Building a Culture of Quantum Information

Charles H. Bennett
IBM Research Yorktown
NY 10598 USA

ICTP Trieste
14 March 2018

Like other parts of mathematics, information science originated as an abstraction from practical experience. Today's information revolution is based on the brilliant abstractions of Turing and Shannon (among others):

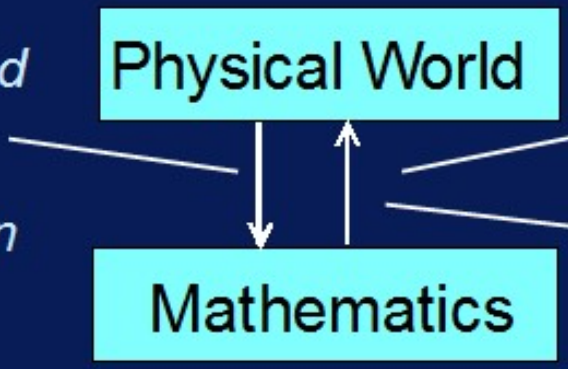
- Turing—a universal, hardware-independent notion of computation
- Shannon—a universal, meaning-independent theory of communication

But now these notions are known to be too narrow.

The subsequent incorporation of a two essentially mathematical concepts from physics has led to a more elegant and powerful theory of information and information processing.

Physical (e.g. thermodynamic) resources required for computation

Landauer's slogan "Information is Physical"



Computational resources required to simulate physical states and evolutions

(More mystically, Wheeler's "It from Bit": involvement of information in the creation of physical reality.)

When Turing, Shannon, von Neumann et al formalized the notions of information and computation, they left out a couple of important ideas

Reversibility —— Thermodynamics of Computation

(Superposition —— Quantum 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 non-interacting objects, it suffices 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.

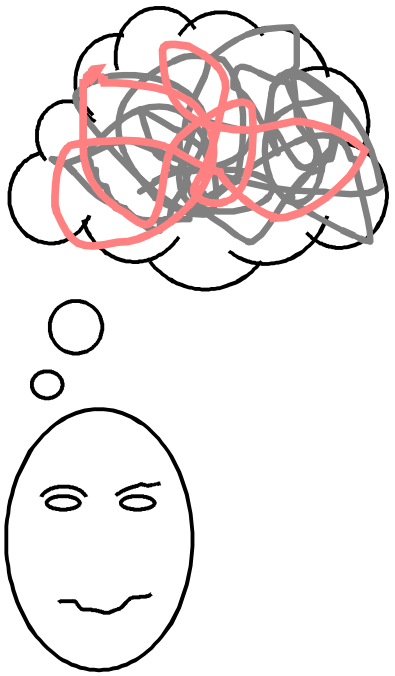
For most of the 20th century, quantum effects in information processing were regarded mainly as a nuisance, because the uncertainty principle makes tiny quantum devices behave less reliably than the classical ideal.

Now it is known that quantum effects also have positive consequences, making possible new kinds of information processing such as quantum cryptography, and dramatically speeding up some classically hard computations.

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.

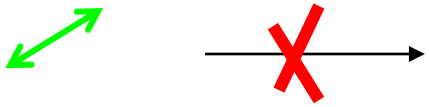
Bits and gates are fungible (independent of physical embodiment), making possible Moore's law.

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

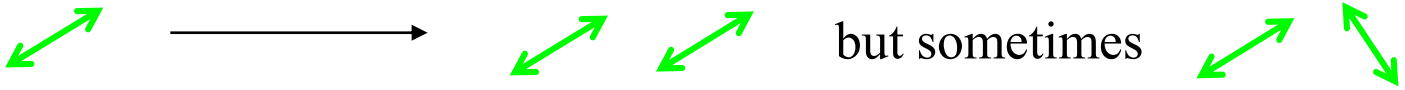
Measuring an unknown photon's polarization exactly is impossible (no measurement can yield more than 1 bit about it).



