QUANTUM INFORMATION PROMISES NEW INSIGHTS

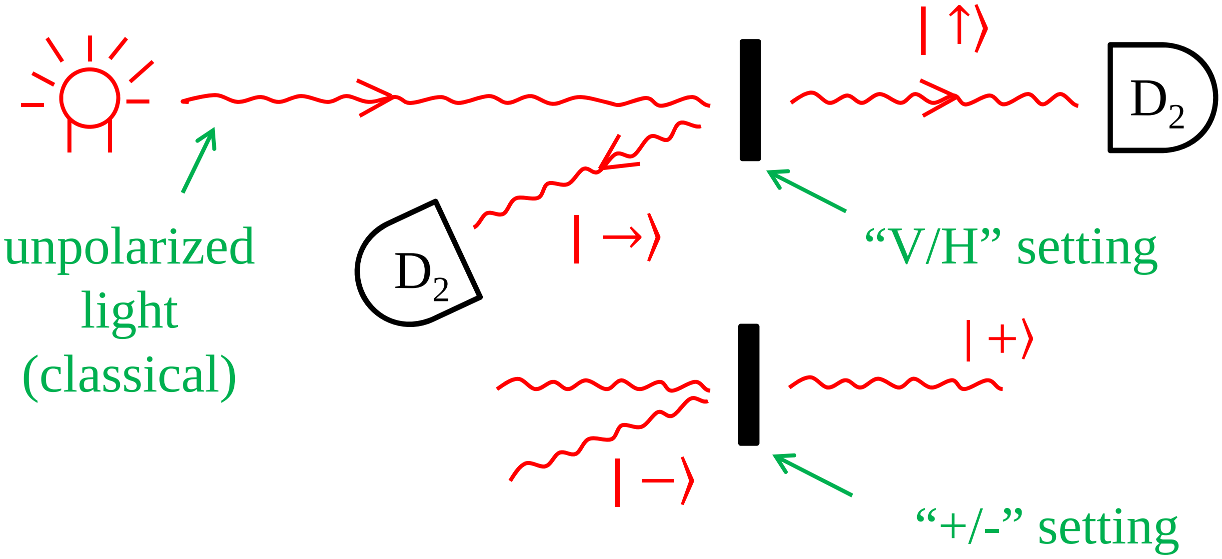
Anthony J. Leggett
Department of Physics
University of Illinois at Urbana-Champaign

PHOTON POLARIZATION— THE ULTIMATE “QUANTUM 2-STATE SYSTEM”

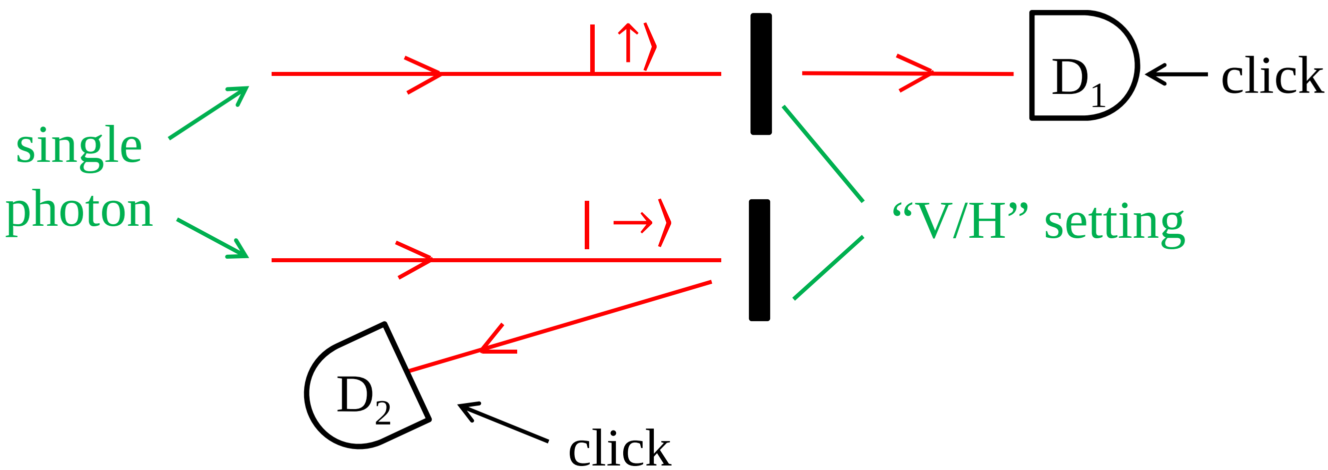
Some possible polarization states of light (photons) propagating towards screen:

