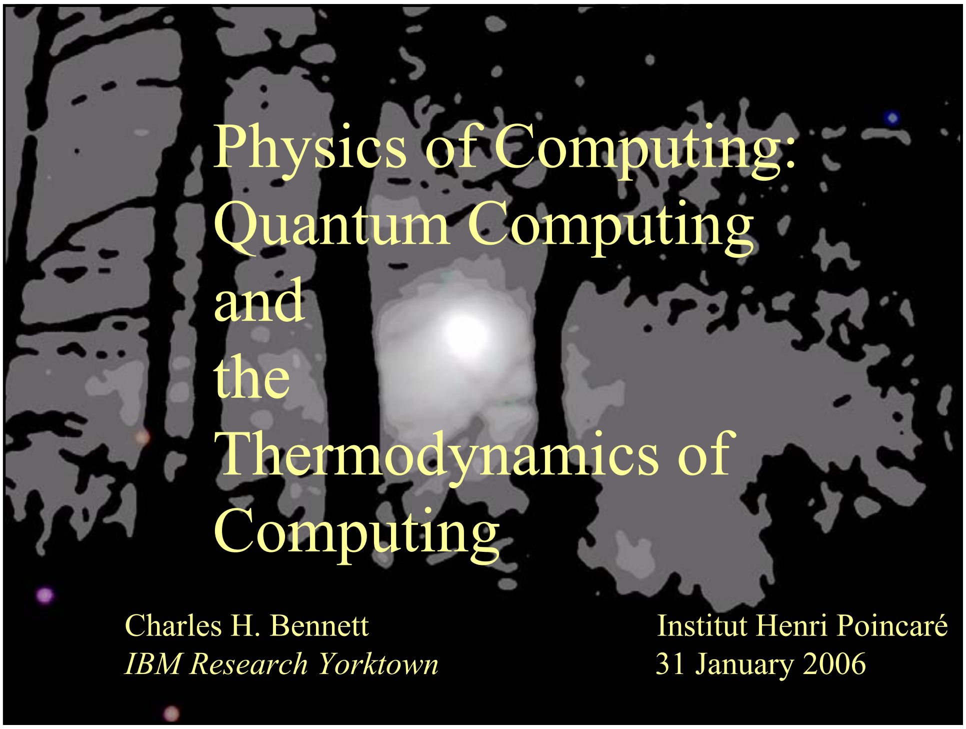
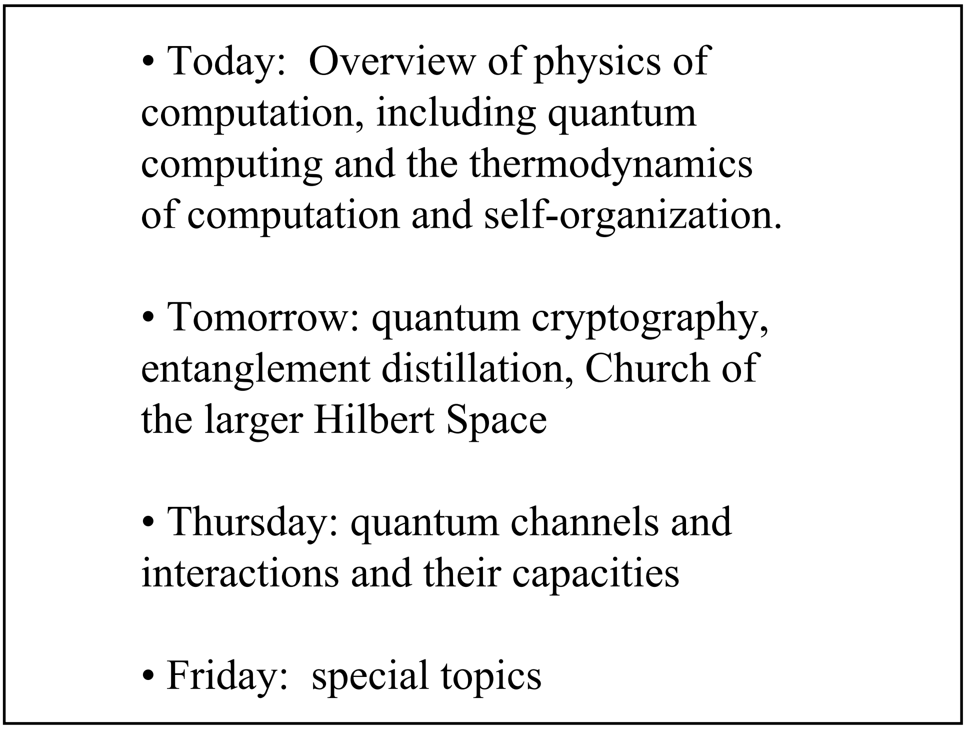


Physics of Computing: Quantum Computing and the Thermodynamics of Computing

Charles H. Bennett
IBM Research Yorktown

Institut Henri Poincaré
31 January 2006



- Today: Overview of physics of computation, including quantum computing and the thermodynamics of computation and self-organization.

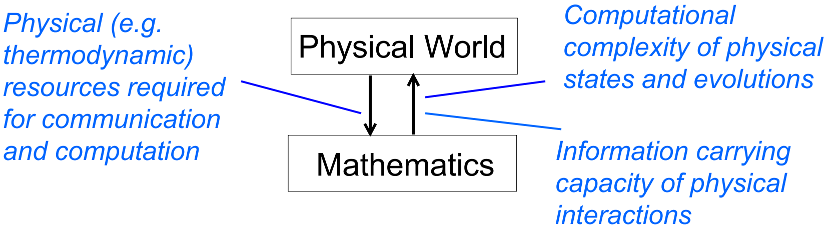
- Tomorrow: quantum cryptography, entanglement distillation, Church of the larger Hilbert Space

- Thursday: quantum channels and interactions and their capacities

- Friday: special topics

"Information is Physical" Rolf Landauer

"It from bit" John Archibald Wheeler



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

Physical World

Mathematics

Computational complexity of physical states and evolutions

Information carrying capacity of physical interactions

When Turing, Shannon, von Neumann and their contemporaries formalized the notions of information and computation, they forgot about the reversibility and the superposition principle

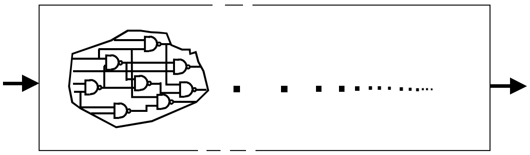
reversibility => thermodynamics of computation

superposition => quantum information/computation theory.

Classical Computation Theory shows how to reduce all computations to a sequence of NANDs and Fanouts. 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…

RSA 129

11438162575788886766923577997614661201021829672124236256256184293570693524573389783059712356395870505898907514759929002687954354 1



Factors

3490529510847650949147849619903898133417764638493387843990820577

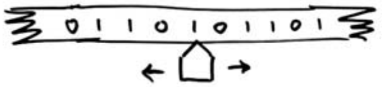
x

32769132993266709549961988190834461413177642967992942539798288533

Some computations require a great many intermediate steps to get to the answer. Factoring large integers is in NP but believed not to be in P.

Computational Universality:

Any sufficiently complicated computer, e.g.



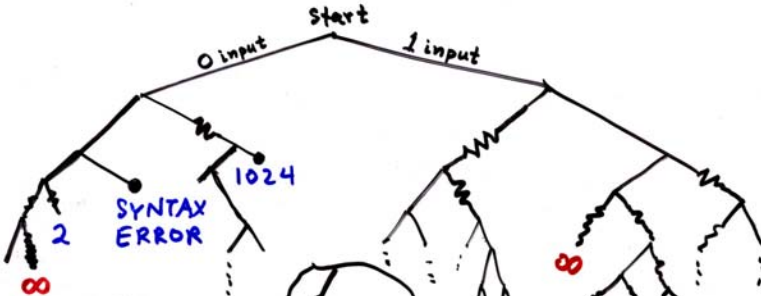
A Universal Turing Machine,

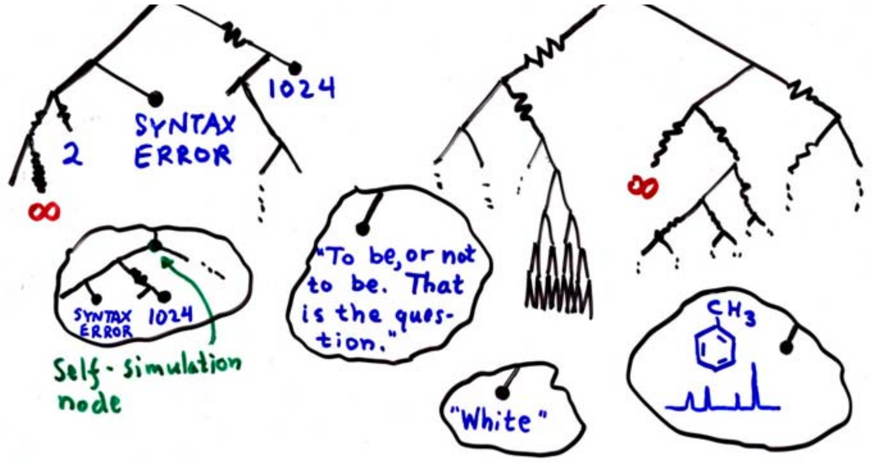
A laptop computer, with extra disks

(but not a pocket calculator or a digital wrist watch)

can simulate any other computer typically to within an additive constant in program size and memory usage and a small polynomial in run time.

