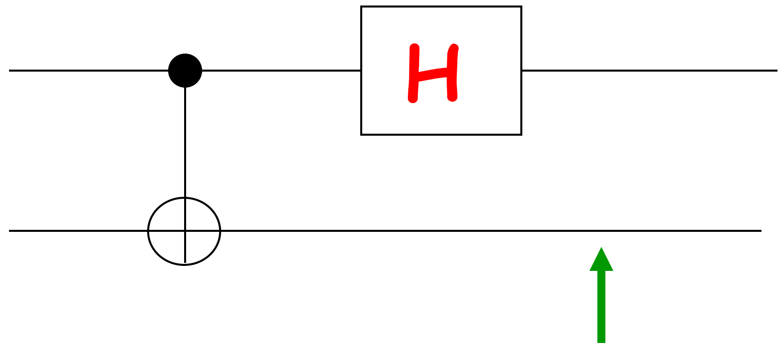
$$\frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|100\rangle + |111\rangle)$$

$$\longrightarrow \quad \frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle)$$

Alice's protocol

$\alpha|0\rangle + \beta|1\rangle$

$\frac{1}{\sqrt{2}}$ $|0\rangle + |1\rangle$



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

$$\frac{\alpha}{\sqrt{2}}(|000\rangle + |011\rangle) + \frac{\beta}{\sqrt{2}}(|110\rangle + |101\rangle)$$

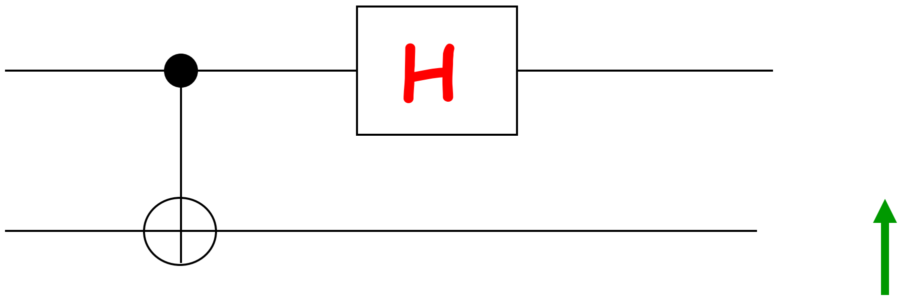
$$\frac{\alpha}{2}(|000\rangle + |100\rangle + |011\rangle + |111\rangle) +$$

