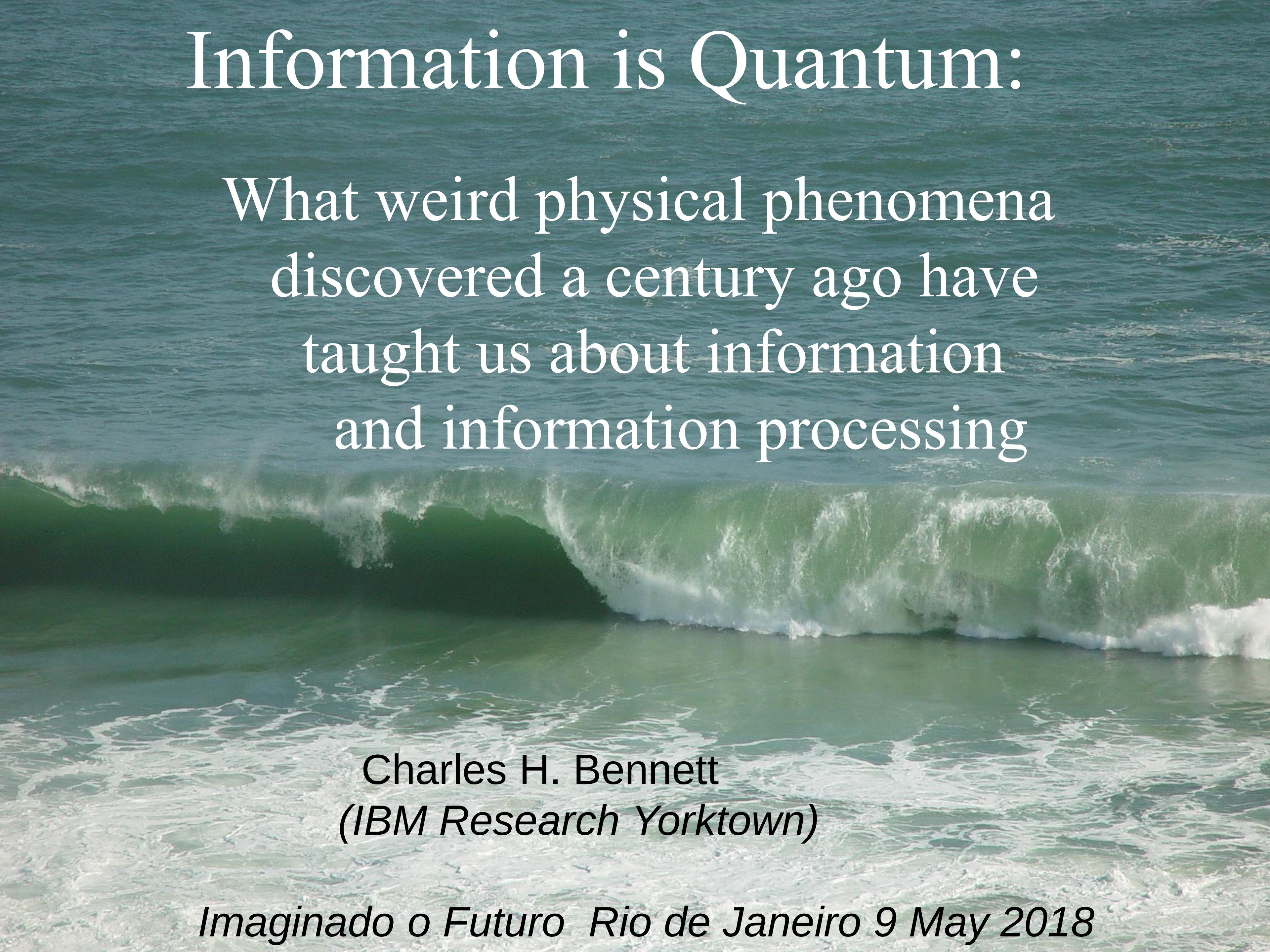


Information is Quantum:

What weird physical phenomena discovered a century ago have taught us about information and information processing

Charles H. Bennett
(IBM Research Yorktown)

Imaginado o Futuro Rio de Janeiro 9 May 2018

Like other parts of mathematics, the theory of information processing originated as an abstraction from everyday experience

Calculation = manipulation of pebbles
Digit = a finger or a toe

Today's digital information revolution is based on these abstractions, as crystallized by Turing, Shannon, and von Neumann in the mid 20th century.

But now these notions are known to be too narrow.

Quantum theory, developed by physicists in the early 1900's, and spectacularly successful in its own field, also provides a more complete and natural arena for developing concepts of communication and computation.

Conventionally, information carriers have been viewed as what a physicist would call **classical** systems:

• Their states in principle are reliably distinguishable, and can be observed without disturbing the system

• To specify the joint state of two or more systems, it is sufficient to specify the state of each one separately.

But for **quantum** systems like atoms or photons:

• Attempting to observe a particle's state in general disturbs it, while obtaining only partial information about the state (uncertainty principle).

• Two particles can exist in an *entangled* state, causing them to behave in ways that cannot be explained by supposing that each particle has some state of its own.

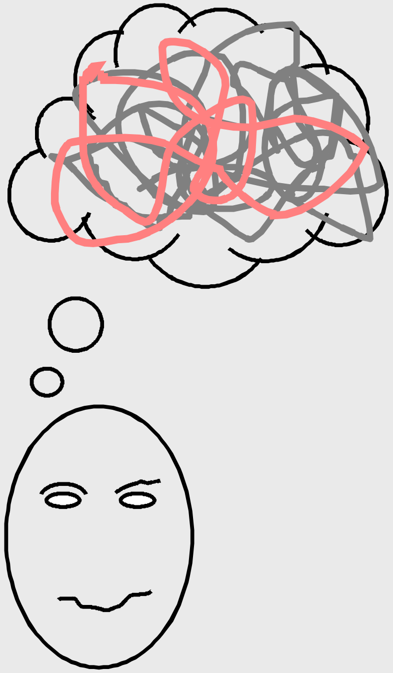
For most of the 20th century, quantum effects in information processing were regarded mainly as a nuisance, because the uncertainty principle makes quantum devices behave less reliably than the classical ideal.

We now know that quantum effects also have positive consequences, making possible new kinds of information processing such as **quantum cryptography**, and **dramatically speeding up** *some* **computations** that would be infeasibly hard classically.

These positive consequences are chiefly due to entanglement.

Ordinary classical information, such as one finds in a book, can be copied at will and is not disturbed by reading it.

Quantum information is more like the information in a dream



- Trying to describe your dream changes your memory of it, so eventually you forget the dream and remember only what you've said about it.

- You cannot prove to someone else what you dreamed.

- You can lie about your dream and not get caught.

But unlike dreams, quantum information obeys well-known laws.

Despite the differences there are important similarities between classical and quantum information

All (classical) information is reducible to bits **0** and **1**.

All processing of it can be done by simple logic gates (**NOT, AND**) acting on bits one and two at a time.

Bits and gates are fungible (independent of physical embodiment), making possible Moore's law.

Quantum information is reducible to **qubits** i.e. two-state quantum systems such as a photon's polarization or a spin-1/2 atom.

Quantum information processing is reducible to one- and two-qubit gate operations.

Qubits and quantum gates are fungible among different quantum systems

The central principle of quantum mechanics is

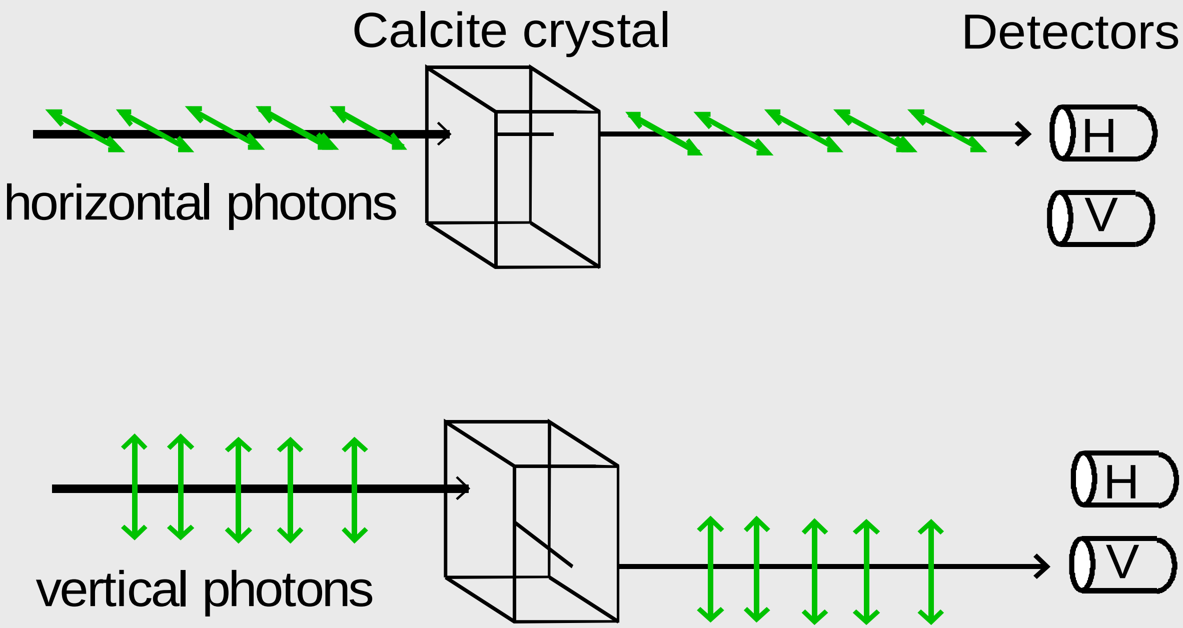
the Superposition Principle:

- Between any two reliably distinguishable states of a physical system (for example vertically and horizontally polarized single photons) there are intermediate states (for example diagonal photons) that are not reliably distinguishable from either original state

- The possible physical states correspond to directions in space—not ordinary 3-dimensional space, but an ***n***-dimensional space where ***n*** is the system's maximum number of reliably distinguishable states.

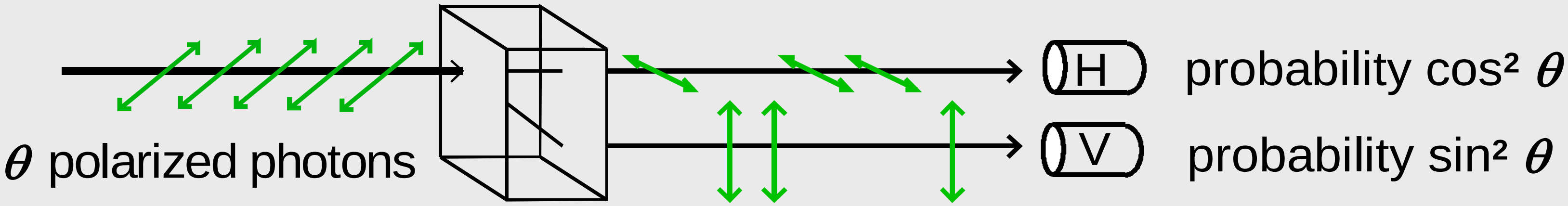
- Any direction is a possible state, but two states are reliably distinguishable if only if their directions are perpendicular.