Monkey randomly supplies input to a universal binary computer, might get it to do any computation. (Chaitin 1975)





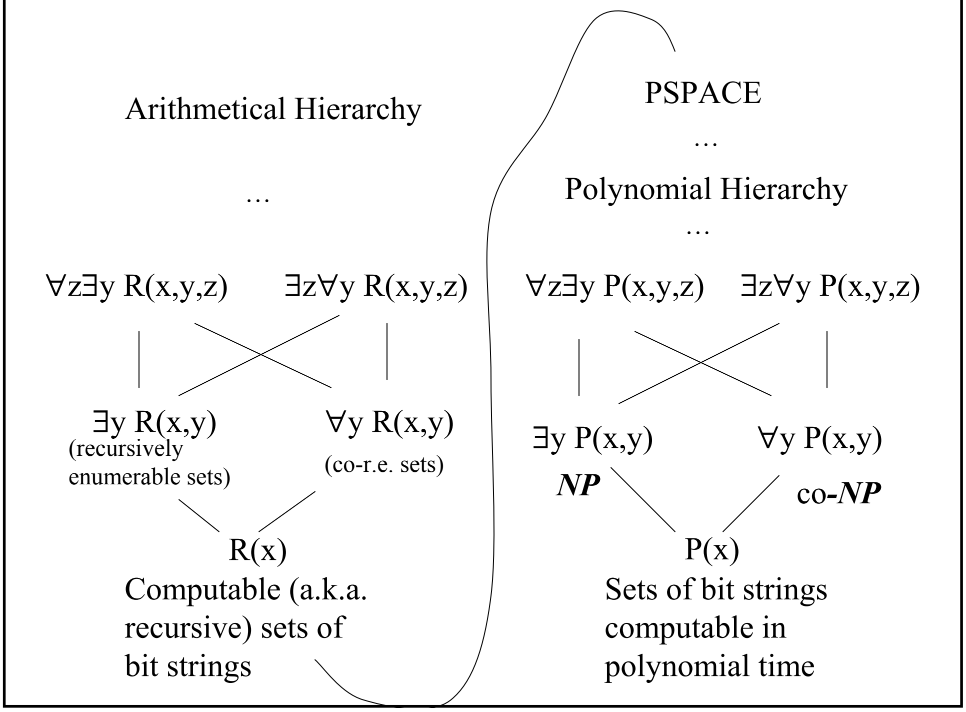
The input-output graph of this or any other universal computer is a microcosm of all cause-effect relations that can be demonstrated by deductive logic or numerical simulation

Knowing the monkey graph is equivalent to being able to solve the Halting Problem.

Would a person gifted with this ability know the answer to all *interesting* mathematical questions?

Goldbach's conjecture – every even number >2 is expressible as the sum of not more than 4 primes.

Twin prime conjecture—there are infinitely many numbers p such that p and p+2 are both prime.



Arithmetical Hierarchy

…

∀z∃y R(x,y,z) ∃z∀y R(x,y,z)

∃y R(x,y) (recursively enumerable sets)

∀y R(x,y) (co-r.e. sets)

R(x)
Computable (a.k.a. recursive) sets of bit strings

PSPACE

…

Polynomial Hierarchy

…

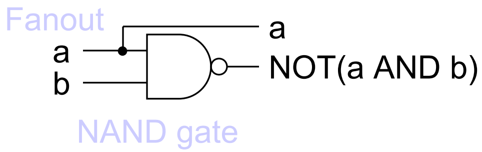
∀z∃y P(x,y,z) ∃z∀y P(x,y,z)

∃y P(x,y) ***NP***

∀y P(x,y) co-***NP***

P(x)
Sets of bit strings computable in polynomial time

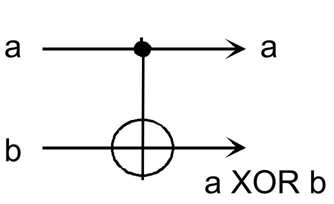
Conventional computer logic uses irreversible gates, eg NAND, but these can be simulated by reversible gates. Toffoli gate is universal.

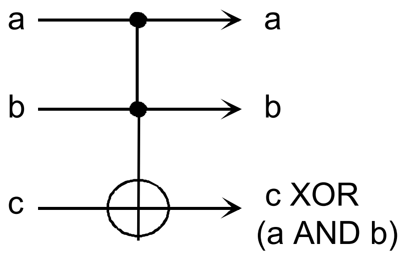


NAND gate

no inverse

Reversible logic was used to show that computation is thermodynamically reversible in principle. Now it is needed for quantum computation.





XOR gate

Toffoli gate

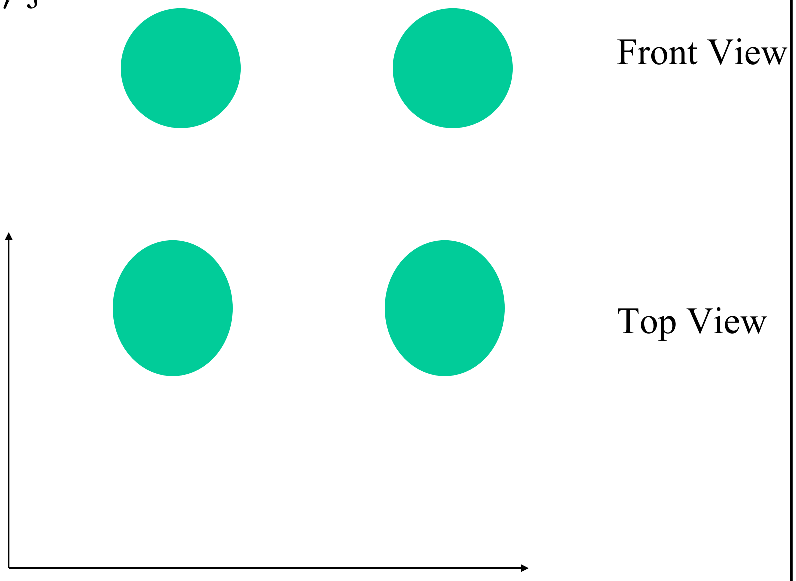
self-inverse

Logical Reversibility and Thermodynamics

- Landauer Principle: each erasure of a bit, or other logical 2:1 mapping of the state of a physical computer, increases the entropy of its environment by k log 2.

- Reversible computers, which by their hardware and programming avoid these logically irreversible operations, can in principle operate with arbitrarily little energy dissipation per step.

Landauer's Principle



Front View

Top View

Environ-mental degree of freedom

Information bearing degree of freedom

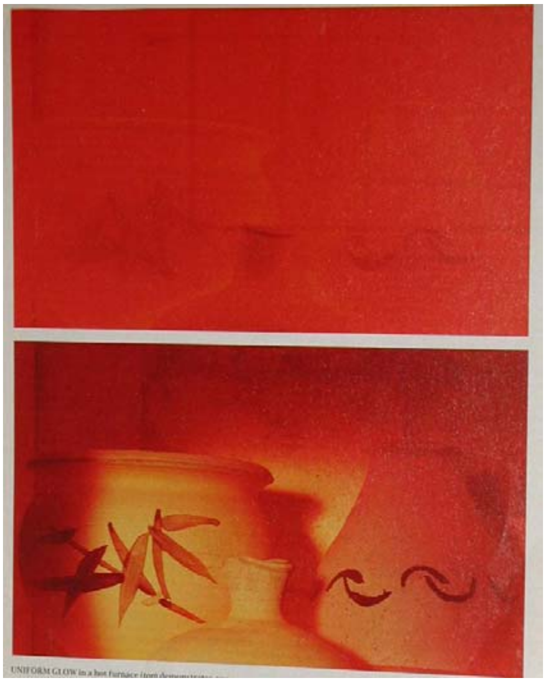
Second Law of Thermodynamics:

No physical process has as its sole result is the conversion of heat into work.

It is impossible to extract work from a gas at constant volume if all parts are initially at the same temperature and pressure.

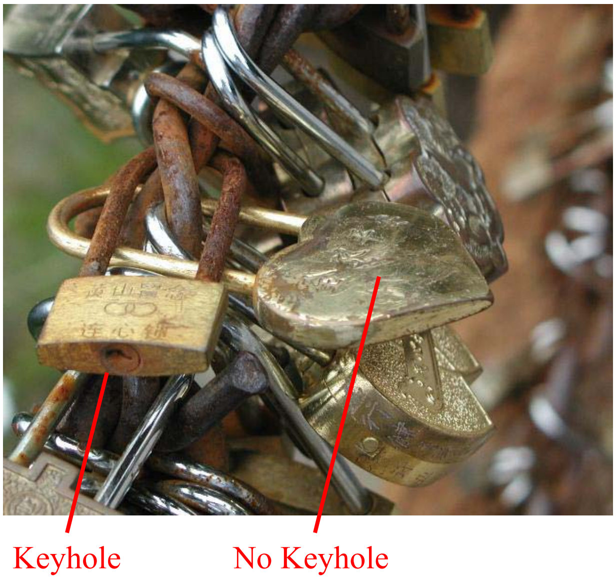
It is impossible to see anything inside a uniformly hot furnace by the light of its own glow.

No process has as its sole result the erasure of information.



UNIFORM GLOW in a hot furnace (top demonstrates

Irreversibility in affairs of the heart. The symbolic value of irreversibility is illustrated by the east Asian custom of lovers' locks.



Most lovers use ordinary padlocks, but then one must worry who has the key. A false lover could return at midnight and unlock it.

But one lock at Huangshan, China is of better design. It has no keyhole. Once locked, it can never be unlocked.

Good for lovers, bad for bicycles.

Ordinary irreversible computation can be viewed as an approximation or idealization, often quite justified, in which one considers only the evolution of the computational degrees of freedom and neglects the cost of exporting entropy to the environment.

