

Introduction to Quantum Information



Charles H. Bennett
IBM Research
Yorktown

YouQu 2015
HRI Allahabad
24 Feb 2015

Science can be a very satisfying career.

(I always wanted to be a scientist, from before age 5,
so I'm not the best person to ask.)

- Always something new to do and be curious about.
- Ability to appreciate progress in all areas of science, not only your own. Scientists, professional or amateur, can still almost be “renaissance persons,” at least with respect to the natural world.
- Less backsliding than any other area of human endeavor.
- If you are patient, and live long enough, you can see questions answered you've been wondering about for decades, maybe even help answer them.

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 (**AND, NOT**) acting on bits one and two bits.

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

A Venn diagram illustrating the relationship between different types of information. It consists of a large light blue oval containing a smaller gray oval. Inside the gray oval, the text "(Classical) Information" is centered. Below this text, a red rectangular box with a black border contains the text "Information Technology". The text "Quantum Information" is positioned below the gray oval, within the light blue oval.

(Classical)
Information

Information Technology

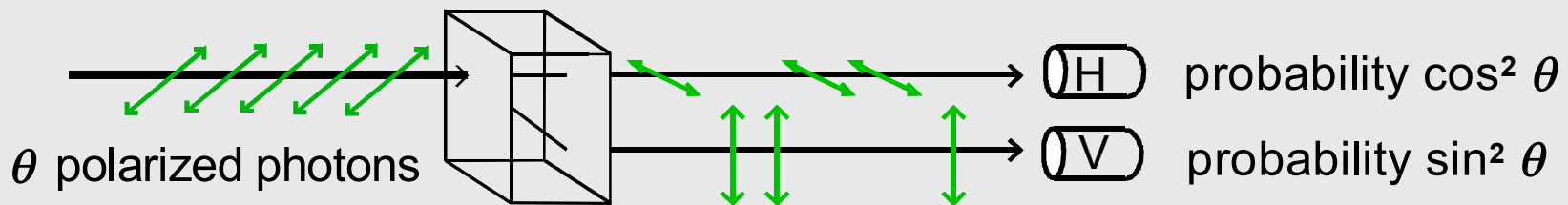
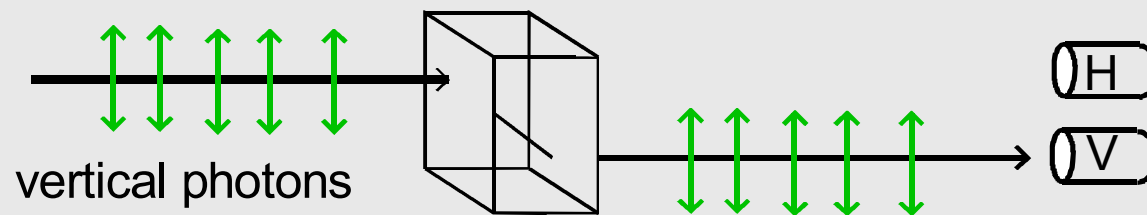
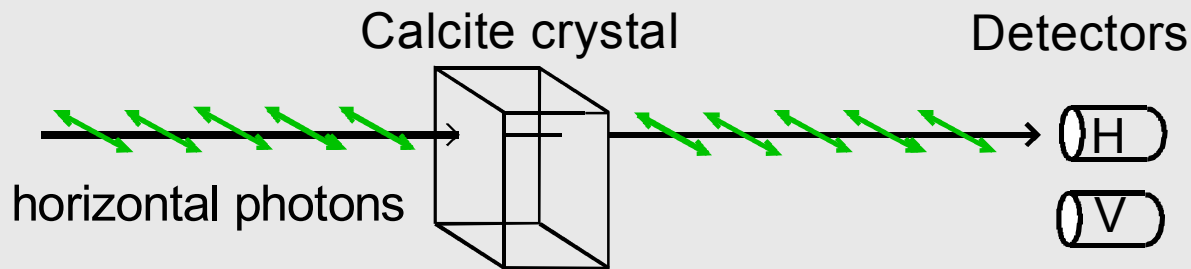
Quantum Information

The central principle of quantum mechanics is the

Superposition Principle:

- Between any two reliably distinguishable states of a physical system there is a continuum of intermediate states that are not reliably distinguishable from either original state.
- Physical states behave mathematically like directions in space. (Not ordinary three dimensional space, but a space of dimensionality equal to the system's maximum number of reliably distinguishable states.)
- Two states are reliably distinguishable if and only if their corresponding directions are perpendicular.

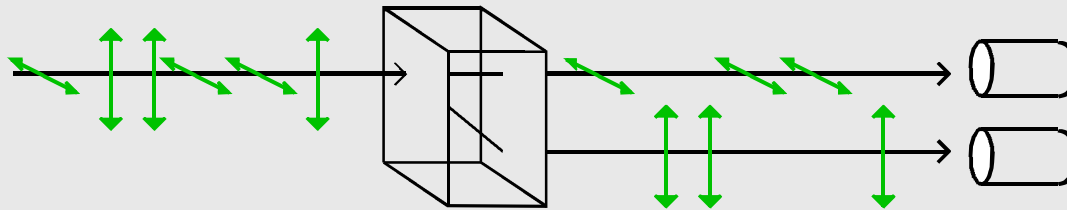
Using Polarized Photons to Carry Information



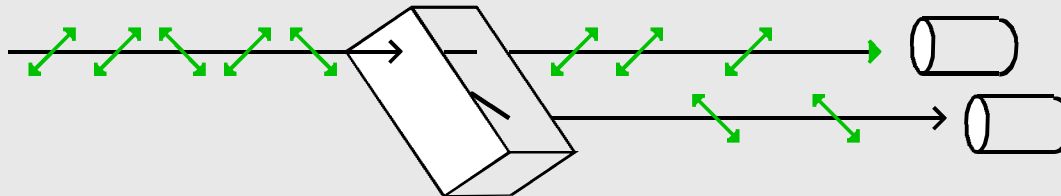
Photons behave reliably if measured along an axis parallel or perpendicular to their original polarization. Used in this way, each photon can carry one reliable bit of information.

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.



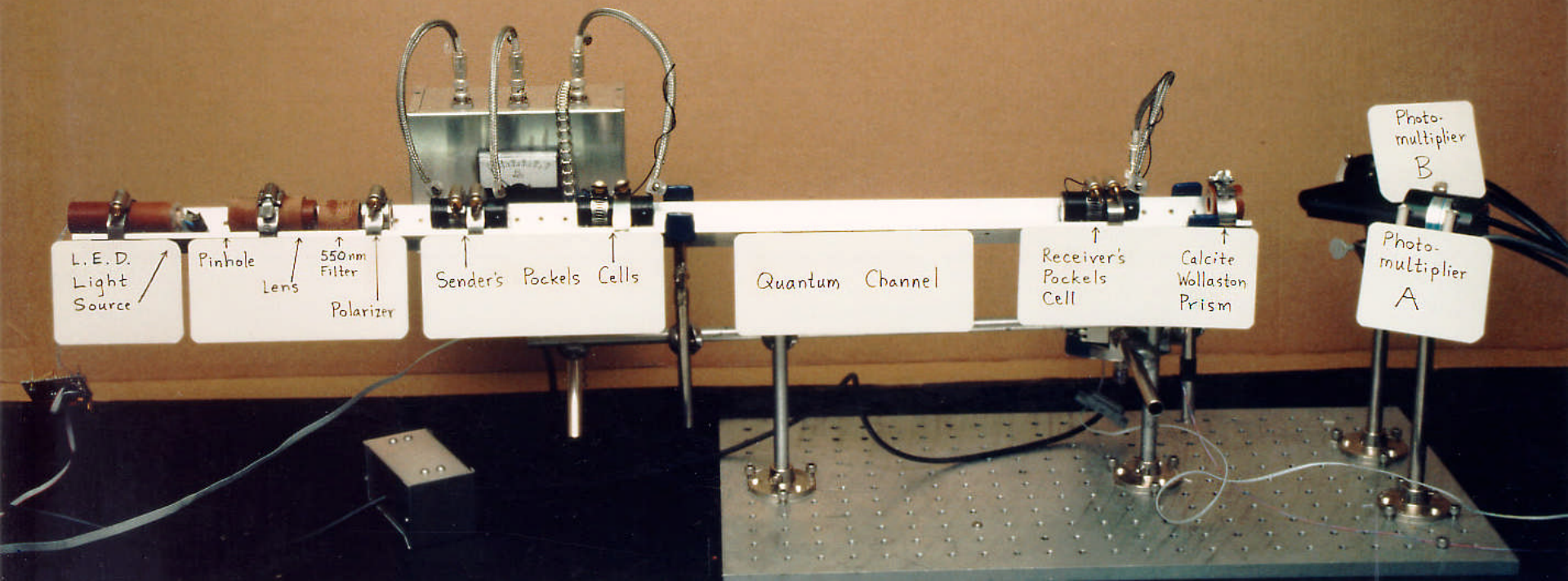
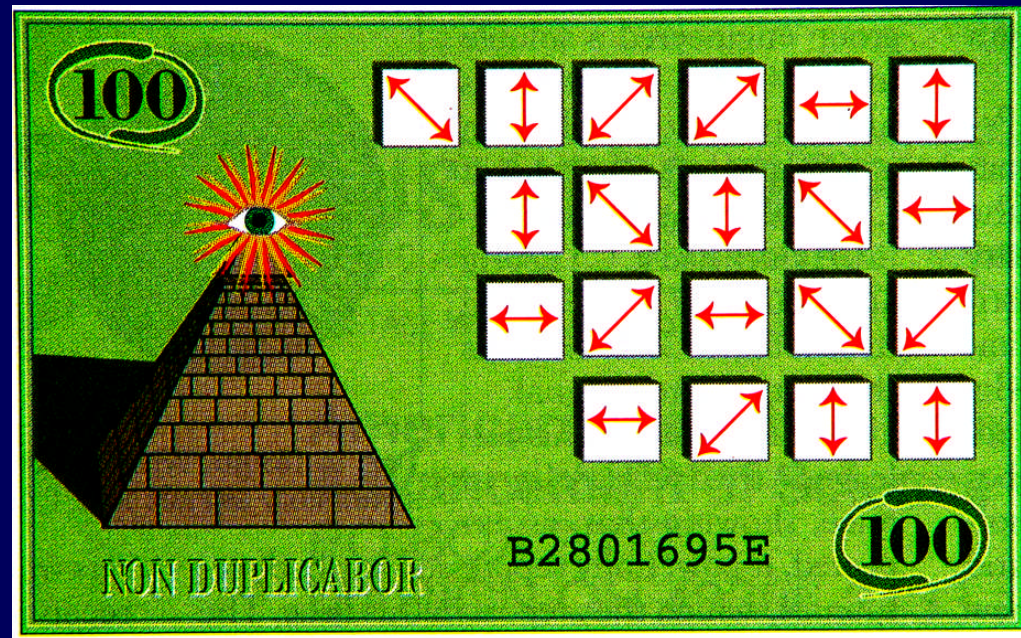
A diagonal measurement distinguishes diagonal photons reliably but randomizes rectilinear photons.