Using Polarized Photons to Carry Information



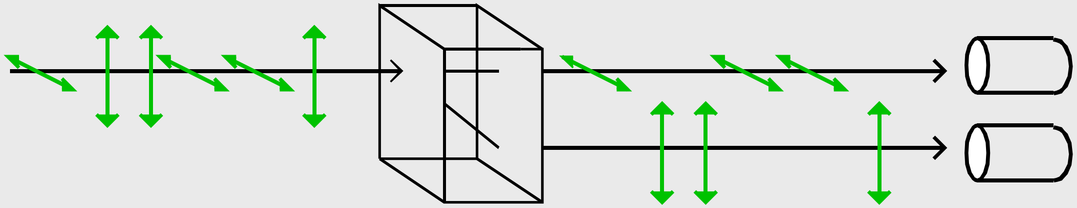
Photons behave reliably if measured along an axis parallel or perpendicular to their original polarization.

Used in this way, each photon can carry one reliable bit of information.

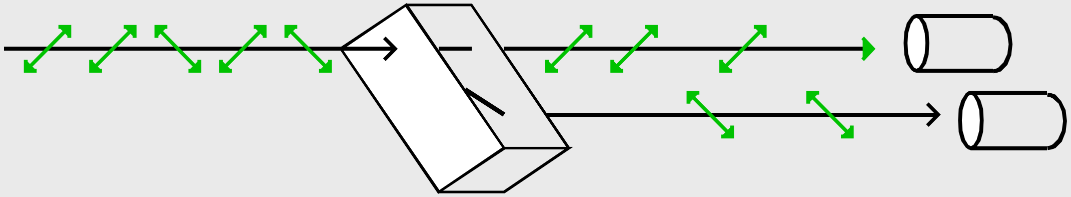

H
V
θ polarized photons
probability $\cos^2 \theta$
probability $\sin^2 \theta$

But measuring the photons along any other axis causes them to **behave randomly**, forgetting their original polarization direction.

A rectilinear (ie vertical vs horizontal) measurement distinguishes vertical and horizontal photons reliably, but randomizes diagonal photons.

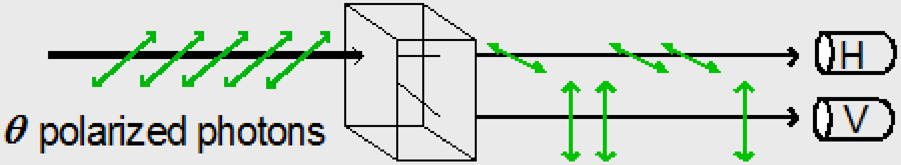


A diagonal measurement distinguishes diagonal photons reliably but randomizes rectilinear photons.



No measurement can distinguish all four kinds. This is not a limitation of particular measuring apparatuses, but a fundamental consequence of the uncertainty principle. This fundamental limitation gives rise to the possibility of quantum money and quantum cryptography.

Prof. William Wootters' pedagogic analogy for quantum measurement



Like a pupil confronting a strict teacher, a quantum system being measured is forced to choose among a set of distinguishable states (here 2) characteristic of the measuring apparatus.

Teacher: Is your polarization vertical or horizontal?

Pupil: Uh, I am polarized at about a 55 degree angle from…

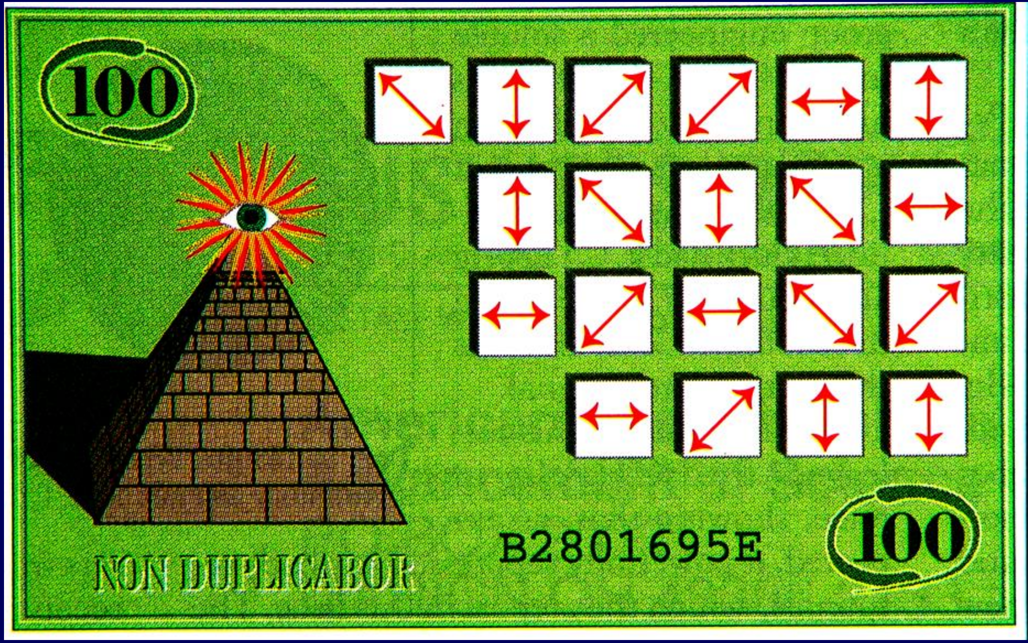
Teacher: **I believe I asked you a question.** Are you vertical or horizontal?

Pupil: Horizontal, sir.

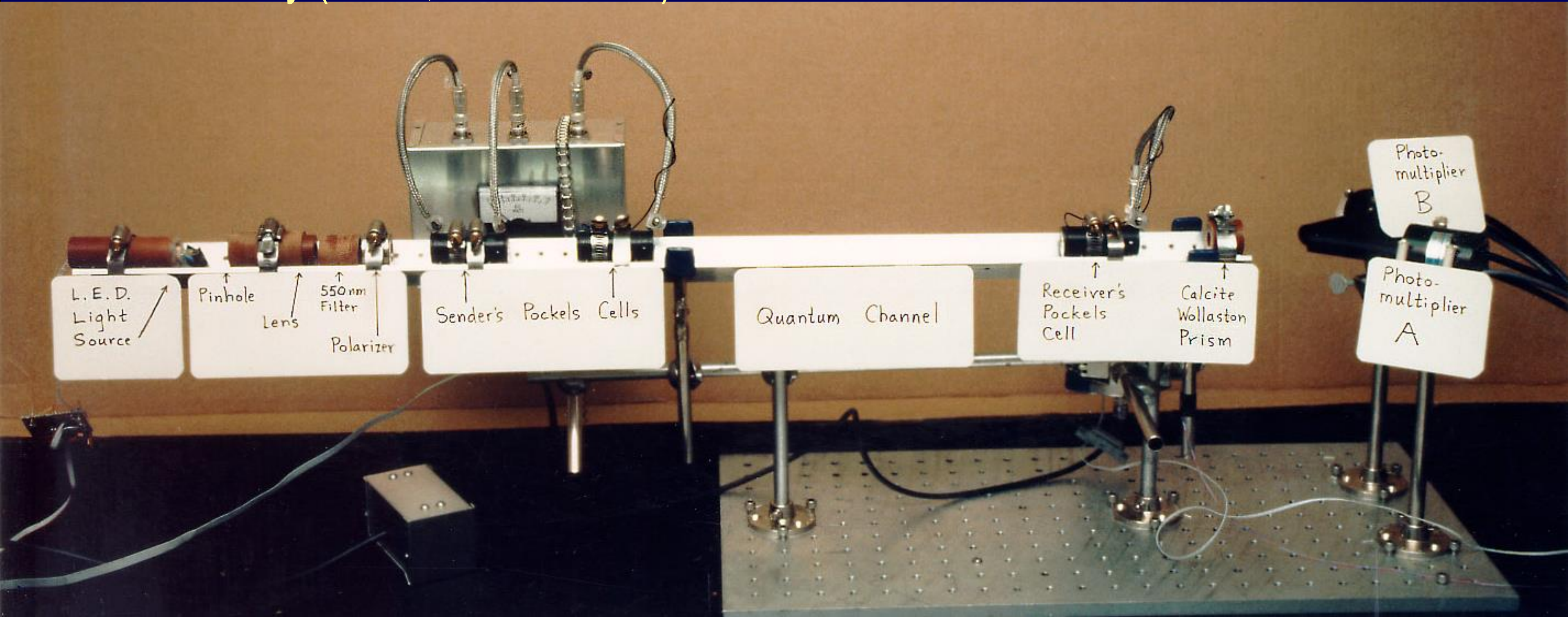
Teacher: Have you ever had any other polarization?

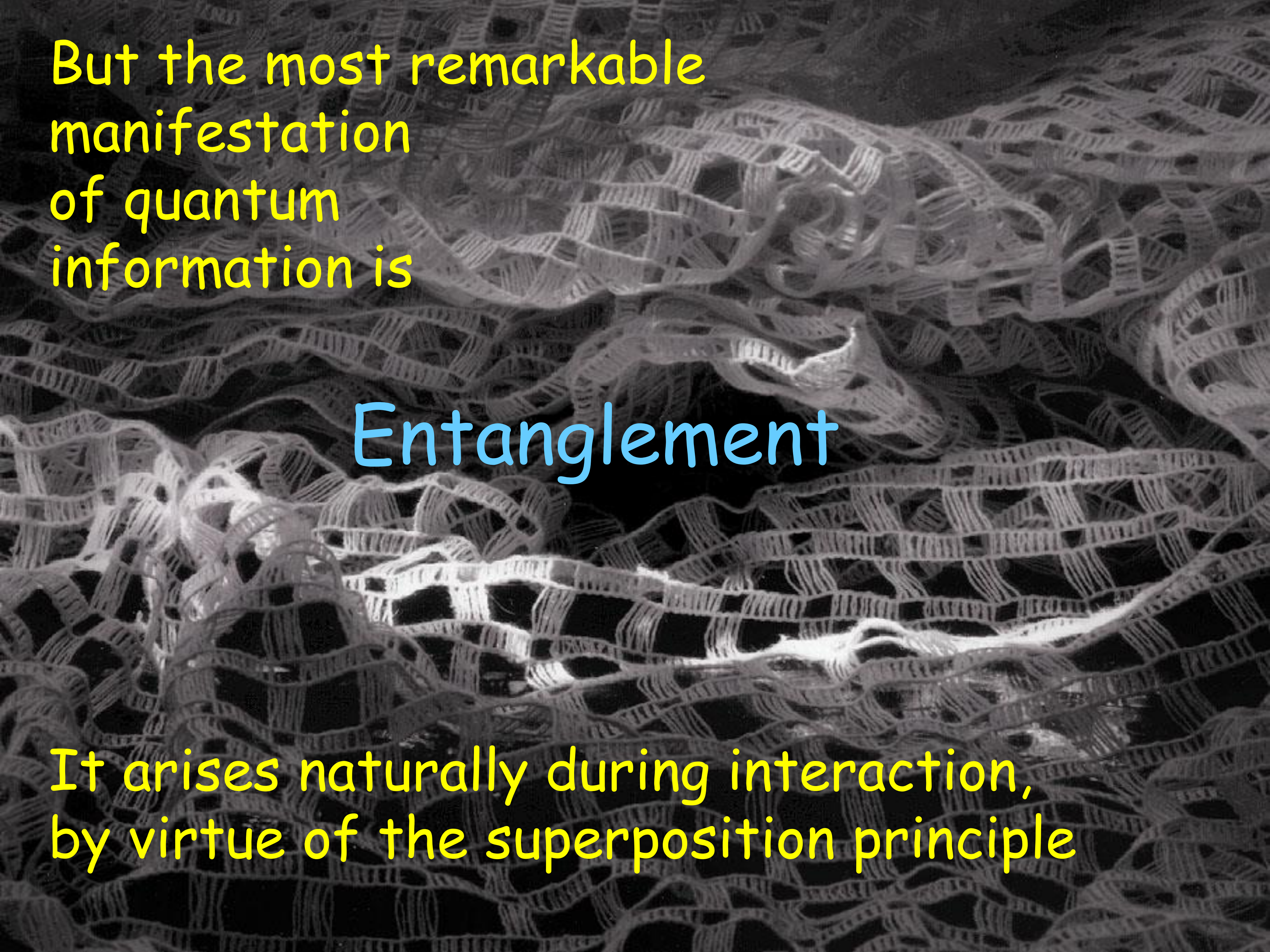
Pupil: No, sir. I was always horizontal.