We will return to this later.

A bigger change of mindset: Quantum Information

Information in microsopic bodies such as photons or nuclear spins obeys quantum laws. Such information

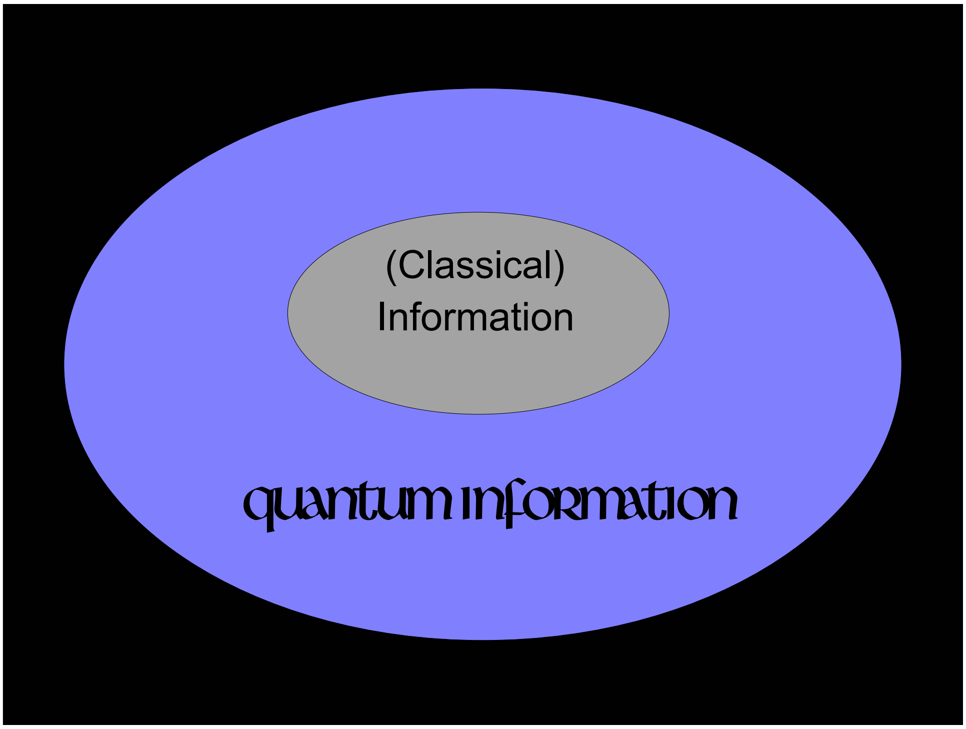
- cannot be read or copied without disturbance.

- can connect two spacelike separated observers by a correlation too strong to be explained by classical communication. However, this "entanglement" cannot be used to send a message faster than light or backward in time.

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



(Classical)
Information

quantum information

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.

1. A linear vector space with complex coefficients and inner product $< \phi | \psi > = \Sigma \, \phi_i^* \psi_i$

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

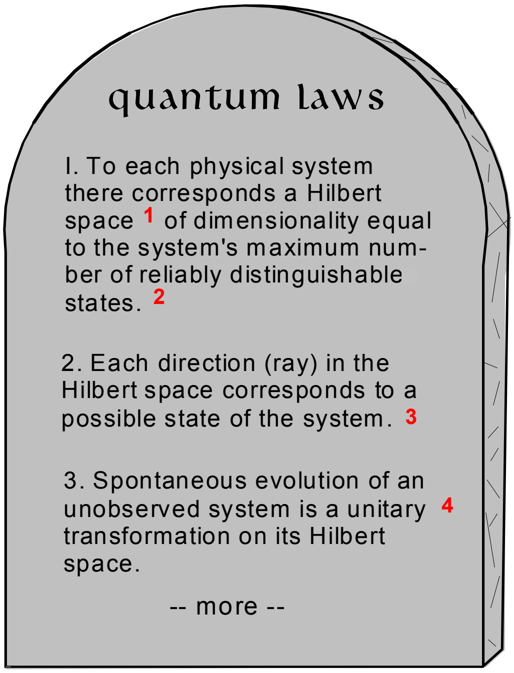
$\leftrightarrow = \begin{pmatrix}0\\1\end{pmatrix}$ $\updownarrow = \begin{pmatrix}1\\0\end{pmatrix}$

3. E.g. for photons, other polarizations

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

$\circlearrowright = \begin{pmatrix}i\\1\end{pmatrix}$ $\circlearrowleft = \begin{pmatrix}i\\-1\end{pmatrix}$

4. Unitary = Linear and inner-product preserving.



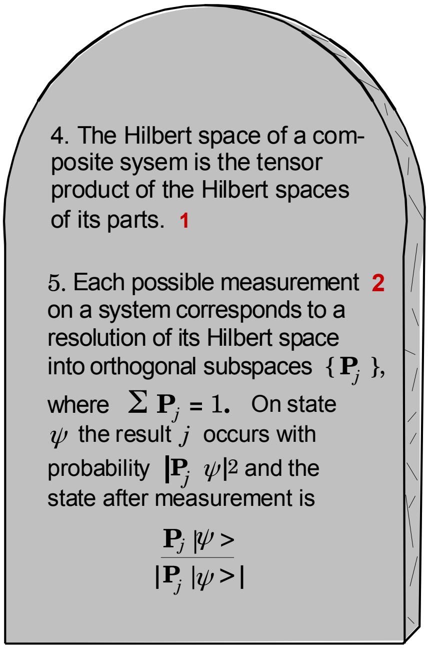
quantum laws

I. 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 sysem 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 $\{\mathbf{P}_j\}$, where $\Sigma\,\mathbf{P}_j = 1$. On state ψ the result j occurs with probability $|\mathbf{P}_j\ \psi|^2$ and the state after measurement is

$$\frac{\mathbf{P}_j\,|\psi>}{|\mathbf{P}_j\,|\psi>|}$$

1. Thus a two-photon system can exist in "product states" such as ↔ ↔ and ↔ ⤢ but also in "entangled" states such as

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

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 $\mathbf{P}_j$.

superposition principle

Between any two reliably distinguishable states of a quantum system

(for example vertically and horizontally polarized single photons)

there exists other states that are not reliably distinguishable from either original state

(for example diagonally polarized photons)

A historical question:

Why didn't the founders of information and computation theory (Turing, Shannon, von Neumann, et al) develop it on quantum principles from the beginning?

Maybe because they unconsciously thought of information and information processing devices as macroscopic. They did not have before them the powerful examples of the genetic code, the transistor, and the continuing miniaturization of electronics.

But even in the 19th Century, some people thought of information in microscopic terms
(Maxwell's Demon 1875)

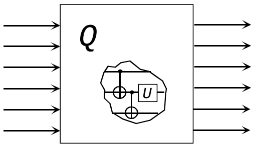
Perhaps more important (Nicolas Gisin)

Until recently, most people, under the influence of Bohr and Heisenberg, thought of quantum mechanics in terms of the uncertainty principle and unavoidable limitations on measurement. Schroedinger and Einstein understood early on the importance of entanglement, but most other people failed to notice, thinking of the EPR paradox as a question for philosophers.   Meanwhile engineers thought of quantum effects as a nuisance, causing tiny quantum devices to function unreliably. The appreciation of the positive application of quantum effects to information processing grew slowly.

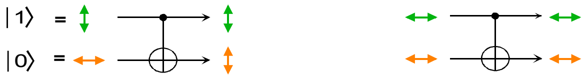
First: Quantum cryptography - use of uncertainty to prevent undetected eavesdropping

Now: Fast quantum computation, teleportation, quantum channel capacity, quantum distributed computation, quantum game theory, quantum learning theory, quantum economics, quantum voting…

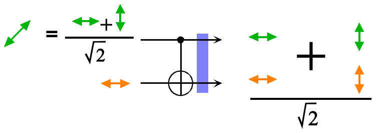
Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.



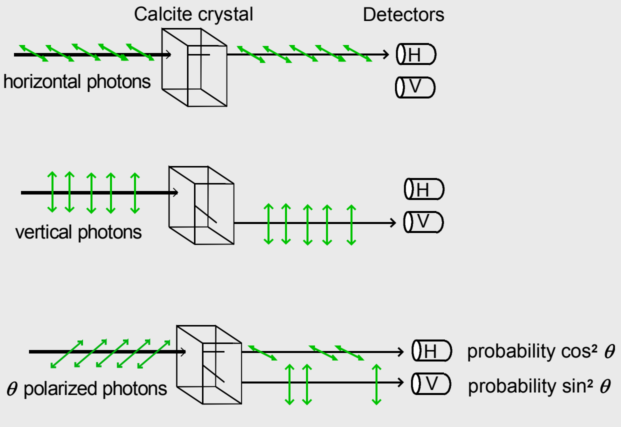
The 2-qubit XOR or "controlled-NOT" gate flips its 2nd input if its first input is 1, otherwise does nothing.



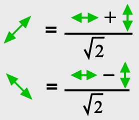
A superposition of inputs gives a superposition of outputs.



An entangled or EPR state

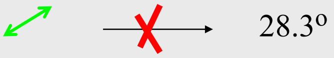


(Mathematically, a superposition is a weighted sum or difference, and can be pictured as an intermediate *direction* in space)

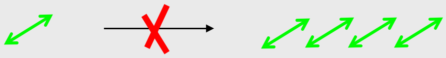


Non-orthogonal states like ↔ and ⤢ are in principle imperfectly distinguishable. ↔ always behaves somewhat like ⤢ and vice versa. This is the basis of quantum cryptography.