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.

Quantum money (Wiesner '70, '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, E91...)



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



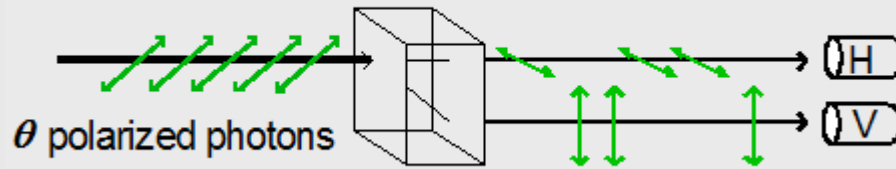
Cloning an unknown photon is impossible. (If either cloning or measuring were possible the other would be also).



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.



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 horizontal.

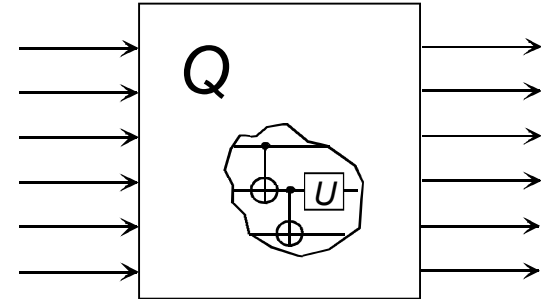
Teacher: **I believe I asked you a question.** Are you vertical or horizontal?

Pupil: Horizontal, sir.

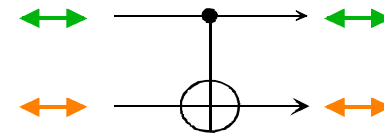
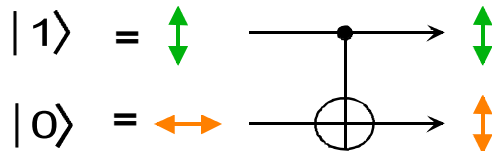
Teacher: Have you ever had any other polarization?

Pupil: No, sir. I was always horizontal.

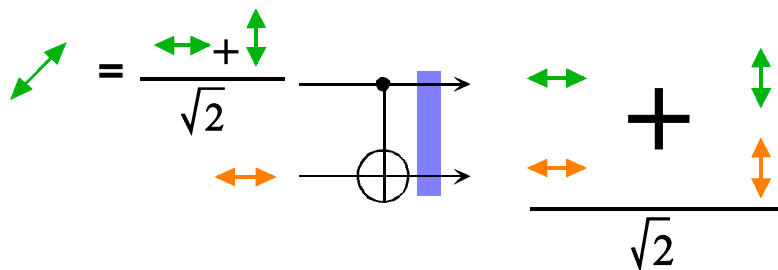
Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.



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

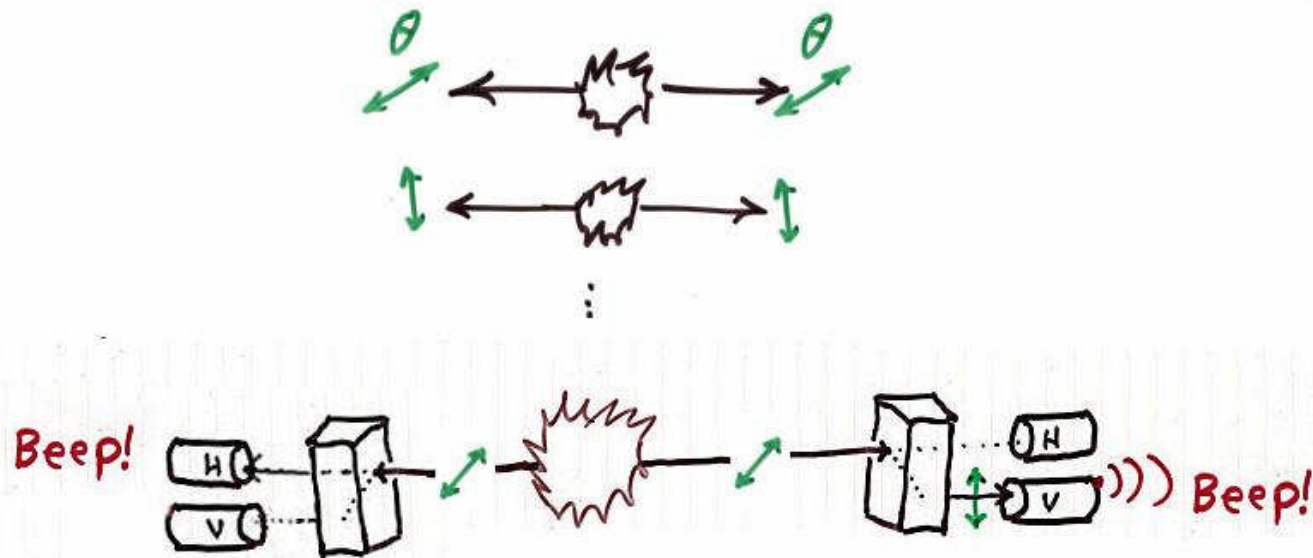
This entangled state of two photons behaves in ways that cannot be explained by supposing that each photon has a state of its own.

$$\frac{\begin{pmatrix} \text{green } \longleftrightarrow \\ \text{orange } \longleftrightarrow \end{pmatrix} + \begin{pmatrix} \text{green } \updownarrow \\ \text{orange } \updownarrow \end{pmatrix}}{\sqrt{2}} = \frac{\begin{pmatrix} \text{green } \nearrow \\ \text{orange } \nearrow \end{pmatrix} + \begin{pmatrix} \text{green } \nwarrow \\ \text{orange } \nwarrow \end{pmatrix}}{\sqrt{2}} \neq \begin{pmatrix} \text{green } \nearrow \\ \text{orange } \nearrow \end{pmatrix}$$

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.

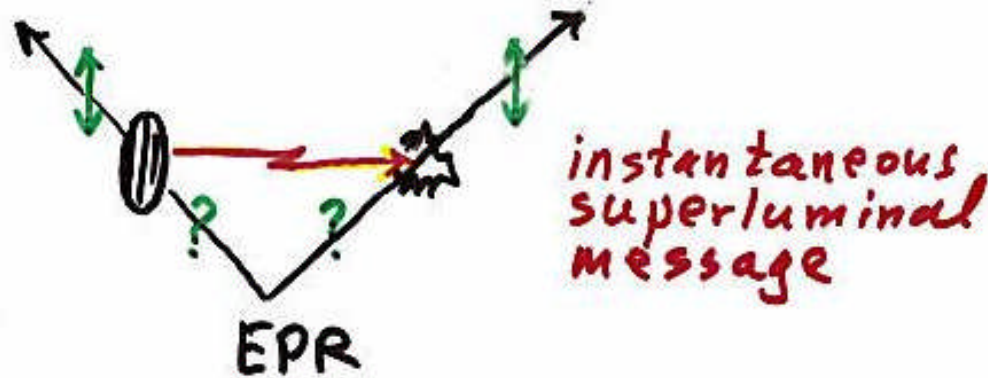
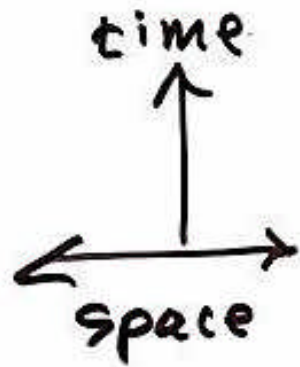
Alternative Explanations of EPR effect.

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



This explanation fails. Sometimes the source would emit 2 diagonal 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.

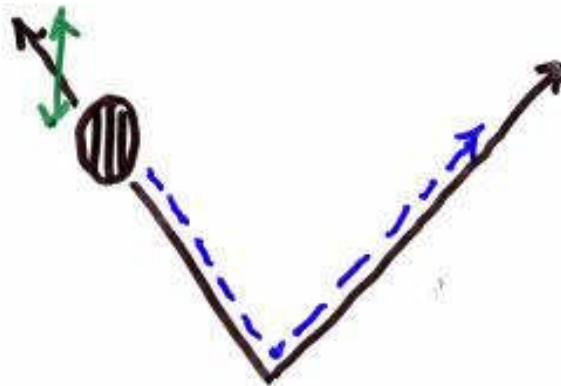
2. Instantaneous Action at a Distance



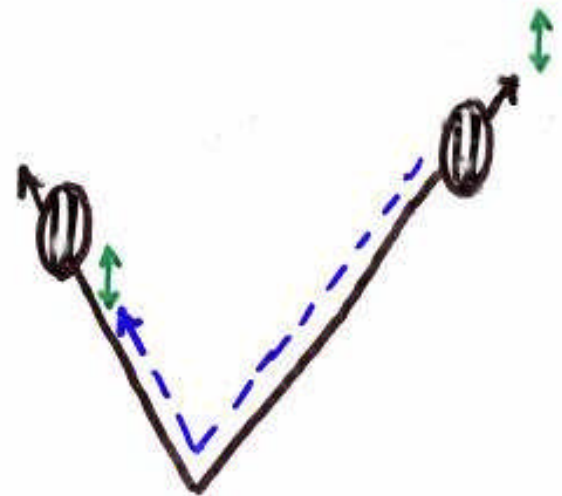
No. Violates special relativity and besides, how does the first particle know where to send the message to?