Quantum money (Wiesner '68, '83) cannot be copied by a counterfeiter, but can be checked by the bank, which knows the secret sequence of polarized photons it should contain.



Quantum cryptography uses polarized photons to generate shared secret information between parties who share no secret initially (BB84, BBBSS92…)



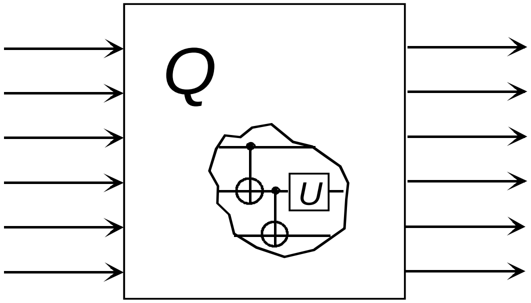


But the most remarkable manifestation of quantum information is

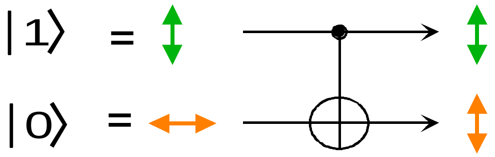
Entanglement

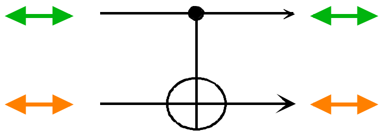
It arises naturally during interaction, by virtue of the superposition principle

Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.

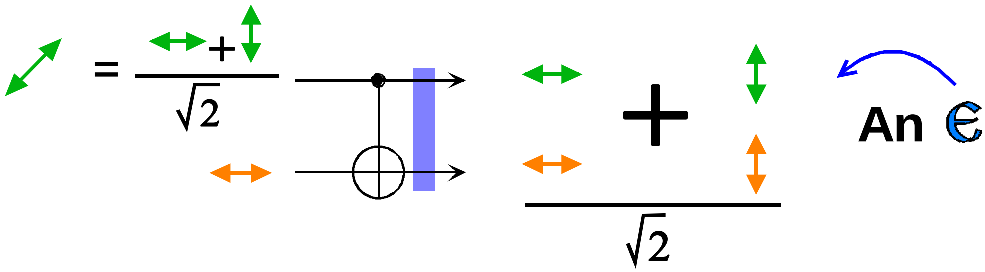


The 2-qubit XOR or "controlled-NOT" gate flips its 2nd input if its first input is 1, otherwise does nothing.



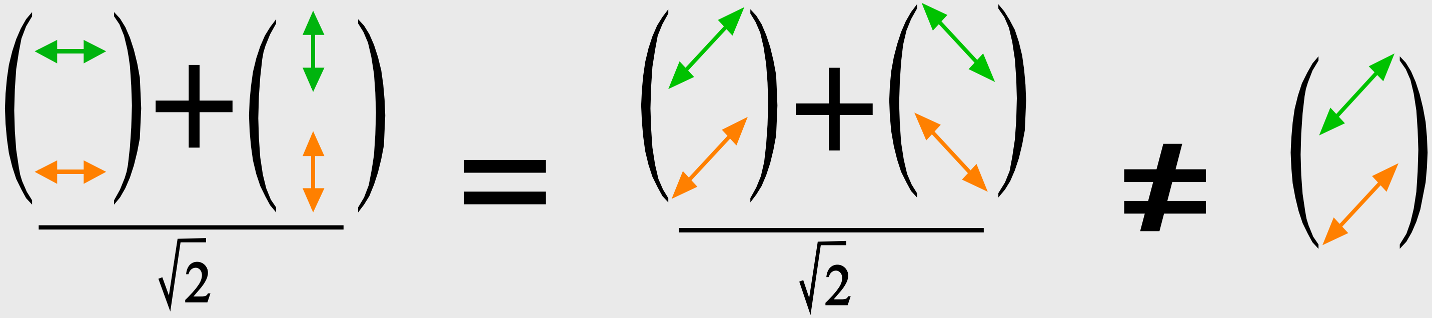


A superposition of inputs gives a superposition of outputs.



An entangled state

This entangled state of two photons behaves in ways that cannot be explained by supposing that each photon has a state of its own.



The two photons may be said to be in a definite state of *sameness* of polarization even though neither photon has a polarization of its own.

Entanglement sounds like a fuzzy new-age idea.

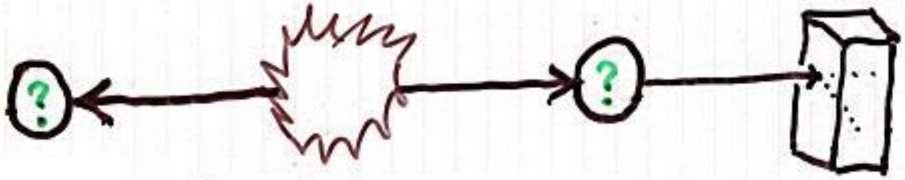
(In San Francisco in 1967, the “Summer of Love”, one often met people who felt they were in perfect harmony with one another, even though they had no firm opinions about anything.)

Wikiwatcher1 CC Share alike

Hippies believed that with enough LSD, everyone could be in perfect harmony with everyone else.

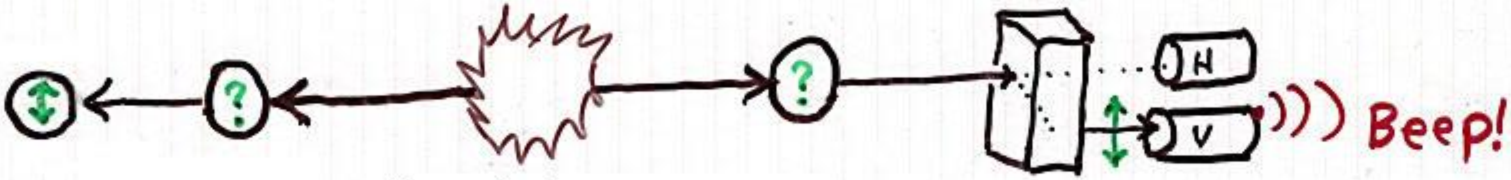
Now we have a quantitative theory of entanglement and know it is *monogamous*: the more entangled two systems are with each other, the less entangled they can be with anything else.

How entangled particles behave, and trying to explain it in everyday language:



Two photons are created in an "entangled" state.

Measuring either one, along any axis, gives a random result...

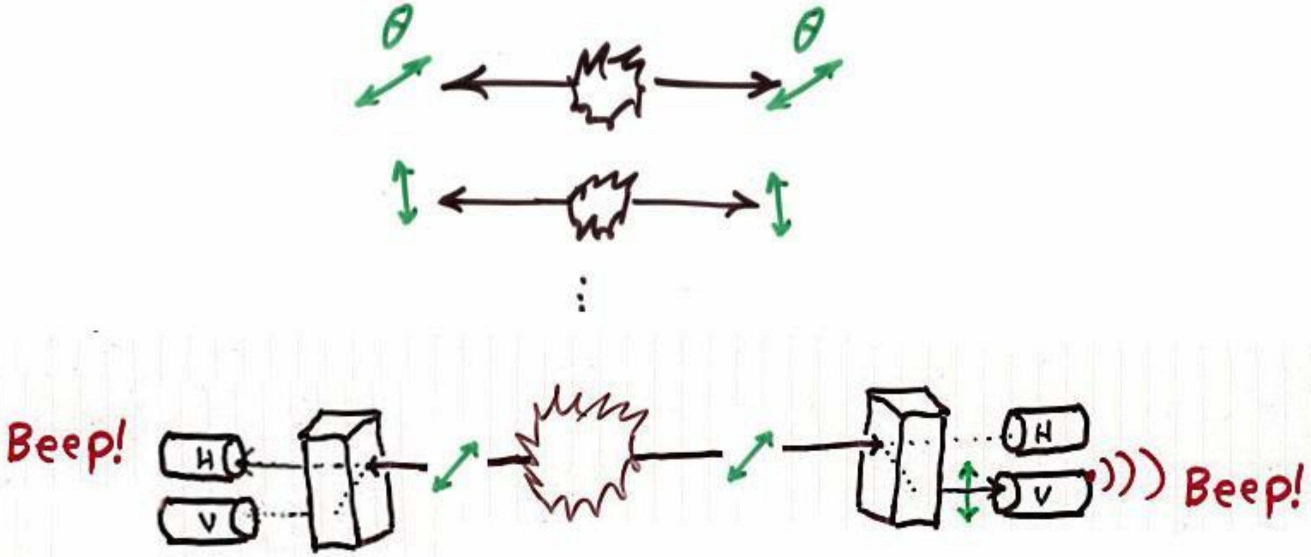


Two photons are created in an "entangled" state.

And simultanteously causes the other photon to acquire the same polarization.

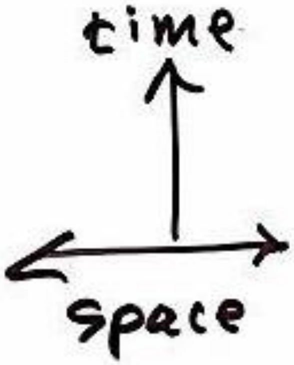
Alternative Explanations

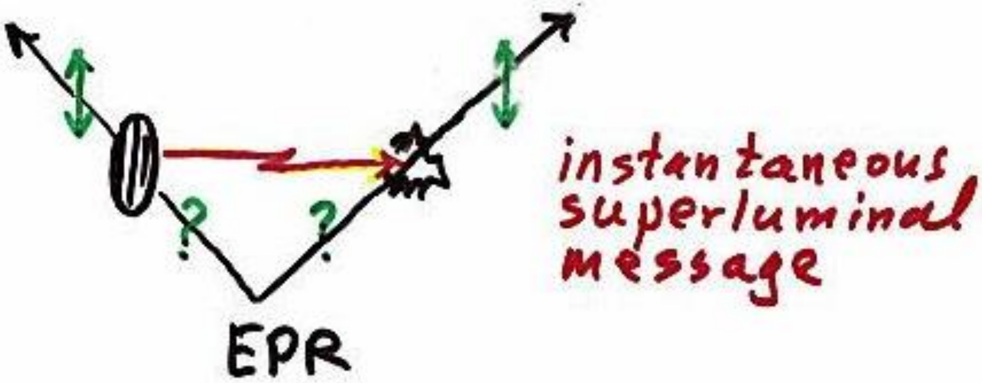
1. At each shot, source emits 2 photons with the same random polarization.