$$\frac{\beta}{2}(|010\rangle - |110\rangle + |001\rangle - |101\rangle)$$

Alice's protocol

$$\alpha|0\rangle + \beta|1\rangle$$

$$\frac{1}{\sqrt{2}} \left(|0\rangle|0\rangle + |1\rangle|1\rangle \right)$$

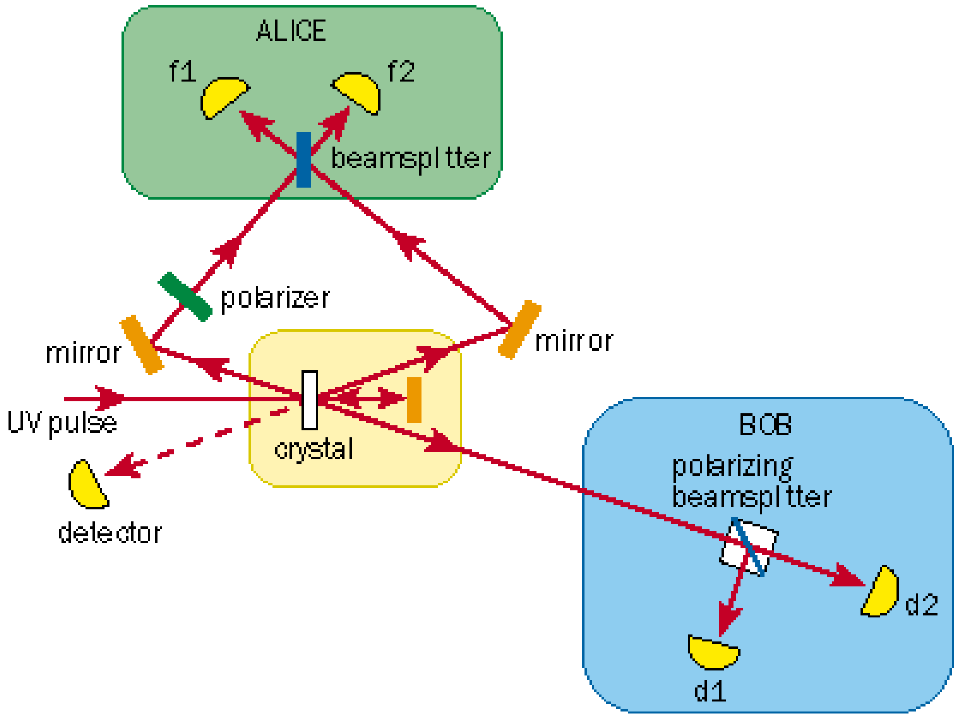


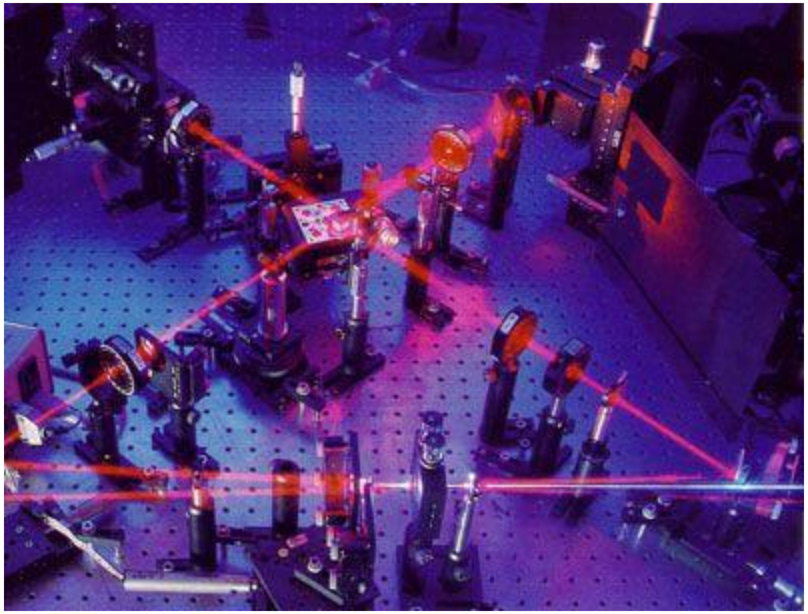
$$\frac{\alpha}{2}(|000\rangle + |100\rangle + |011\rangle + |111\rangle) +$$
$$\frac{\beta}{2}(|010\rangle - |110\rangle + |001\rangle - |101\rangle)$$

$$\frac{1}{2}[|00\rangle(\alpha|0\rangle + \beta|1\rangle)] + \frac{1}{2}[|10\rangle(\alpha|0\rangle - \beta|1\rangle)] +$$
$$\frac{1}{2}[|01\rangle(\alpha|1\rangle + \beta|0\rangle)] + \frac{1}{2}[|11\rangle(\alpha|1\rangle - \beta|0\rangle)]$$

Bob's protocol

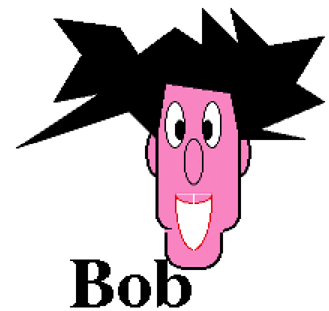
Alice with prob. $\frac{1}{4}$ in one of:	Bob
$\|00\rangle(\alpha\|0\rangle + \beta\|1\rangle)$	do nothing
$\|01\rangle(\alpha\|1\rangle + \beta\|0\rangle)$	bit flip
$\|10\rangle(\alpha\|0\rangle - \beta\|1\rangle)$	phase flip
$\|11\rangle(\alpha\|1\rangle - \beta\|0\rangle)$	bit flip and phase flip