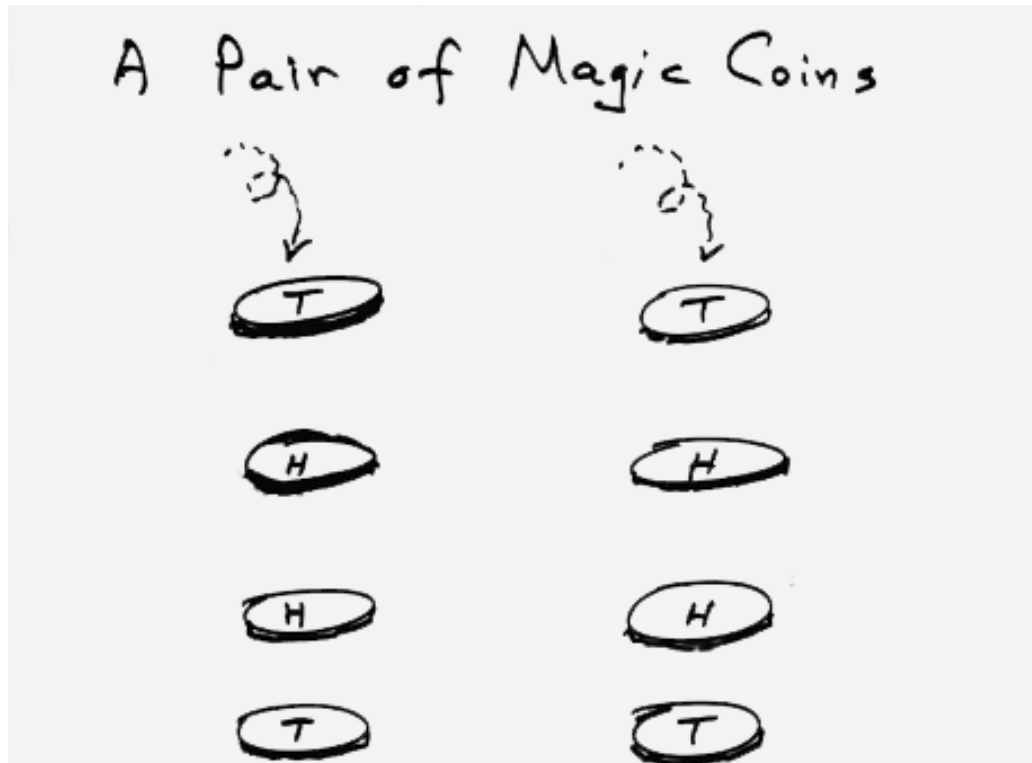
3. Quantum Mechanics - the right answer

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 (EPR effect) OR
2. Receiver disregards message (Cassandra myth).

Most states of any composite quantum system are **entangled**: states of the whole which behave in ways that cannot be explained by imagining that each part has a state of its own.

Entanglement allows two particles to be in a perfectly definite joint state, even though each one by itself is completely random. Like two hippies who are feel perfectly in tune with each other, even though neither has an opinion on anything.



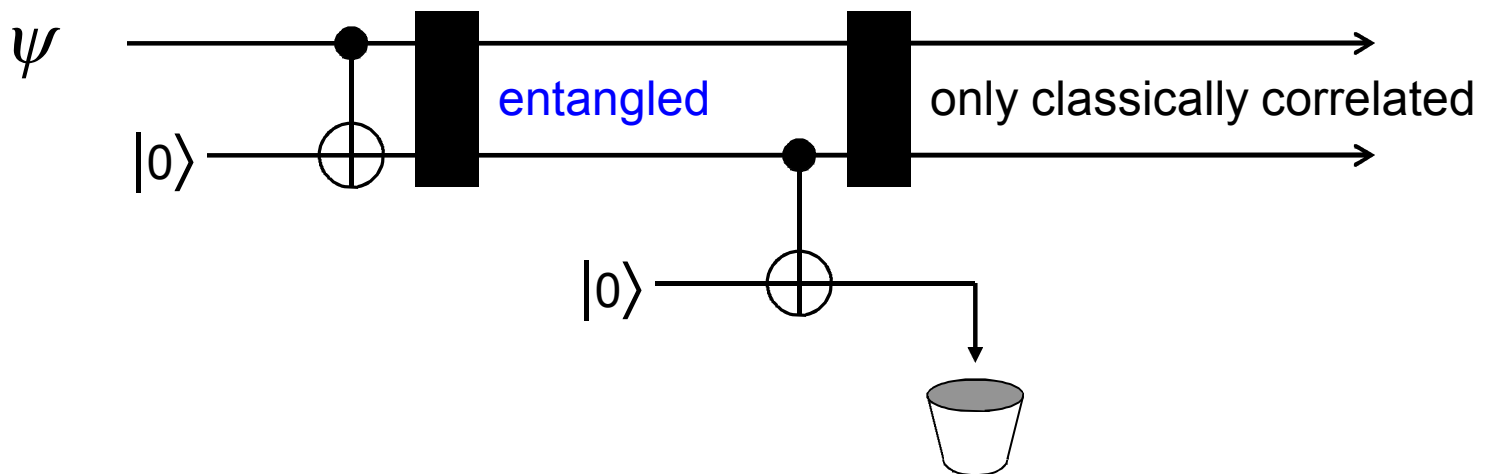
Hippies believed that with enough LSD, everyone could be perfectly in tune with everyone else.

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

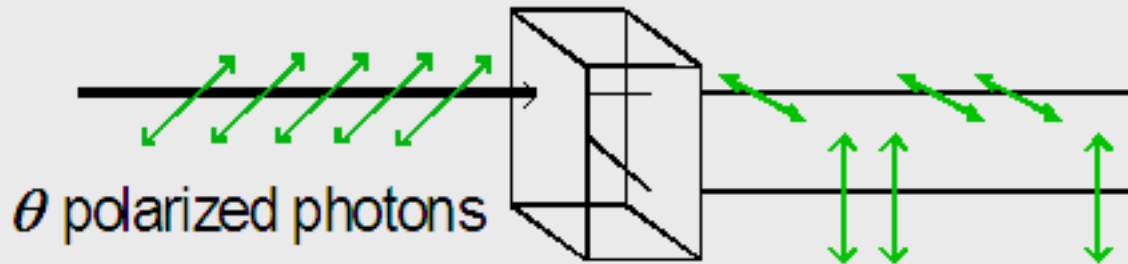
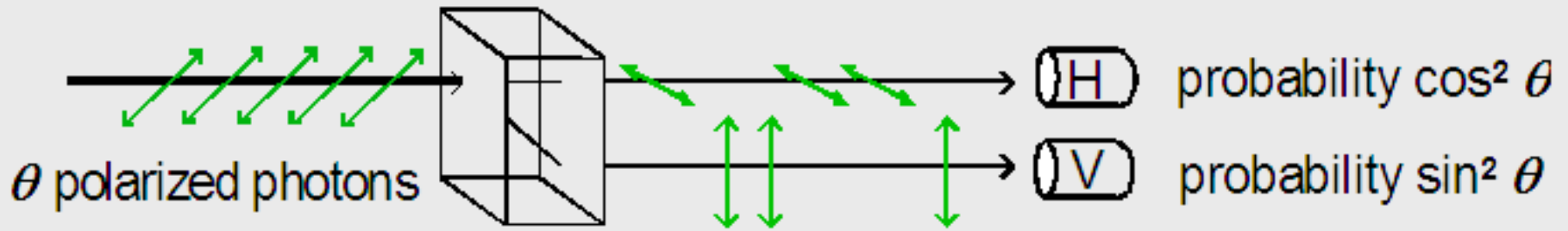
Monogamy of Entanglement

- If A and B are maximally entangled with each other, not only can't they be entangled with anyone else, they can't even be even classically correlated with anyone else.
- Indeed classical correlation typically arises from unsuccessful attempts to clone entanglement.

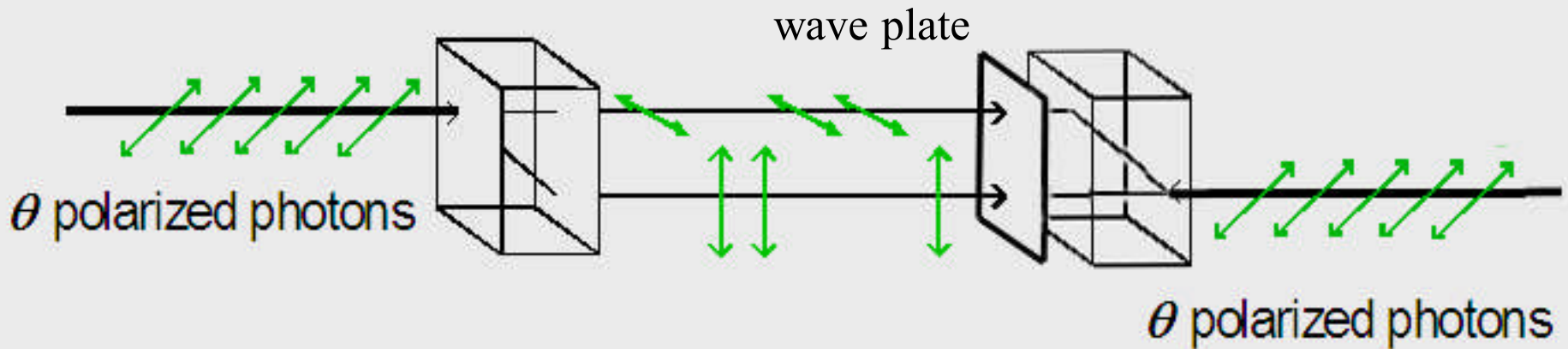
“Two is a couple, three is a crowd.”



Undoing a quantum Measurement



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

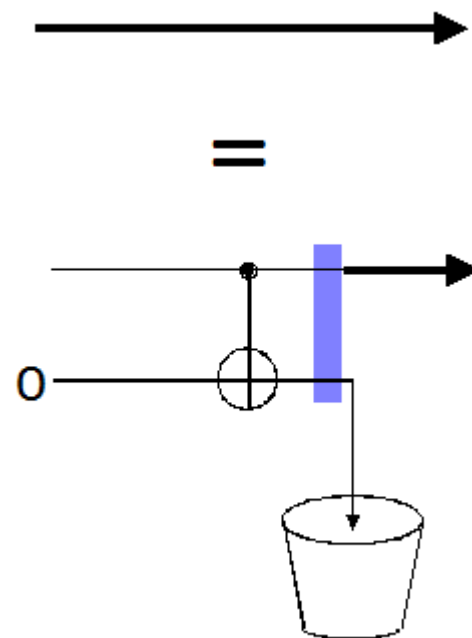
A Classical Bit is a qubit with one of the Boolean values 0 or 1

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.

