Information is Quantum

What ideas from early 20th century physics taught us about the nature of information and what can be done with it

Charles H. Bennett
IBM Research Yorktown

Ingarden Lecture
2020-11-25

Like other parts of mathematics, information science originated in abstractions from everyday experience, in particular two daring 20th century abstractions:

A universal, hardware-independent notion of computation (Turing 1936)

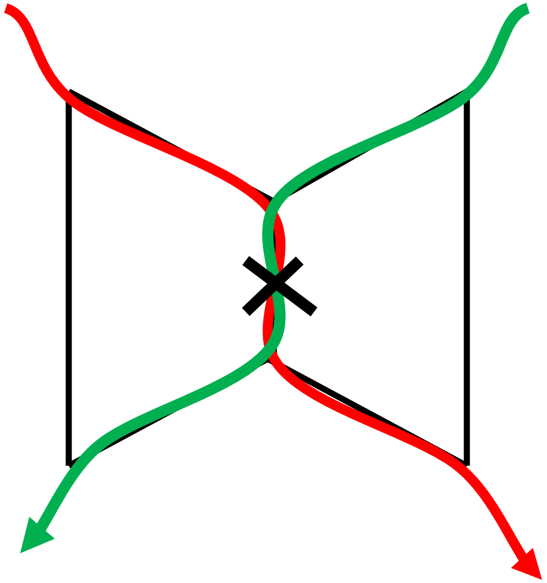
Even more revolutionary was

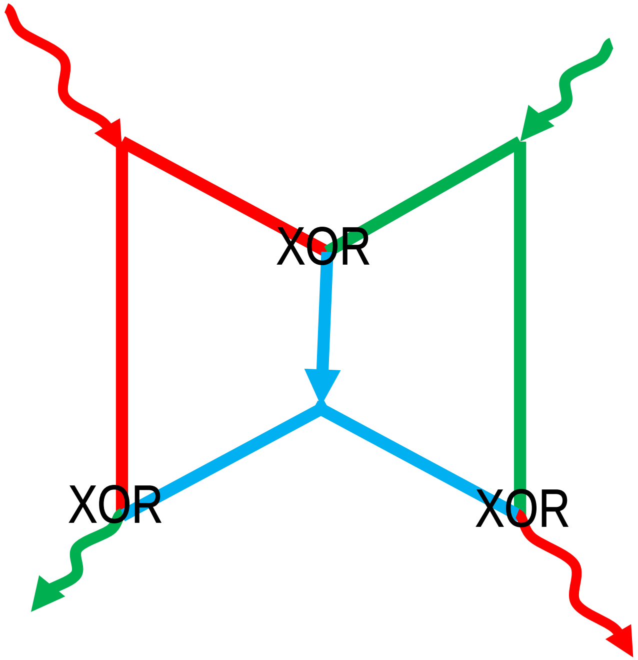
A universal, meaning-independent notion of communication (Shannnon 1948) and a way of quantifying it using entropy, a concept originated by physicists.

But in retrospect, these abstractions abstracted away a little too much.

Babbage called his analytical engine's memory its **store**, and its processor its **mill**. But even classical information is different from material commodities like grain.

Because it can be copied, information can flow more efficiently through networks





Wiesner's 1968 paper *Conjugate Coding* (submitted to IEEE-IT around 1970 and but only published in 1983) showed how quantum mechanics can be used to perform two tasks outside the scope of Shannon's theory.

- Multiplexing two messages into a quantum signal from which the receiver can recover either message at will, but not both.
- Money that is physically impossible to counterfeit.

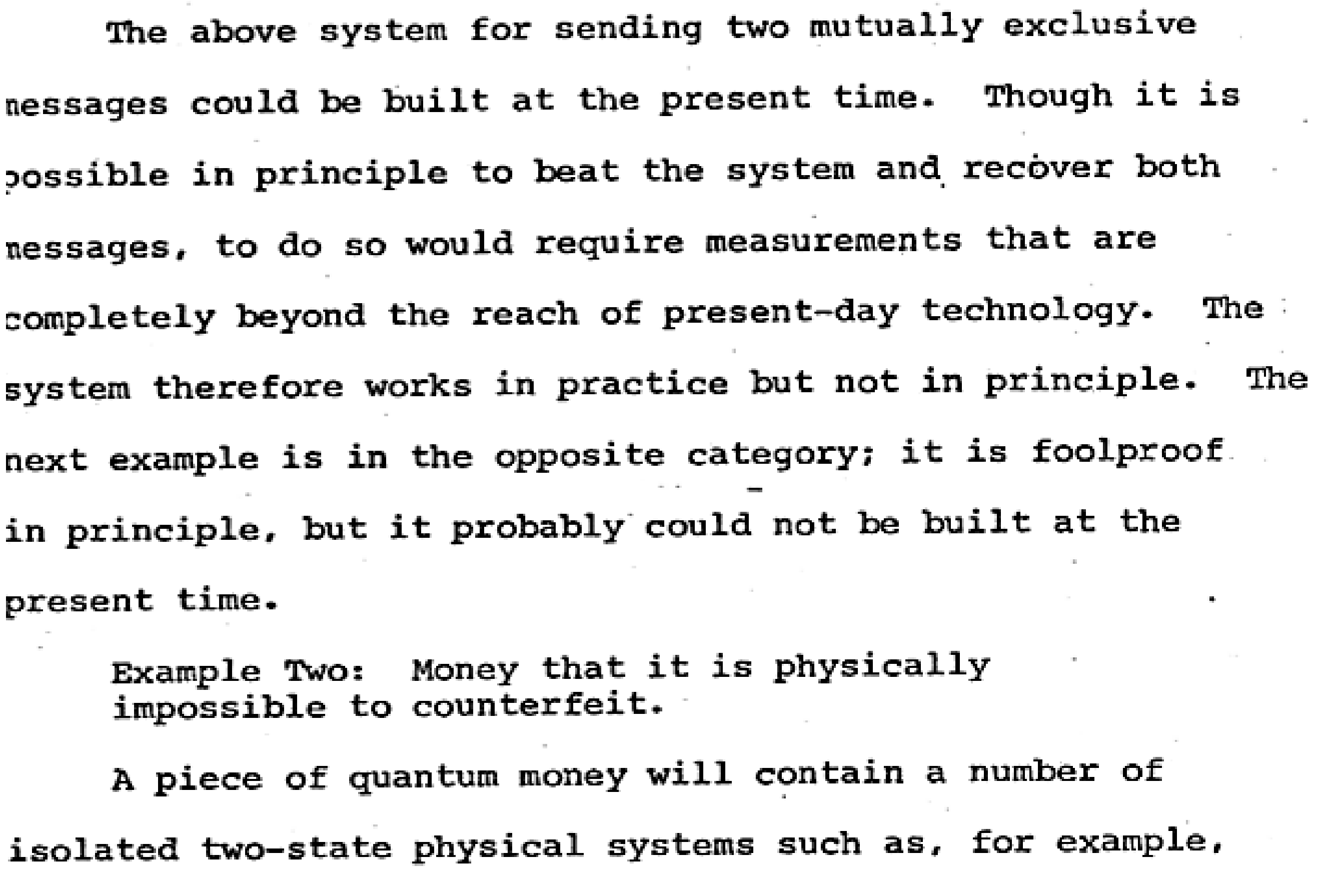
There ... of three messages,

o two of w ... y transmits a

hird binar ... polarization

tates at 4 ... xtension to more

han three

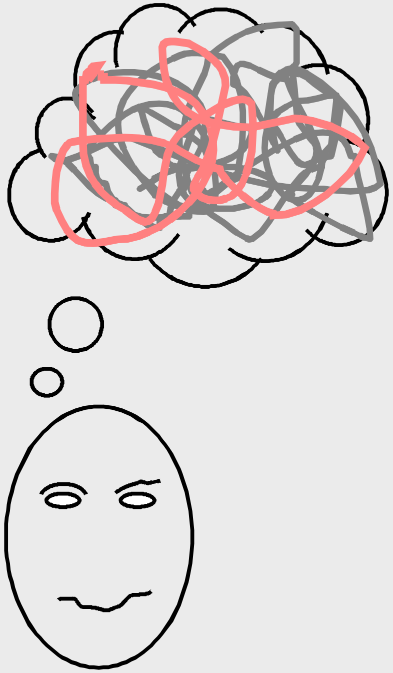


The above system for sending two mutually exclusive messages could be built at the present time. Though it is possible in principle to beat the system and recover both messages, to do so would require measurements that are completely beyond the reach of present-day technology. The system therefore works in practice but not in principle. The next example is in the opposite category; it is foolproof in principle, but it probably could not be built at the present time.

Example Two: Money that it is physically impossible to counterfeit.

A piece of quantum money will contain a number of isolated two-state physical systems such as, for example, 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.

The central principle of quantum mechanics is

the Superposition Principle:

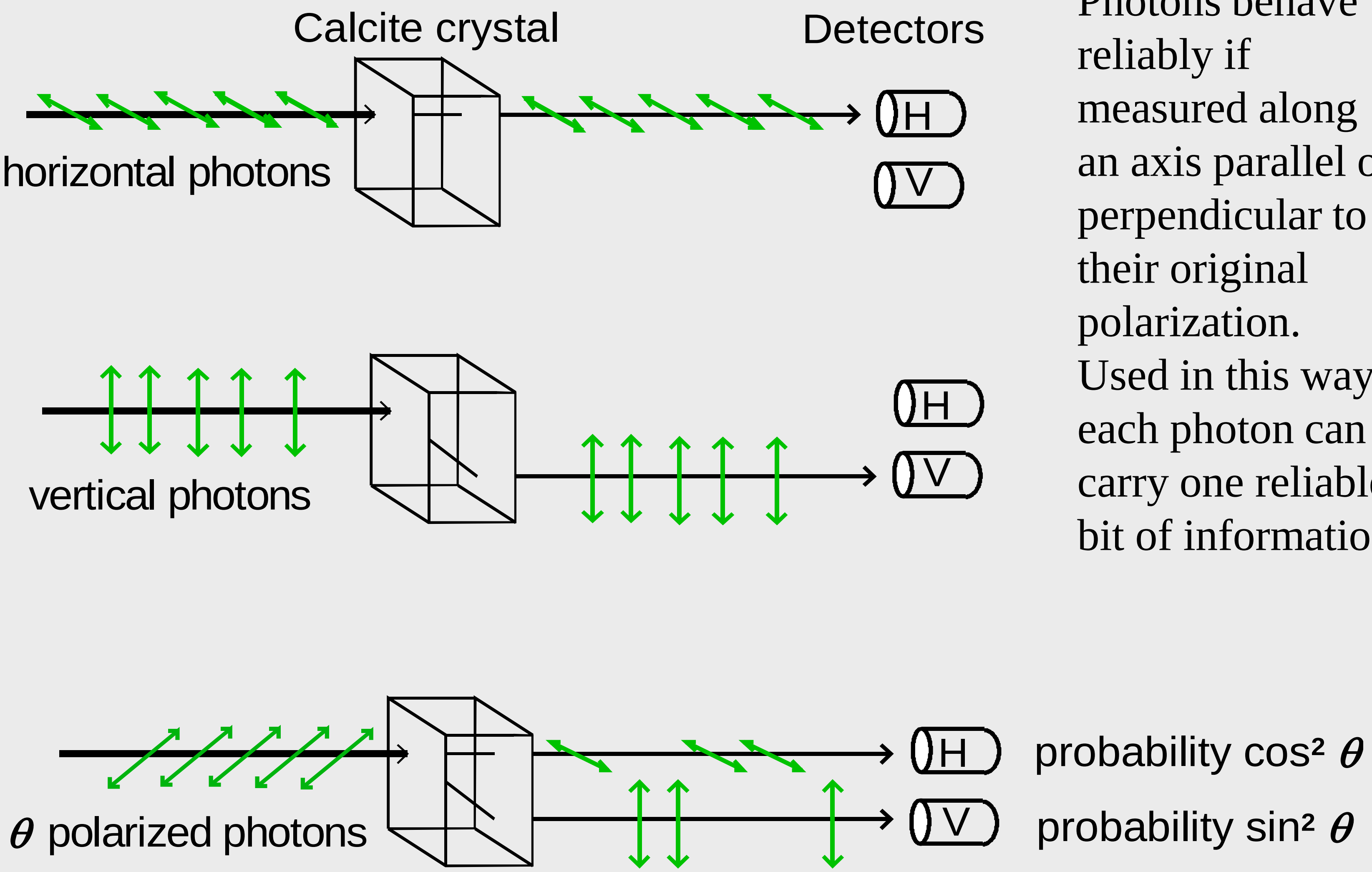
- Between any two reliably distinguishable states of a physical system (for example vertically and horizontally polarized single photons) there are intermediate states (for example diagonal photons) that are not reliably distinguishable from either original state.