28.3°

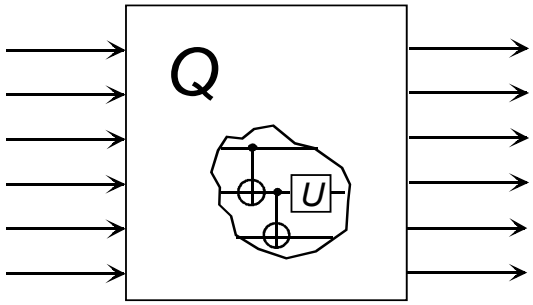
Cloning an unknown photon is impossible. (If either cloning or measuring were possible the other would be also).

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.



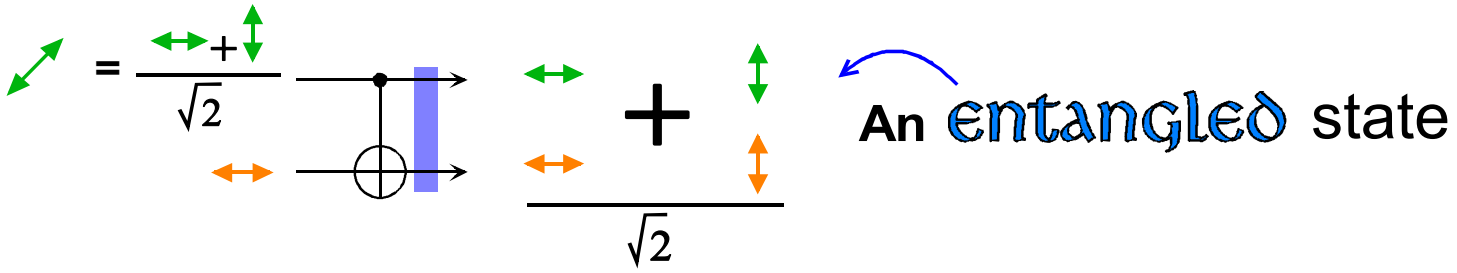
but sometimes

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

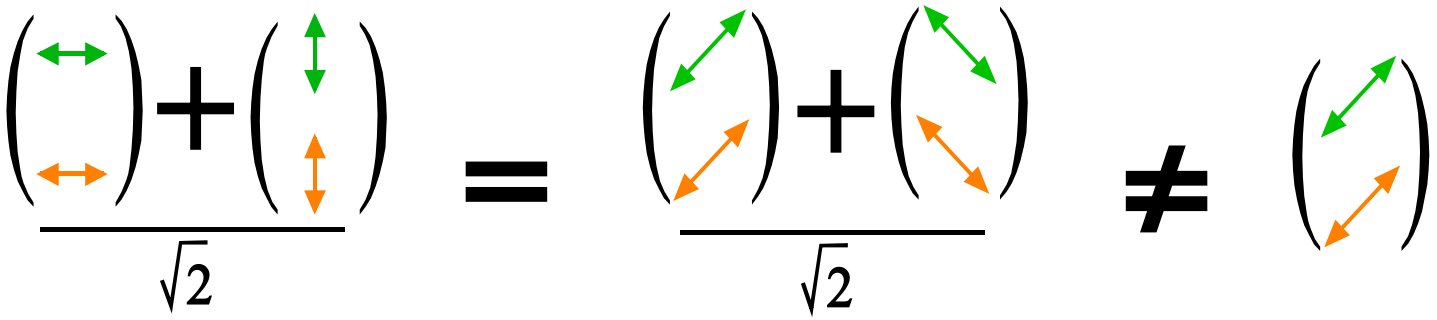


The 2-qubit XOR or "controlled-NOT" gate flips its 2nd input if its first input is 1, otherwise does nothing.

A superposition of inputs gives a superposition of outputs.



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 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.