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.

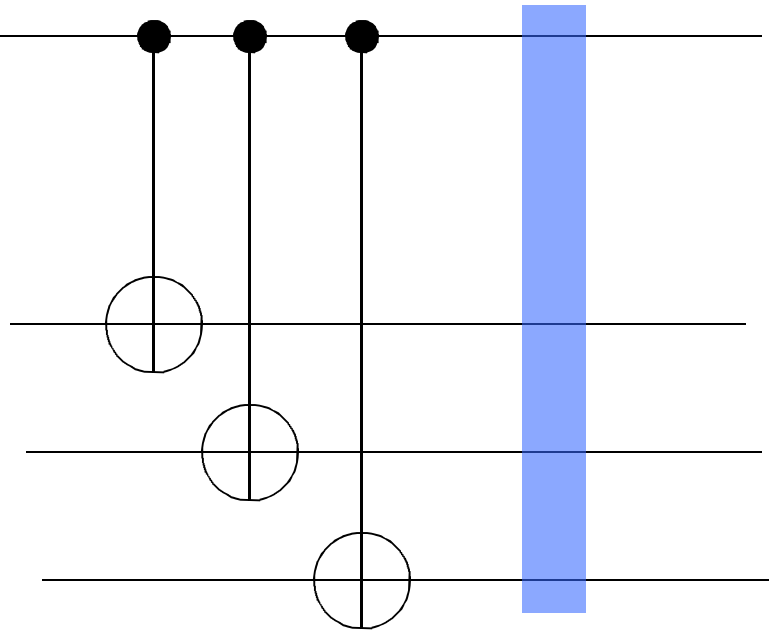
Most systems in nature, other than tiny ones like photons, interact so strongly with their environment as to become entangled with it almost immediately .

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

How does entanglement hide itself,
creating the appearance of a classical world?

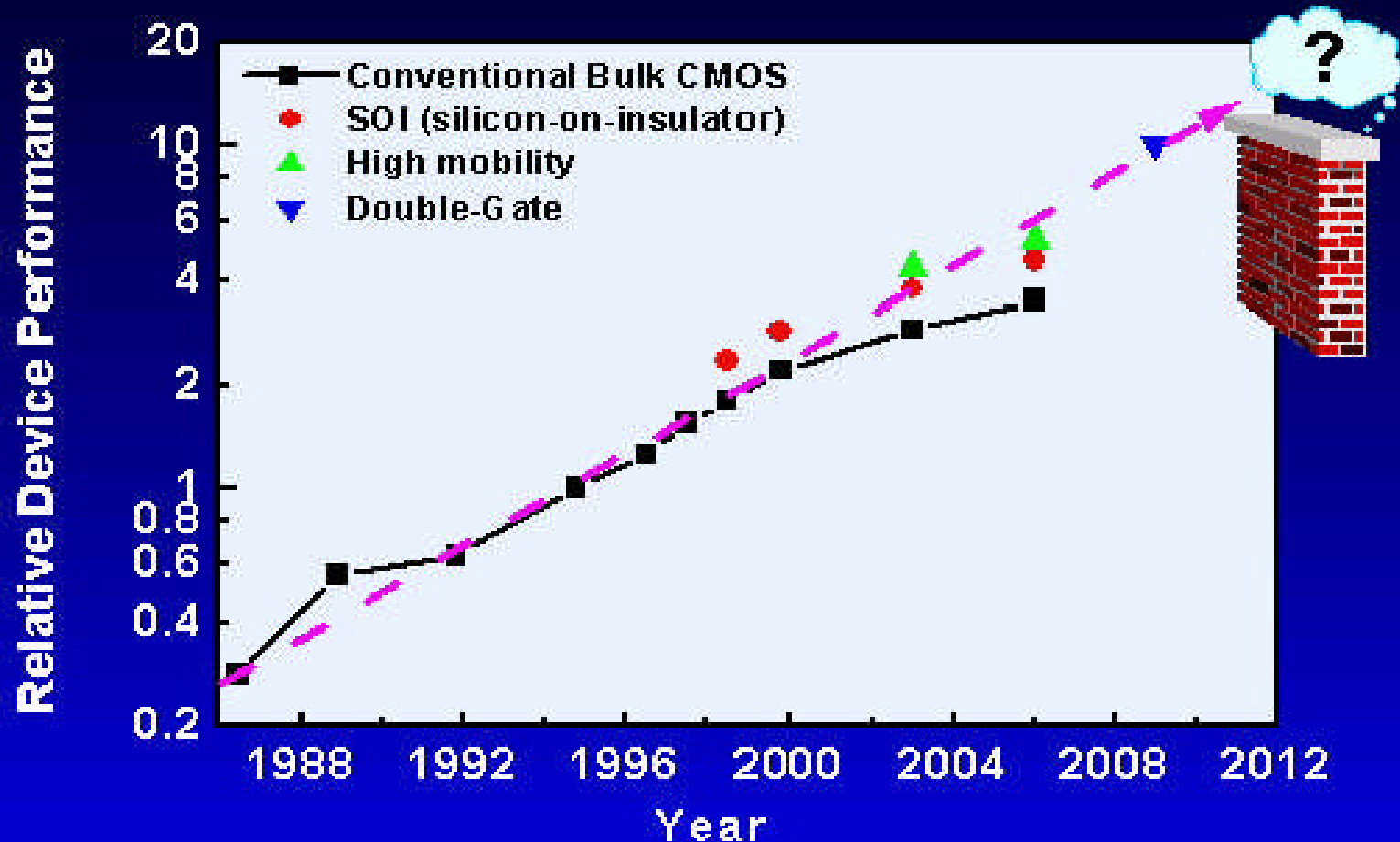
ψ
System

Parts
of the
system's
environ-
ment



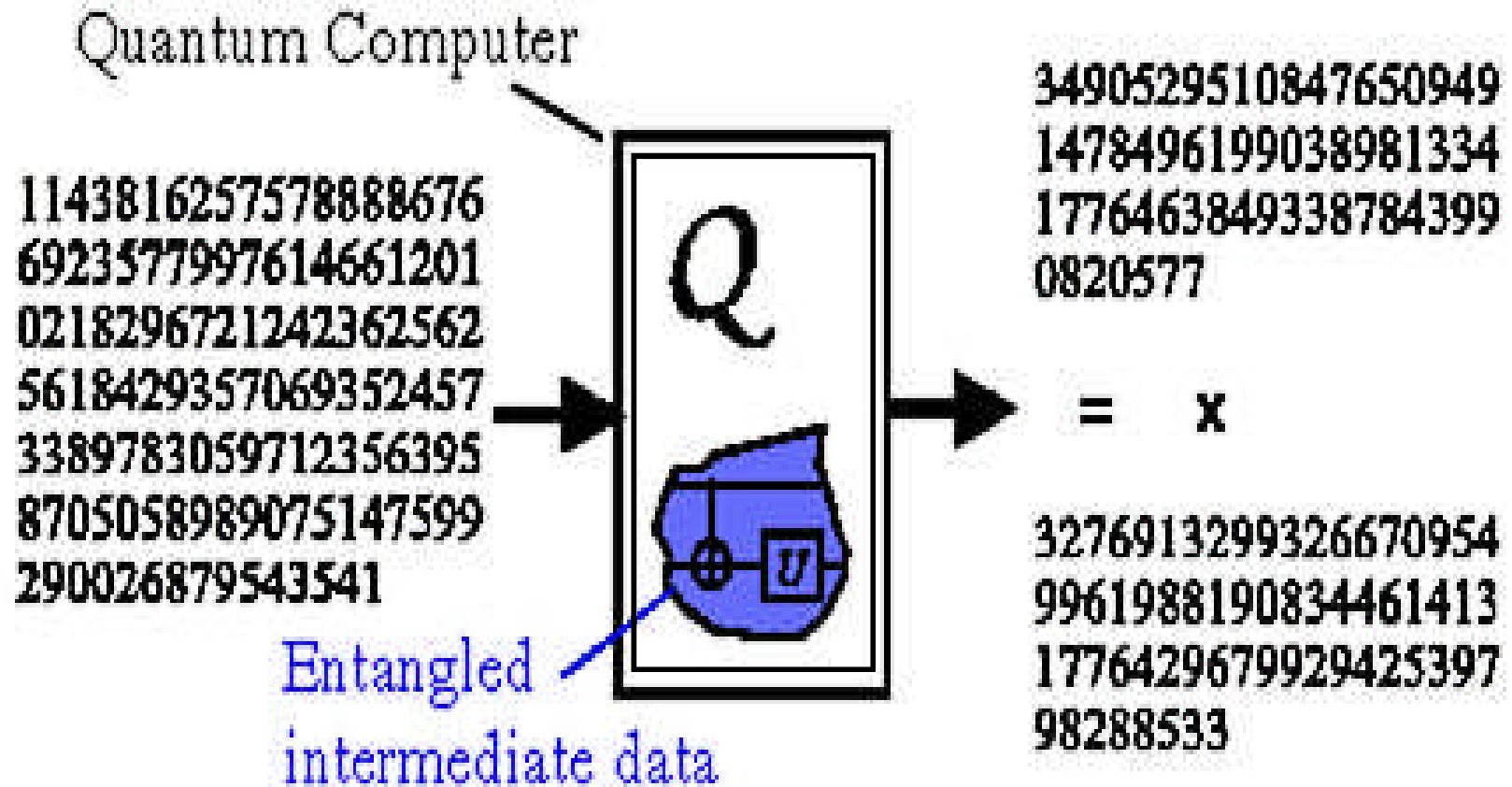
*Massive eavesdropping
causes the system to get
classically correlated
with many parts of its
environment. But because
of monogamy, it remains
entangled only with the
whole environment.*

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?