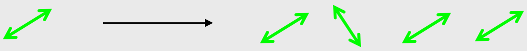
Measuring an unknown photon’s polarization exactly is impossible (no measurement can yield more than 1 bit about it).



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

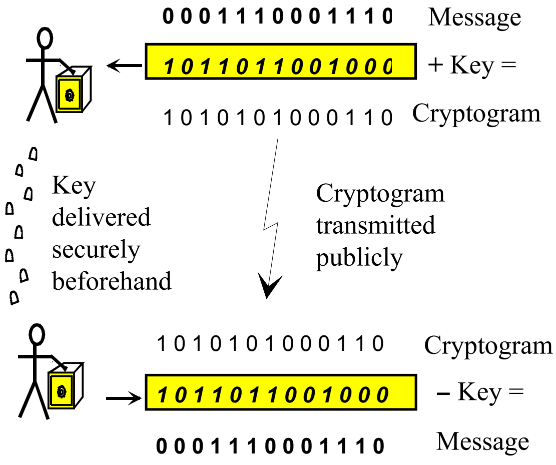


If you try to amplify an unknown photon by sending it into an ideal laser, the output will be polluted by just enough noise (due to spontaneous emission) to be no more useful than the input in figuring out what the original photon’s polarization was.



Cryptography:
the One Time Pad

allows messages to be transmitted in absolute privacy over public channels, but requires the sender and receiver to have shared secret random data (“key”) beforehand. One key digit is used up for each message digit sent. The key cannot be reused. If it, system becomes insecure.



0001110001110 Message

1011011001000 + Key =

1010101000110 Cryptogram

Key delivered securely beforehand

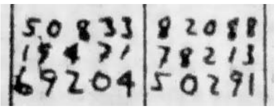
Cryptogram transmitted publicly

1010101000110 Cryptogram

1011011001000 – Key =

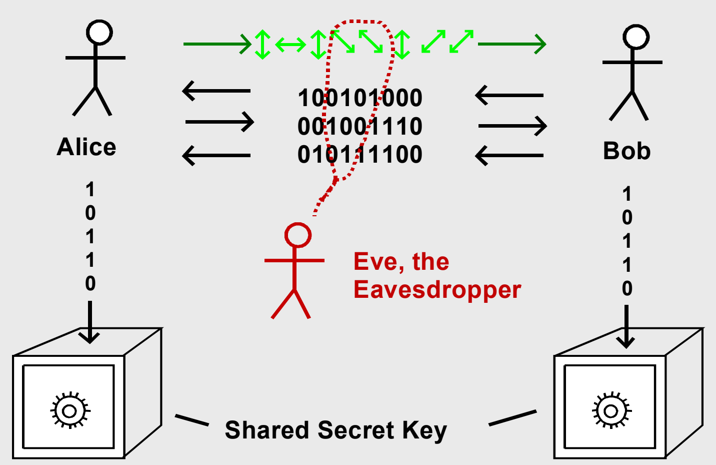
0001110001110 Message

One time pad worksheet used by Che Guevara



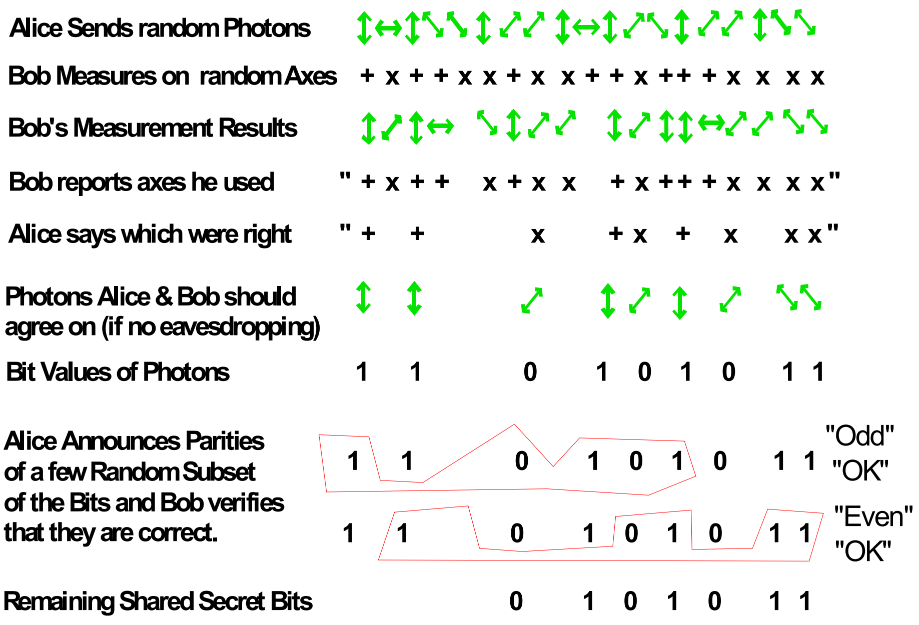
50833 82088 message
19471 78213 key
69204 50291 cryptogram

Quantum Cryptography avoids the need to hand-deliver the key.



In the end, Alice and Bob will either agree on a shared secret key, or else they will detect that there has been too much eavesdropping to do so safely. They will not, except with exponentially low probability, agree on a key that is not secret.

Quantum Cryptographic Key Distribution (BB84 Protocol)



Alice Sends random Photons ↕↔↕⤡⤡↕⤢⤢↕↔↕⤢⤡↕⤢⤢↕⤡⤡

Bob Measures on random Axes + x + + x x + x x + + x ++ + x x x x

Bob's Measurement Results ↕⤢↕↔ ⤡↕⤢⤢ ↕⤢↕↕↔⤢⤢⤡⤡

Bob reports axes he used " + x + + x + x x + x ++ + x x x x"

Alice says which were right " + + x + x + x x x"

Photons Alice & Bob should agree on (if no eavesdropping) ↕ ↕ ⤢ ↕ ⤢ ↕ ⤢ ⤡⤡

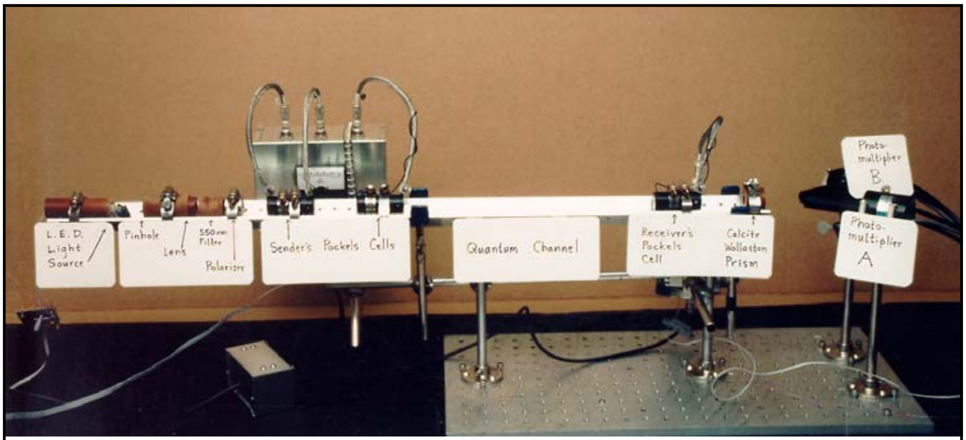
Bit Values of Photons 1 1 0 1 0 1 0 1 1

Alice Announces Parities of a few Random Subset of the Bits and Bob verifies that they are correct.

1 1 0 1 0 1 0 1 1 "Odd" "OK"

1 1 0 1 0 1 0 1 1 "Even" "OK"

Remaining Shared Secret Bits 0 1 0 1 0 1 1

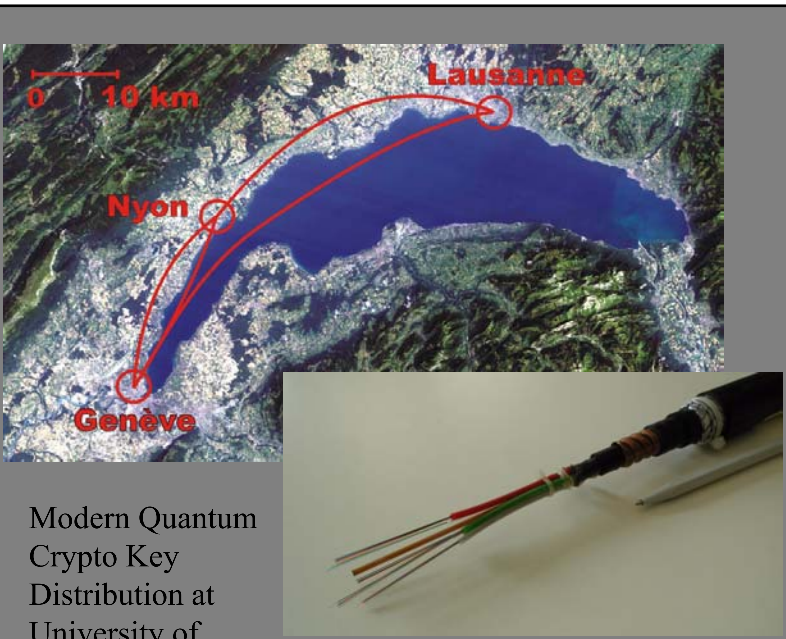


Original Quantum Cryptographic Apparatus built in 1989 transmitted information secretly over a distance of about 30 cm.

Sender's side produces very faint green light pulses of 4 different polarizations.

Quantum channel is an empty space about 30 cm long. There is no Eavesdropper, but if there were she would be detected.