- The system's possible 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. (More precisely, quantum states correspond to rays in an ***n***-dimensional Hilbert space, like Euclidean space but with complex coefficients.)

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

- A closed quantum system's time evolution conserves distinguishability. (In open systems distinguishability may decrease but can never increase.)

Using Polarized Photons to Carry Information

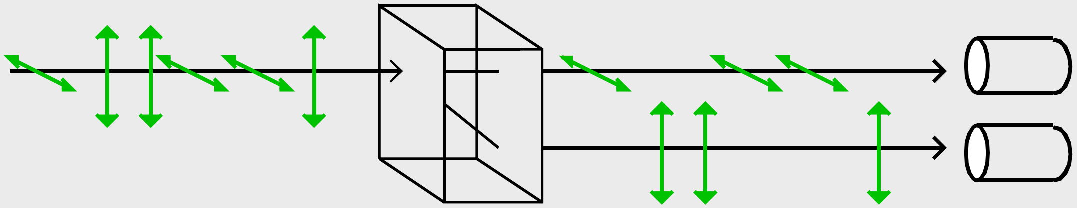


Photons behave reliably if measured along an axis parallel or perpendicular to their original polarization.

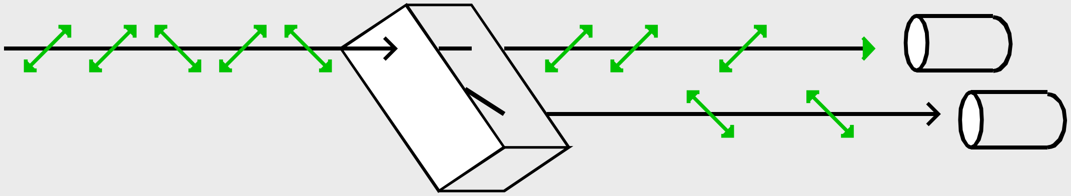
Used in this way, each photon can carry one reliable bit of information.

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.

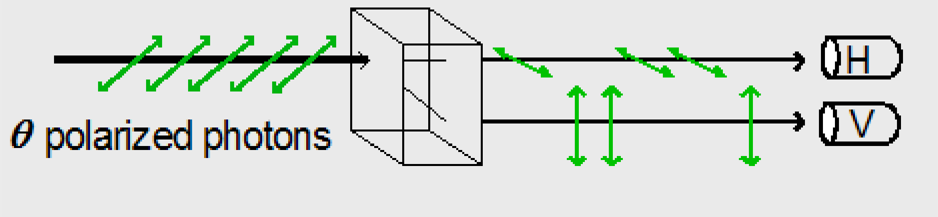


A diagonal measurement distinguishes diagonal photons reliably but randomizes rectilinear photons.



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 Measurement (Bill Wootters' pedagogic analogy)



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 fr…

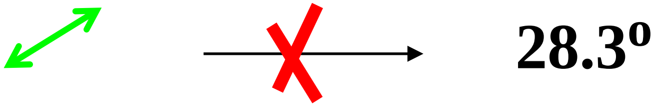
Teacher: **I believe I asked you a question.** Are you vertical or horizontal?

Pupil: Horizontal, sir.

Teacher: Have you ever had any other polarization?

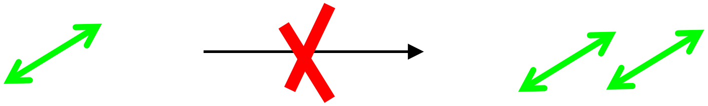
Pupil: No, sir. I was always horizontal.

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

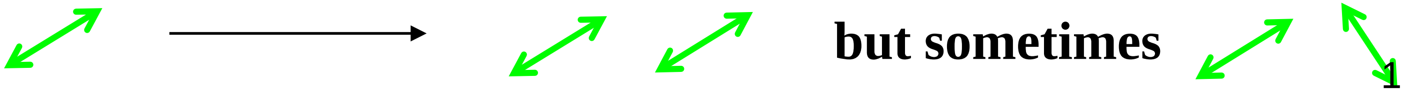


28.3°

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

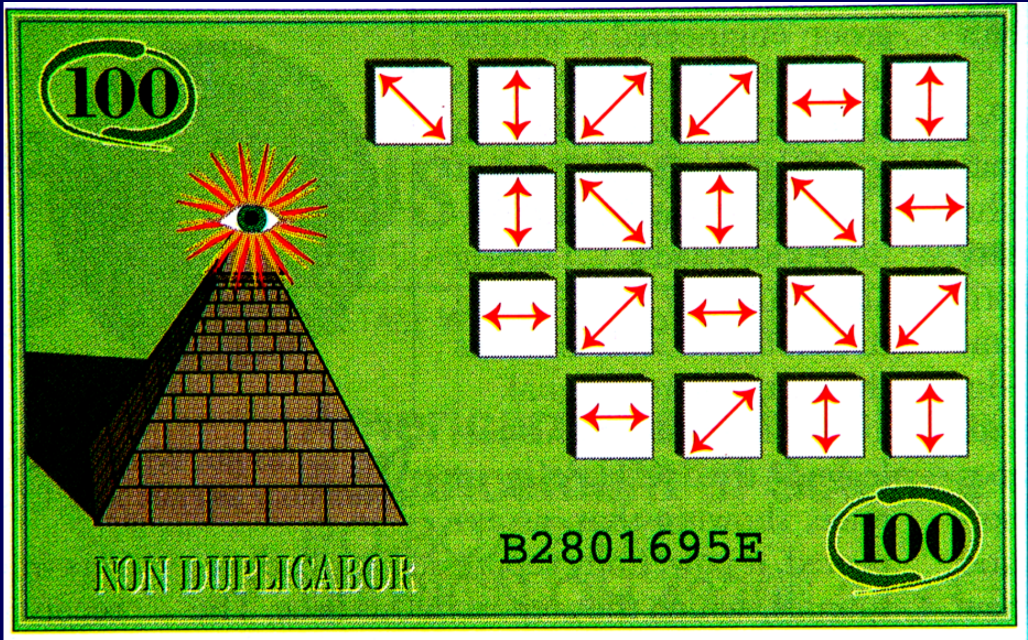


If you try to amplify an unknown photon by sending it into an ideal laser, the output will be polluted by just enough noise (due to spontaneous emission) to be no more useful than the input in figuring out what the original photon’s polarization was.

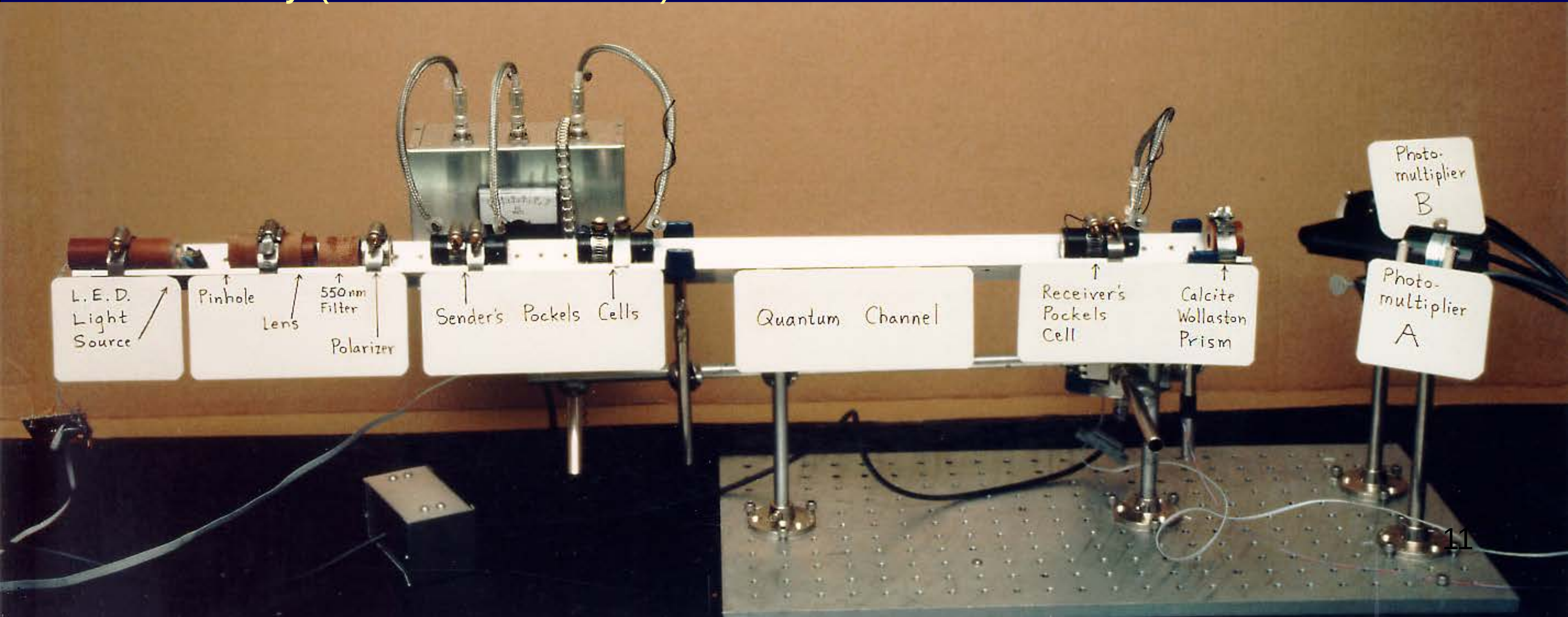


but sometimes

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…)



Despite the differences from classical information there are important similarities

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

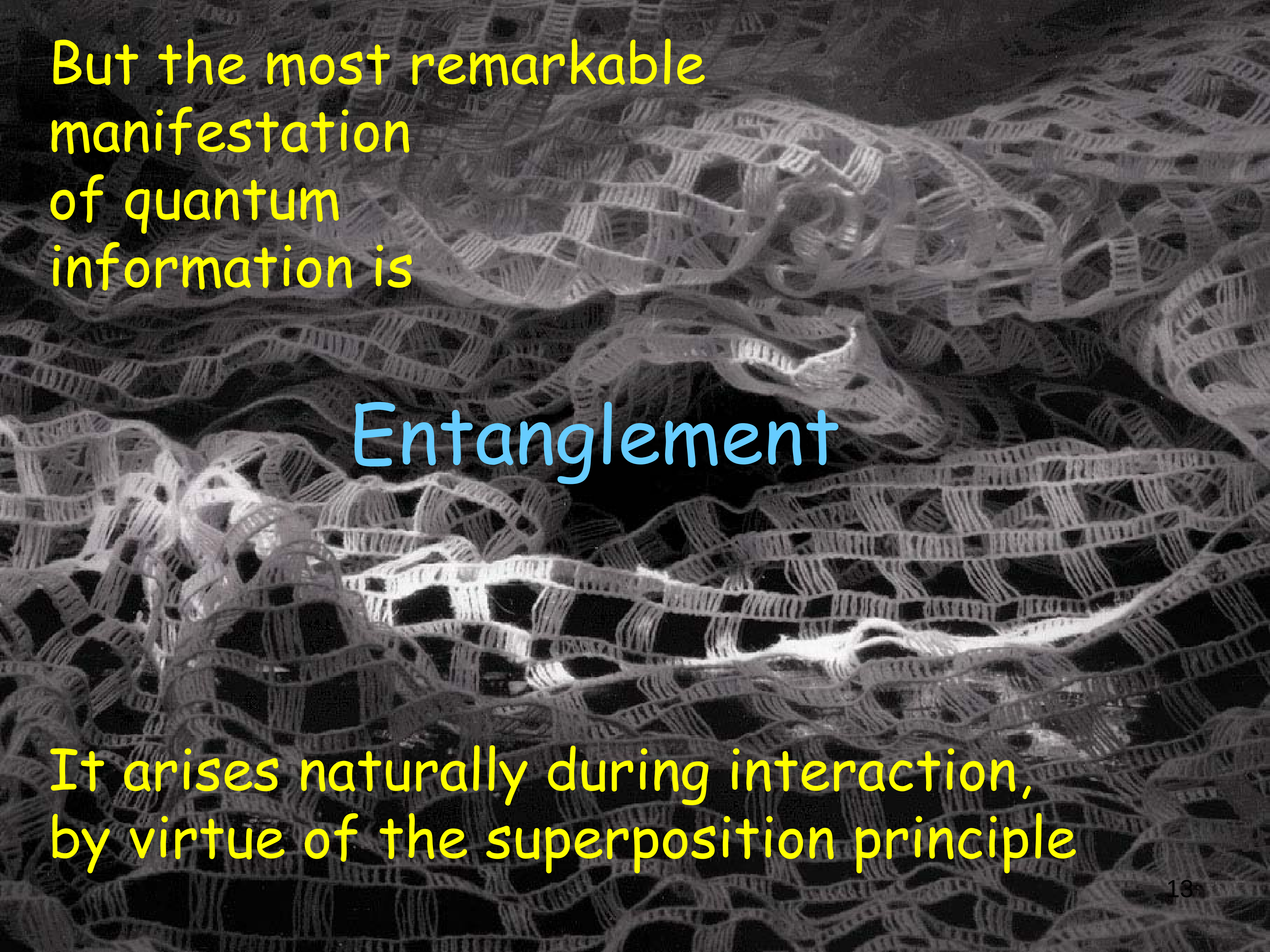
All processing of it can be done by simple logic gates (**NOT, AND**) acting on bits one and two at a time.