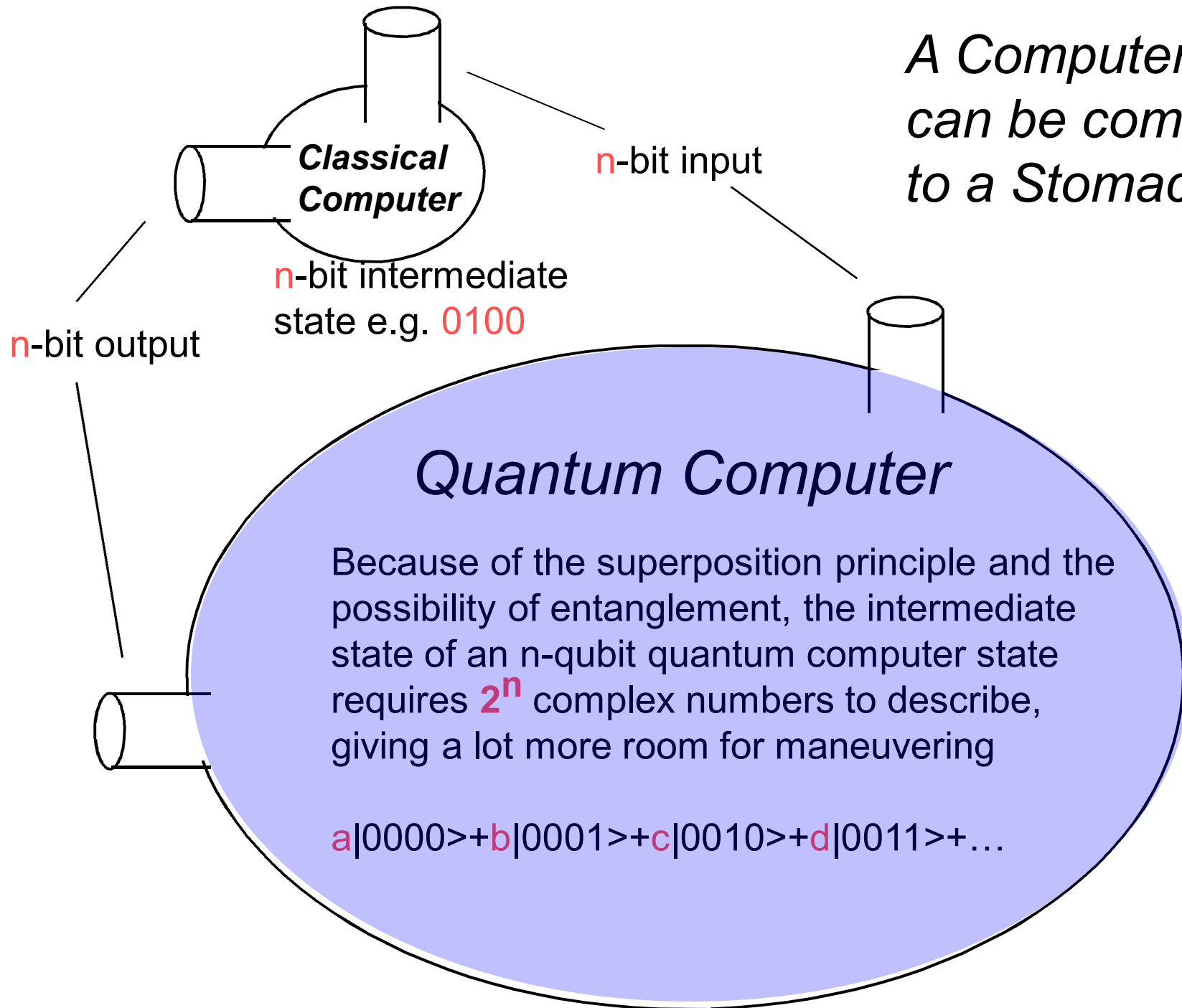
A quantum computer could solve some hard problems, like factoring, much faster than any known method on a classical computer.

Or to put it quantumly, some easy problems become much harder when there's an eavesdropper looking at all the intermediate stages of the computation.



carefully insulated to prevent
eavesdropping by the environment

*A Computer
can be compared
to a Stomach*



But isn't a quantum computer just a fancy kind of analog computer? We know analog computers don't work well.

	Digital		Analog		Quantum
Information required to specify a state	n bits	\approx	n real numbers	\ll	2^n complex numbers
Information extractable from state	n bits	\approx	n real numbers	\approx	n bits
Good error correction	yes	\approx	no	\ll	yes

The Downside of Entanglement

Quantum data is exquisitely sensitive to **decoherence**, a randomization of the quantum computer's internal state caused by entangling interactions with the quantum computer's environment.

Fortunately, decoherence can be prevented, in principle at least, by quantum error correction techniques developed since 1995, including

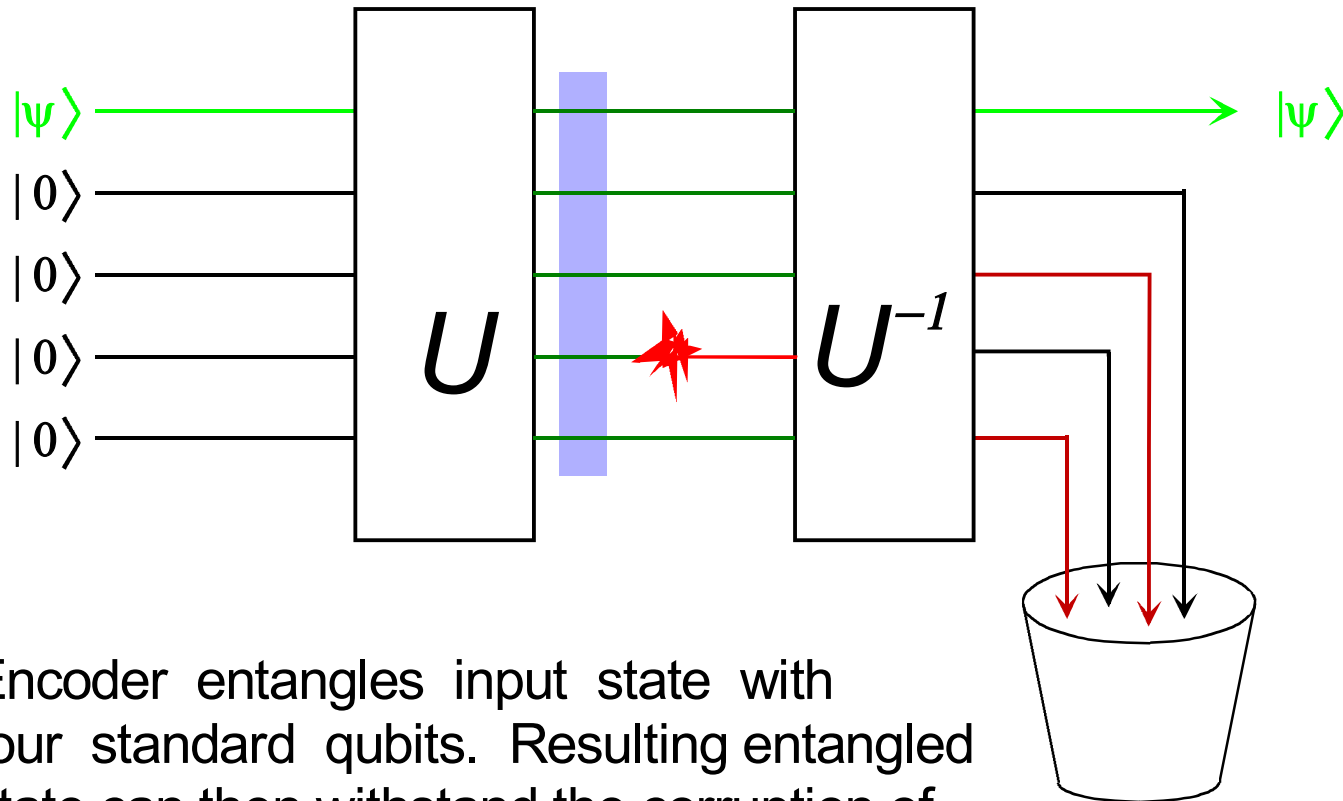
Quantum Error Correcting Codes

Entanglement Distillation

Quantum Fault-Tolerant Circuits

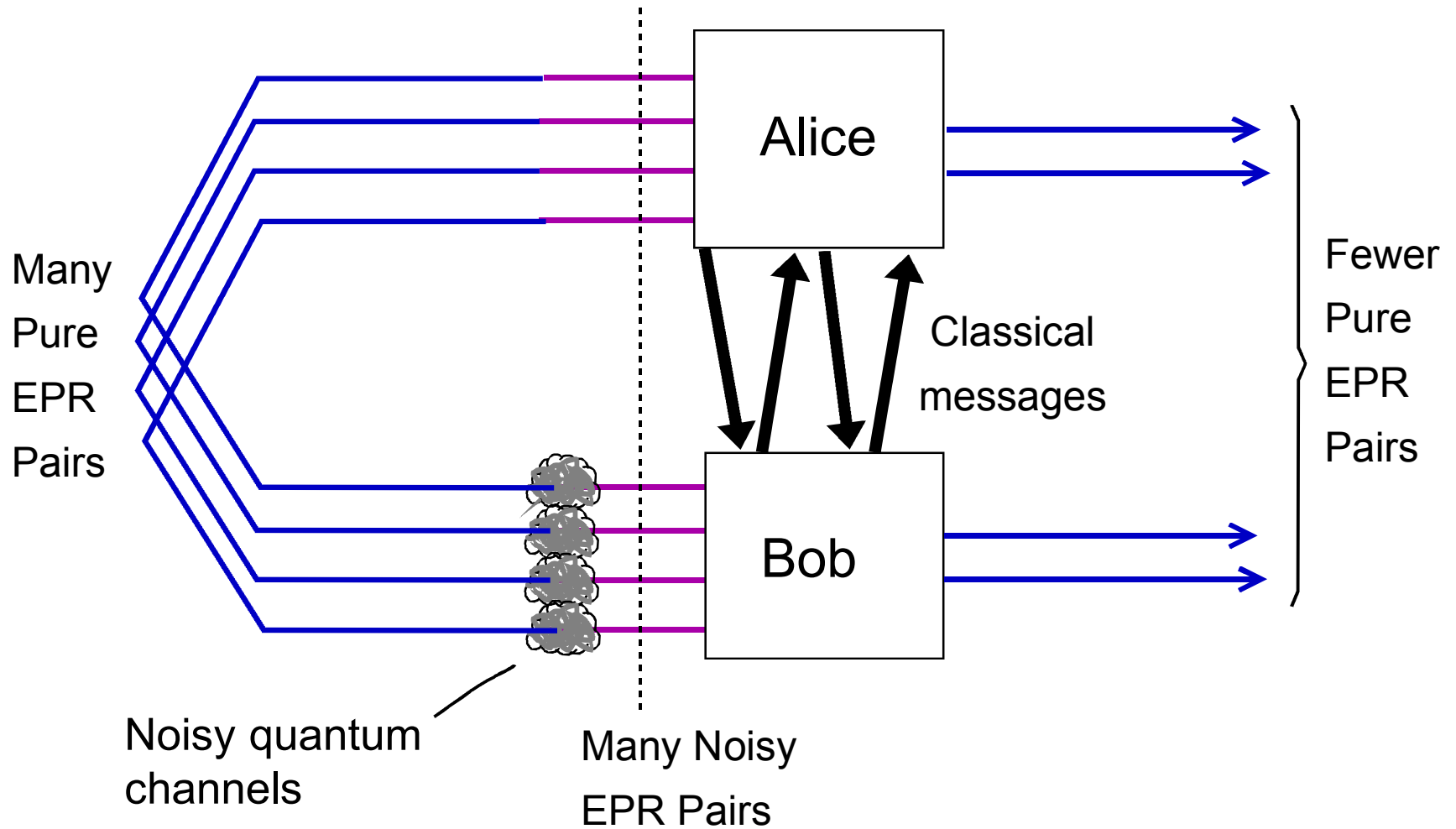
These techniques, combined with hardware improvements, will probably allow practical quantum computers to be built, but not any time soon.