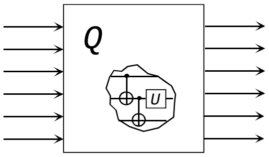
Calcite prism separates polarizations. Photomultiplier tubes detect single photons.



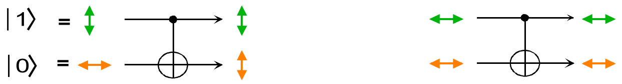
Modern Quantum Crypto Key Distribution at University of Geneva

Also experiments at several other labs, and two commercial systems.

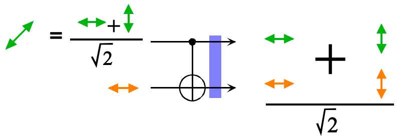
Any quantum data processing can be done by 1- and 2-qubit gates acting on qubits.



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



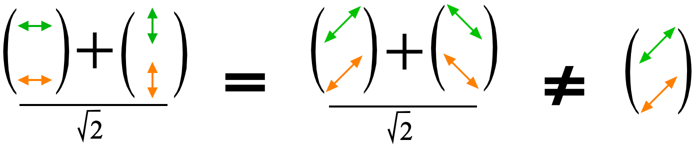
A superposition of inputs gives a superposition of outputs.



or EPR state

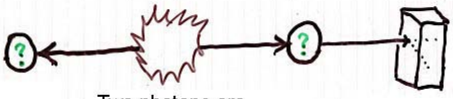
An entangled or EPR tate.

an entangled state is a state of a whole system that is not expressible in terms of states of its parts.



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.

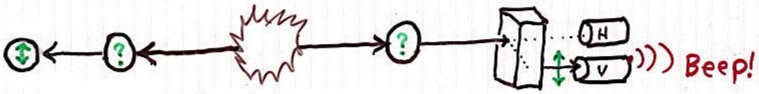
Einstein Podolsky Rosen Effect



Two photons are
created in an
"entangled" state.

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

Einstein Podolsky Rosen Effect

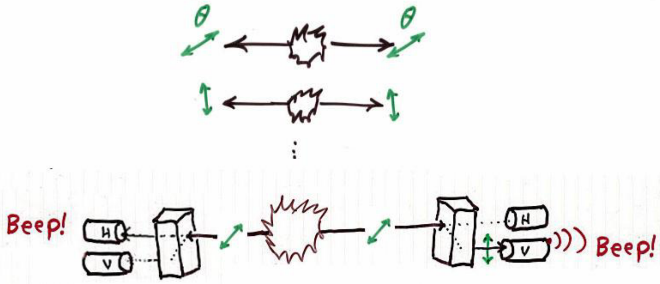


Two photons are
created in an
"entangled" state.

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

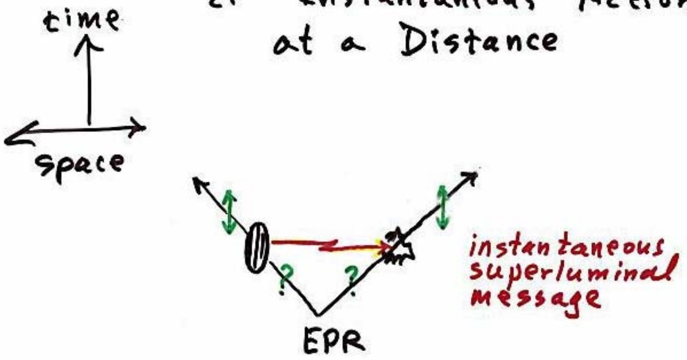
And simultanteously causes
the other photon to acquire
the same polarization.

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 digonal photons, and if these were both measured on the V/H axis, sometimes one would behave V and the other H. In fact, they always behave the same, both V or both H.

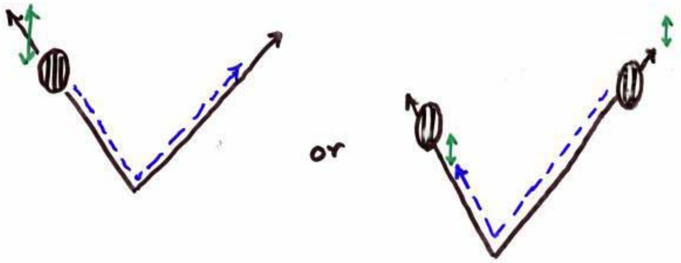
2. Instantaneous Action at a Distance



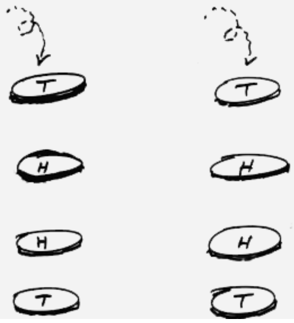
No. Violates special relativity and besides, how does the first particle know where to send the message to?

3. Quantum Mechanics - the right answer

4. Random Uncontrollable Message
Backward in time

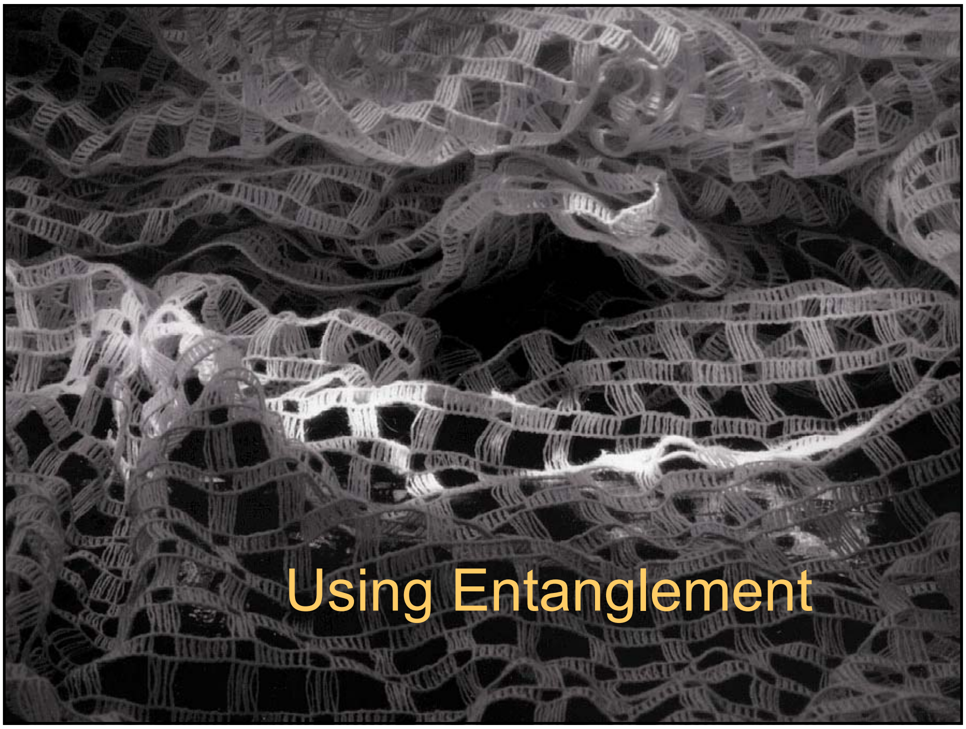


A Pair of Magic Coins



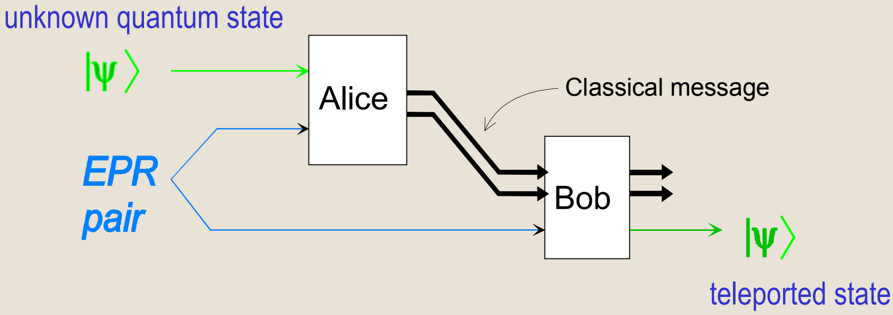
A “message” backward in time is safe from paradox under two conditions, either of which frustrates your ability to advise your broker what stocks to buy or sell yesterday:

1. Sender can’t control message (EPR effect) OR
2. Receiver disregards message (Cassandra myth).



Using Entanglement

Entanglement is useful for Quantum Teleportation,
a way to transmit quantum information when no quantum channel is available.



unknown quantum state

$|\psi\rangle$

Alice

Classical message

EPR pair

Bob

$|\psi\rangle$

teleported state

Prior sharing of an EPR pair allows Alice to disembody an unknown qubit into a 2-bit classical message and preexisting entanglement. When Bob receives the classical message, he can reconstruct the unknown state exactly, but cannot copy it. The EPR link from Alice to Bob goes backward in time, but cannot by itself carry any meaningful message.