Wikiwatcher1 CC Share alike

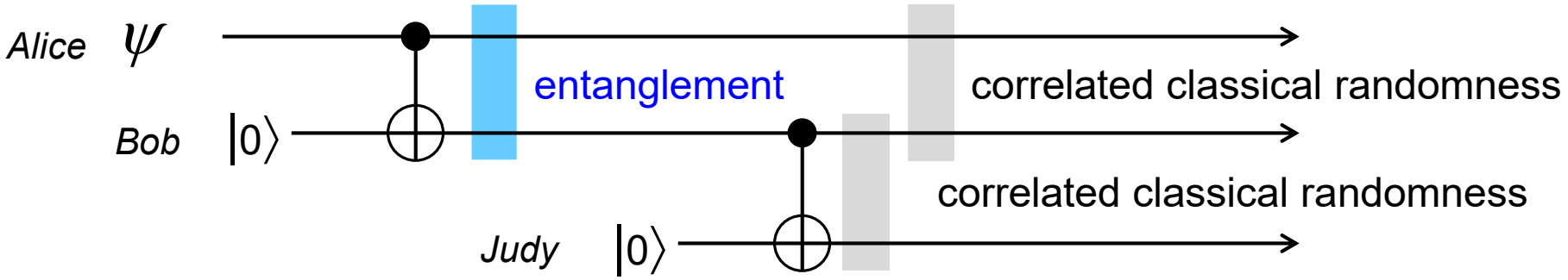
Hippies believed that with enough LSD, everyone could be perfectly in tune with everyone else.

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.

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."



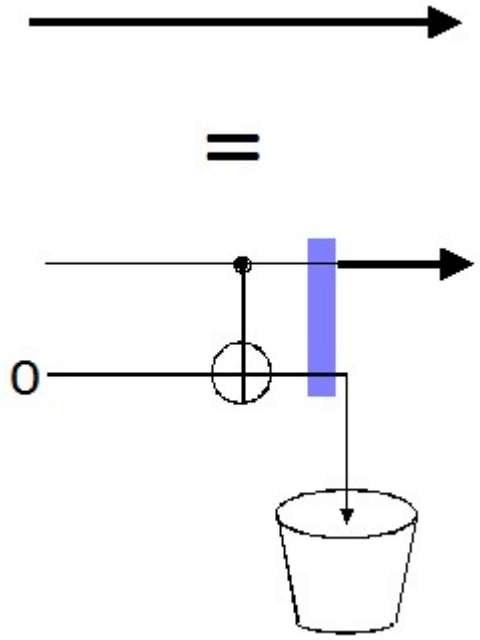
If one of Bob's girlfriends leaves the scene, Bob will find his relationship with the other reduced to mere correlated randomness. If they both stick around, he ends up perfectly entangled, not with either one, but with the now nontrivial *relationship* between them, an appropriate punishment.

Expressing Classical Data Processing in Quantum Terms

A Classical Bit is a qubit with one of the binary 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. If the environment is lost or discarded, the data gets randomized.



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.

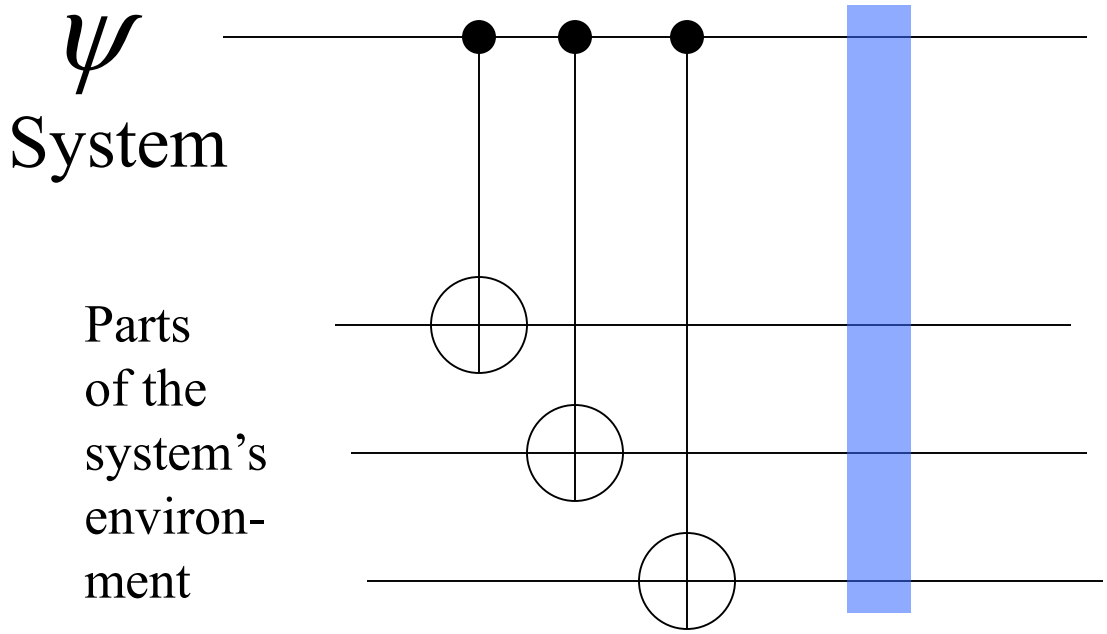
Then why wasn't it discovered before the 20th century?