$|\uparrow\rangle$	$|\rightarrow\rangle$	$|\nearrow\rangle$	$|\searrow\rangle$
“$|V\rangle$”	“$|H\rangle$”	“$|+\rangle$”	“$|-\rangle$”

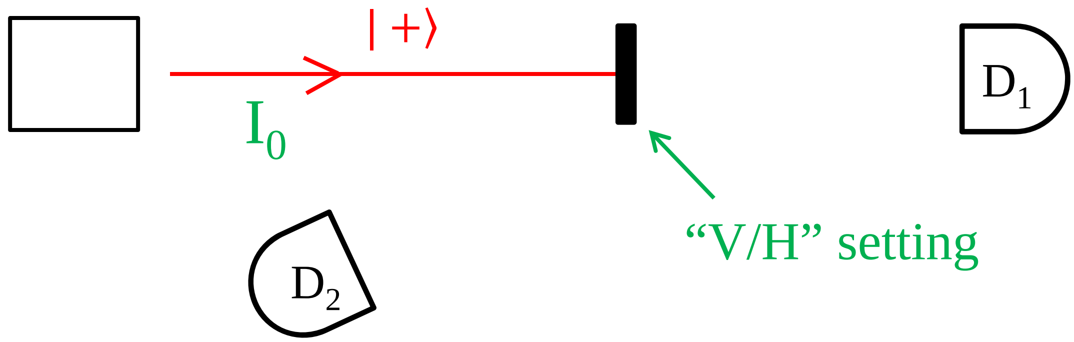
Polarizer:



What happens at quantum level?



But what if



?

Classically, resolve $|+\rangle$ into $|H\rangle$ and $|V\rangle$ components:

electric field $\longrightarrow$ $E_+ = \frac{1}{\sqrt{2}}(E_H + E_V)$

E_V is transmitted, E_H is reflected, so

$$I_1 = I_2 = \frac{1}{2}\, I_o \qquad \text{(Malus's law)}$$

output of D_1 output of D_2

But what happens at the quantum level?

"A single photon cannot be split!", so for each photon

either D_1 clicks ("photon is $|V\rangle$")
or D_2 clicks ("photon is $|H\rangle$")
✓ (experimentally observed)

$$P_1 = P_2 = ½$$

prob. of click in D_1 — prob. of click in D_2

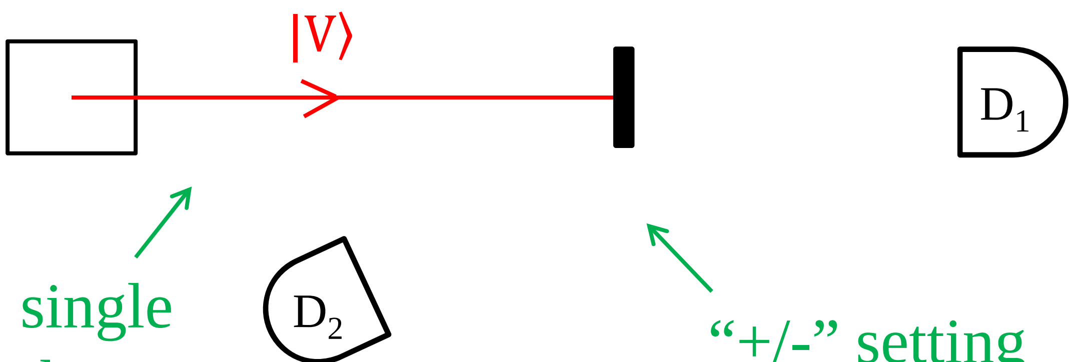
(quantum version of Malus's law)

So: is each individual photon indeed either $|V\rangle$ or $|H\rangle$?
(ensemble is "mixture" of $|V\rangle$ and $|H\rangle$)

Is the original $|+\rangle$ beam a "mixture" of $|V\rangle$ and $|H\rangle$?

(i.e. is each individual photon either $|V\rangle$ or $|H\rangle$?)