Alice's and Bob's roles in teleportation

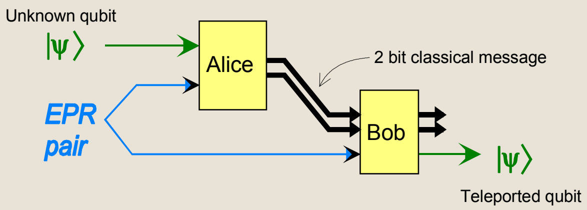
Alice performs a joint measurement of the unknown input qubit ψ and her half of the shared EPR pair in the so-called Bell basis

According to Alice's result, Bob performs one of four unitary transformations, the so-called Pauli operators I, X, Y, and Z, on his half of the EPR pair.

|00> +|11>	I (do nothing)	$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$
|00> -|11>	Z phase shift	$\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$
|01> +|10>	X bit flip	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$
|01> -|10>	Y flip & shift	$\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}$

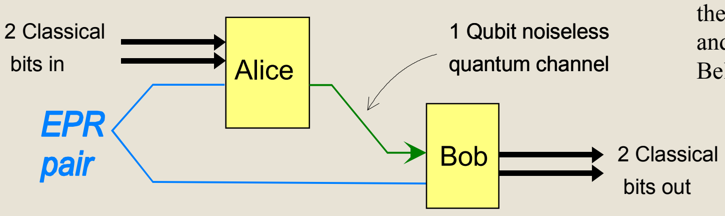
Result: Bob's qubit is left in the same state as Alice's was in before teleportation. If Alice's qubit was itself entangled with some other system, then Bob's will be when the teleportation is finished.

Quantum Teleportation



A dual process to teleportation

Quantum Superdense Coding

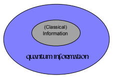


Here Alice does the Pauli rotation and Bob does the Bell measurement.

doubles the classical capacity of any noiseless quantum channel

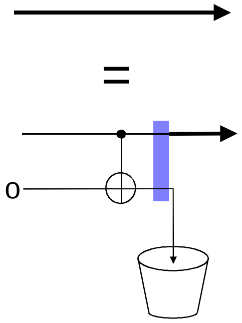
Expressing classical data processing in quantum terms.

A classical bit is just 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 occurs because the data passing through the wire interacts with its environment, causing the environment to learn the value of the data, if it was **0** or **1**, and otherwise become entangled with it.)



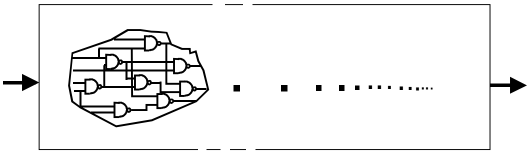
A classical channel is a quantum channel with an eavesdropper.

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

Classical Computation Theory shows how to reduce all computations to a sequence of NANDs and Fanouts. 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…

RSA 129

1143816257578888676
6923577997614661201
0218296721242362562
5618429357069352457
3389783059712356395
8705058989075147599
290026879543541



Factors

3490529510847650949
1478496199038981334
1776463849338784399
0820577

x

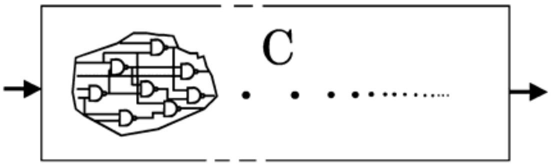
3276913299326670954
9961988190834461413
1776429679929425397
98288533

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.)

RSA 129

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541



Factors

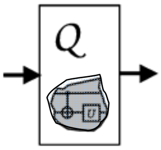
3490529510847650949147849619903898133417764638493387843990820577

x

32769132993266709549961988190834461413177642967992942539798288533

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

114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541



3490529510847650949147849619903898133417764638493387843990820577

x

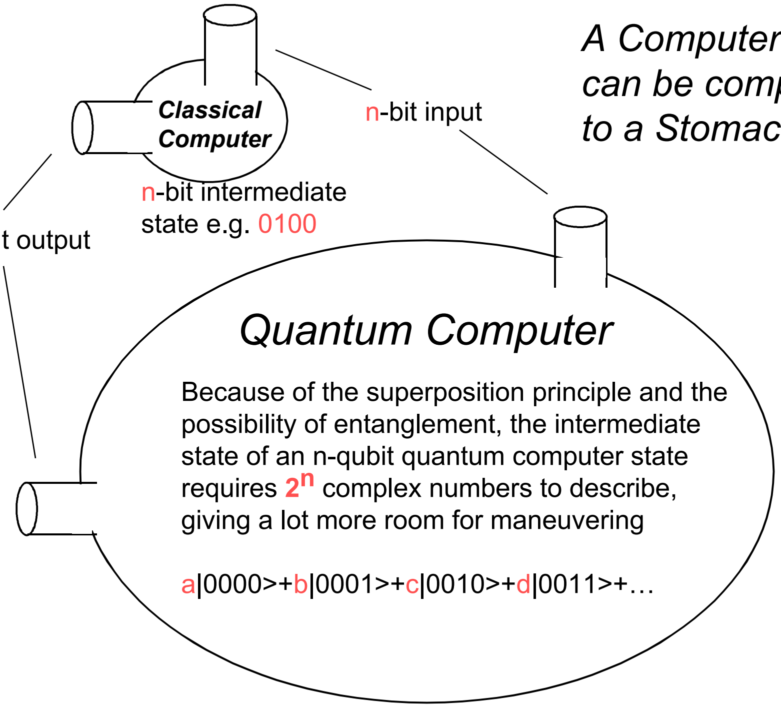
32769132993266709549961988190834461413177642967992942539798288533

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.)

A Computer can be compared to a Stomach



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

a|0000>+b|0001>+c|0010>+d|0011>+…

How Much Information is "contained in" n qubits, compared to n classical bits, or n analog variables?

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

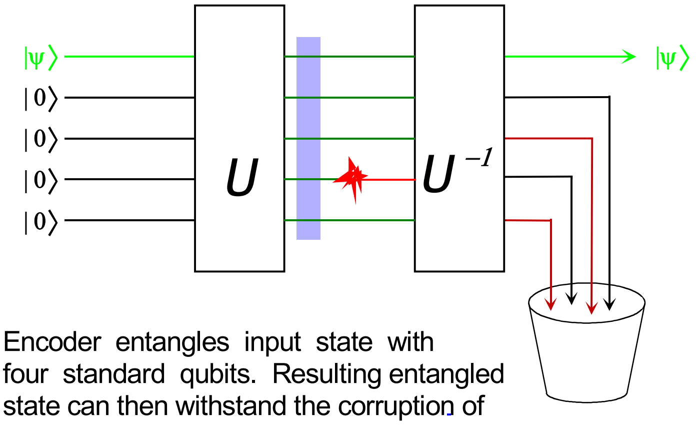
Quantum Error Correcting Codes

Entanglement Distillation

Quantum Fault-Tolerant Circuits

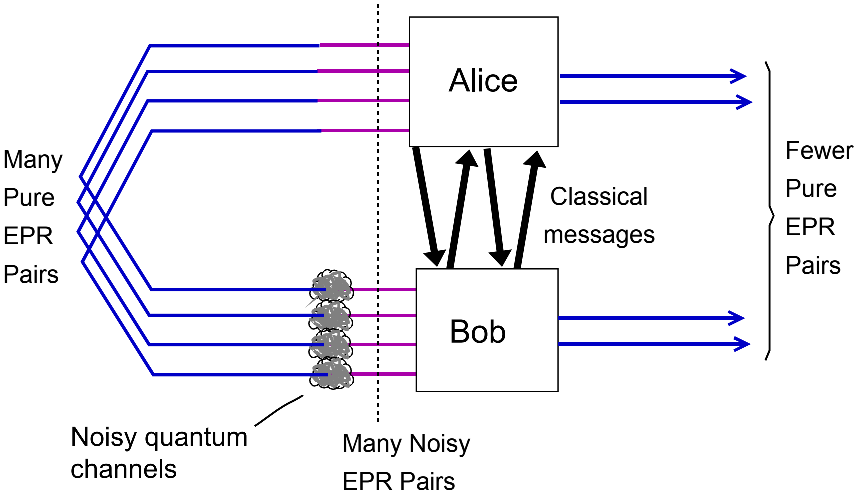
These techniques, combined with hardware improvements, will probably allow practical quantum computers to be built, but not any time soon.

The Simplest Quantum Error-Correcting Code

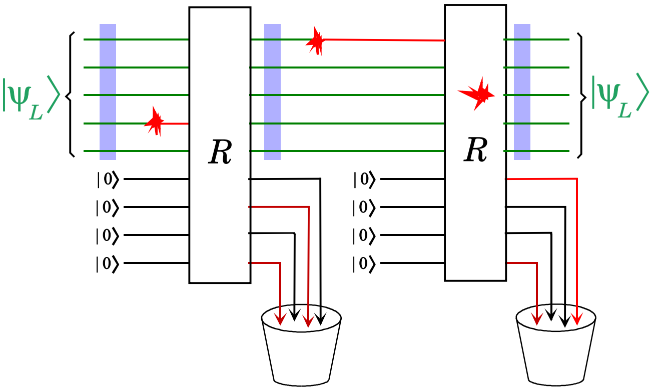


Encoder entangles input state with four standard qubits. Resulting entangled state can then withstand the corruption of any one of its qubits, and still allow recovery of the exact initial state by a decoder at the receiving end of the channel

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.

How do Quantum Speedups Work?

Shor’s algorithm – exponential speedup of factoring – Depends on fast quantum technique for finding the period of a periodic function

Grover’s algorithm – quadratic speedup of search – works by gradually focusing an initially uniform superposition over all candidates into one concentrated on the designated element. Speedup arises from the fact that a linear growth of the amplitude of the desired element in the superposition causes a quadratic growth in the element’s probability.