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?



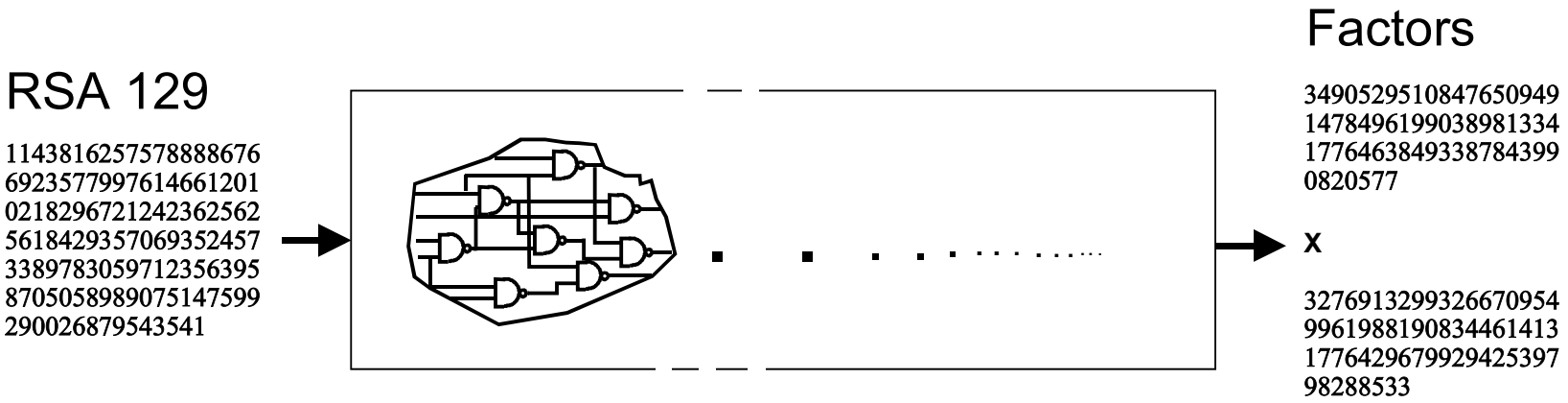
Massive eavesdropping causes the system to get classically correlated with many parts of its environment. But because of monogamy, it remains entangled only with the ***whole*** *environment.*

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.

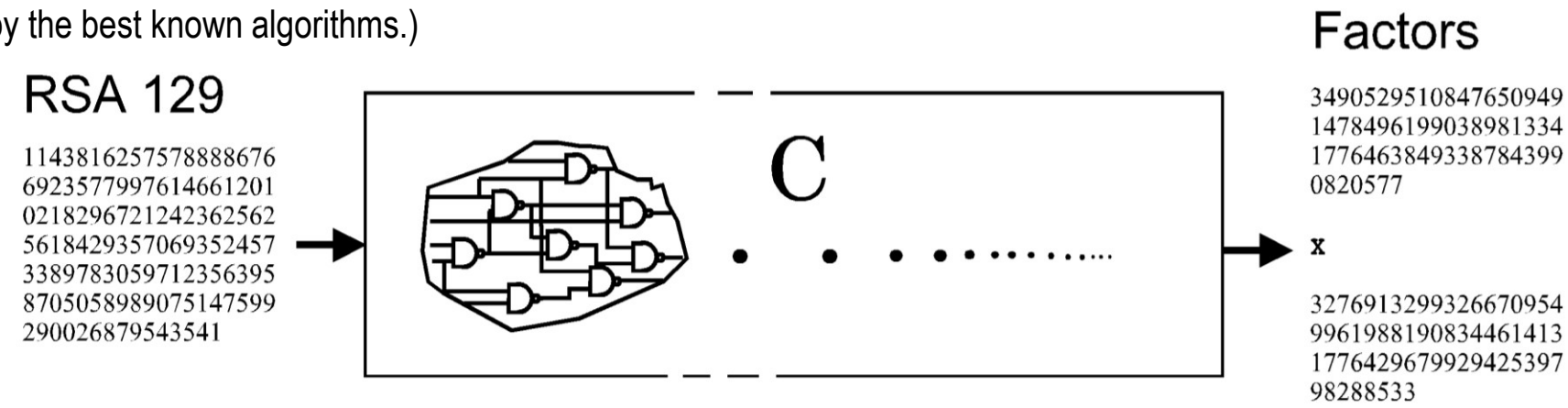
(This typically happens when the environment is ***not*** *at thermal equilibrium, and when it contains many subsystems that interact more strongly with the system than with each other and… The earth's environment is like that.)*