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

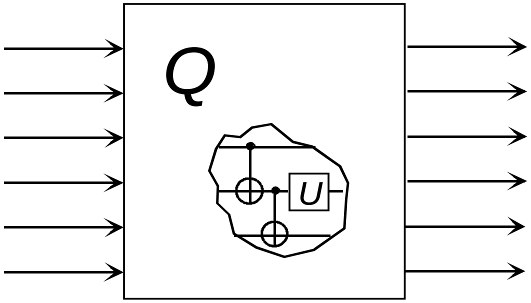


But the most remarkable manifestation of quantum information is

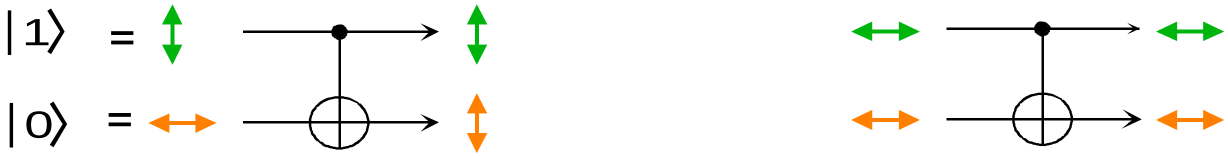
Entanglement

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

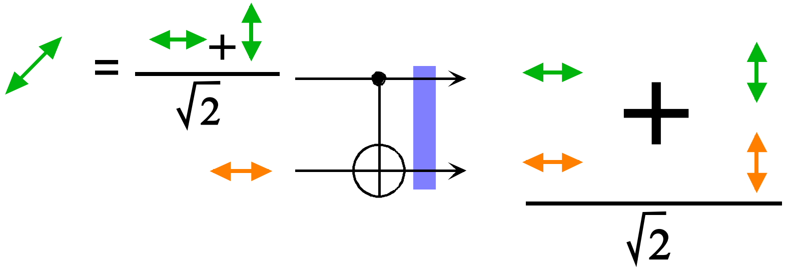
Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.



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

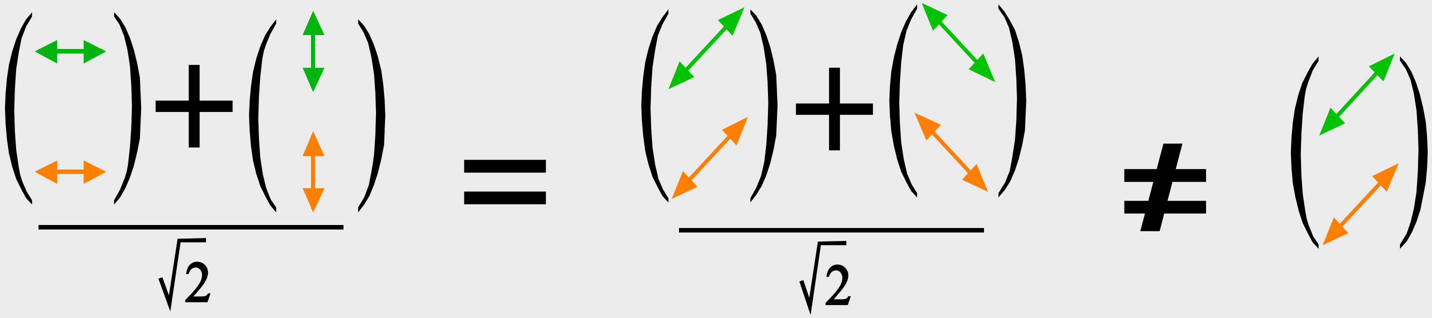


A superposition of inputs gives a superposition of outputs.



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.

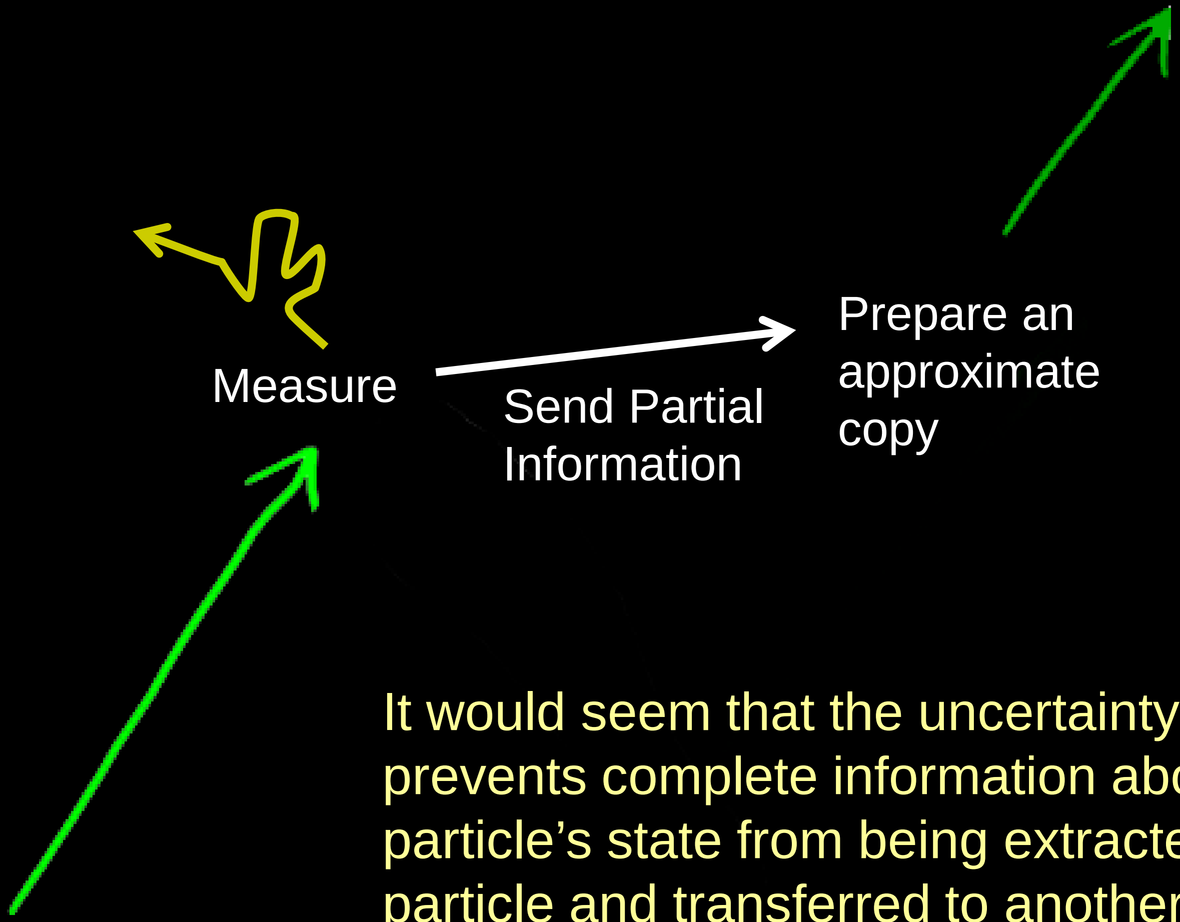
(In San Francisco in 1967, the "Summer of Love", one often met people who felt they were in perfect harmony with one another, even though they had no firm opinions about anything.)

Wikiwatcher1 CC Share alike

Hippies thought 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.

Using entanglement



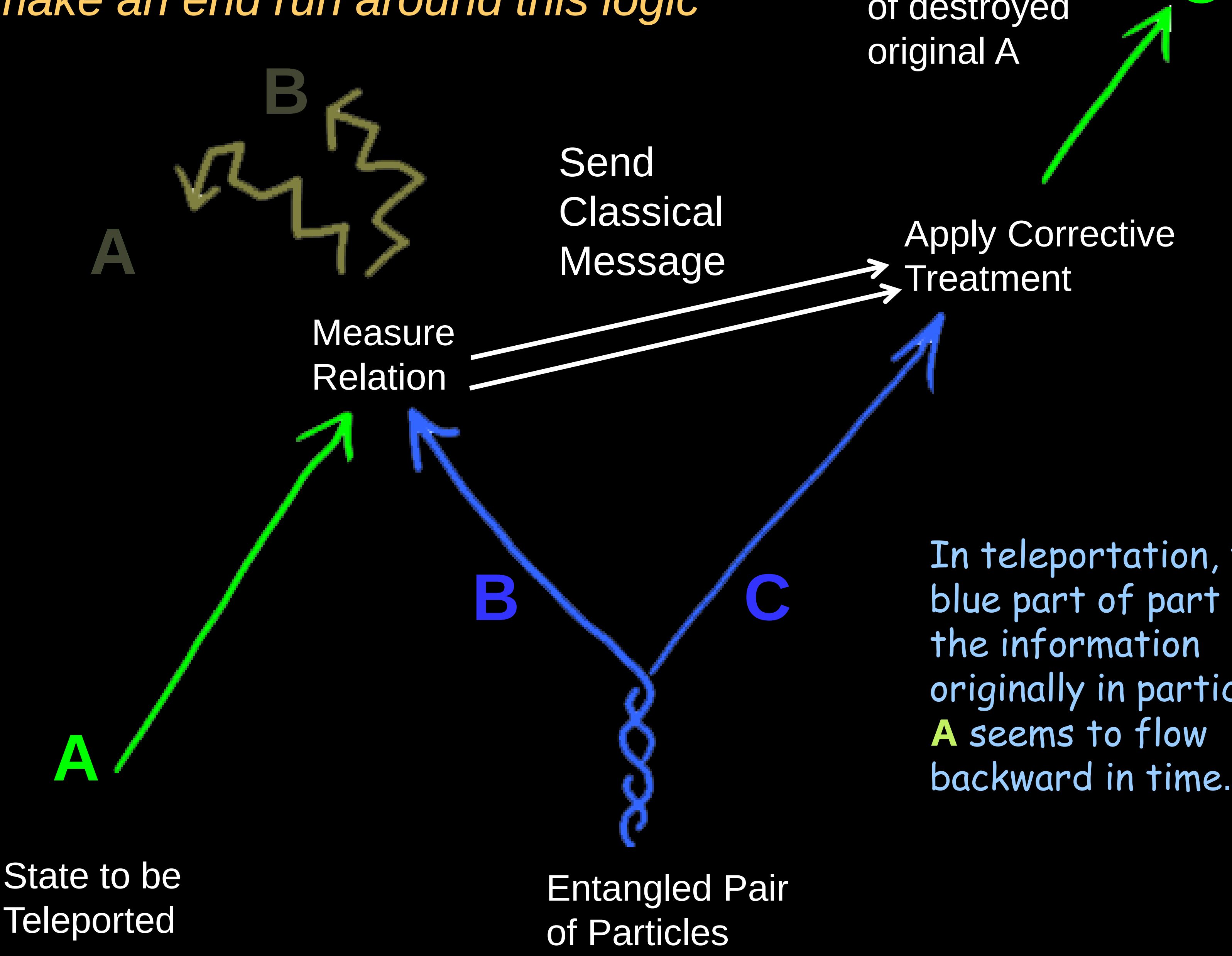
Measure

Send Partial Information

Prepare an approximate copy

It would seem that the uncertainty principle prevents complete information about a particle’s state from being extracted from that particle and transferred to another particle, which has never been anywhere near the first particle.