The Simplest Quantum Error-Correcting Code

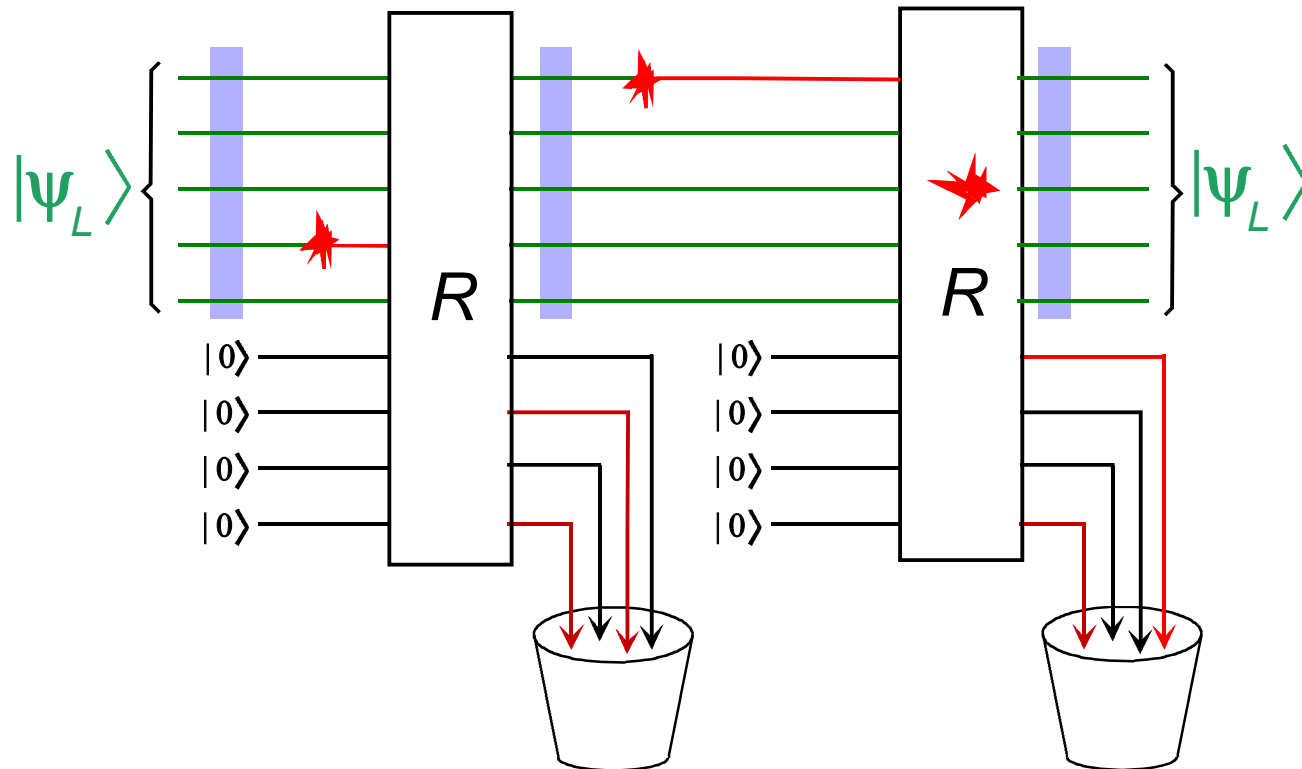


Encoder entangles input state with four standard qubits. Resulting entangled state can then withstand the corruption of any one of its qubits, and still allow recovery of the exact initial state by a decoder at the receiving end of the channel

Entanglement Distillation



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.

Pure vs. Mixed States,
Density Matrices,
and the Church of the
Larger Hilbert Space



1. A linear vector space with complex coefficients and inner product

$$\langle \phi | \psi \rangle = \sum \phi_i^* \psi_i$$

2. For polarized photons two, e.g. vertical and horizontal

$$\leftrightarrow = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \updownarrow = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

3. E.g. for photons, other polarizations

$$\nearrow = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \searrow = \begin{pmatrix} +1 \\ -1 \end{pmatrix}$$

$$\curvearrowright = \begin{pmatrix} i \\ 1 \end{pmatrix} \quad \curvearrowleft = \begin{pmatrix} i \\ -1 \end{pmatrix}$$

4. Unitary = Linear and inner-product preserving.

quantum laws

1. To each physical system there corresponds a Hilbert space ¹ of dimensionality equal to the system's maximum number of reliably distinguishable states. ²

2. Each direction (ray) in the Hilbert space corresponds to a possible state of the system. ³

3. Spontaneous evolution of an unobserved system is a unitary ⁴ transformation on its Hilbert space.

-- more --

4. The Hilbert space of a composite system is the tensor product of the Hilbert spaces of its parts. **1**

5. Each possible measurement **2** on a system corresponds to a resolution of its Hilbert space into orthogonal subspaces $\{P_j\}$, where $\sum P_j = 1$. On state ψ the result j occurs with probability $|P_j \psi|^2$ and the state after measurement is

$$\frac{P_j |\psi\rangle}{|P_j \psi|}$$

1. Thus a two-photon system can exist in "product states" such as $\leftrightarrow \leftrightarrow$ and $\leftrightarrow \nearrow$ but also in "entangled" states such as

$$\frac{\leftrightarrow \leftrightarrow - \leftrightarrow \updownarrow}{\sqrt{2}}$$

in which neither photon has a definite state even though the pair together does

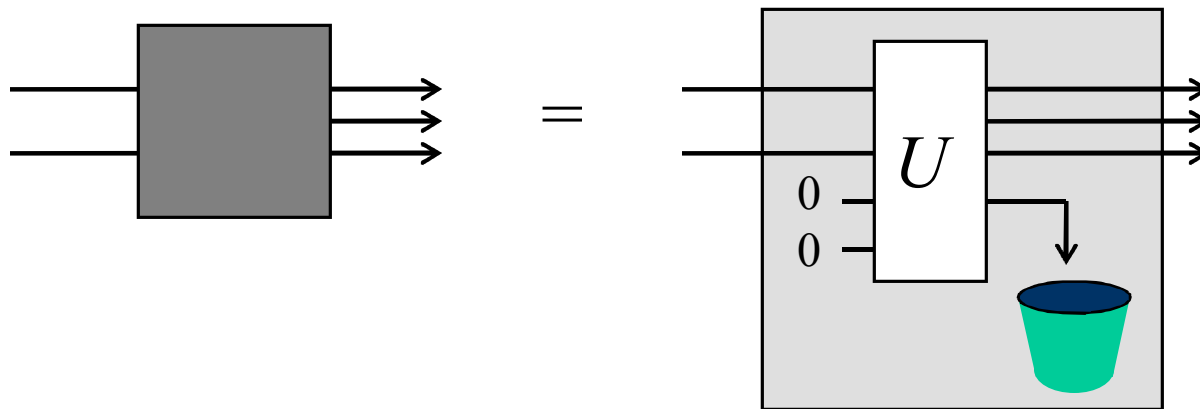
2 Believers in the "many worlds interpretation" reject this axiom as ugly and unnecessary. For them measurement is just a unitary evolution producing an entangled state of the system and measuring apparatus. For others, measurement causes the system to behave probabilistically and forget its pre-measurement state, unless that state happens to lie entirely within one of the subspaces P_j .

Unitary evolution is reversible, preserving distinguishability.

But quantum systems in interaction with an environment can undergo irreversible loss of distinguishability.

- noisy or lossy channels, which lose classical information
- classical wires, which spoil superpositions
- erasure, which destroys distinguishability completely

Any physically possible evolution of an open quantum system can be modeled as a unitary interaction with an environment, initially in a standard 0 state.

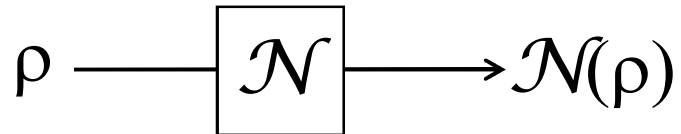


Mixed states describe situations of incomplete information

- An ensemble of pure states ψ_j with probabilities p_j . Its density matrix ρ is given by the weighted sum of the projectors onto these states. Despite seeming to contain incomplete information about the ensemble, ρ describes all that can be learned by measuring specimens from the ensemble.
- Ensembles with the same ρ are indistinguishable.

The Church of the larger Hilbert Space

- A system S in a mixed state ρ^S can, without loss of generality, be regarded as a subsystem of a larger bipartite system RS in a pure state Ψ^{RS} , where R denotes a non-interacting reference system.
- “Steering” Any ensemble $\{p_j, \psi_j\}$ compatible with ρ^S can be remotely generated by performing measurements on the R part of Ψ^{RS} . Measurement outcome j occurs with probability p_j , leaving S in state ψ_j .