Classical Computation Theory shows how to reduce all computations to a sequence of ANDs and NOTs. It classifies problems into solvable and unsolvable, and among the solvable ones classifies them by the resources (e.g. time, memory, luck) required to solve them. Complexity classes P, NP, PSPACE…

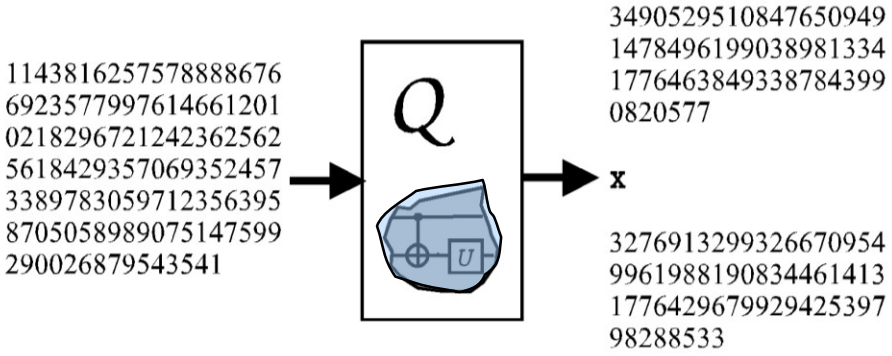


Some computations require a great many intermediate steps to get to the answer. Factoring large integers is an example. This factoring job took 8 months on hundreds of computers. It could be done much faster on a quantum computer, if one existed.

(For a classical computer, factoring appears to be exponentially harder than multiplication, by the best known algorithms.)