ALICE
f1
f2
beamsplitter
polarizer
mirror
mirror
UV pulse
crystal
detector
BOB
polarizing
beamsplitter
d2
d1



Quantum Communication Complexity

$F(X,Y) \longrightarrow \{0,1\}$



Classical bits

$X = x_1\, x_2 \ldots x_n$ $\qquad$ $Y = y_1\, y_2 \ldots y_n$

$|0 \cdots\cdots 0\rangle$

With EPR pairs $\qquad +$

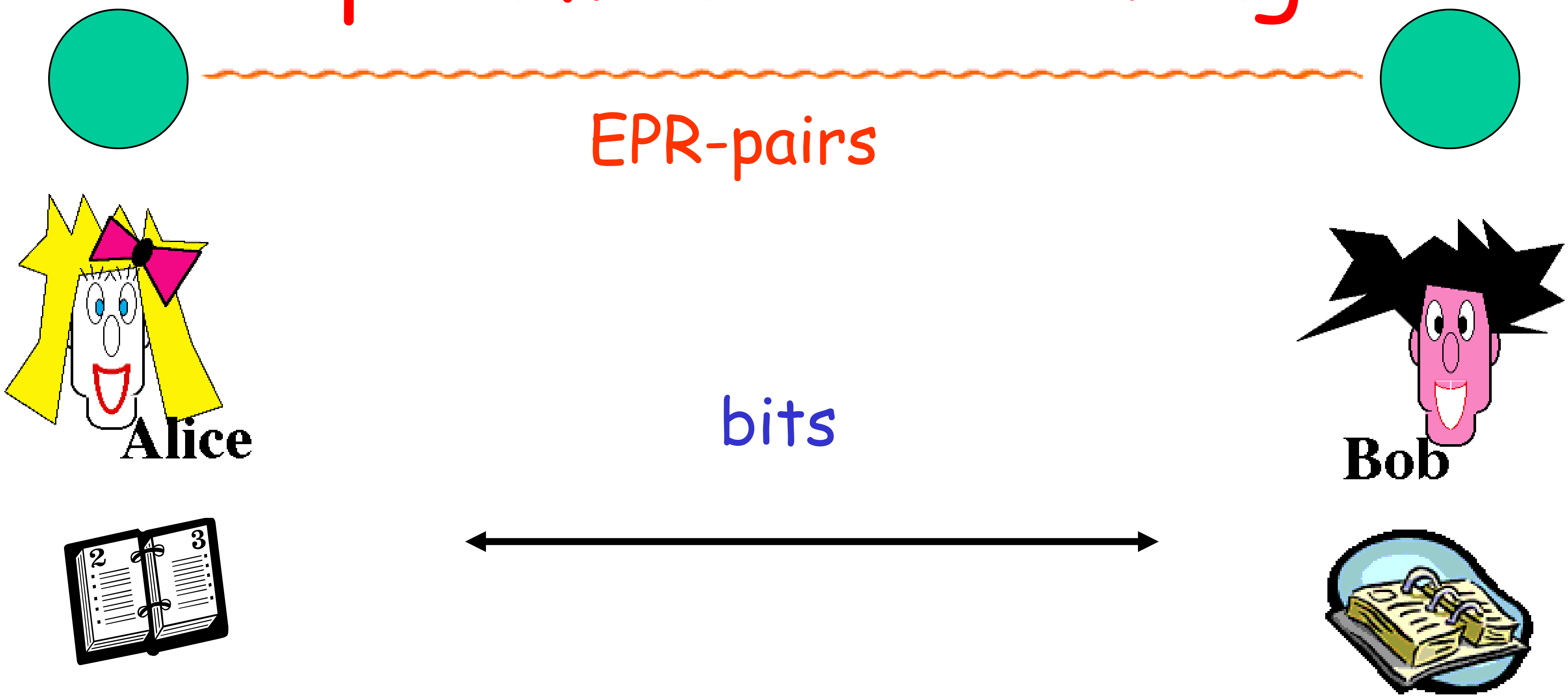
$|1 \cdots\cdots 1\rangle$

Question: Can EPR pairs reduce communication for certain F's?