But Quantum Teleportation permits us to make an end run around this logic



Teleported replica of destroyed original A

Send Classical Message

Apply Corrective Treatment

Measure Relation

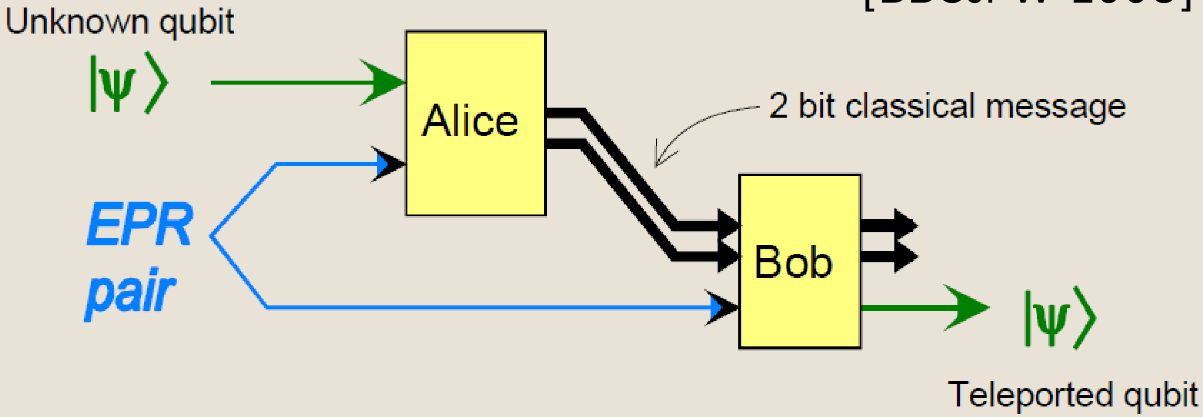
State to be Teleported

Entangled Pair of Particles

In teleportation, the blue part of part of the information originally in particle **A** seems to flow backward in time.

Quantum Teleportation

[BBCJPW 1993]



Unknown qubit

$|\psi\rangle$

EPR pair

Alice

2 bit classical message

Bob

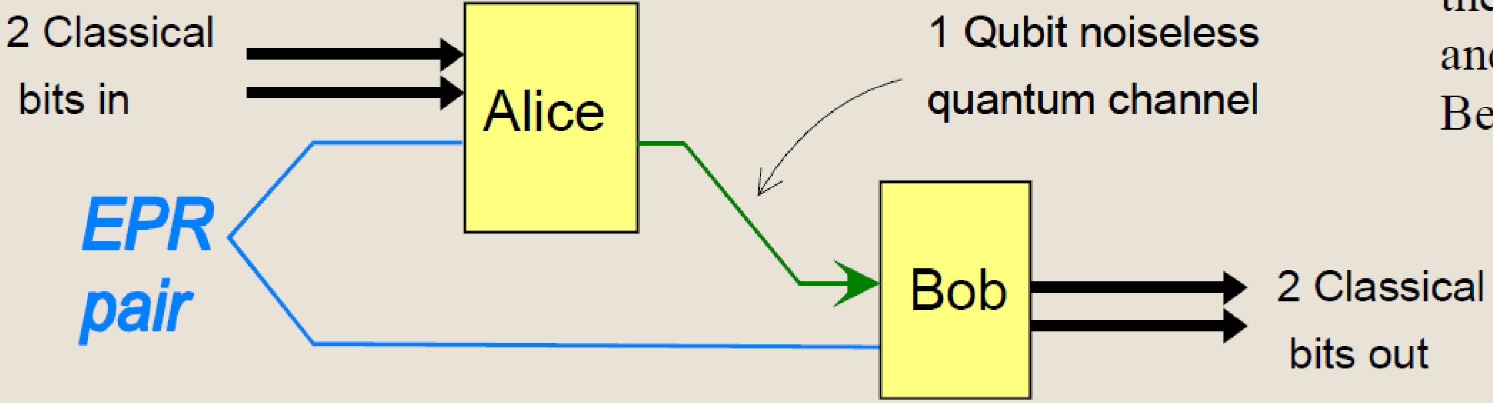
$|\psi\rangle$

Teleported qubit

Superdense Coding

[Wiesner ’70] [B, Wiesner ’92]

(a dual process to teleportation)



2 Classical bits in

EPR pair

Alice

1 Qubit noiseless quantum channel

Bob

2 Classical bits out

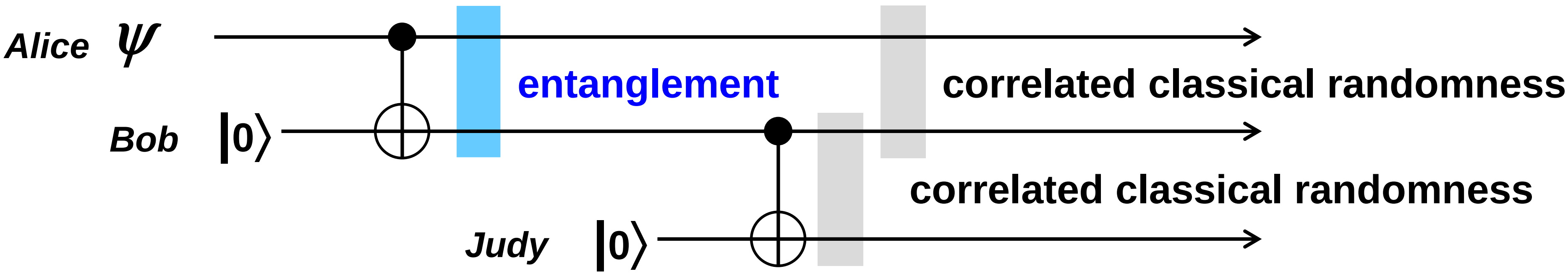
Here Alice does the Pauli rotation and Bob does the Bell measurement.

doubles the classical capacity of any noiseless quantum channel

The Monogamy of Entanglement

- If A and B are maximally entangled with each other, they can't they be entangled with anyone else.
- 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 the scene, Bob will find his relationship with the other reduced to mere correlated randomness. If they both stick around, he ends up perfectly entangled, not with either one, but with the now nontrivial *relationship* between them, an appropriate punishment. [Colette 1929]

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 .

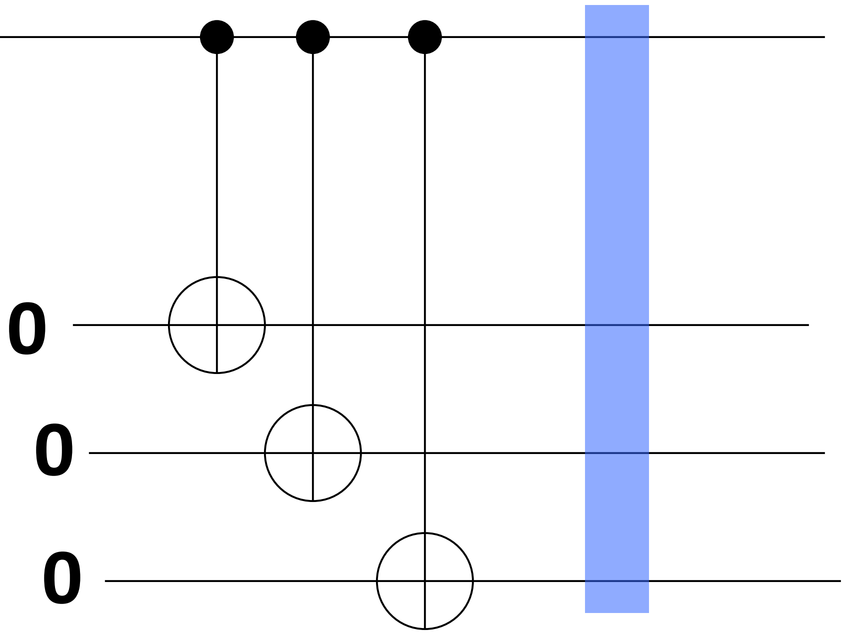
This destroys any previous entanglement that may have existed between internal parts of the system, changing it into mere correlated randomness.

How entanglement hides, creating a classical-appearing world

ψ

System

Parts of the system’s low-entropy environment e.g. photons from the sun



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.*

Information becomes classical by being replicated redundantly throughout the environment. (Zurek, Blume-Kohout et al)

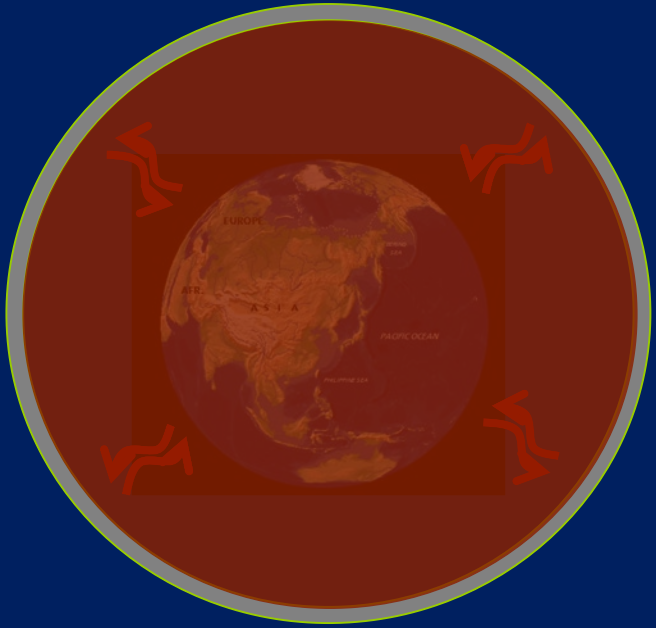
“Quantum Darwinism” Maybe “Quantum Spam” would be a better name.

(This typically happens when the environment is not at thermal equilibrium, and contains many subsystems that interact in a commuting fashion with the system but not with each other. The earth’s environment is like that.)

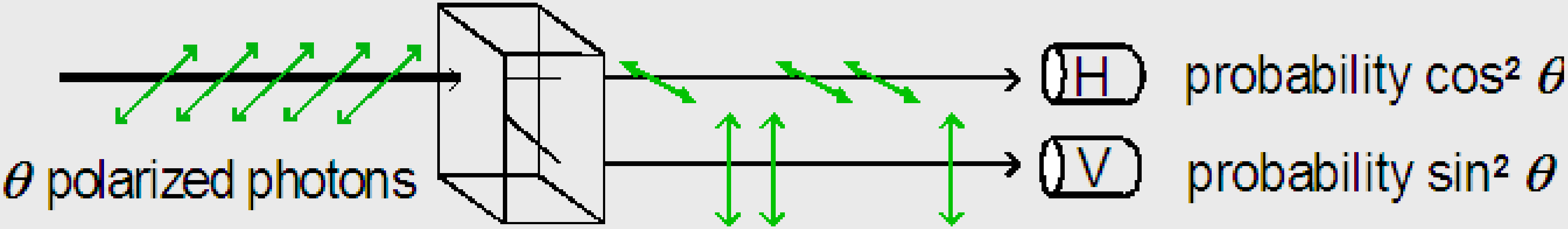
Riedel and Zurek have pointed out the role of non-thermal illumination in creating classical correlations in everyday life, e.g. photons from the sun reflecting off objects on the surface of the Earth to produce massively redundant records of their positions.