This explanation fails. Sometimes the source would emit 2 digonal photons, and if these were both measured on the V/H axis, sometimes one would behave V and the other H. In fact, they always behave the same, both V or both H.

2. Instantaneous Action at a Distance

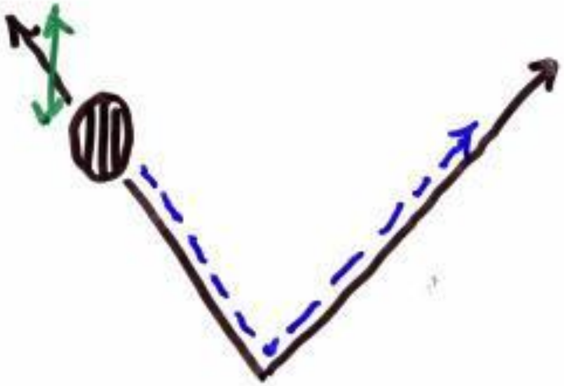




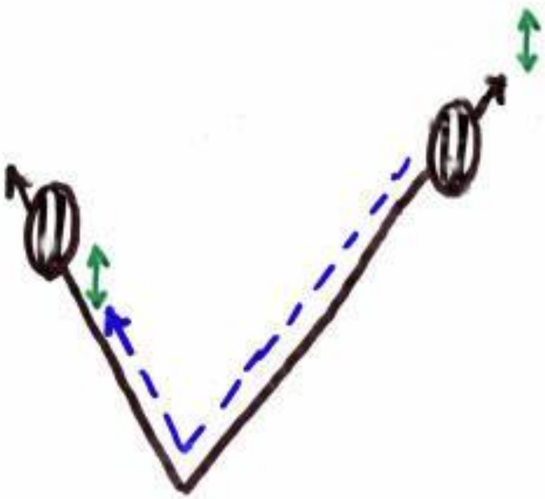
No. Violates special relativity and besides, how does the first particle know where to send the message to?

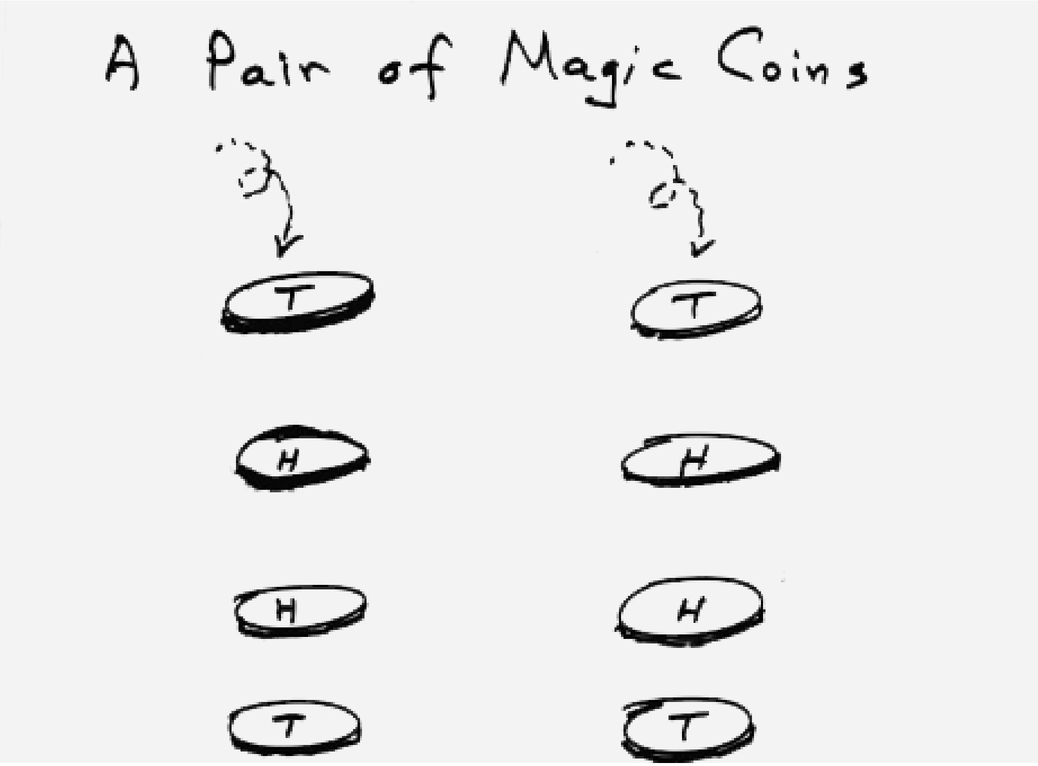
3. Quantum Mechanics - the right answer

4. Random Uncontrollable Message
Backward In time



or





A “message” backward in time is safe from paradox under two conditions, either of which frustrates your ability to advise your broker what stocks to buy or sell yesterday:

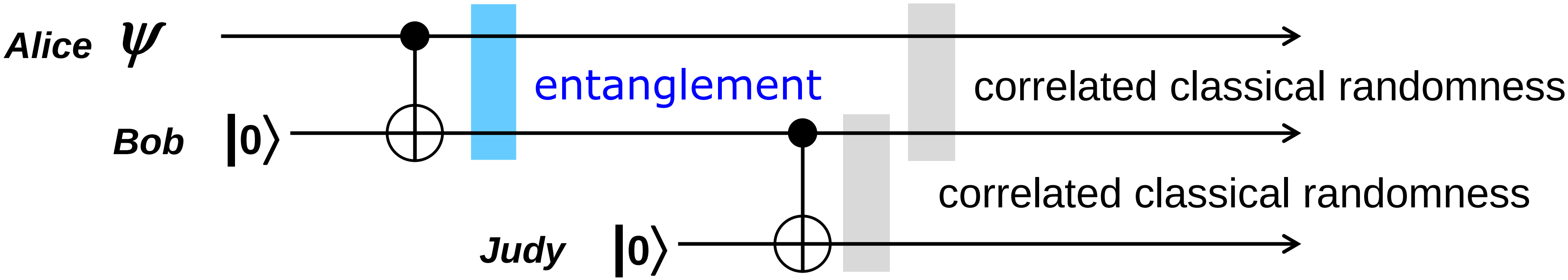
1. Sender can’t control message (entanglement)   OR
2. Receiver disregards message (Myth of Cassandra foretelling the destruction of Troy but unable to prevent it because no one believes her).

The Monogamy of Entanglement

- If A and B are maximally entangled with each other, they can’t they be entangled with anyone else.

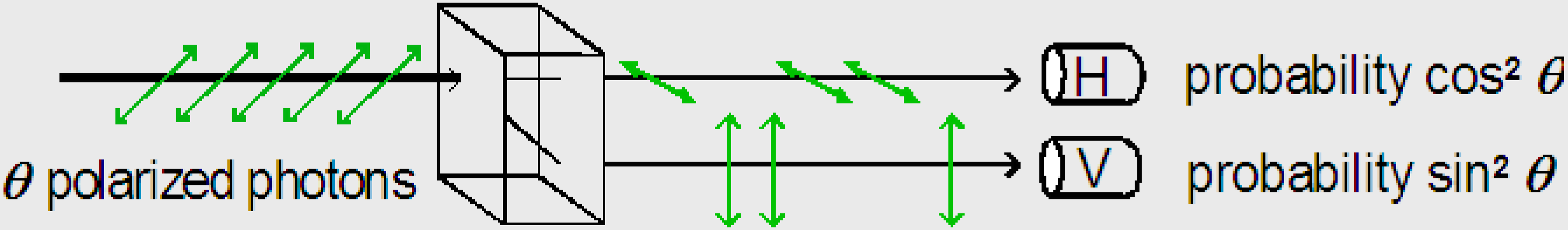
- Indeed classical correlation typically arises from vain attempts to clone entanglement. If one member of an entangled pair tries to share the entanglement with a third party, each pairwise relation is reduced to mere correlated randomness.

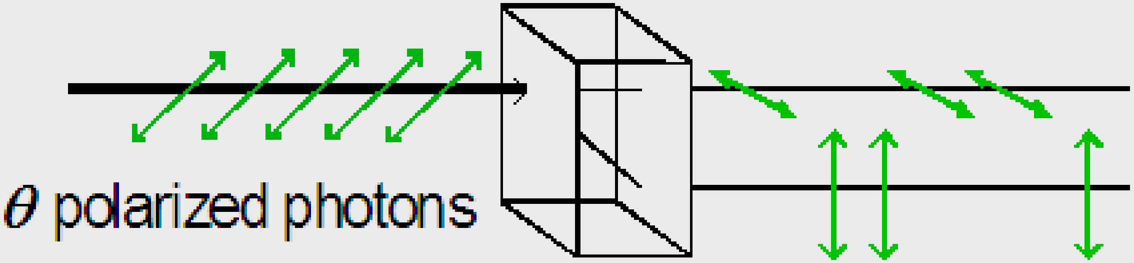
“Two is a couple, three is a crowd.”


Alice ψ
Bob $|0\rangle$
Judy $|0\rangle$
entanglement
correlated classical randomness
correlated classical randomness

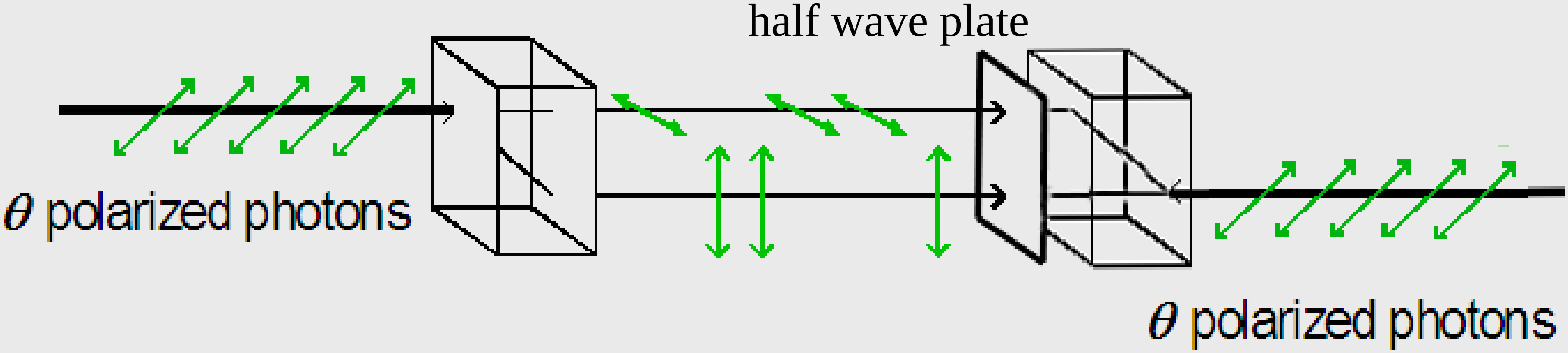
If one of Bob’s girlfriends leaves, Bob will find his relation to the other degraded to mere correlated randomness. But if they both stay, he ends up perfectly entangled, not with either one, but with the now nontrivial *relationship* between them, an appropriate punishment.

Entanglement and the origin of Quantum Randomness





If no one observes the photons, their random “behavior” can be undone.