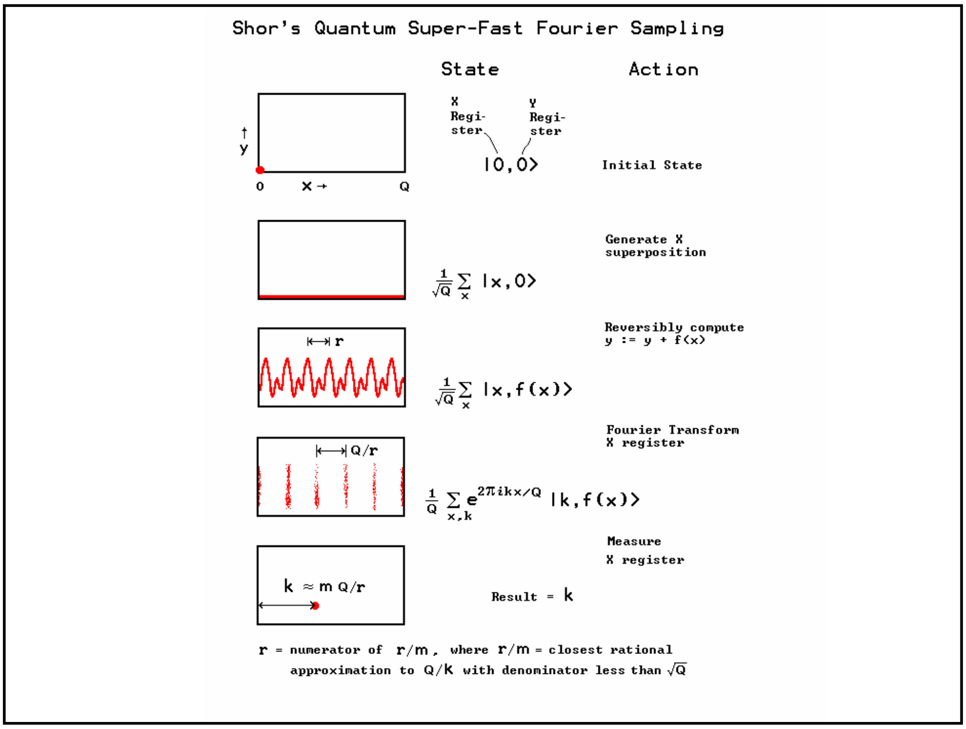
Well-known facts from number theory.

Let N be a number we are trying to factor.

For each $a<N,$ the function $f_a(x) = a^x \bmod N$ is periodic with period at most N. Moreover it is easy to calculate. Let its period be r_a. All known classical ways of finding r_a from a are hard.

Any algorithm for calculating r_a from a can be converted to an algorithm for factoring N.

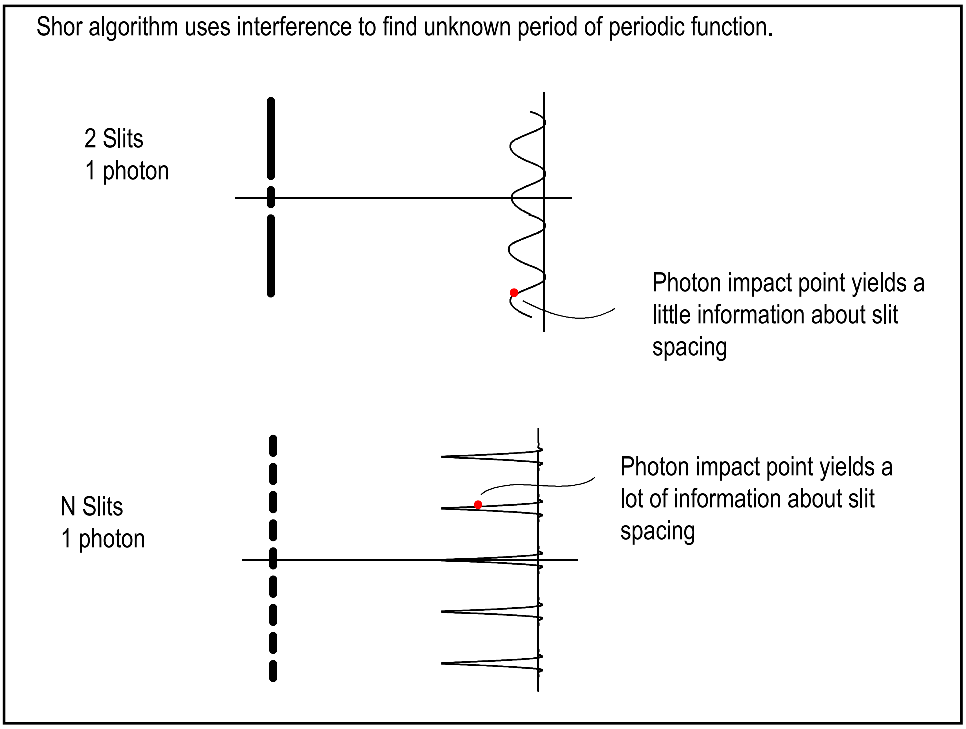
Quantum mechanics makes this calculation easy.



Shor's Quantum Super-Fast Fourier Sampling

State	Action
$|0,0\rangle$	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 $y := y + f(x)$
$\frac{1}{Q}\sum_{x,k} e^{2\pi ikx/Q}|k,f(x)\rangle$	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.

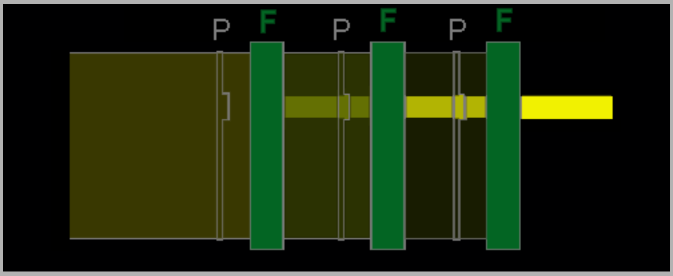
2 Slits
1 photon

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.

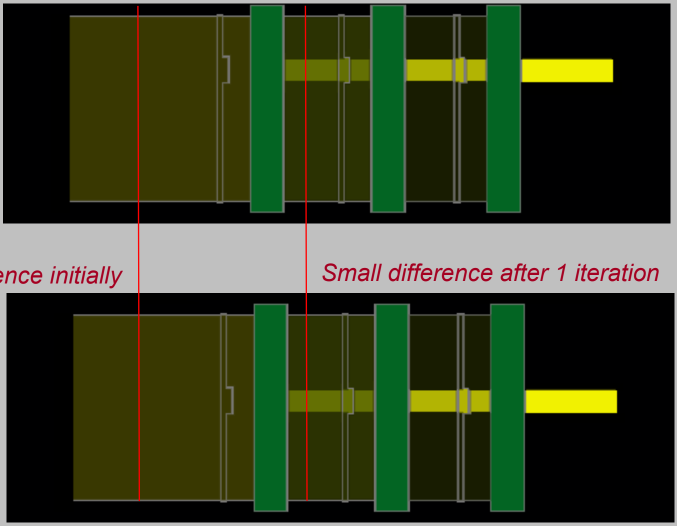


P = phase plate
F = fixed optics

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?

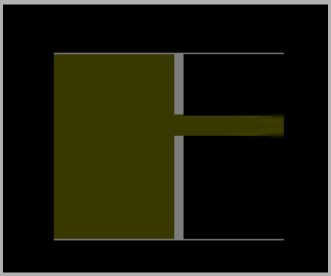
Original optical Grover experiment.

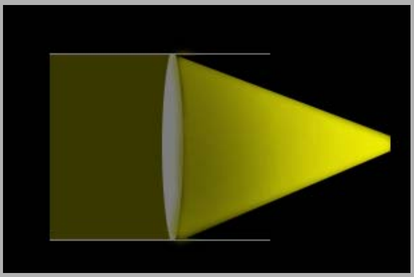


Repeat the experiment with the phase bump in a different location.

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.





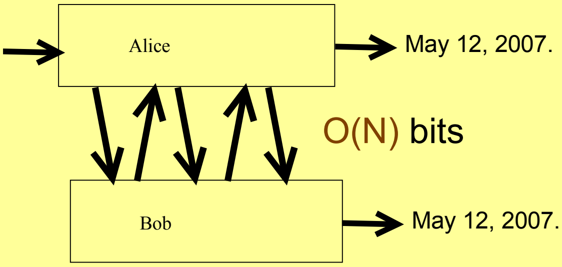
Mask out all but desired area. Has disadvantage that most of the light is wasted. Like classical trial and error. If only 1 photon used each time, N tries would be needed.

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.

What else is quantum information good for?

1. Quantum Savings in *Communication Complexity*

When can we meet for lunch?



Alice

May 12, 2007.

O(N) bits

Bob

May 12, 2007.

Quantum communication cost is only **O(sqrt(N) log N)** bits.

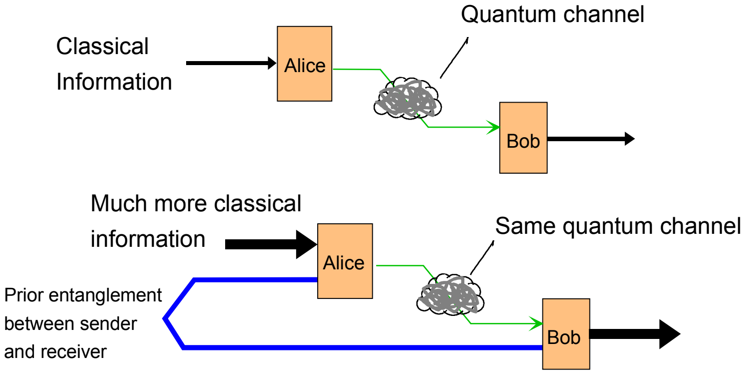
(Buhrman, Cleve and Wigderson)

Fast quantum protocol for the lunch scheduling problem is a distributed form of Grover’s algorithm.