Teleportation

- Qubit Model can be simulated by EPR model.
- Teleport qubit at cost of 2 classical bits and 1 EPR pair.
- EPR-pairs can reduce communication cost:
  - use qubit protocol +
  - teleportation

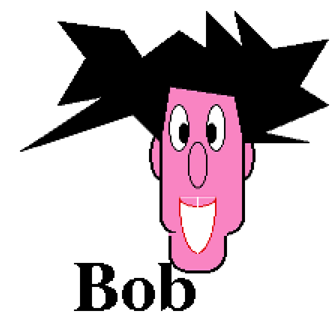
Apoinment Scheduling



Quantum: $\sqrt{n}$ bits communicatie

Classical: n bits communicatie

EPR en information



Alice can not send *information* to Bob, but she can save *information* for certain communication problems

Other Links

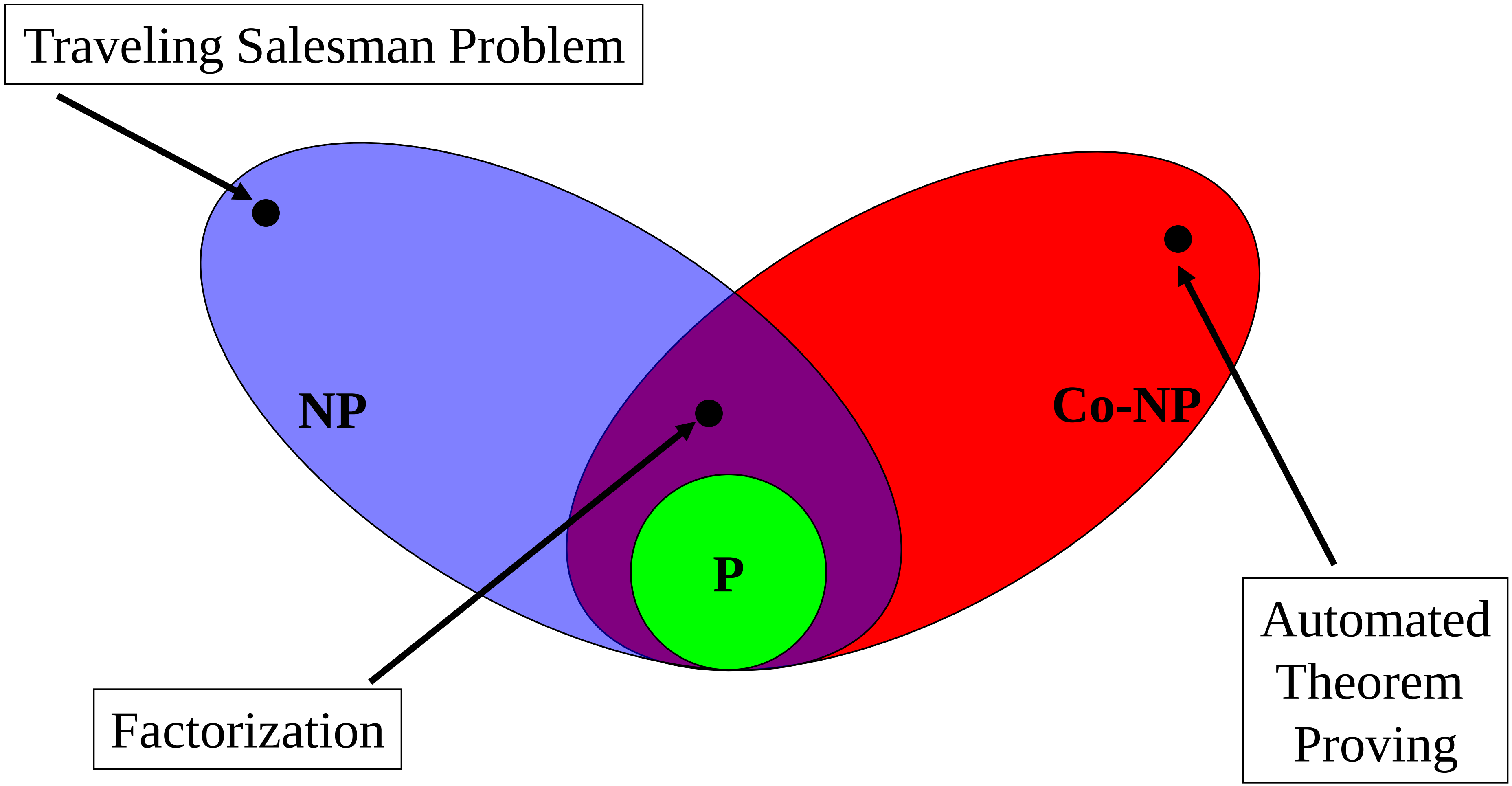
- Quantum Communication Complexity
- Better Non-locality experiments
  - Resistant to noise
  - Resistant to detection loophole
  - Optimality of parameters