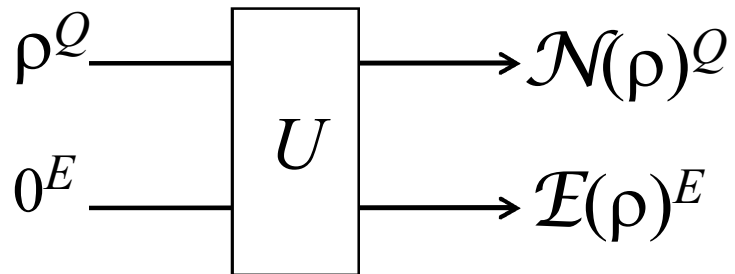


$$\mathcal{N}(\rho) = \sum_k A_k \rho A_k^\dagger$$

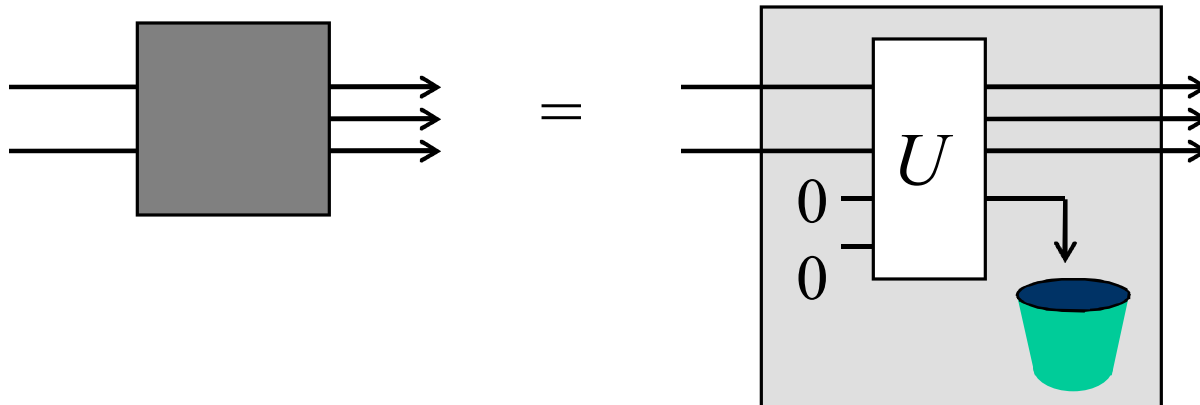
where A_k are matrices such that

$$\sum_k A_k^\dagger A_k = 1$$

Kraus representation.



Unitary representation.



Entanglement measures

- Entanglement Cost E_C , the asymptotic efficiency with which pure ebits can be converted into the state in question by local operations and classical communication (LOCC).
- Distillable Entanglement E_D , the asymptotic efficiency with which the state can be converted into pure ebits by LOCC.
- For pure bipartite states, $E_D = E_C$.
- For mixed states E_D can be less than E_C . Indeed some mixed states (bound entangled states) have no distillable entanglement but positive (1-shot) entanglement cost.

Recognizing Entanglement



Channels map density matrices onto density matrices in a linear fashion.

Are all such positive maps physically possible?

No. Consider the transpose. It maps density matrices onto density matrices, but when applied to part of a bipartite system, in an entangled state, produces a nonphysical matrix with negative eigenvalues.

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

partial transpose \Rightarrow

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

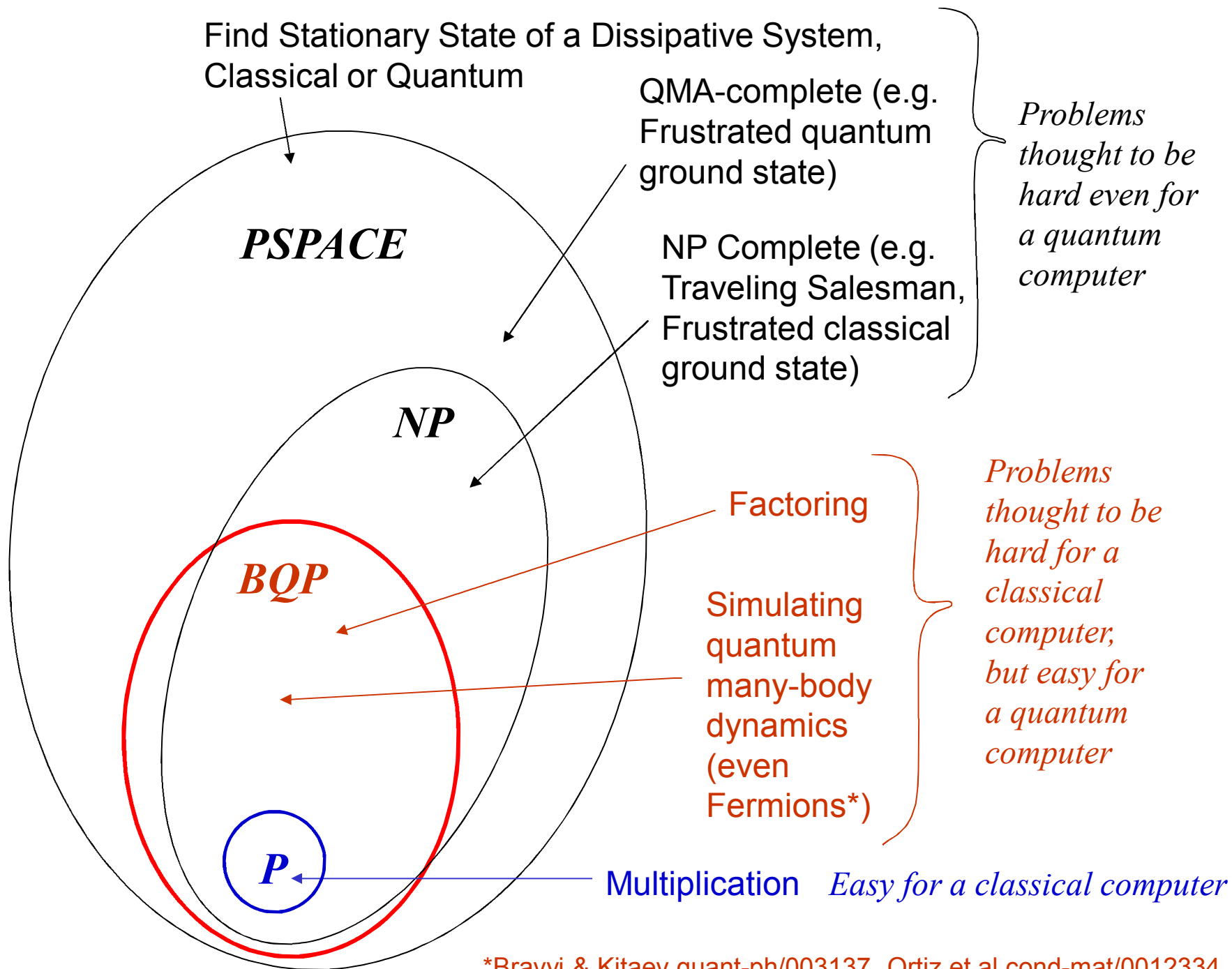
EPR state with
eigenvalues
(1,0,0,0)

Nonphysical
eigenvalues
(-1/2, 1/2, 1/2, 0)

Negativity of partial transpose is a *sufficient* condition for a mixed state to be entangled (Peres-Horodecki condition).



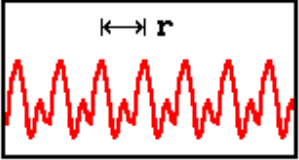
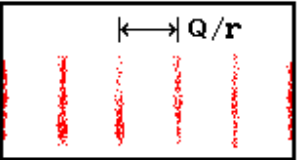
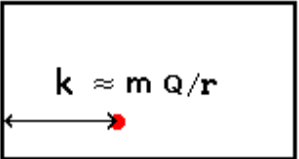
Quantum Speedups





*Bravyi & Kitaev quant-ph/003137, Ortiz et al cond-mat/0012334

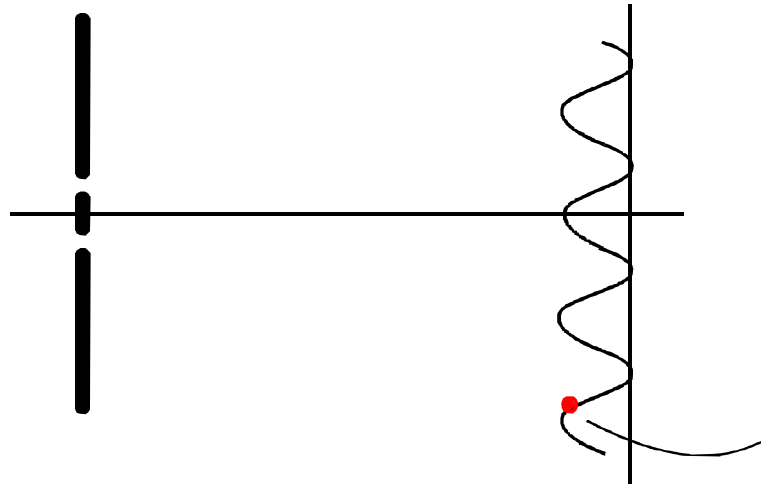
Shor's Quantum Super-Fast Fourier Sampling

	State	Action
	x Register y Register $ 0, 0\rangle$	Initial State
	$\frac{1}{\sqrt{Q}} \sum_x x, 0\rangle$	Generate x superposition
	$\frac{1}{\sqrt{Q}} \sum_x x, f(x)\rangle$	Reversibly compute $y := y + f(x)$
	$\frac{1}{Q} \sum_{x,k} e^{2\pi i k x / Q} k, f(x)\rangle$	Fourier Transform x register
	Result = k	Measure x register

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

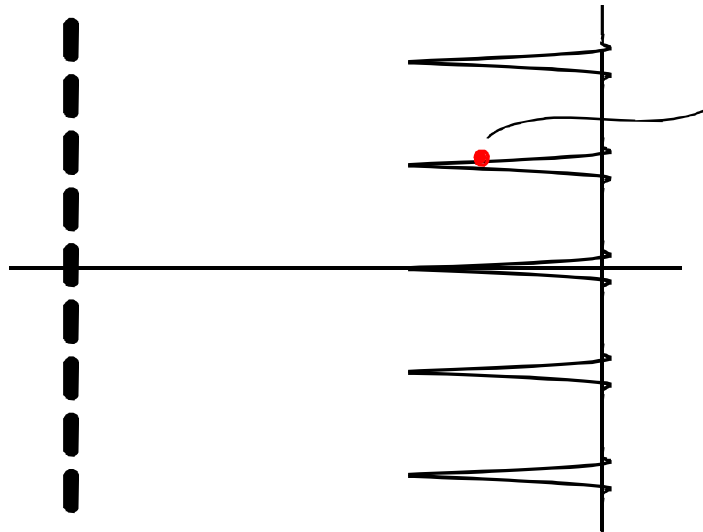
Shor algorithm uses interference to find unknown period of periodic function.