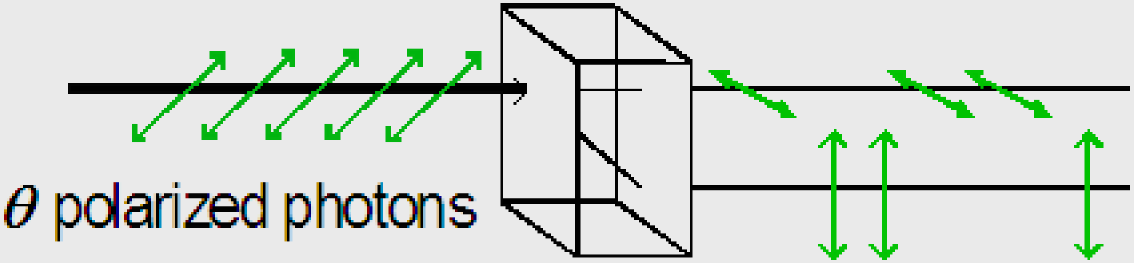
If these photons continue to propagate away in free space, the system will never equilibrate and the redundant record will be permanent, though inaccessible, even outliving the Earth.

But if the reflected photons were instead trapped inside a reflective box, they would be repeatedly absorbed and re-emitted from the Earth, obfuscating the former redundant correlations as the system equilibrates, and rendering the system no longer classical.

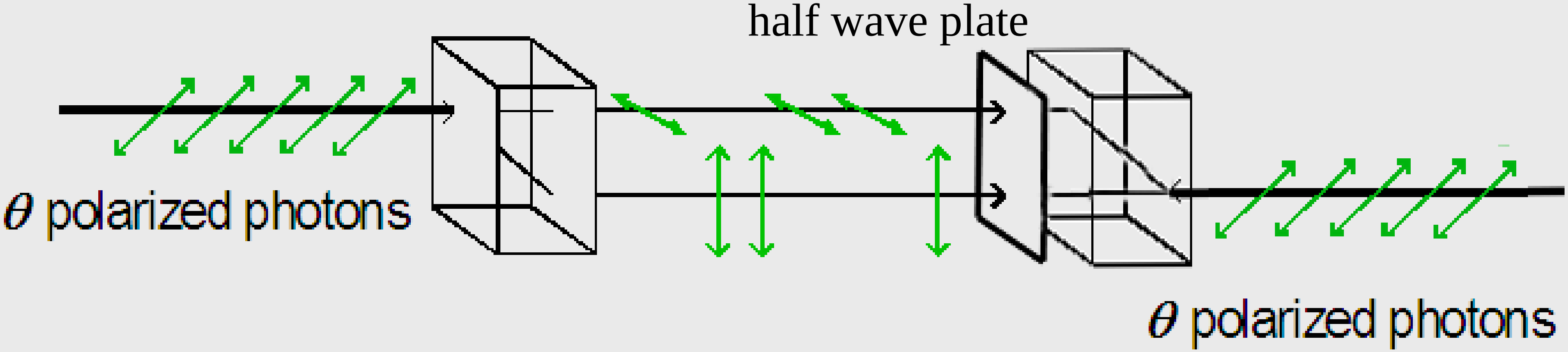


Entanglement and the origin of Quantum Randomness


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



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



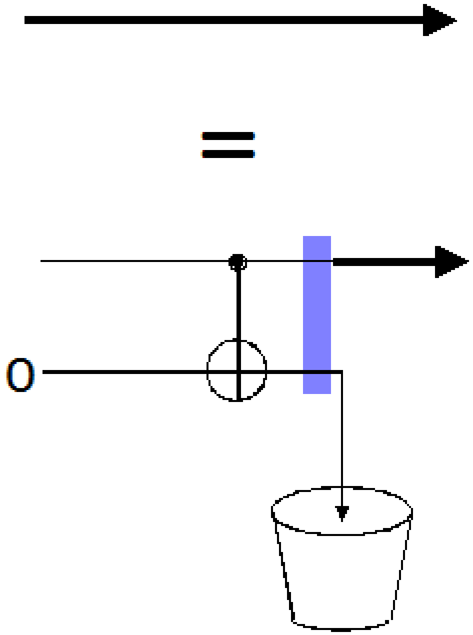
Metaphorically speaking, it is the **public embarrassment** of the pupil, in front of the whole class, that makes him forget his original polarization.

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.

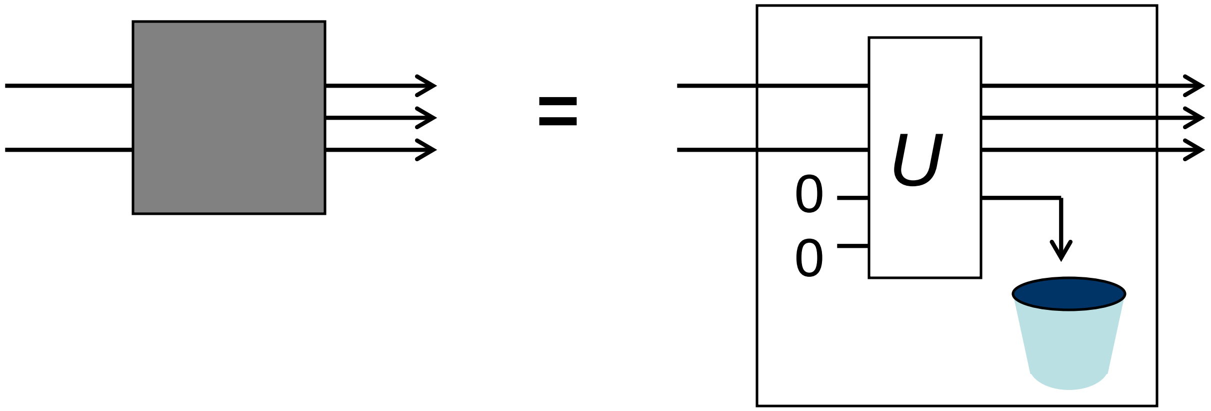
A classical computer is a quantum computer handicapped by having eavesdroppers on all its wires.

What is a Quantum Channel?

Unitary evolution is reversible, preserving distinguishability. But quantum systems in interaction with an environment can undergo a loss of distinguishability, e.g.

- transmission of photons through an optical fiber
- 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.



The Church of the Larger Hilbert Space

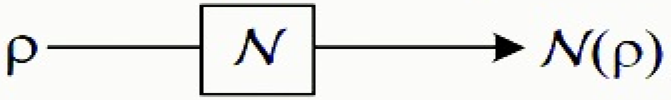
This is the name given by John Smolin to the habit of always thinking of a mixed state as a pure state of some larger system; and of any nonunitary evolution as being embedded in some unitary evolution of a larger system: No one can stop us from thinking this way; and Church members find it satisfying and helpful to their intuition:

This doctrine only makes sense in a quantum context, where because of entanglement a pure whole can have impure parts: Classically; a whole can be no purer than its most impure part.

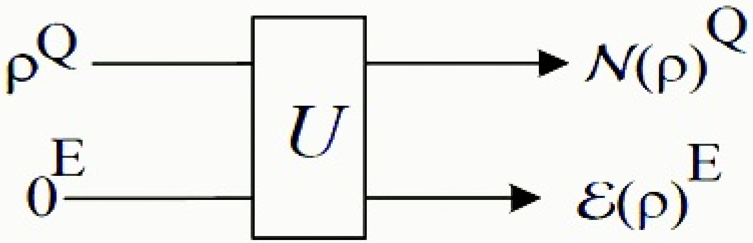
Cf. Biblical view of impurity (Matthew 18:8)

> *If thy hand or thy foot offend thee, cut them off, and cast them from thee: it is better for thee to enter into life halt or maimed, rather than having two hands or two feet to be cast into everlasting fire.*

Noisy channel viewed as a
linear map on density matrices



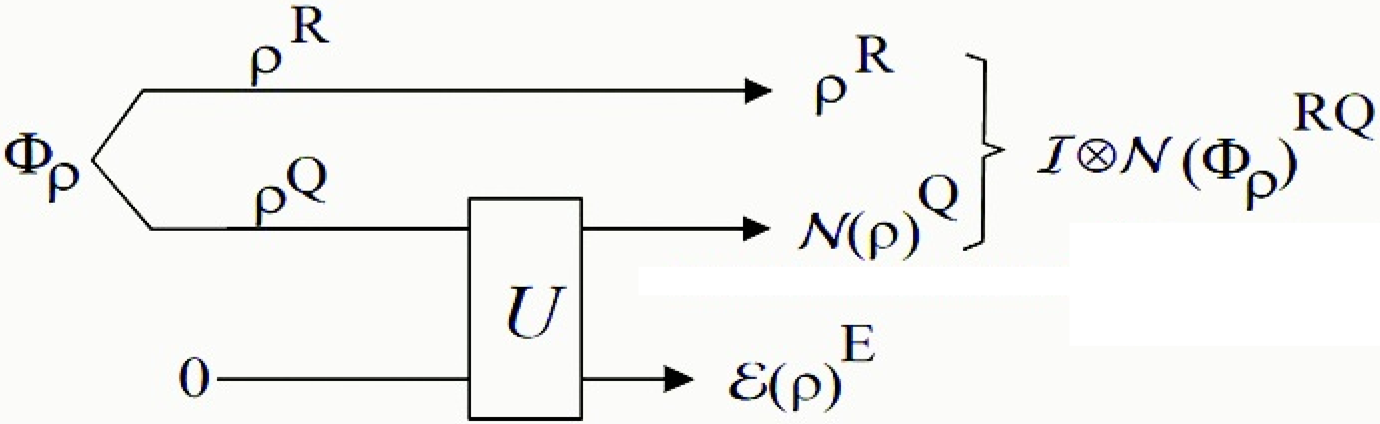
Noisy channel viewed as
interaction with environment



CLHS invoked to
purify noisiness of
channel

Input viewed as entangled
with a reference system R

CLHS invoked again
to purify mixedness
of input



In classical information theory, the compressibility of a source X and the capacity of a channel $\mathbf{N}$ both have simple mathematical expressions.

$$H(X) = -\Sigma_x \; p(x) \log p(x),$$

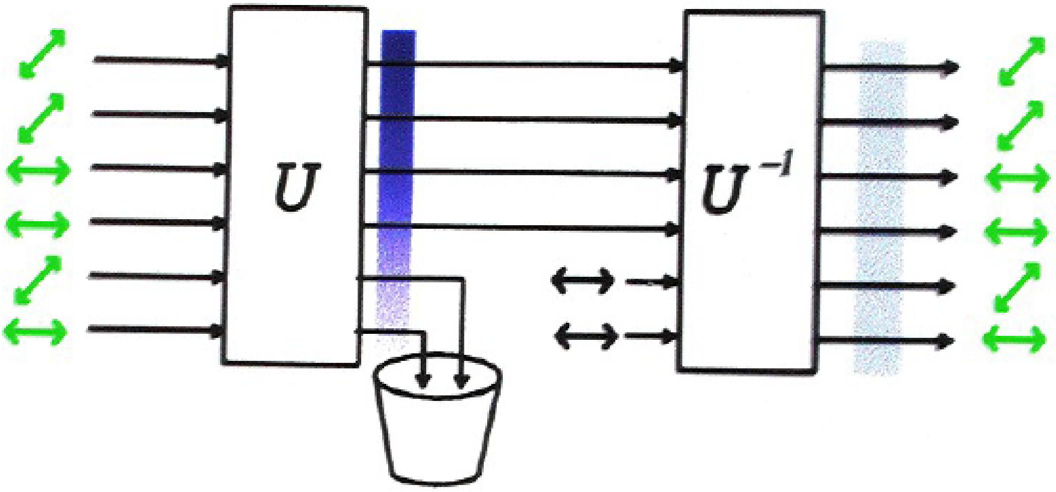
Where $p(x)$ is the probability that the random variable X takes the value x.

$$C(\mathbf{N}) = \max_X \; [\, H(X) + H(\mathbf{N}(X)) - H(X,\mathbf{N}(X)) \,]$$

In other words, a channel's capacity is the maximum, over input distributions of the *mutual information* between input and output.

> *An analogous quantum quantity, using von Neumann entropies, was studied in 1997 by Cerf and Adami, but its operational significance remained unclear.* [CA97 Phys.Rev.Lett.]