Entanglement

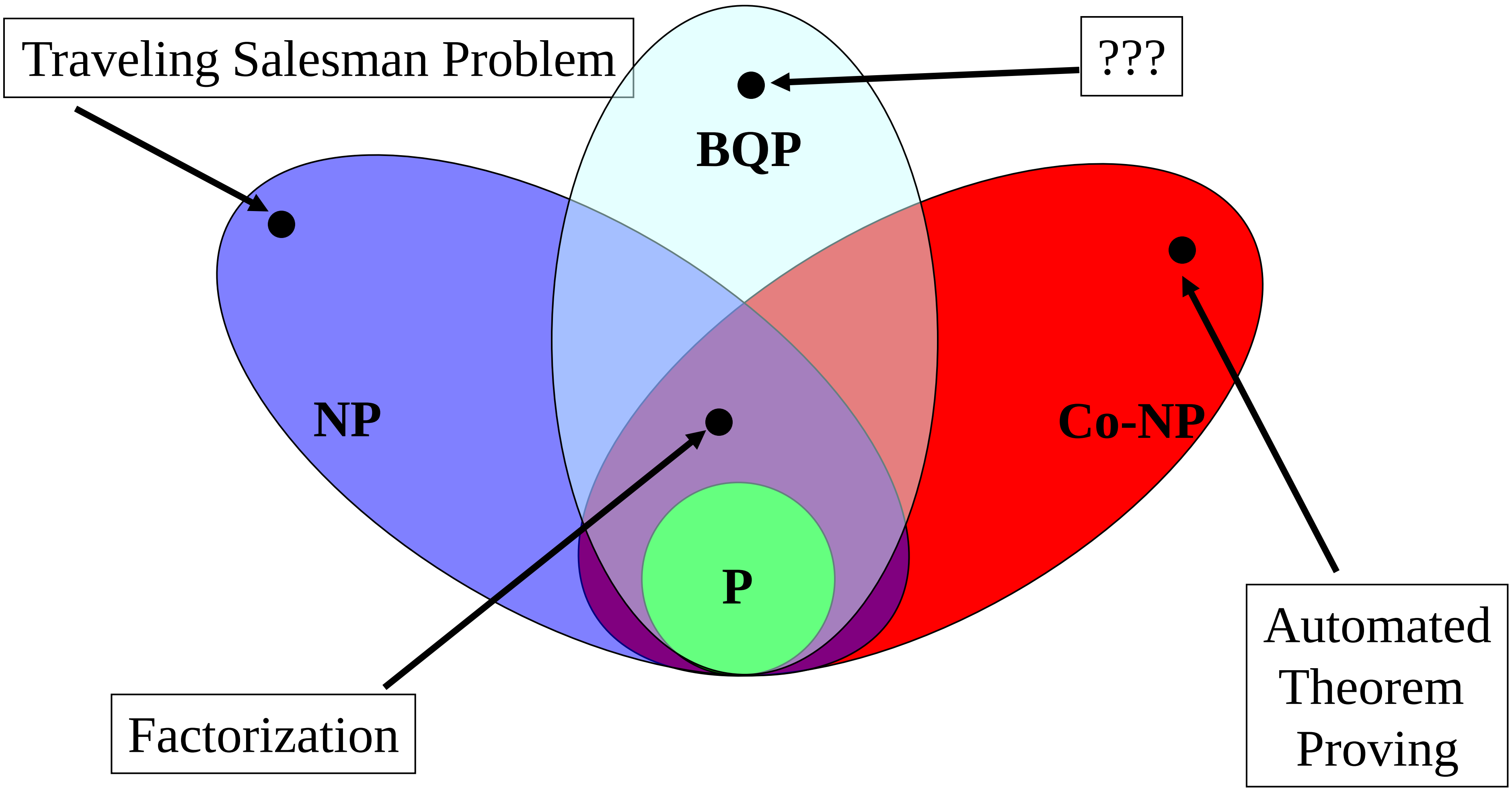
- Communincation Complexity
- Cryptography
- Essential for quantum speed up
  - Unentangled quantum alg. can be simulated efficiently
- Quantum interactive games
- Link with Functional Analysis & Grothednieck's constant