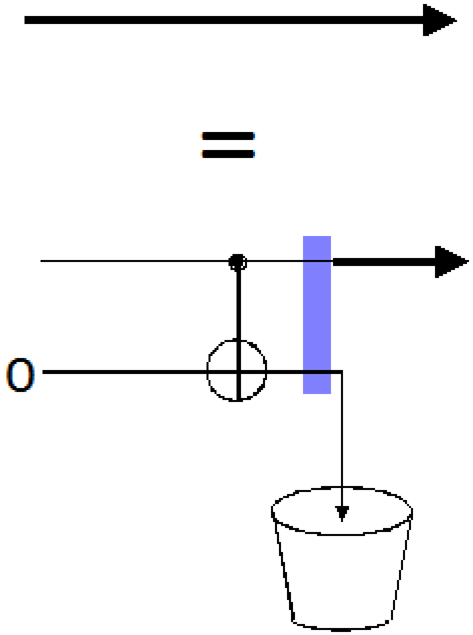
Metaphorically speaking, it is the **public embarrassment** of the pupil, in front of the whole class, that makes him forget his original polarization.

Expressing Classical Data Processing in Quantum Terms

A Classical Bit is a qubit with one of the Boolean values 0 or 1

A classical wire is a quantum channel that conducts 0 and 1 faithfully but randomizes superpositions of 0 and 1.

This happens because the data passing through the wire interacts with its environment, causing the environment to acquire a copy of it, if it was 0 or 1, and otherwise become entangled with it.



wastebasket symbolizes loss of
Information into the environment

A classical channel is a quantum channel with an eavesdropper.

A classical computer is a quantum computer handicapped by having eavesdroppers on all its wires.

Entanglement is ubiquitous: almost every interaction between two systems creates entanglement between them.

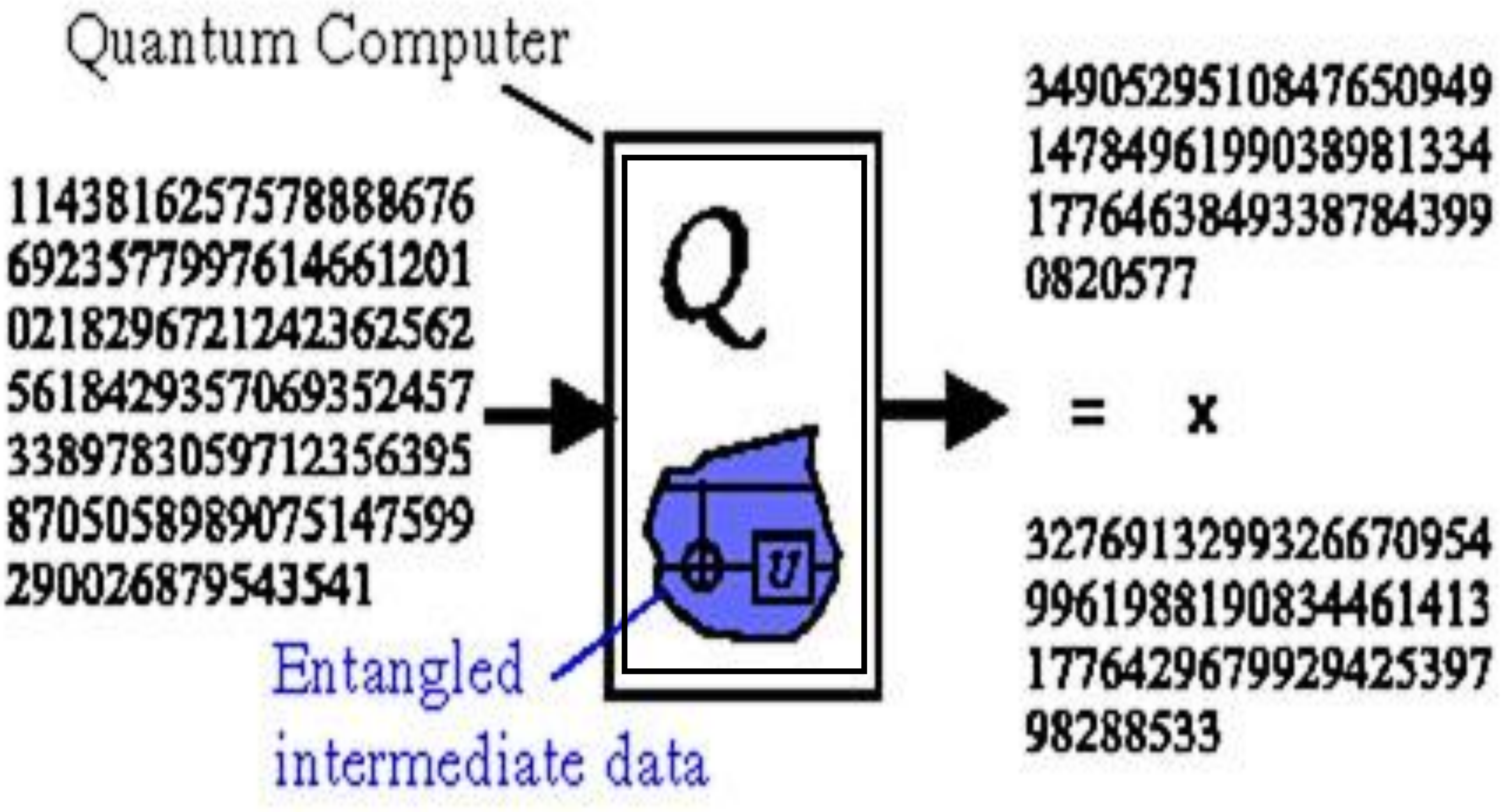
Then why wasn’t it discovered before the 20th century?

Because of its monogamy.

Most systems in nature, other than tiny ones like photons, interact so strongly with their environment as to become entangled with it almost immediately .

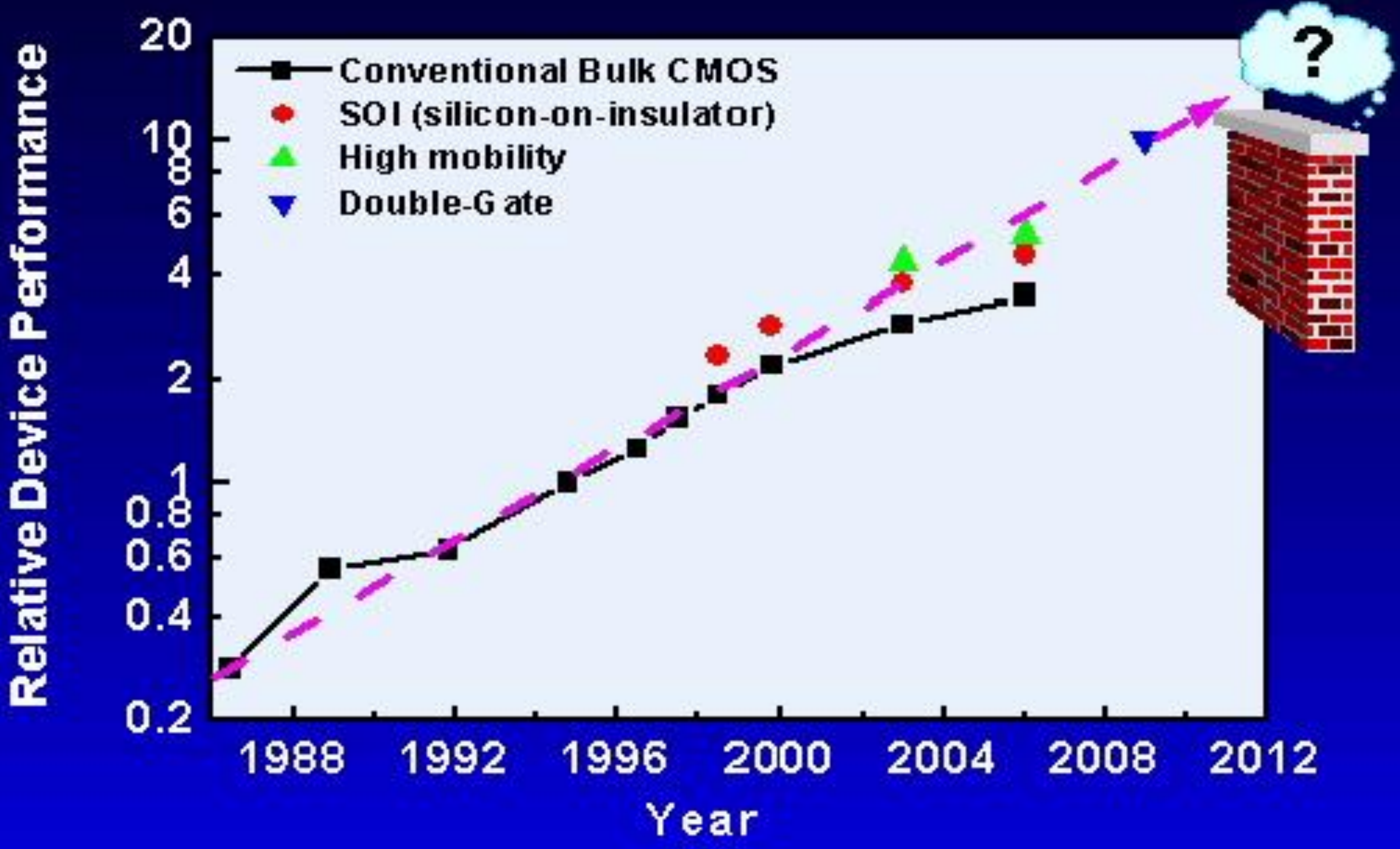
This destroys any previous entanglement that may have existed between internal parts of the system, changing it into mere correlated randomness.