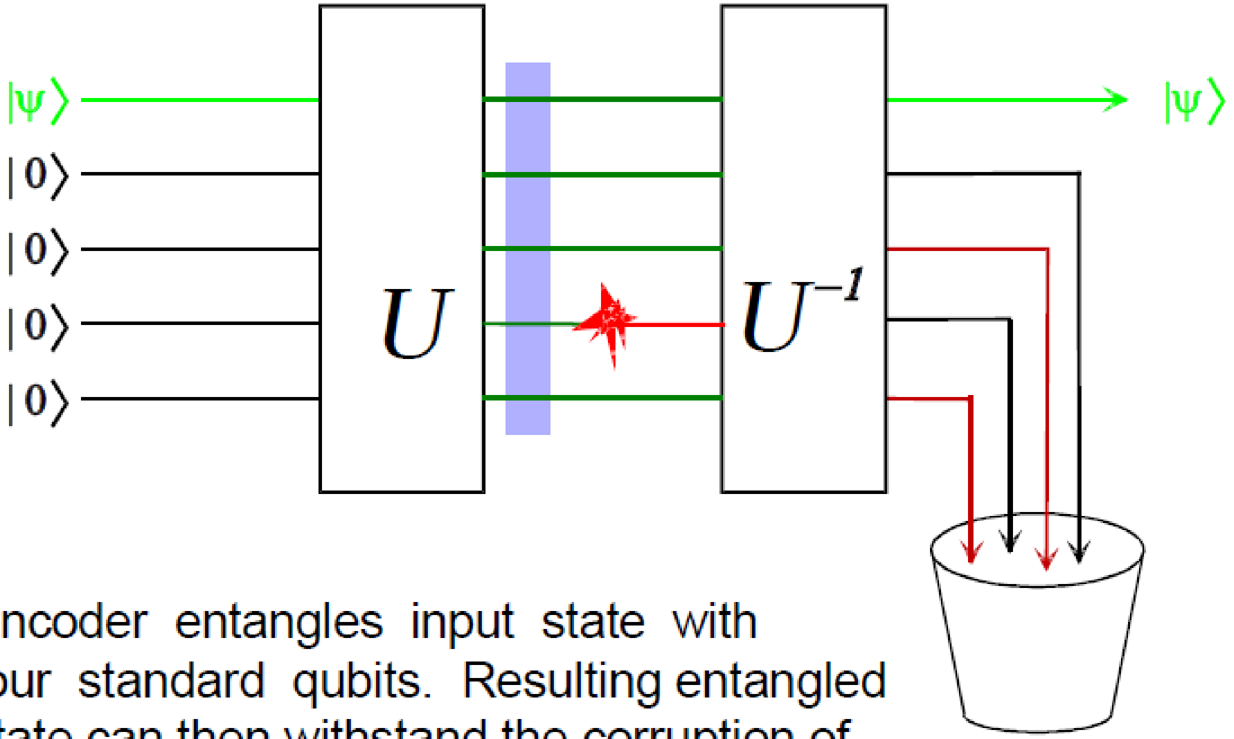
Quantum Data Compression



A source emitting 0 and 45 degree photons has a peculiarly quantum kind of redundancy because the states are nonorthogonal. Schumacher compression squeezes out this redundancy with arbitrarily little disturbance in the limit of large block size.

More generally any quantum source ρ can be compressed to a size equal to its von Neumann entropy $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$, but no smaller.

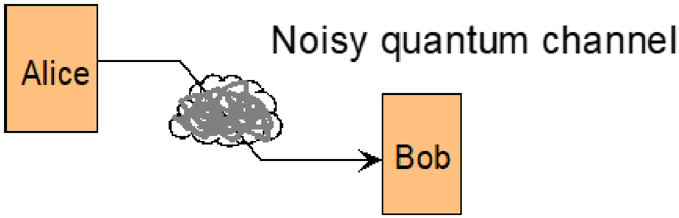
Quantum Error Correcting Code (QECC)



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.

Analogously to a classical channel's capacity, ***Quantum Capacity Q*** *is given by the performance of the best QECCs in the limit of large block size.*

Multiple capacities of Quantum Channels

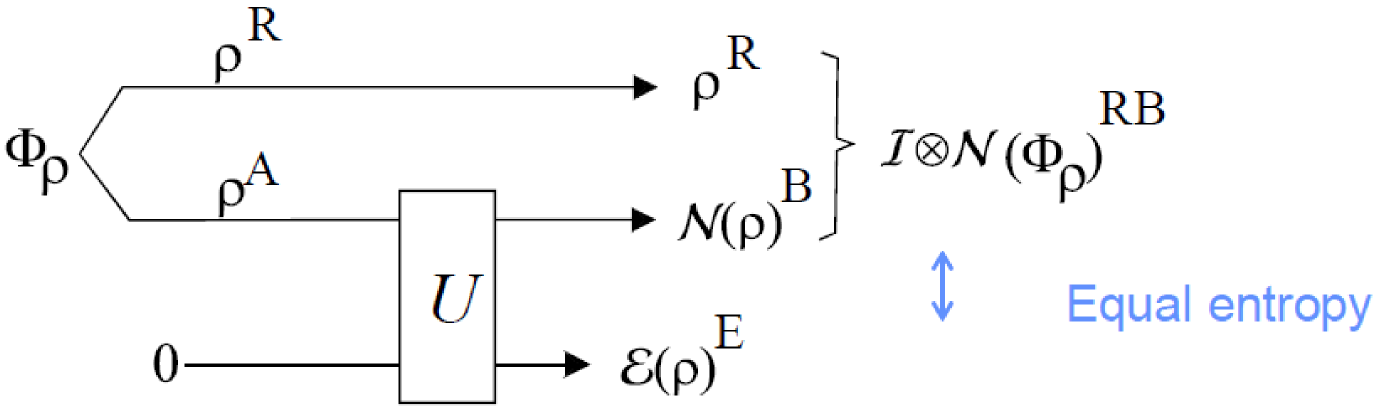


Q Quantum (qubits per channel use, via quantum error-correcting codes)
C Classical (bits per channel use, with a quantum encoder and decoder)
P Private (classical capacity private from an adversary with access to the channel's environment). $Q \leq P \leq C$

In addition, there are various assisted capacities, e.g.

Q_2 Quantum capacity assisted by two-way classical communication
C_E Classical capacity assisted by prior sender:receiver entanglement
($Q_E = C_E/2$ by teleportation and superdense coding)

For quantum channels, these assisted capacities can be greater than the corresponding unassisted capacities.



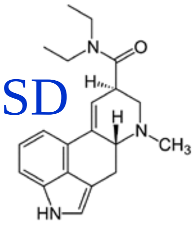
Entropic Expressions for Channel Capacities

Nonadd-tivity H ’09

Holevo

$$C = \lim_{n\to\infty} \max_{\{p_i,\rho_i\}} \left(S(\mathcal{N}^{\otimes n}(\rho)) - \Sigma\, p_i S(\mathcal{N}^{\otimes n}(\rho_i))\right) /n$$

LSD



$$Q = \text{Coherent Info.} = \lim_{n\to\infty} \max_{\rho}\ S(\mathcal{N}^{\otimes n}(\rho)) - S(\mathcal{E}^{\otimes n}(\rho))/n$$

BSST ‘01

$$C_E = \text{Quantum Mutual Info.} = \max_{\rho}\ S(\rho) + S(\mathcal{N}(\rho)) - S(\mathcal{E}(\rho))$$

SRS ’08

$$P = \text{Private Info.} = \lim_{n\to\infty} \max_{\{p_x,\Psi_x\}} (I(X;\mathcal{N}^{\otimes n}) - I(X;\mathcal{E}^{\otimes n}))/n$$

Entanglement both complicates and simplifies the theory of quantum channels, as compared the Shannon theory of classical channels.

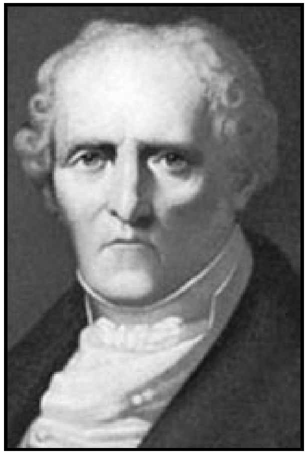
Because of the possibility of entanglement among channel inputs, the quantum capacity *Q* of a quantum channel does not have a simple single-letter formula—it is defined only regularized formula in the limit of large block size.

For the same reason, even the *classical* capacity *C* of a quantum channel lacks a single-letter formula.

However the entanglement-assisted capacity of a quantum channel does have a simple single letter formula.

Does Free Stuff make the world better?

Robert Owen, Charles Fourier, Edward Bellamy:
Free goods & services?



Fourier, Emma Goldman…Haight-Ashbury
Free Love?

Timothy Leary, Ken Kesey: Free LSD?

(Gutenberg, the Internet, LOCC) Free Classical Communication?

Well maybe in some ways, but unfortunately it amplifies fake news and gives us no simple formula for Q_2

(Aram Harrow, ITP2001 poster session) Free Entanglement?

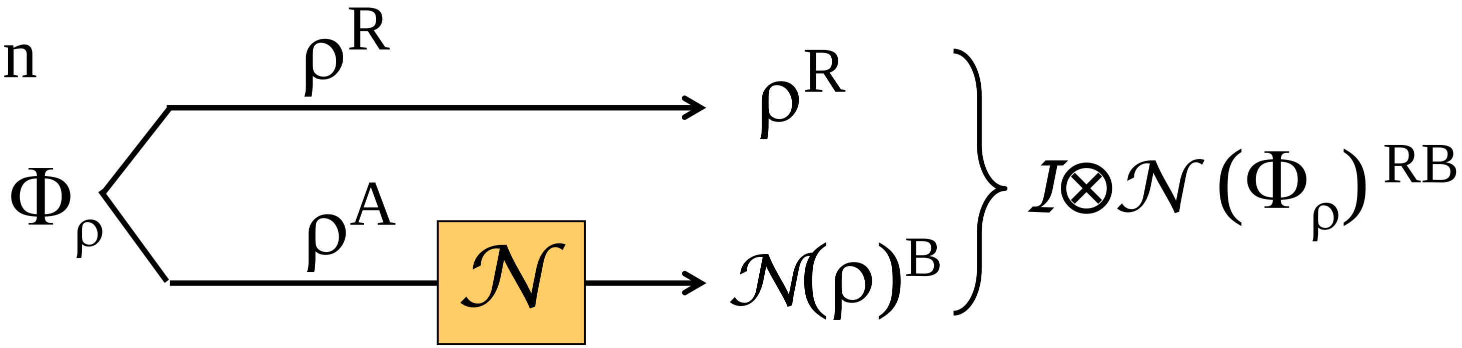
Yes! By simplifying the theory of channel capacities in a way that would have amused Shannon.

One way in which quantum laws are simpler than classical is the universality of interaction.

Classically, there are distinct kinds of interaction that cannot be substituted for one another. For example, if I’m a speaker and you’re a member my audience, no amount of talking by me enables you to ask me a question.