The real world
&
Complexity Theory

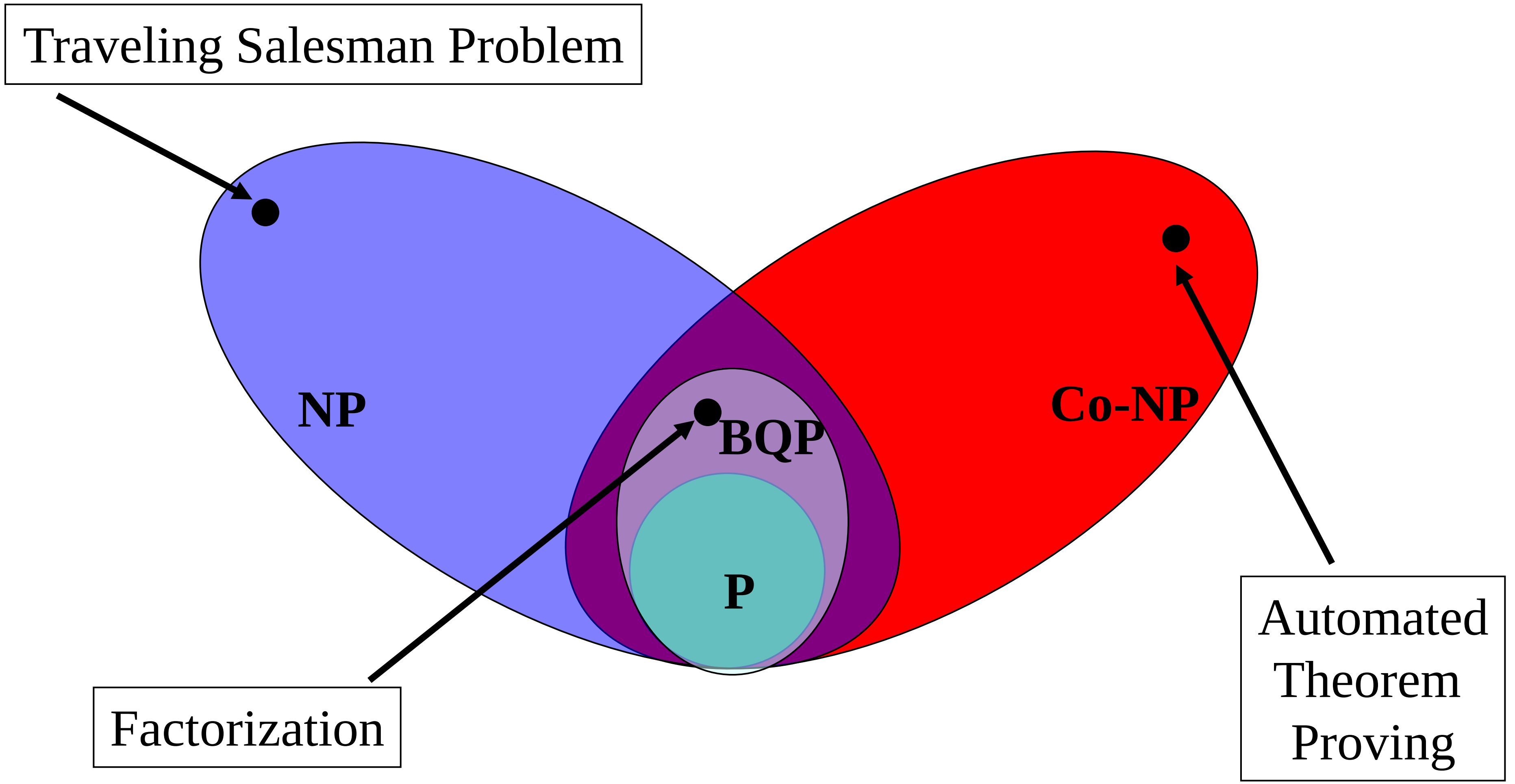
real world


Traveling Salesman Problem
NP
Co-NP
P
Factorization
Automated Theorem Proving

real world ?


Traveling Salesman Problem
???
BQP
NP
Co-NP
P
Factorization
Automated Theorem Proving

real world ?



Traveling Salesman Problem
NP
Co-NP
BQP
P
Factorization
Automated Theorem Proving