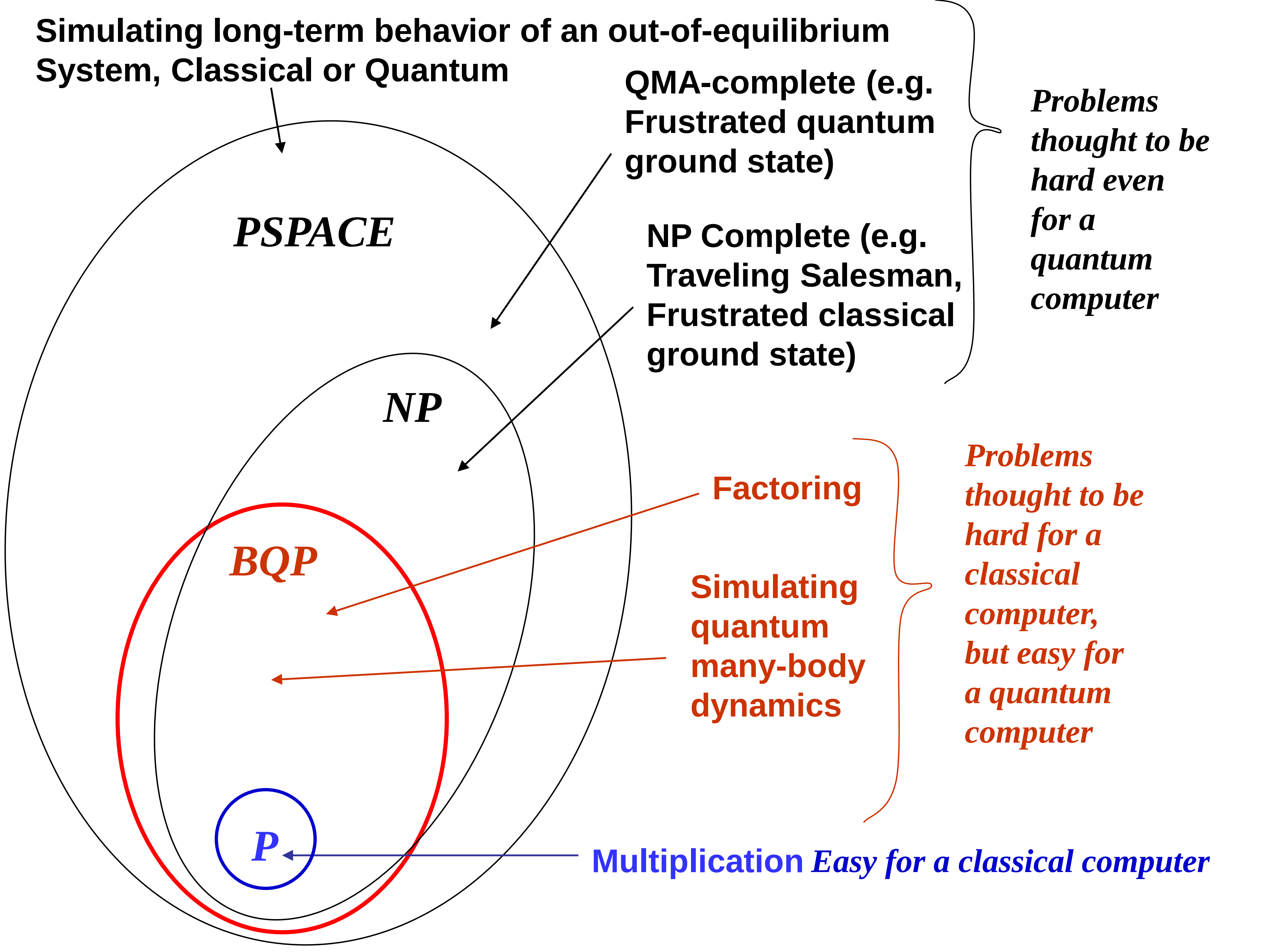
Of course the main reason there is so much interest in quantum information processing is a practical one: if a **quantum computer** could be built it would greatly speed up some classically hard computations, like factoring large numbers.



But building a quantum computer is hard, because the data inside it must be protected from eavesdropping till the computation is done.

Computer performance has been increasing exponentially for several decades (Moore's law). But this can't go on for ever. Can quantum computers give Moore's law a new lease on life? If so, how soon will we have them?





Simulating long-term behavior of an out-of-equilibrium System, Classical or Quantum

QMA-complete (e.g. Frustrated quantum ground state)

NP Complete (e.g. Traveling Salesman, Frustrated classical ground state)

Problems thought to be hard even for a quantum computer

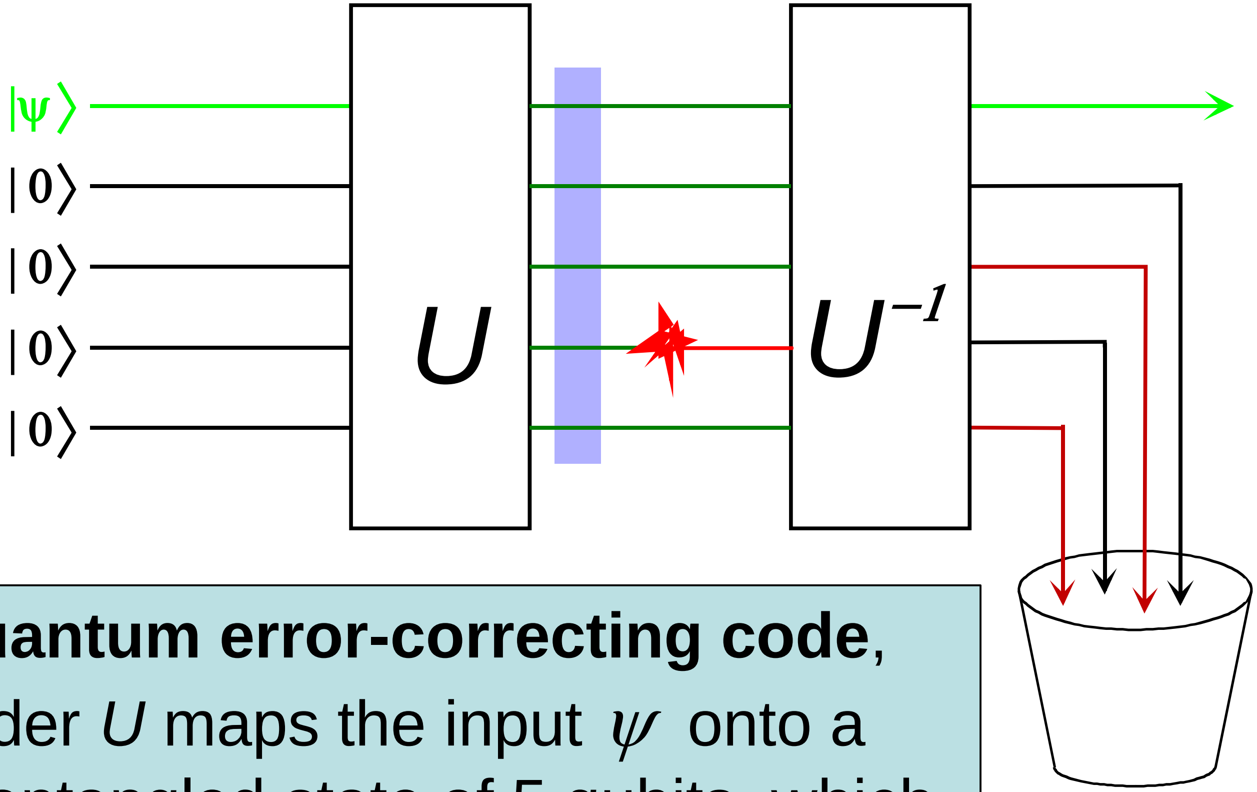
Factoring

Simulating quantum many-body dynamics

Problems thought to be hard for a classical computer, but easy for a quantum computer

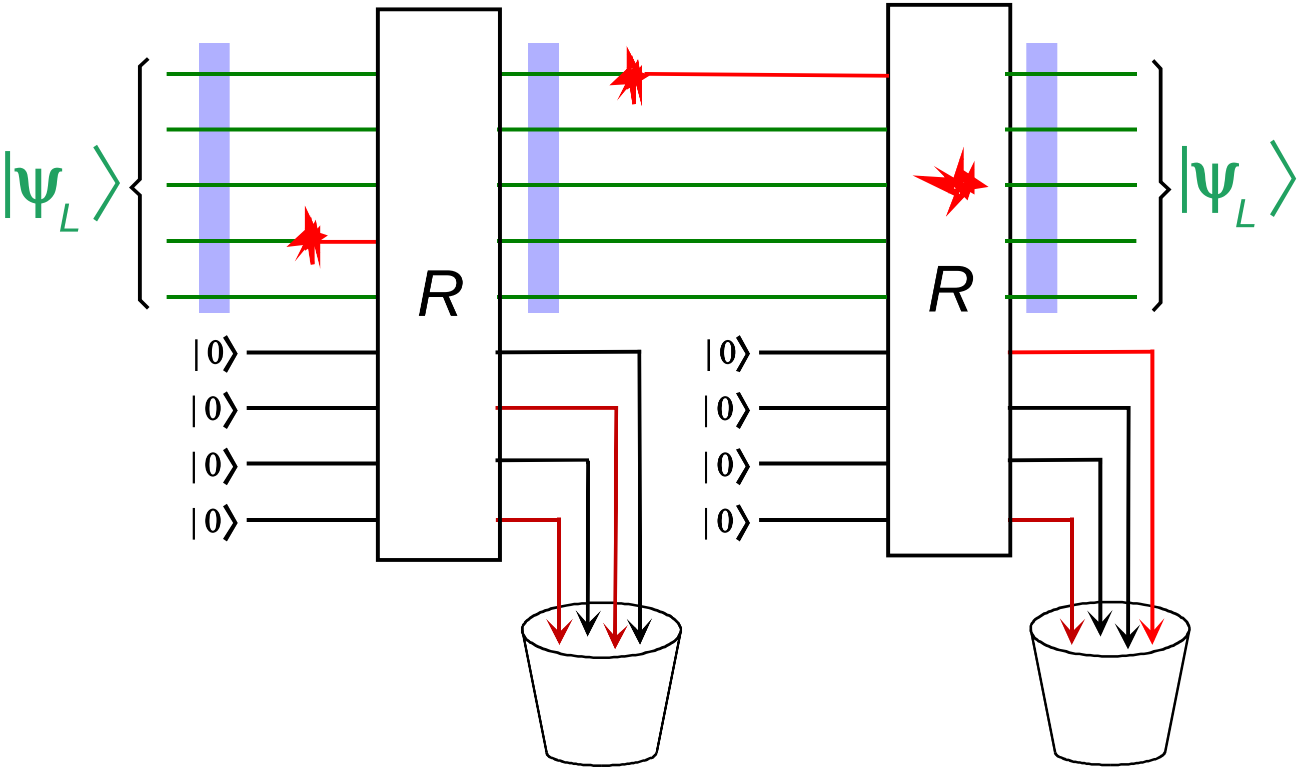
Multiplication *Easy for a classical computer*

Perfectly isolating a quantum computer from its environment is impossible, but if it can be 99.9% or so isolated, quantum error correction techniques can do the rest.



In this **quantum error-correcting code**, the encoder *U* maps the input ψ onto a robustly entangled state of 5 qubits, which can withstand the corruption of any one qubit and still allow the input to be perfectly recovered at the receiving end.

Quantum Fault Tolerant Computation



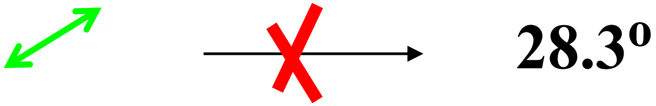
Clean qubits are brought into interaction with the quantum data to siphon off errors, even those that occur during error correction itself.

Conclusions

- Quantum information provides a coherent basis for the theory of communication, computing, and interaction between systems, within which classical behavior emerges as a special case.
- A classical communications channel is a quantum channel with an eavesdropper (maybe only the environment). A classical computer is a quantum computer handicapped by having eavesdroppers on all its wires.
- Quantum information processing has exciting applications in cryptography, computing, simulation and measurement that need to be explored experimentally and theoretically. Though a quantum computer would speed up some computations dramatically, it would not bring back Moore’s law.

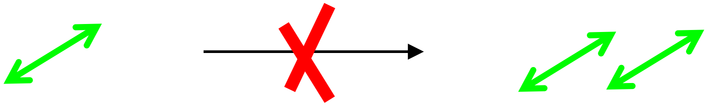
Like the roundness of the earth, or fact that matter is made of atoms, the quantum nature of information is a fundamental but non-obvious aspect of our universe that everyone should know about. Scientists and engineers need to understand it deeply, cultivating a **quantum intuition**, the better to discover and implement its applications.

Measuring an unknown photon’s polarization exactly is impossible (no measurement can yield more than 1 bit about it).