Quantumly, interactions are intrinsically bidirectional. Indeed there is only one kind of interaction, in the sense that any interaction between two systems can be used to simulate any other.

entangled purification of input **ρ**



ρ^R ρ^R

Φ_ρ

ρ^A $\mathcal{N}$ $\mathcal{N}(\rho)^B$

$\mathcal{I}\otimes\mathcal{N}(\Phi_\rho)^{RB}$

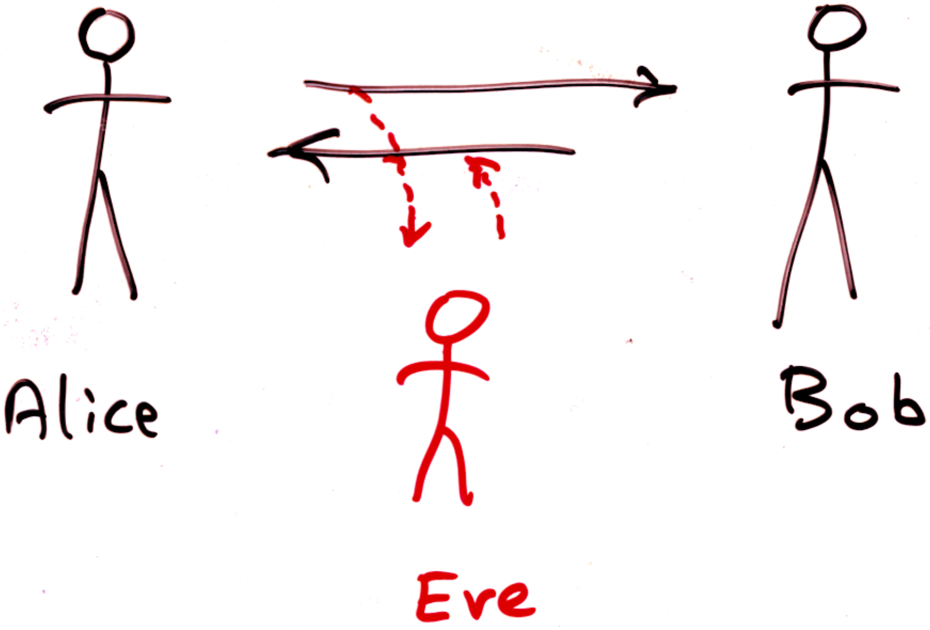
$$C_E(\mathcal{N}) = \max_\rho [S(\rho) + S(\mathcal{N}(\rho)) - S(\mathcal{I}\otimes\mathcal{N}(\Phi_\rho))]$$

Entanglement-assisted capacity C_E of a quantum channel $\mathcal{N}$ is the maximum over channel inputs **ρ** of the (von Neumann) **input entropy** plus the **output entropy** minus their **joint entropy** (more precisely the joint entropy of the output and a reference system entangled with the former input) [B, Shor, Smolin, Thapliyal 2001], [Holevo 2001].

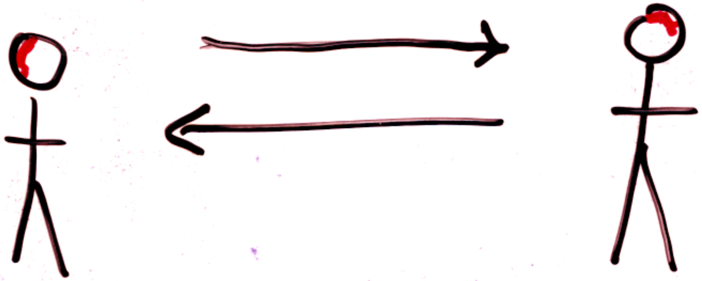
So, in retrospect, what Shannon discovered was an elegantly simple formula for entanglement-assisted capacity, which, for the special case of a classical channel happens to be the same as its unassisted capacity.

Key Distribution is Cold War era cryptography. The good guys trust each other and know who the bad guy is.

Often today, especially in the business world, there is no bad guy per se. But, human nature being what it is, the good guys no longer trust each other. Nevertheless they must cooperate and make joint decisions. But they wish to do so circumspectly, as if they were dealing through a trusted intermediary. Of course there is no one they trust well enough to hire for that job. What to do?



2 Good Guys and 1 Bad Guy



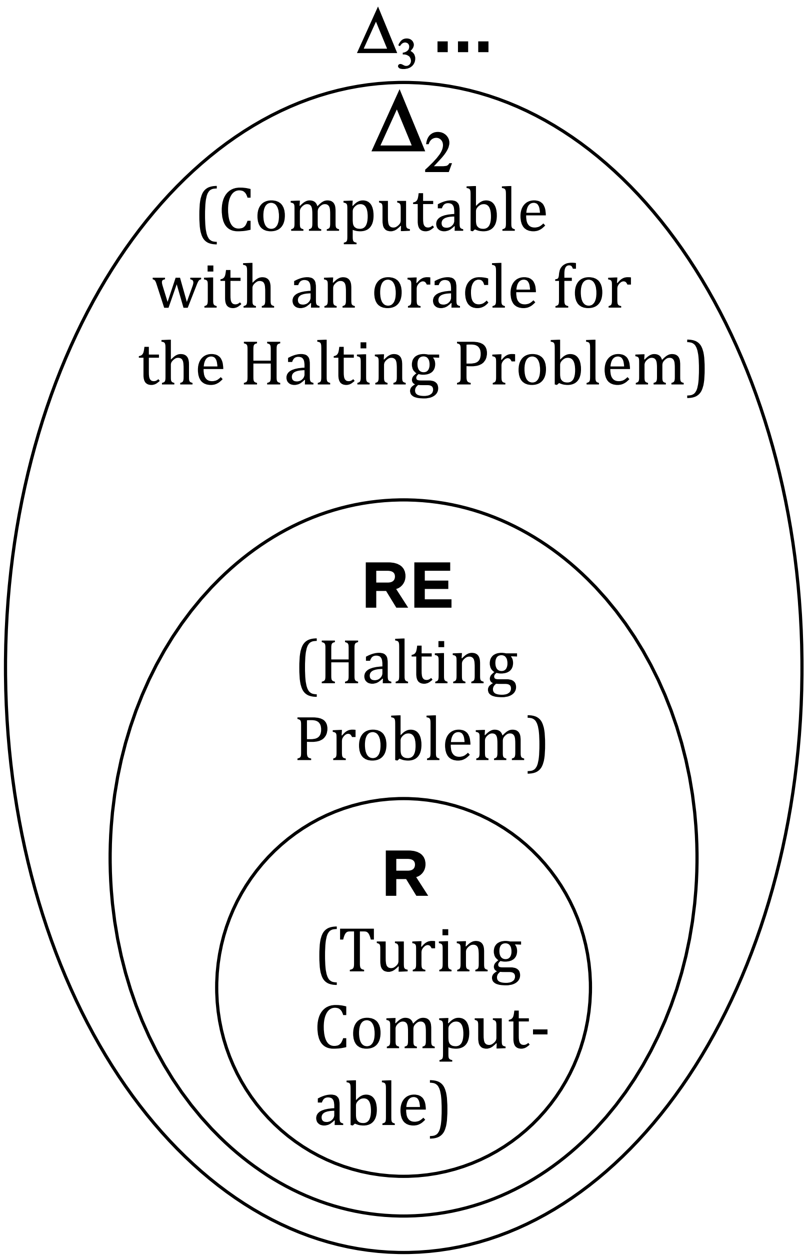
2 Good Guys who don’t trust each other

Wiesner’s other invention—the multiplexing of two messages into a physical form such that reading one message spoils the other—also turned out to be of considerable cryptographic importance.

Michael Rabin and other classical cryptographers showed that the ability to do so could be used to accomplish other important cryptographic task mentioned earlier: discreet negotiation between 2 mutually distrustful parties.

Wiesner, Mayers, Lo and Chau showed that the multiplex and all related schemes can be broken in principle, by an adversary armed with a quantum computer able to store quantum information for an unlimited time.

Shaffner, Damgaard, Fehr and Salvail showed conversely that if neither negotiating party can store quantum information, techniques related to Wiesner’s multiplex provide a way to achieve provably discreet 2-party negotiation (quant-ph/0508222, FOCS)



Turing 1936 showed that a computer can't solve its own halting problem. Problems equivalent to the Halting Problem are called recursively enumerable or **RE**.

Despite some early hopes to the contrary, quantum computers cannot solve the Halting Problem. The class of computable functions is the same for quantum computers as for classical computers.

‘50s through present: focus shifts toward a parallel but more practical theory of computational ***tractability,*** with **P** (polynomial time) being a rough analog of **R** (computable), and **NP** of **RE**. Other complexity classes include **PSPACE**, the polynomial hierarchy, and **IP** = polynomial time interactive proof, in the scenario where an infinitely wise but untrustworthy prover (Merlin) tries to convince a polynomially time bounded verifier (Arthur) of membership in the set under discussion. 1992 surprising result that **IP=PSPACE**

’90s through present: focus on quantum vs classical computational complexity classes (since quantum and classical computability are equivalent), and the effect of entanglement on computational complexity *(And of course the grand project of building a useful quantum computer)*

Jan. 2020 Unexpected reconnection: Ji, Natarajan, Vidick, Wright and Yuen showed **MIP*=RE**, in other words

> Membership in a set can be proven by **M**ultiple non-communicating but entangled (*****) provers, **I**nteracting with a **P**olynomial time bounded Verifier, **iff** the set is the halting set of some Turing machine.

As Scott Aaronson summarizes the **MIP*=RE** paper [JNVWY20],

(1) There is a protocol by which two entangled provers can convince a polynomial-time verifier of the answer to any computable problem whatsoever (!!), or indeed that a given Turing machine halts.

(2) There is a two-prover game, analogous to the Bell/CHSH game, for which Alice and Bob can do markedly better with a literally infinite amount of entanglement than they can with any finite amount of entanglement.

(3) There is no algorithm even to approximate the entangled value of a two-prover game (i.e., the probability that Alice and Bob win the game, if they use the best possible strategy and as much entanglement as they like). Instead, this problem is equivalent to the halting problem.

(4) There are types of correlations between Alice and Bob that can be produced using infinite entanglement, but that can't even be approximated using any finite amount of entanglement.

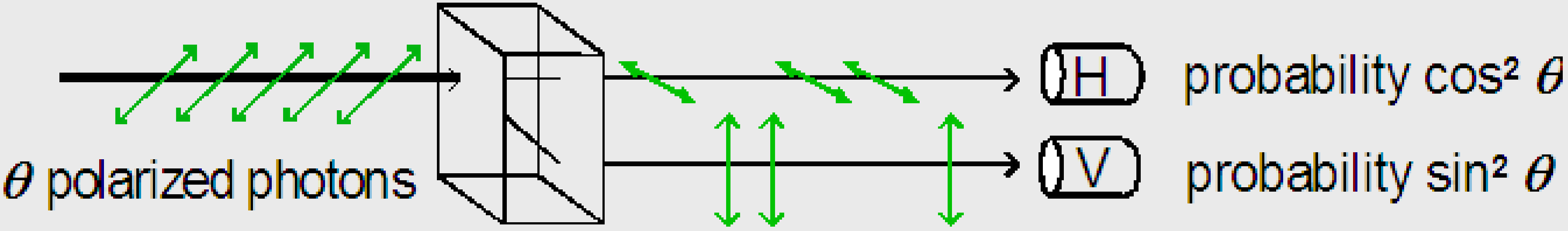
(5) The Connes embedding conjecture, a central conjecture from the theory of operator algebras dating back to the 1970s, is false.

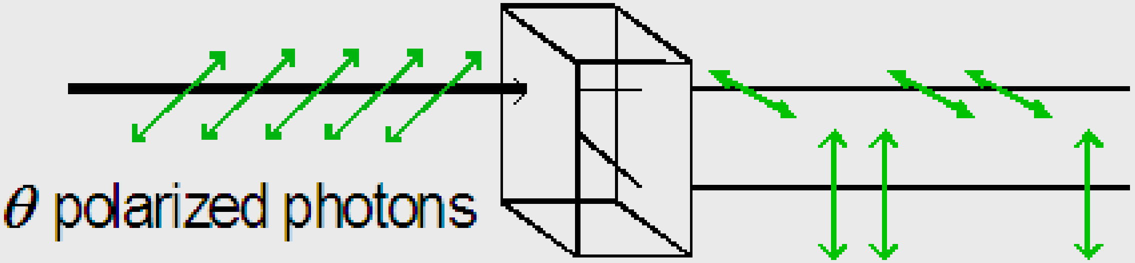
Conclusions

- Quantum information provides a coherent basis for the theory of communication, computing, and interaction between systems, within which classical behavior emerges as a useful 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.
- Fascinating and unexpected properties of information, owing to its fundamentally quantum nature, are still being discovered.