Quantum Cryptography

Quantum key generation

- Quantum mechanical protocol to securely generate secret "random" key between Alice and Bob.
- Unbreakable in combination with Vernam cipher

Bennett

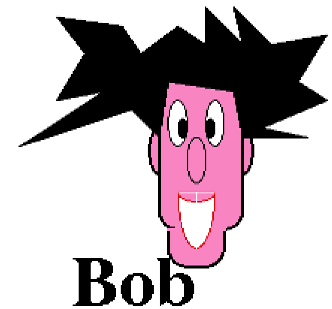
1984

Brassard

Quantum Cryptography
secret key generation

00111010

qubits



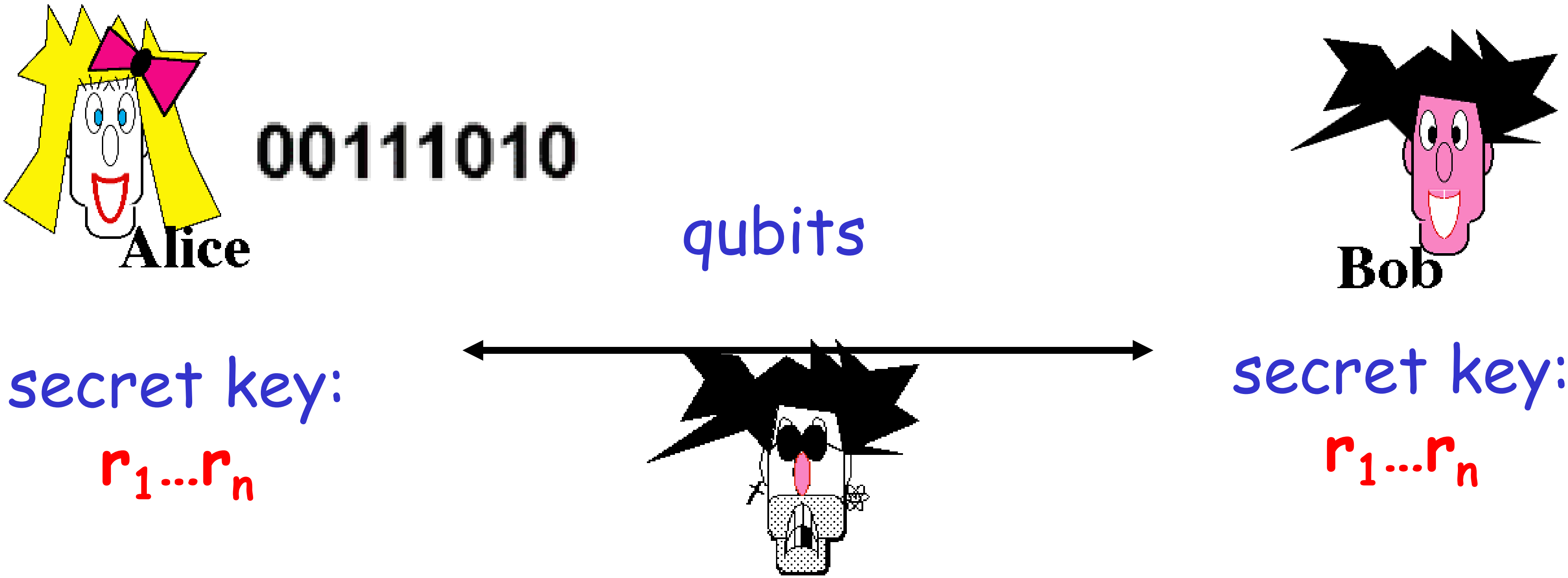
secret key:

$r_1 \ldots r_n$

secret key:

$r_1 \ldots r_n$

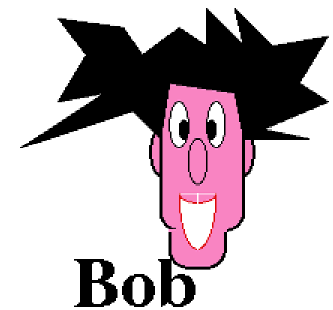
Quantum Cryptography secret key generation



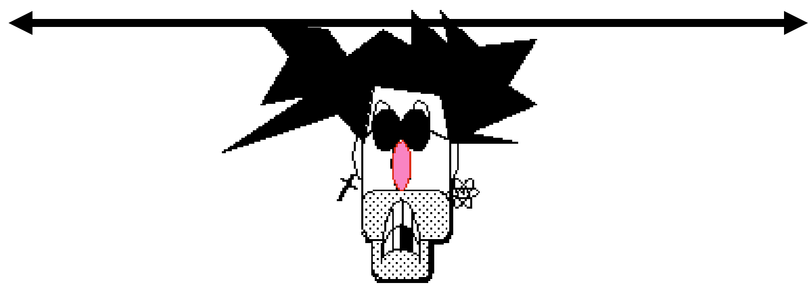
Quantum Cryptography secret key generation

00111010

qubits



secret key:
$r_1 \ldots r_n$



secret key:
$r_1 \ldots r_n$

Eavesdropper has to disturb qubit!

Can be detected by Alice & Bob

id Quantique

A quantum leap for cryptography

Clavis - PLUG & PLAY QUANTUM CRYPTOGRAPHY

Quantum Key Distribution is a technology that exploits a fundamental principle of quantum physics - observation causes perturbation - to exchange cryptographic keys over optical fiber networks with absolute security.

Quantum Crypto

- Impossibility of bit commitment
- Quantum key distribution scheme
- Quantum Coin-flipping
- Quantum string commitment (CWI)
- Quantum Information theory (CWI)
  - much richer field than classical information theory
- Quantum secure positioning (CWI)

Recent Developments

- New Algorithms
  - Pell's equations
  - searching/sorting etc.
  - Matrix problems
- Limitations to quantum computing
- Applications of quantum computing:
  - Physics, foundations of physics
  - classical comp. science & mathematics

Very Recent

- Surprising intrerplay between
  - Nonlocality
  - Communication complexity
  - Approximation algorithms (SDP)
  - Functional analysis
- Studying questions about nonlocality solve 35 year old problem in Banach space theory [Briet,B,Lee,Vidick 09]

Current Challenges

- Implementing more qubits
- New Algorithms
- Better Understanding of power of Quantum Computation
- Other Applications
- Quantum Cryptography
- Nonlocality, SDP, Functional Analysis

Quantum Computing FAQ

Q: What can Quantum Information Science do now?

A: Allow the building of prototype quantum communications systems whose security against undetected eavesdropping is guaranteed by fundamental laws of physics.

Q: When will we have full-scale quantum computer?

A: Too early to tell. Maybe 20 years.

Q: What could a quantum computer do?

A1: Enormously speed up some computations, notably factoring, thereby making many currently used codes insecure.

A2: Significantly speed up a much broader class of computations, including the traveling salesman problem, allowing them to be done in the square root of the number of steps a classical computer would require.

A3: Allow the efficient simulation of quantum systems, to aid physics and chemistry research.

Q: Does a quantum computer speed up all computations equally?

A: No. Some are sped up exponentially, some quadratically, and some not at all.

Q: What else can Quantum Information Science do?

A1: Facilitate other tasks involving distributed computing and secrecy.

A2: Contribute to better precision measurements and time standards.

…