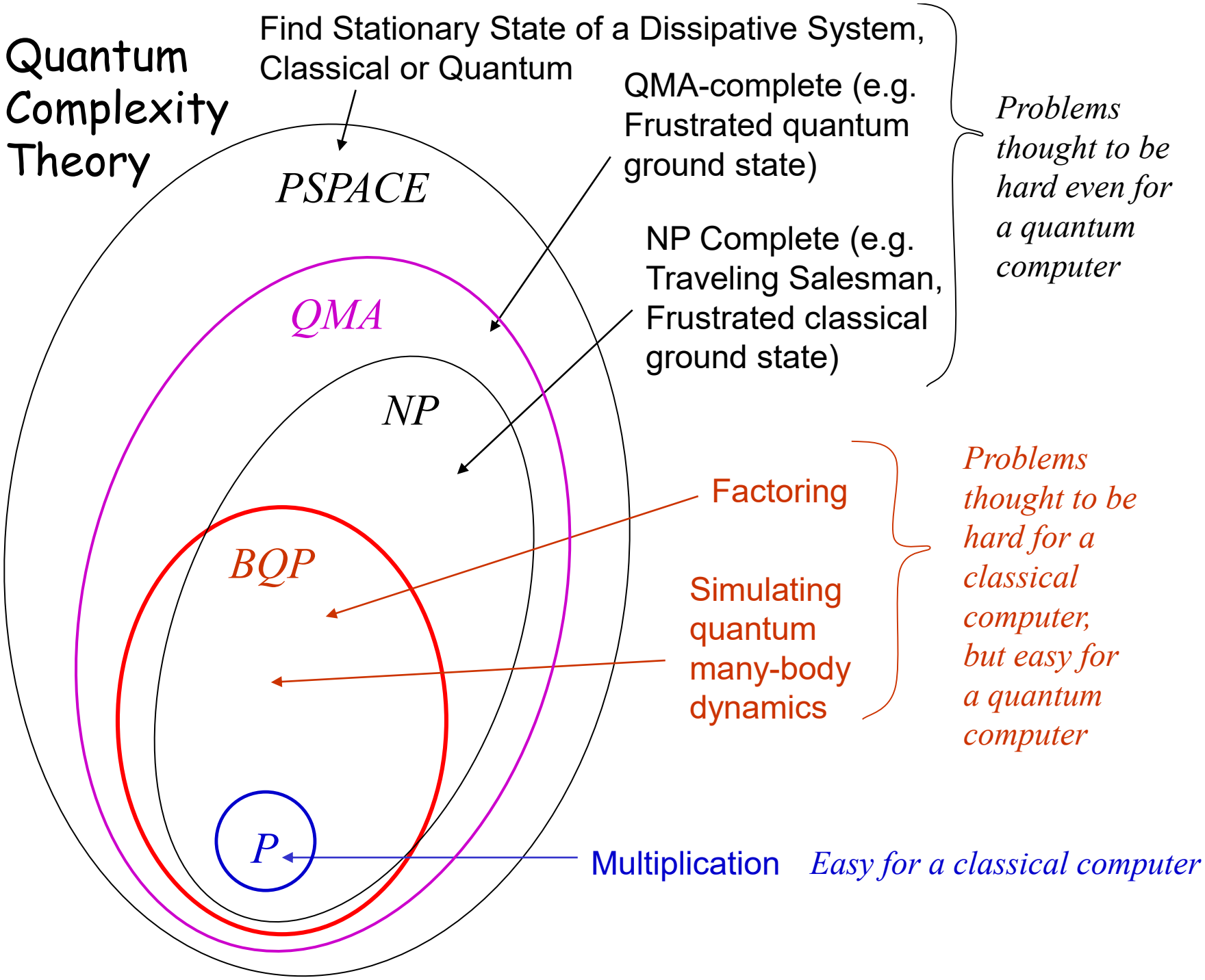
Same Input and Output, but Quantum processing of intermediate data gives



Exponential speedup for Factoring (Shor algorithm)

Quadratic speedup for Search (Grover algorithm)

(For a quantum computer, factoring is about as easy as multiplication, due to the availability of **entangled** intermediate states. But quantum computers area hard to build because the qubits inside must be protected from eavesdropping by the environment.)


Quantum Complexity Theory
Find Stationary State of a Dissipative 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
PSPACE
QMA
NP
BQP
P
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

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.

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.

Lesson: wrong ideas sometimes stimulate scientific progress.

Conversely, as we shall see later, correct ideas—indeed quantum mechanics itself—sometimes retard scientific progress.

The analogy between mathematical computation and physical dynamics is very old. E.g. 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

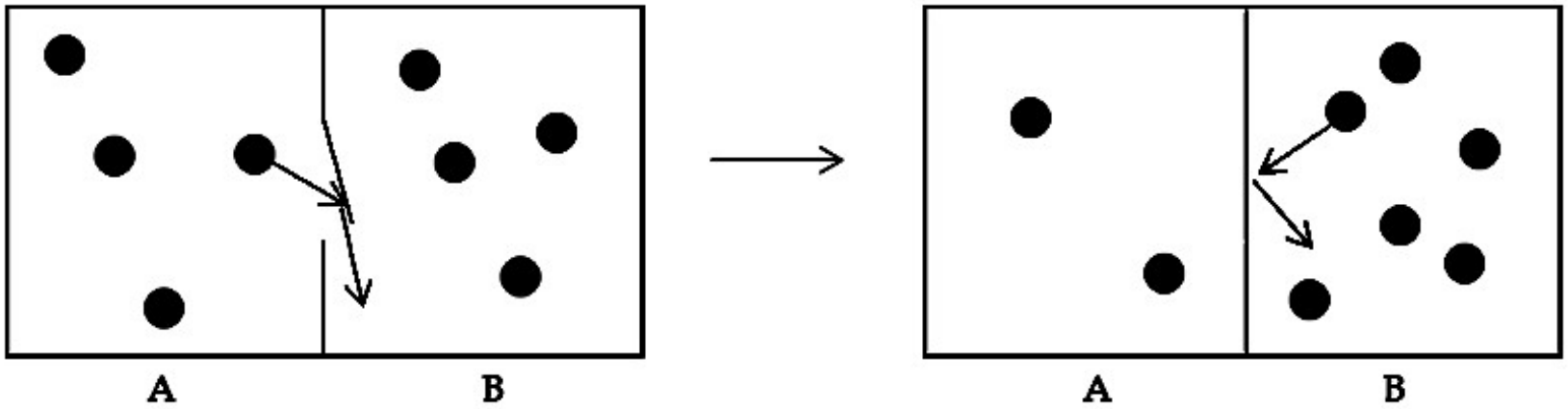
Note that the computation Laplace envisioned is deterministic and reversible, features seemingly lost with quantum indeterminism, but then recovered in a more inclusive form by considering entanglement.