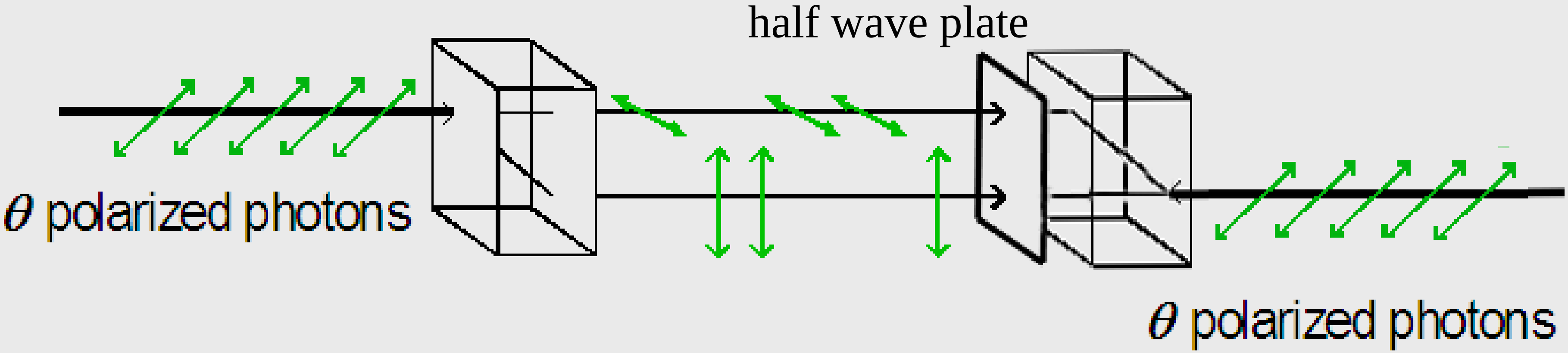
Like the roundness of the earth, or fact that matter is made of atoms, the quantum nature of information is a fundamental but non-obvious aspect of our universe that everyone should know about. Properly explained, it can be made comprehensible and fascinating.

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.

The Einstein -Bohr debate: an early phase of the cultural adjustment that gave birth to quantum information theory

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, and entanglement. Einstein was deeply troubled by both disparaging indeterminacy as “God playing dice,” and 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.

Einstein disliked quantum mechanics, and his distaste for it, together with his fame (being the only 20th century scientist whose name is a household word) which helped people grasp relativity, retarded their grasp of quantum mechanics and especially entanglement. Even in the 21st century most science journalists are clueless about it.

Einstein thought entanglement was spooky (*spukhafte Fernwirkung*), but his wrong take on it, as action at a distance, refuses to die. That's *spukhafte Spätwirkung.*

Mistakenly believing entanglement could be used for long-range communication, Nick Herbert published a paper in 1982 and Jack Sarfatti tried to patent this imagined application of it. The swift refutation of these proposals, 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".

Sarfatti’s and Herbert’s ideas about entanglement were so wrong that they facilitated the acceptance of the no-cloning theorem as a central fact about quantum information. The theorem had actually been proved in 1970, by J. L. Park, [Foundations of Physics, 1, 23-33, (1970)], but his paper went unnoticed until the theorem was rediscovered by Dieks and by Wootters and Zurek at a time more ripe for its importance to be appreciated.

Moral:
Bad ideas sometimes stimulate scientific progress.

Conversely, good ideas—indeed quantum mechanics itself—sometimes retard scientific progress.

The analogy between computation and physical dynamics is very old. For example Galileo’s “The book of nature is written in the language of mathematics” and Laplace’s elegant description of a universe governed by Newtonian mechanics,

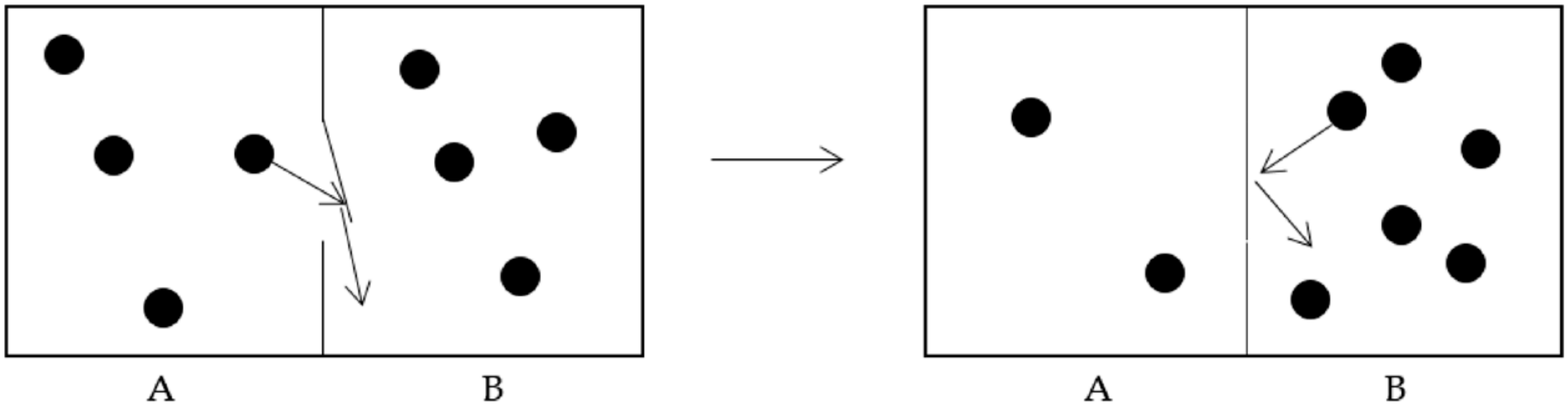
“We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect which at a certain moment would know all forces that set nature in motion, and all positions of all items of which nature is composed, if this intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes.”
Pierre Simon Laplace 1814

Note that this computation is deterministic and reversible, a feature seemingly lost with quantum indeterminism, but then recovered in a more inclusive form with unitary quantum evolution.

Information Physics was born in 1867 with Maxwell’s Demon

“If we conceive of a being whose faculties are so sharpened that he can follow every molecule in its course, such a being, whose attributes are as essentially finite as our own, would be able to do what is impossible to us. For we have seen that molecules in a vessel full of air at uniform temperature are moving with velocities by no means uniform, though the mean velocity of any great number of them, arbitrarily selected, is almost exactly uniform. Now let us suppose that such a vessel is divided into two portions, A and B, by a division in which there is a small hole, and that a being, who can see the individual molecules, opens and closes this hole, so as to allow only the swifter molecules to pass from A to B, and only the slower molecules to pass from B to A. He will thus, without expenditure of work, raise the temperature of B and lower that of A, in contradiction to the second law of thermodynamics”.

In 1912 Smoluchowski gave us the trapdoor or ratchet version of the demon, along with a correct exorcism of it.   A spring-loaded trapdoor door, light enough to be pushed open by molecular impacts, would seem to violate the Second Law, effortlessly collecting molecules on the right in a pressure version of Maxwell’s temperature demon.



But, Smoluchowski argued, if the door were that light and the spring that weak, the door would soon heat up to the same temperature as the gas and undergo random motion of its own, swinging open and shut. It would then swing shut against a molecule that had wandered in front of it, pushing it to the left, just as often as it would be pushed open by a molecule striking it from the left, and there would be no net flow.

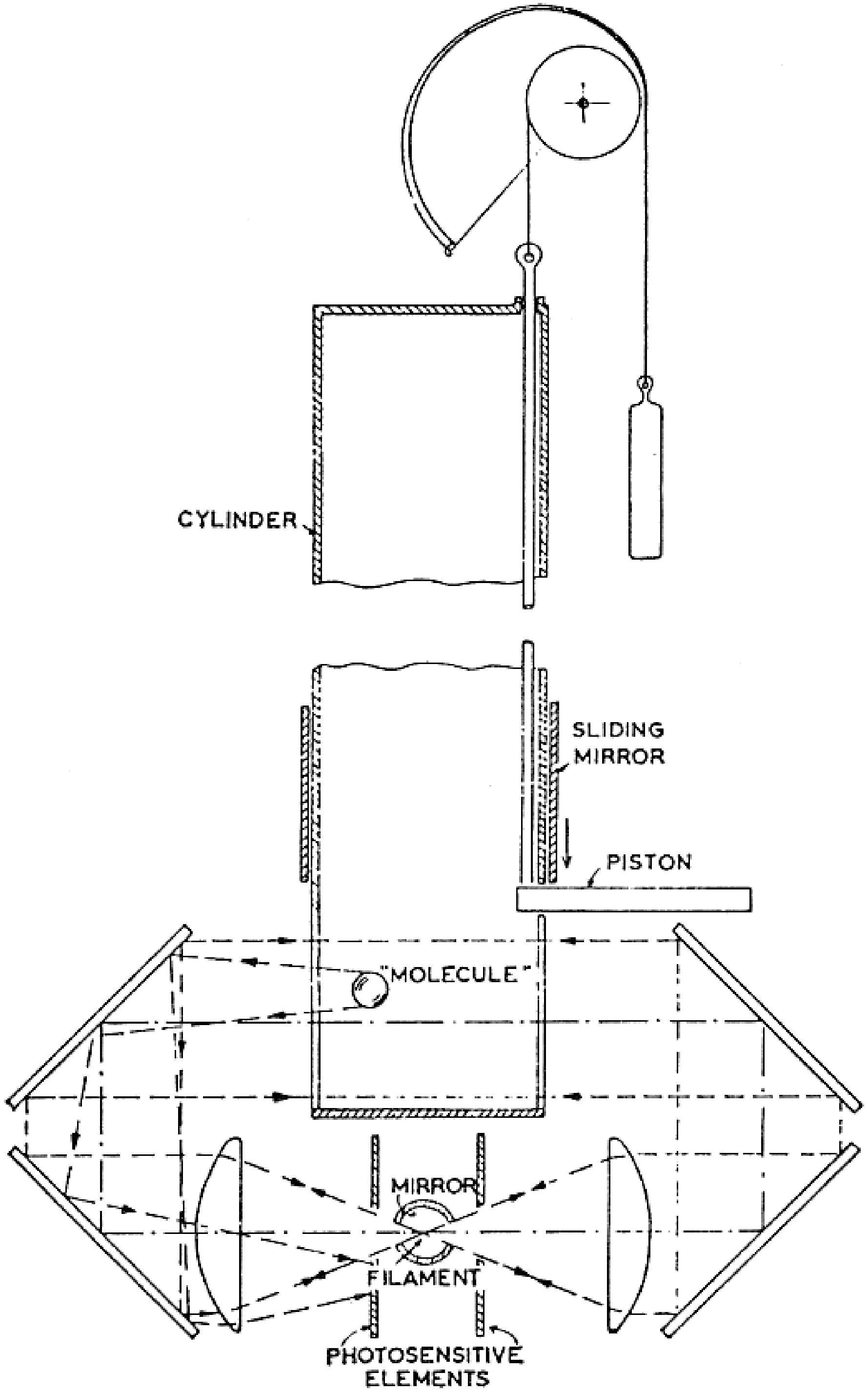
Despite Laplace’s deterministic universe, whose vast mechanism presumably included the brains of all its inhabitants, early 20th century physicists became strangely reluctant to think of *thought* itself as a mechanistic process, causing Smoluchowski’s correct exorcisim of the demon to unravel somewhat in subsequent decades. The title of Leo Szilard’s 1929 paper, exemplifies this timidity

“On the decrease of entropy in a thermodynamic system by the intervention of intelligent beings.”

The situation was further muddied by the discovery of quantum mechanics, which problematized the previously uncontroversial act of measurement. This tempted physicists to look for an irreducible cost of *information acquisition*, *transmission* or *processing*, when they would have done better to think like Smoluchowski. Even von Neumann incorrectly asserted in a 1949 lecture that each elementary act of information, each decision of a two-way alternative or transmission of a bit of information, must have a thermodynamic cost of kT ln 2 at temperature T. In 1961 Rolf Landauer correctly identified *information destruction* as the fundamentally costly act.

Examples of that sloppy thinking due to misapplication of quantum mechanics to Maxwell’s demon include Leon Brillouin's 1956 argument that to even see a molecule, against the background of quantum black body radiation at temperature T, a demon would need to expend at least one photon more energetic than kT.

Denis Gabor's 1961 refutation of his own high-compression version of Szilard’s engine was the most intricately unnecessary invocation of quantum optics to prove what Smoluchowski had already proved.



Denis Gabor's high-compression Szilard engine (1961).

- Light beam circulates losslessly across one end of a long cylinder
- Photosensors detect when molecule wanders into the beam, and insert a piston to trap it there.
- Piston extracts kT ln (V/V_0) work by a very long isothermal power stroke.
- Some of the work is used to reset piston & recreate the light beam.
- Since it takes only a fixed amount of work w to do that, one can break the Second Law by making V so large that kT $\ln(V/V_0) > w$.

What keeps it from breaking the 2nd Law?

Can you guess Gabor's answer? (hard)

Can you guess the correct answer? (easy)