If so:
by symmetry



single photon

"+/-" setting

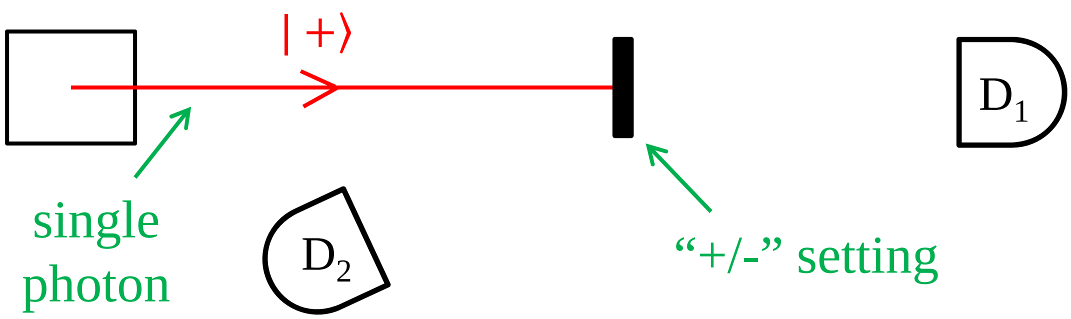
$$P_1 = P_2 = ½$$

output of D_1 output of D_2

Similarly for $|H\rangle$. So $P(-|V) = P(-|H) = ½$.
But $|+\rangle$ is mixture of $|V\rangle$ and $|H\rangle$, so

$$P(-|+) = ½$$

i.e.



$P_1 = P_2 = ½$

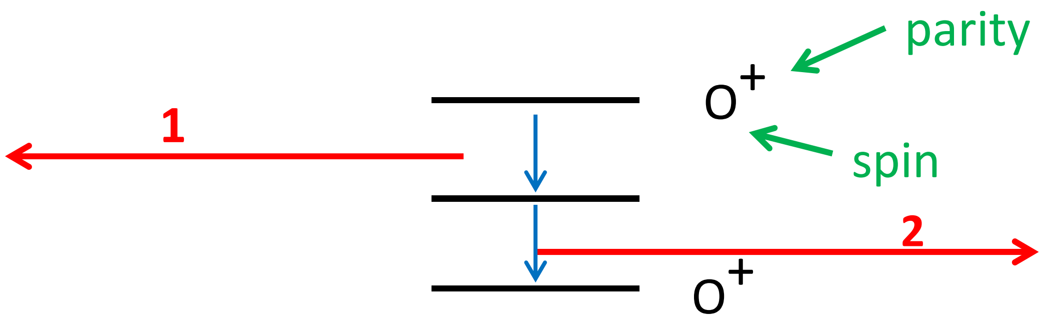
in contradiction to experiment!

Conclusion:

$|+\rangle$ is a quantum superposition of $|V\rangle$ and $|H\rangle$, and this is not equivalent to a mixture: each $|+\rangle$ photon is not "either" $|V\rangle$ "or" $|H\rangle$

← superposition principle

POLARIZATION OF PHOTON PAIRS



For photon propagating into page, denote states of circular polarization by

$$|\circlearrowright\rangle \equiv |\mathrm{R}\rangle$$ ⟵ right-circularly polarized

$$|\circlearrowleft\rangle \equiv |\mathrm{L}\rangle$$ ⟵ left-circularly polarized

The conservation of total angular momentum is consistent with either

$|\mathrm{R}\rangle_1 \mathrm{R}\rangle_2$ or $|\mathrm{L}\rangle_1 \mathrm{L}\rangle_2$ ("product" states)

But if we don't know (and can't find out!) which if these occurred, must describe polarization state of photons by quantum superposition:

$$\Psi_Y = \frac{1}{\sqrt{2}}(|\mathrm{R}\rangle_1 \mathrm{R}\rangle_2 + \mathrm{e}^{\mathrm{i}\phi}|\mathrm{L}\rangle_1 \mathrm{L}\rangle_2)$$

(actually, parity conservation $\Rightarrow \mathrm{e}^{\mathrm{i}\phi} = 1$ so (not obvious!) can equally well write $\Psi_Y = \frac{1}{\sqrt{2}}(|\mathrm{H}\rangle_1 \mathrm{H}\rangle_2 + |\mathrm{V}\rangle_1 \mathrm{V}\rangle_2)$). This is not equivalent to a "classical mixture" of $|\mathrm{R}\rangle_1 \mathrm{R}\rangle_2$ and $|\mathrm{L}\rangle_1 \mathrm{L}\rangle_2$! In fact, (Bell, 1964):

If we assume local causality and the standard "arrow of time," then the experimental predictions of Ψ_Y are inconsistent with the assignation of any properties (not just polarization) to the individual photons 1 and 2! (and subsequent experiment unambiguously favors predictions of Ψ_Y).