Maxwell's Demon

Now let us suppose that…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. *James Clerk Maxwell 1867*

M. Smoluchowski's trap door demon, and his refutation of it in a pioneering 1912 paper on fluctuations at thermal equilibrium.

An inanimate mechanism, such as a spring-loaded trap door, light enough to be pushed open by molecular impacts, would seem to violate the Second Law, effortlessly collecting molecules on one side in a pressure version of Maxwell's temperature demon.



But, Smoluchowski argued, if the door were that light and the spring that weak, as soon as the door reached the same temperature as the gas, it would 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, exactly 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, early 20th century physicists were reluctant to think of ***mental processes*** as mechanistic, so Smoluchowski's neat solution to the Maxwell demon problem unraveled somewhat in subsequent decades. This puzzling reluctance is reflected in the title of Szilard's 1929 paper, in which he introduced his now-famous Szilard engine, *"On the decrease of entropy in a thermodynamic system by the intervention of intelligent beings,"*

The situation was further obscured by the ***success of quantum mechanics,*** which problematized the previously uncontroversial act of measurement. This tempted physicists to look for an irreducible cost of *information processing*, when they would have done better to think like Smoluchowski. Several great physicists, without thinking about it carefully, opined that every elementary act of information processing, such as copying, or transmitting a bit, or comparing two bits, must consume an amount of energy approximately equal to the average heat energy of a molecule.

In 1961 Rolf Landauer correctly identified ***information erasure*** as the only fundamentally costly information-processing act.

Basic Science and the Future: Haste makes Waste

Most people, interested in what science can do to solve what they see as today's most pressing problems, take a short term view…but

- Scientific progress is mostly incremental. Breakthroughs are overrated.
- The most important applications of any scientific discovery are hardly ever the ones people think of first.
- Even in applied science, ideas go through ups and downs of popularity, their potential alternately over- and underestimated.
    - For example a hot topic today, even hotter than quantum computing, is machine learning and artificial intelligence. This optimism is probably largely justified by recent progress, but for many decades AI was a cold field, whose ability to solve real-world problems like language translation had been disappointing.

Therefore, the most cost-effective science policy is steady support of good science, with little regard for its perceived applications.

About 20 years ago, I met a scientist at Jet Propulsion Labs who was nearing retirement. He said his proudest accomplishment was working on the Voyager spacecraft, which used the gravitational slingshot effect to visit the four big outer planets. When scientists originally proposed this, the Washington bureaucrats in charge said

"Just do Jupiter and Saturn"

"But the planets won't be in a good position again for 200 years"

"Congress understands 2 years, not 200. Just do Jupiter and Saturn."

There ensued a quiet conspiracy, in which the scientists and engineers over-designed many features of the two spacecraft to make sure they would last far longer than necessary for their official mission. Then, years after the launch, the mission was modified to add Uranus and Neptune to the itinerary, with spectacular results.

But scientists can't try this too often, or no one will trust us any more.

Benefits of the new theory of Information Processing

- A better understanding of its energy costs.
- New kinds of cryptography and communication.
  If a quantum computer can be built, it would dramatically speed up some hard computations, but many other computations would not be sped up.)
- Improvements in precision measurement
- Insights into black hole physics and quantum gravity

Beyond that, entanglement is a feature of nature so central that every educated person should have an elementary understanding of it, like Einstein's interconnection of space and time, the roundness of the earth, the fact that matter is made of atoms, and hereditary information is carried by DNA.