2 Slits
1 photon



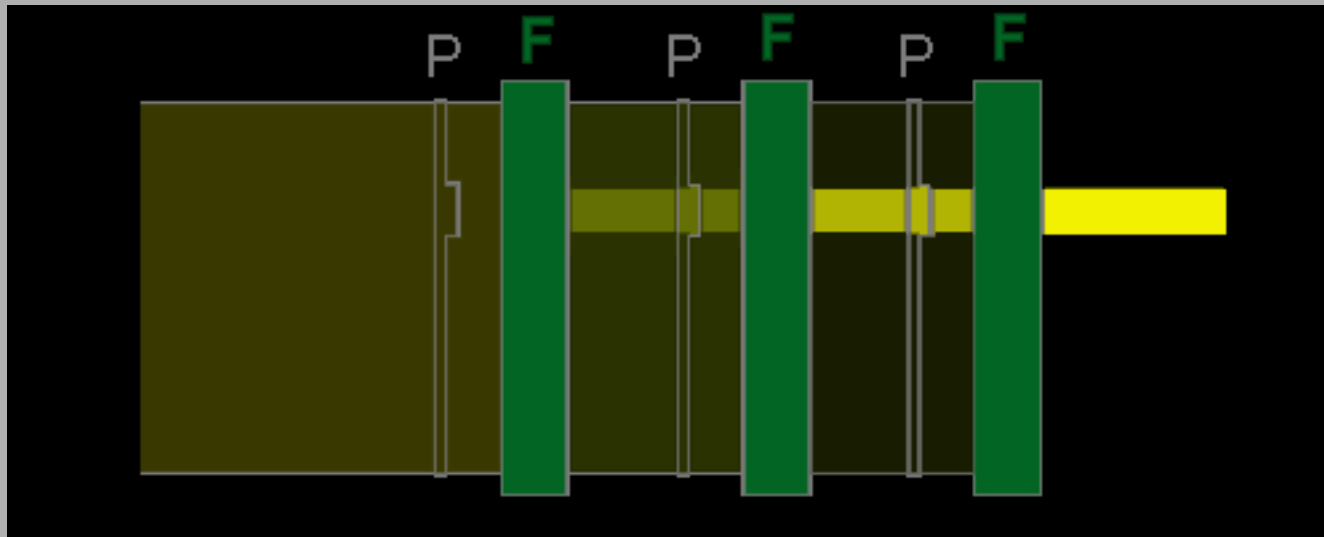
Photon impact point yields a
little information about slit
spacing

N Slits
1 photon



Photon impact point yields a
lot of information about slit
spacing

Grover's quantum search algorithm uses about \sqrt{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 \sqrt{N} iterations are required.



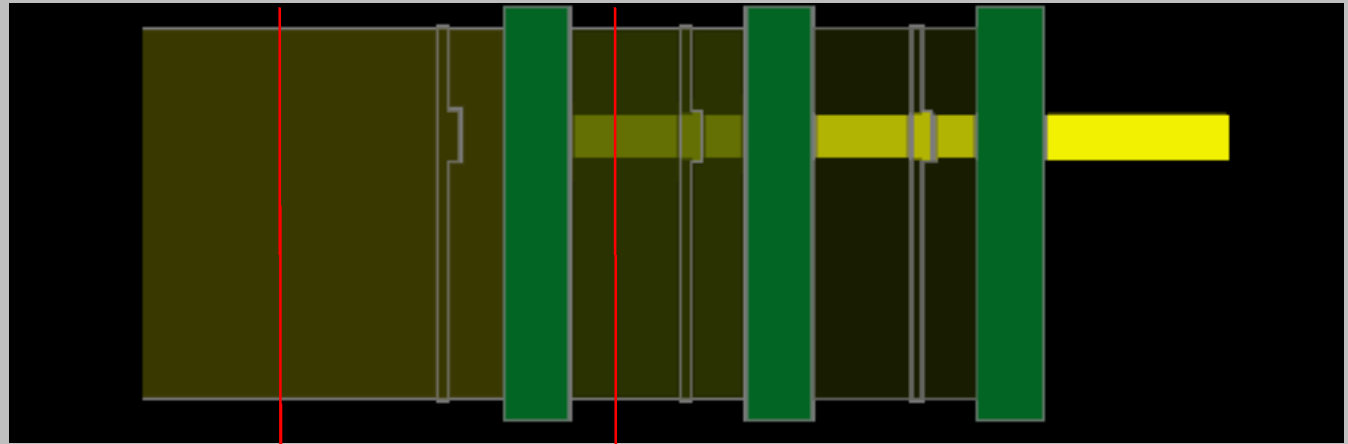
P = phase plate

F = fixed optics

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

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

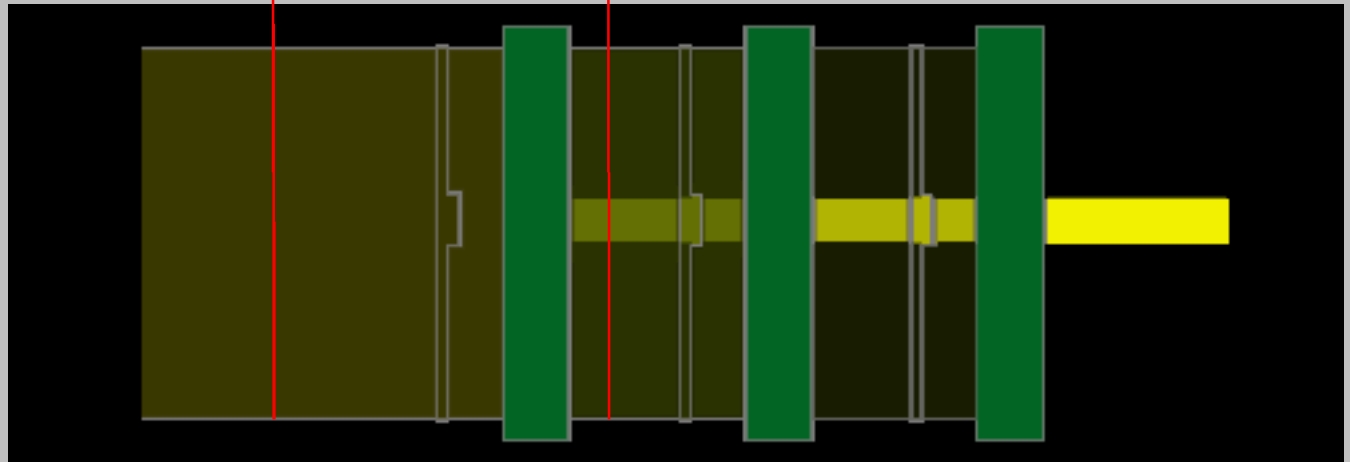
Original
optical
Grover
experiment.



No difference initially

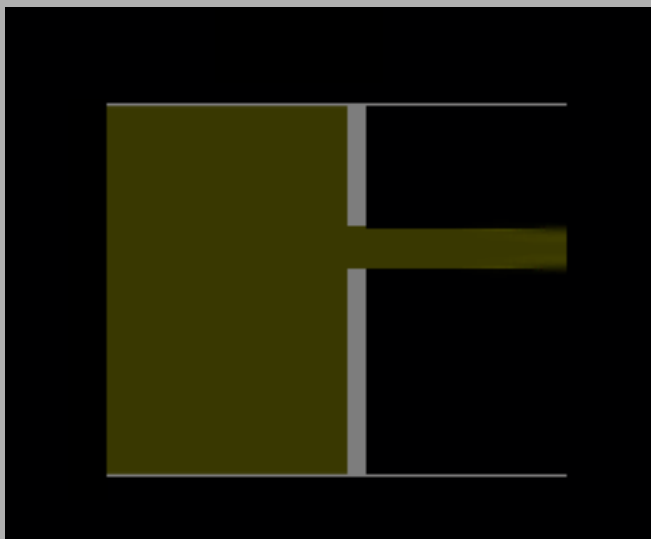
Small difference after 1 iteration

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

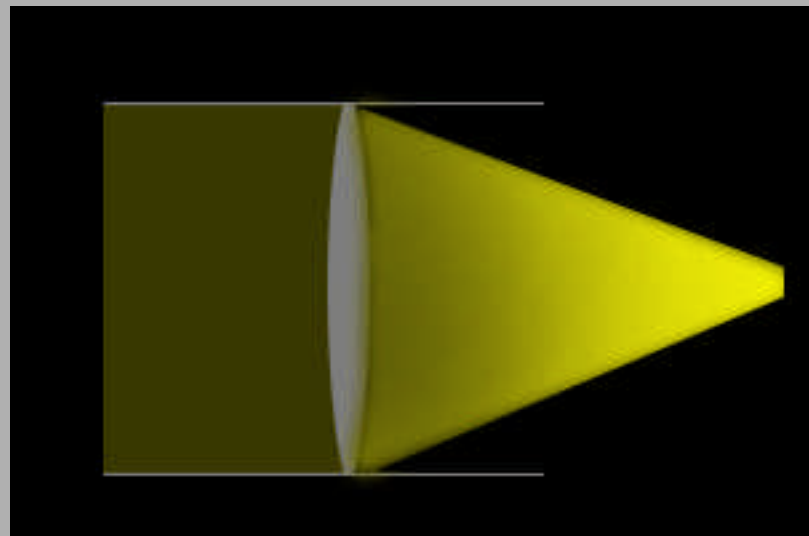


Because most of the beam misses the bump in either location, the difference between the two light fields can increase only slowly. About \sqrt{N} iterations are required to get complete separation. (BBBV quant-ph/9701001)

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.