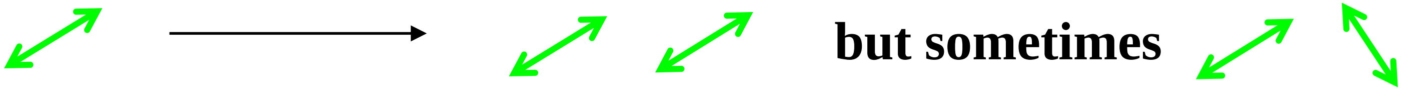


28.3°

Cloning an unknown photon is impossible. (If either cloning or measuring were possible the other would be also).



If you try to amplify an unknown photon by sending it into an ideal laser, the output will be polluted by just enough noise (due to spontaneous emission) to be no more useful than the input in figuring out what the original photon’s polarization was.



but sometimes

Extra Topics:

The Einstein-Bohr debate, and Einstein’s tragic misconception

Easy questions with hard answers:

How much information is contained in a qubit, compared to a bit?

Where do quantum speedups come from?

The Einstein -Bohr debate:

When the weird behavior of subatomic particles became evident in the early 20th century, Niels Bohr argued that physicists must learn to accept it. There were two kinds of weird behavior: indeterminacy---the random behavior of individual particles even under completely controlled conditions and entanglement, in which two particles, no matter how far apart, can behave in ways that are individually random, but too strongly correlated for the particles to have been acting independently. Einstein was deeply troubled by these phenomena, disparaging indeterminacy as “God playing dice,” and the entanglement as “spooky action at a distance.” He spent his remaining years searching unsuccessfully for a more naturalistic theory, where every effect would have a nearby cause. Newton’s mechanics, Maxwell’s electromagnetism, and his own relativity share this common-sense property, without which, Einstein thought, science could no longer aspire to be an orderly explanation of nature.

Meanwhile the rest of the physics community, including greats like Schrödinger, Heisenberg, and Dirac, followed Bohr’s advice and accepted these disturbing phenomena, and the mathematics that explained them, as the new normal.

Now, 90 years later, it’s pretty clear that the most celebrated scientific mind of the 20th century, flexible enough to bend space and time, still wasn’t flexible enough. Quantum randomness and entanglement are real, confirmed by innumerable experiments, and explained in meticulous detail by the theory Einstein disliked. Moreover, quantum theory has played an essential role in technologies such as the laser and the transistor, which could not have been developed on the pre-quantum physics of Newton, Maxwell, and Einstein.

Einstein’s mistake was in viewing entanglement as some kind of influence of one particle on the other. The right way to think of it is by giving up basic common sense idea that if the whole is in a perfectly definite state, each part must be in a perfectly definite state. An entangled state is a different kind of state of the whole, which is perfectly definite but requires the parts each to behave randomly. Making any measurement on one of two entangled particles yields a random result, but from that random result, it is possible to perfectly predict what the other particle would do if subjected to the same measurement.

Schrödinger, who understood entanglement better than Einstein, called this effect “steering” but that’s a bad name for it. No one would want to drive a car with that kind of steering, because it couples two cars in a way that makes neither one controllable.   Both drivers would report that their cars had terrible dangerous steering, so that turning the wheel to the right sometimes caused their car to go right but equally likely caused it to go left. Only afterward, when the drivers compared crash reports, would they realize that their cars had behaved in an eerily correlated way.

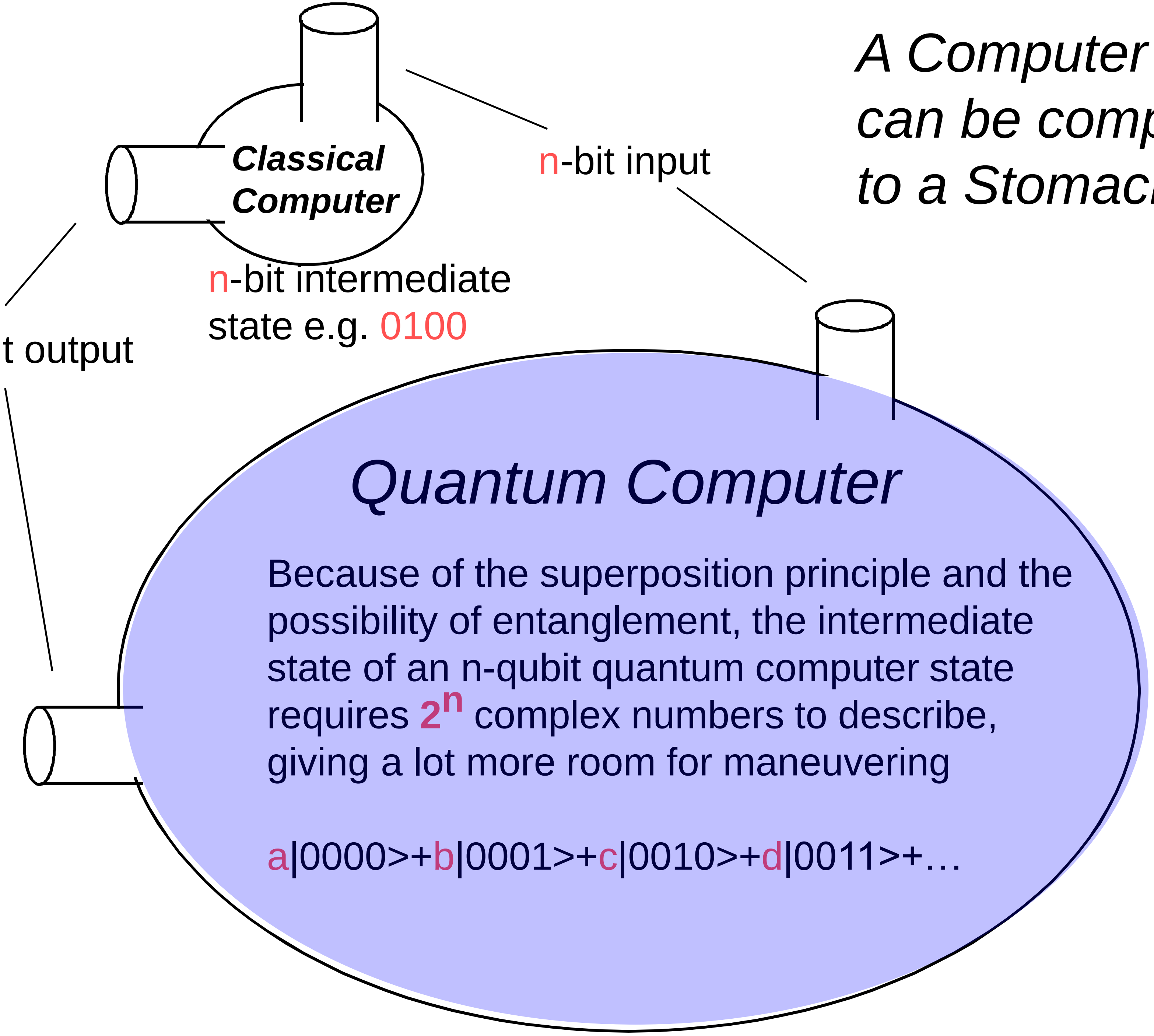
Mistakenly believing entanglement could be used for long-range communication, Nick Herbert published a paper and Jack Sarfatti tried to patent this imagined application of it. The refutation of these proposals in the early 1980s, by Dieks, Wootters and Zurek, is part of what led to modern quantum information theory. But this wrong idea, like perpetual motion, is so appealing that it is perpetually being “rediscovered”.

A proper understanding of entanglement not only explains why it cannot be used to communicate, but how it brings about the other quantum mystery that troubled Einstein, the random behavior of individual particles. Entanglement’s intense correlation is mathematically inseparable from its monogamy, and the random behavior of the parts.

People often ask “How Much Information is contained in n qubits, compared to n classical bits, or n analog variables?” A somewhat ill-posed question, because it neglects the nature of quantum reality, specifically entanglement.

	Digital	Analog	Quantum
Information required to specify a state	n bits	n real numbers, but with precision limited by the hardware	2^n complex numbers
Information extractable from state	n bits		n bits
Good error correction?	yes	no	yes

A Computer can be compared to a Stomach



Classical Computer

n-bit input

n-bit intermediate state e.g. 0100

n-bit output

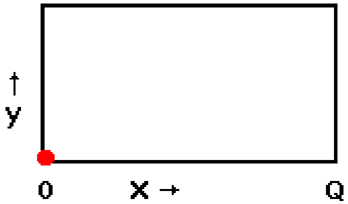
Quantum Computer

Because of the superposition principle and the possibility of entanglement, the intermediate state of an n-qubit quantum computer state requires $\mathbf{2^n}$ complex numbers to describe, giving a lot more room for maneuvering

a|0000>+b|0001>+c|0010>+d|0011>+…

Shor's Quantum Super-Fast Fourier Sampling

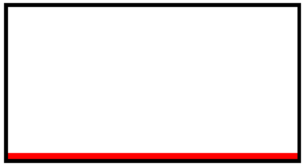
State | Action



X Register, Y Register

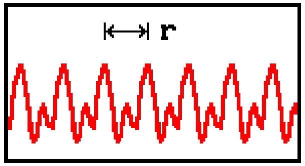
$|0,0\rangle$

Initial State



Generate X superposition

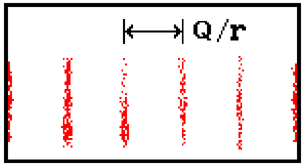
$$\frac{1}{\sqrt{Q}}\sum_x |x,0\rangle$$



Reversibly compute
y := y + f(x)

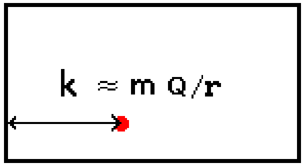
$$\frac{1}{\sqrt{Q}}\sum_x |x,f(x)\rangle$$

Fourier Transform
X register



$$\frac{1}{Q}\sum_{x,k} e^{2\pi ikx/Q}\,|k,f(x)\rangle$$

Measure
X register

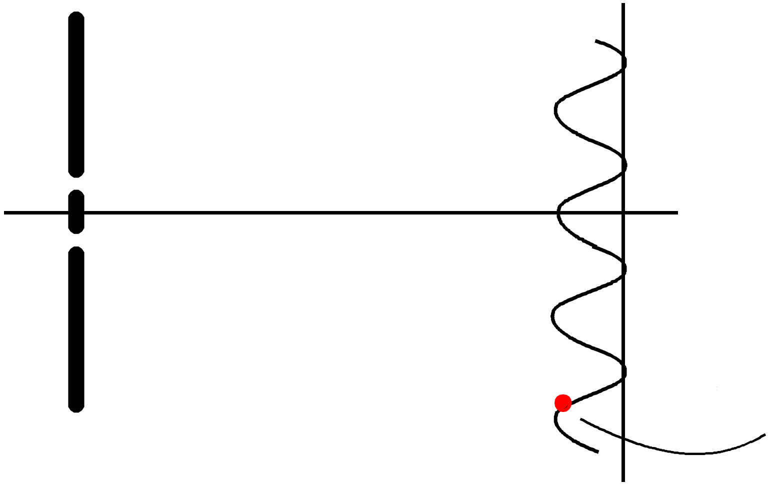


Result = k

r = numerator of r/m, where r/m = closest rational approximation to Q/k with denominator less than $\sqrt{Q}$

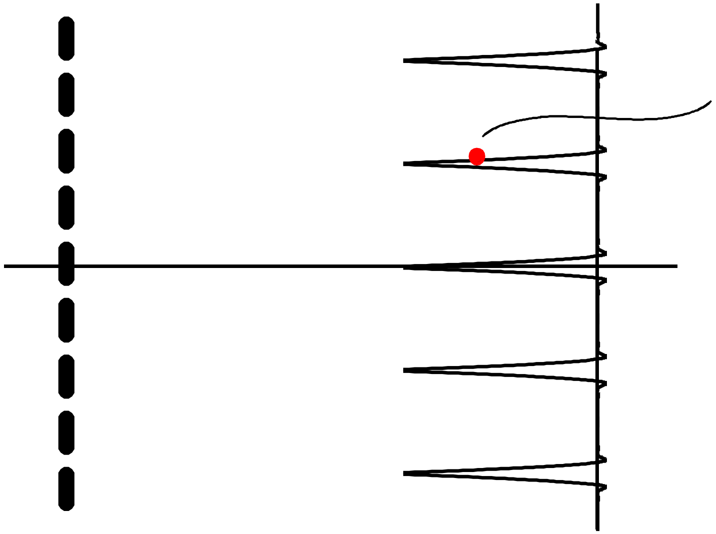
Shor algorithm uses interference to find unknown period of periodic function.