Ψ_Y is an entangled state – a quantum superposition of product states of more than one system. Quantum information exploits (inter alia) the bizarre properties of entangled states.

ENTANGLEMENT AS A RESOURCE

The state of a 2-state system (e.g. photon polarization) is uniquely specified by (<) 2 complex numbers (e.g. the amplitudes for $|H\rangle$ and $|V\rangle$). So if we have N 2-state systems in a product state, we need ~2N complex numbers. However, to specify a general entangled state of N systems we need not ~2N but 2^N complex numbers! e.g. for N = 4, we need to specify separately amplitudes for

$$|HHHH\rangle, |HHHV\rangle, |HHVH\rangle, |HHVV\rangle \ldots$$

($16 = 2^4$ states in all).

Thus, possibility of massively parallel processing … (“quantum computing”)

Alas, a snag: measurement will “reveal” only one of the 2^N states $\Rightarrow$ we lose all information on the $2^N - 1$ others.

Solution (Deutsch 1984, Shor 1995): devise algorithm such that at end system is in just one of the 2^N states, the particular one depending one the answer to our problem.

Application: prime-factoring of large numbers (Shor 1995). (For N binary digits, time taken by classical computer exponential in N, for quantum computer polynomial in N). Interesting primarily for application to (classical) cryptography.

Practical difficulties in building quantum computer:

- “ideal” 2-state system
- scalability
- decoherence …

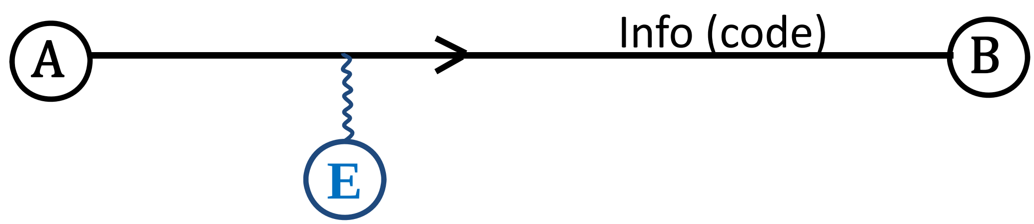
Systems: nuclear spins, trapped ions, superconducting devices …

at present, not practically competitive with classical computing, but …

QUANTUM CRYPTOGRAPHY

(Bennett + Brassard 1984, Ekert 1990)

"Key distribution problem":



In classical (and quantum) cryptography, Alice and Bob can't prevent Eve from listening in. But can they tell whether she is listening in? In classical cryptography, no (as far as as known); Eve can intercept message and pass it on without detection.

Quantum cryptography: exploits no-cloning theorem (direct consequence of superposition principle):/ it is impossible to build a device guaranteed to detect and pass on unaltered a photon of arbitrary (unknown) polarization./

Protocol:

$\uparrow$	$\rightarrow$	$\nearrow$	$\searrow$
"$\lvert V\rangle$"	"$\lvert H\rangle$"	"$\lvert +\rangle$"	"$\lvert -\rangle$"

A emits photons at random, 50% of the time either $|H\rangle$ or $|V\rangle$ and 50% of the time either $|+\rangle$ or $|-\rangle$. Bob also measures at random, 50% of the time with setting H/V, 50% with +/-. At end of (say) 10,000 runs, Alice and Bob compare notes (they can use a classical (insecure) phone line) on "settings," throw away those runs for which they have used different settings and compare notes on the rest.

If Eve is not listening in, then whenever Alice sent $|H\rangle$ ($|V\rangle$) Bob should detect $|H\rangle$ ($|V\rangle$): similarly for $|+\rangle$ ($|-\rangle$).

If Eve is listening in on each run, she has to decide how to set her polarizer! But Eve does not know whether Alice emitted ($|H\rangle$ or $|V\rangle$) or rather ($|+\rangle$ or $|-\rangle$).

QUANTUM CRYPTOGRAPHY (continued)

Suppose e.g. she chooses a $+/-$ setting. Then if Alice in fact emitted $|+\rangle$ or $|-\rangle$, she can measure it and pass it on undetected. But what if Alice emitted $|H\rangle$ or $|V\rangle$? Then she (Eve) has 50% chance if passing it on wrong, and Alice and Bob will fail to agree and thus detect her eavesdropping.