2 Slits
1 photon



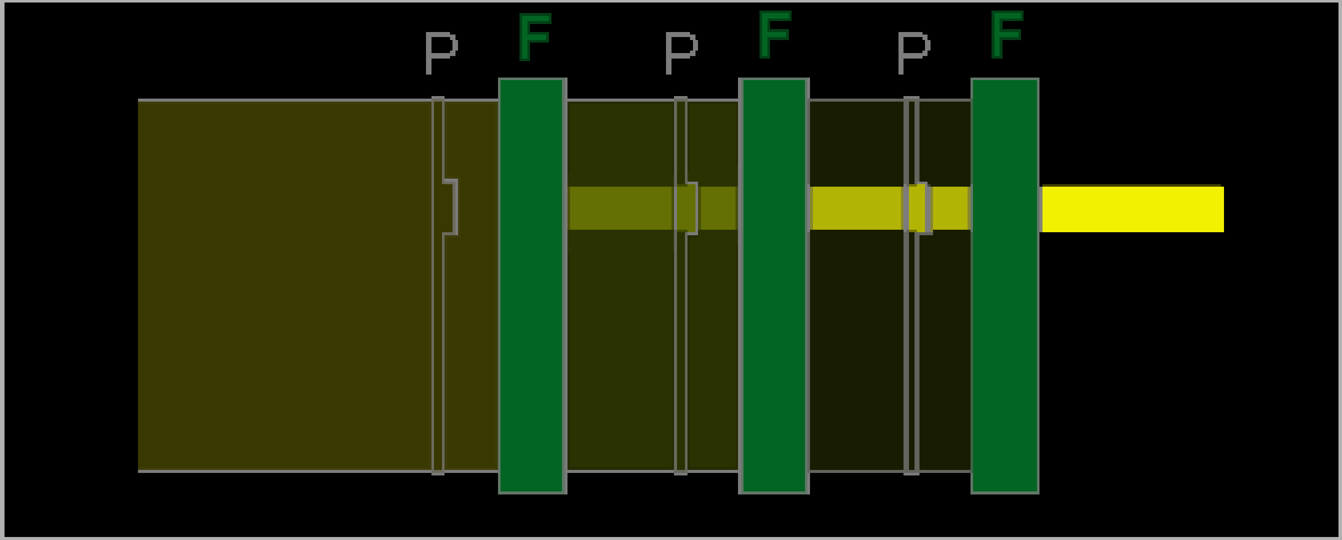
Photon impact point yields a little information about slit spacing

N Slits
1 photon



Photon impact point yields a lot of information about slit spacing

Grover's quantum search algorithm uses about √*N* steps to find a unique marked item in a list of *N* elements, where classically *N* steps would be required. In an optical analog, phase plates with a bump at the marked location alternate with fixed optics to steer an initially uniform beam into a beam wholly concentrated at a location corresponding to the bump on the phase plate.
If there are *N* possible bump locations, about √*N* iterations are required.

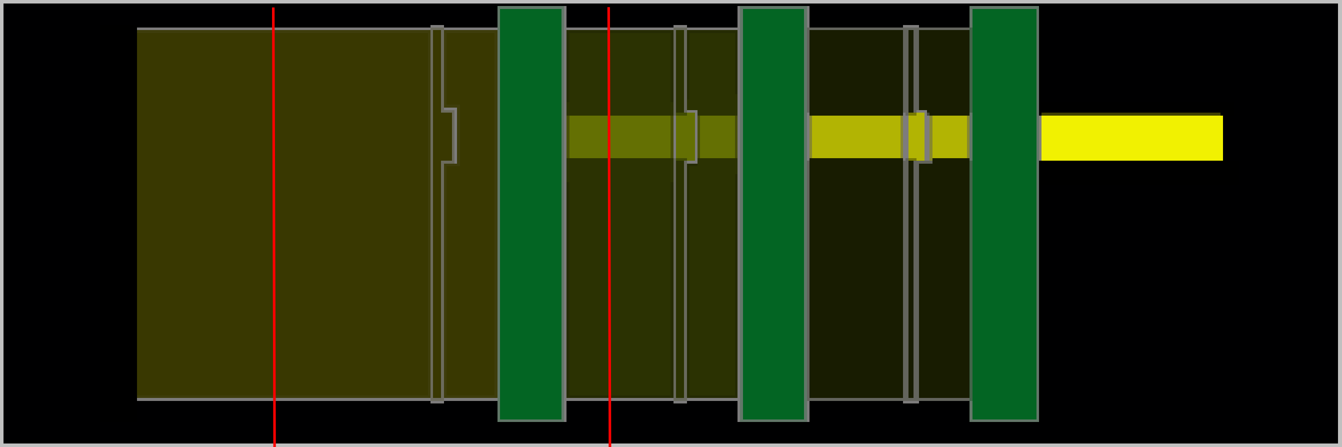


P = phase plate
F = fixed optics

Same optical setup works even with a single photon, so after about √*N* iterations it would be directed to the right location.

Optimality of Grover's Algorithm: Why can't it work in 1 iteration?

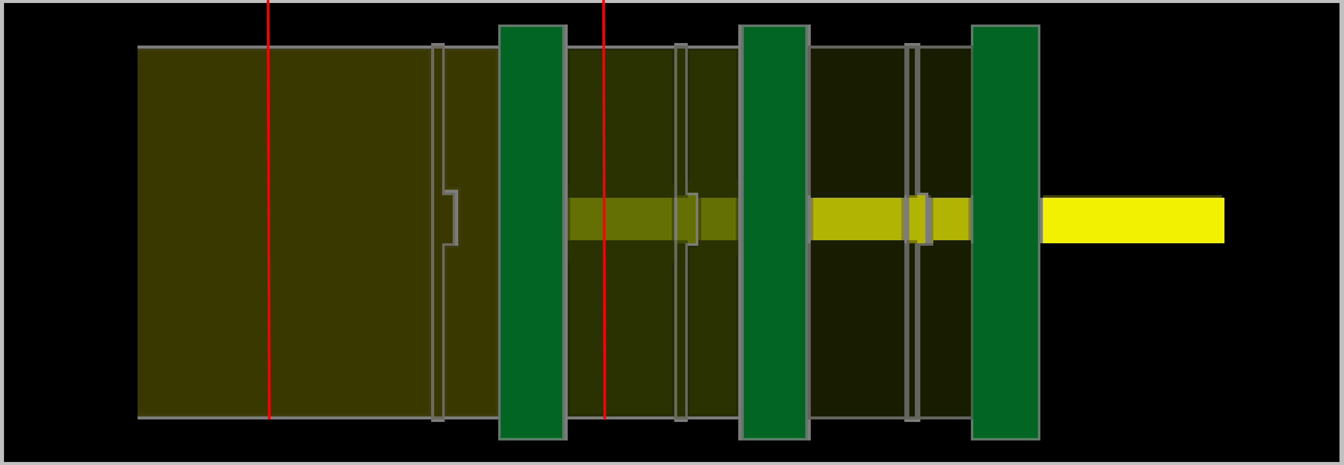
Original optical Grover experiment.



No difference initially

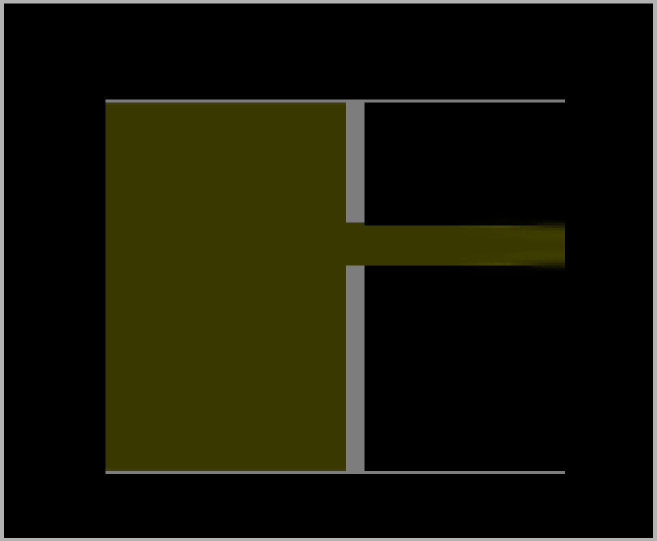
Small difference after 1 iteration

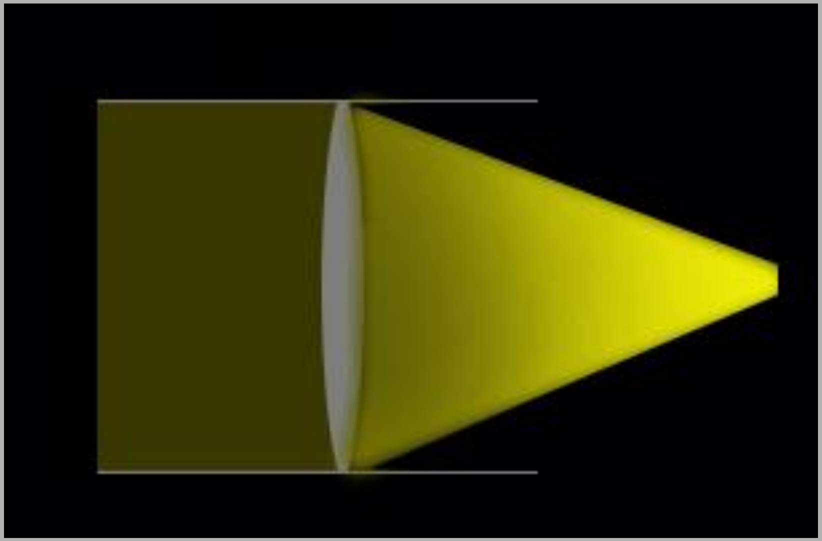
Repeat the experiment with the phase bump in a different location.



Because most of the beam misses the bump in either location, the difference between the two light fields can increase only slowly. About √*N* iterations are required to get complete separation. (BBBV quant-ph/9701001)

Non-iterative ways to aim a light beam.





Mask out all but desired area. Has disadvantage that most of the light is wasted. Like classical trial and error. If only 1 photon used each time, N tries would be needed.

Lens: Concentrates all the light in one pass, but to use a lens is cheating. Unlike a Grover iteration or a phase plate or mask, a lens steers all parts of the beam, not just those passing through the distinguished location.