A register of log *N* qubits, initially containing a uniform superposition of all dates, is passed back and forth between the two parties about √*N* times, gradually building up amplitude on a conflict-free date.

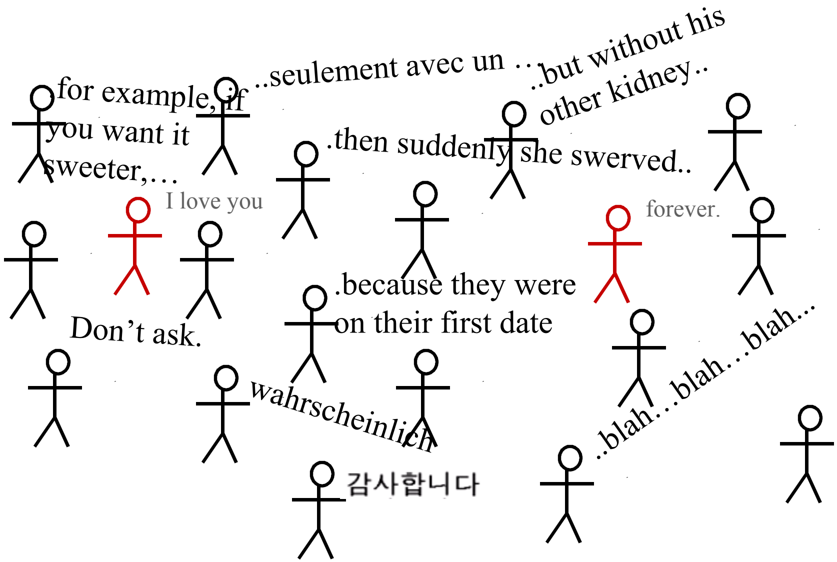
2. Entanglement Enhanced Classical Capacity:

By itself, entanglement itself cannot be used for classical communication (otherwise we would have faster-than-light communication) but it can increase the classical capacity of an existing quantum channel, in some cases by a large factor.


Classical Information
Alice
Quantum channel
Bob
Much more classical information
Alice
Same quantum channel
Prior entanglement between sender and receiver
Bob

Enhancement factor = 2 for noiseless channels, can be arbitrarily large for noisy channels

Prior shared entanglement helps a good deal if Alice and Bob are trying to hold a quiet conversation in a room full of noisy strangers (Gaussian channel in low signal, high noise, low-attenuation limit)


for example, if you want it sweeter,…
..seulement avec un …
..but without his other kidney..
.then suddenly she swerved..
I love you
forever.
Don't ask.
.because they were on their first date
wahrscheinlich
..blah…blah…blah…
감사합니다

But it doesn’t help much if they are far apart in an empty room (high attenuation)

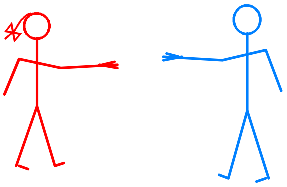
Quantum Laws & the Universality of Interaction

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.

A quantum love story, based on the classic tale of Pyramus and Thisbe.



Alice and Bob are young and in love.

Unfortunately, their parents oppose their relationship, and have forbidden them to visit, or talk, or exchange email.

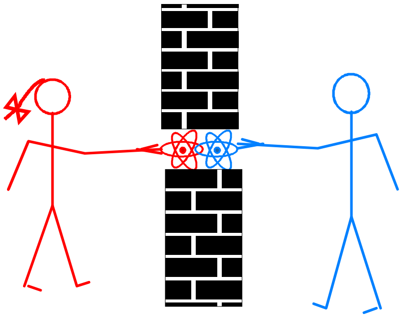
Fortunately, they live next door to one another.

Unfortunately, there's a wall between their two houses.

Fortunately, there's a hole in the wall.

-- more --

Unfortunately, the hole is only big enough for one atom of Alice to interact with one atom of Bob, via an interaction ***H'*** **.**

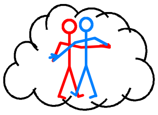


Fortunately, Alice and Bob know quantum mechanics. They know that any interaction can be used to create entanglement, and that interactions are intrinsically bidirectional and private: A cannot affect B without B affecting A. If C interferes or eavesdrops, the joint state of A and B will be degraded and randomized.

-- more --

The young lovers wish to experience the life they would have had if they had been allowed to interact not by the one-atom interaction **H'** but by the many-atom interaction **H**, which is a physicist's way of saying always being in each other's arms.

How can they use the available **H'** to simulate the desired **H** ?



They can of course separately prepare their respective interacting atoms in any initial states, and thereafter alternate through-the-wall interactions under H' with local operations among their own atoms, each on his/her own side of the wall.

Using the hole in the wall, they can prepare entangled states. We assume each has a quantum computer in which to store and process this entanglement. Whenever they need to communicate classically, to coordinate their operations, they can use the interaction **H'** to do that too. Thus the joint states they can experience are all those that can be achieved by shared entanglement and classical communication. Of course it will take a lot of time and effort.

-- more --

The joint states they can experience are all those that can be achieved by shared entanglement and classical communication.

But this is *all* quantum states of A and B!

If their parents had only plugged the hole in the wall and allowed them unlimited email, their future would have been much bleaker.

They could never have become entangled, and their relationship would have remained Platonic and classical. In particular, it would have had to develop with the circumspection of knowing that everything they said might be overheard by a third party.

As it is, with the hole remaining open, by the time they get to be old lovers, they can experience exactly what it would have been like to be young lovers (if they are still foolish enough to want that).

-- The End --

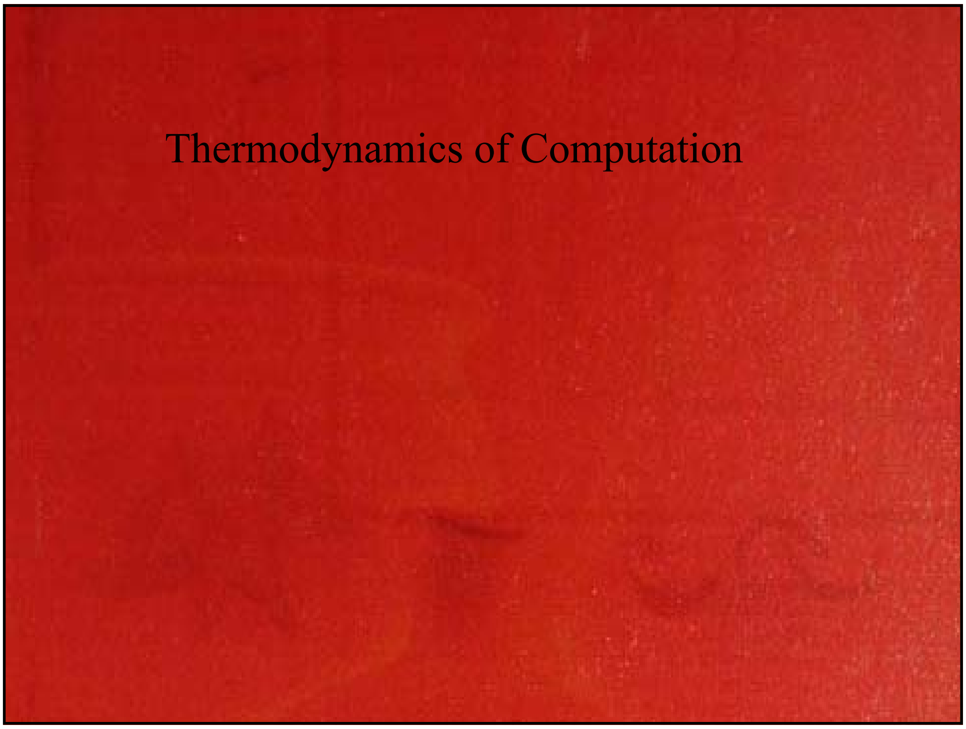
Summary

Quantum Information obeys laws that subtly extend those governing classical information, making possible novel effects such as quantum cryptography, fast quantum algorithms for factoring and search, quantum improvements in communication complexity, as well as teleportation and other kinds of etanglement-assisted communication.

Classical information and computation theory is best thought of as a subset of quantum information/computation. A classical bit is a qubit with the value 0 or 1. A classical wire is a wire with an eavesdropper.

Strange phenomena involving quantum information are still being discovered.

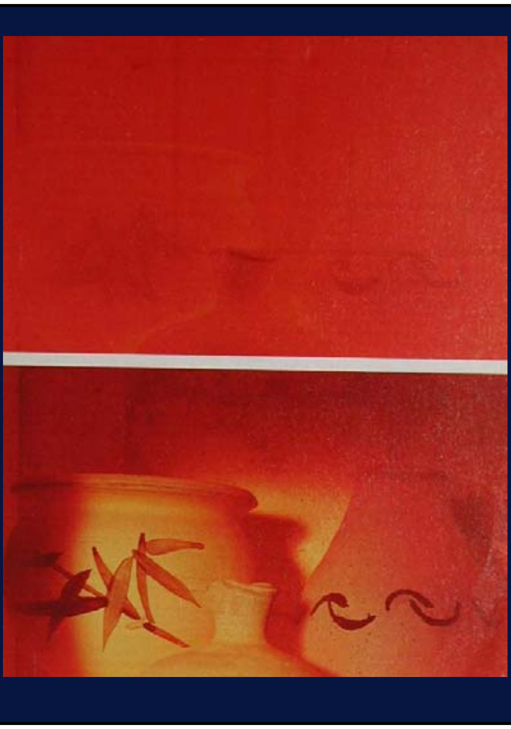
Thermodynamics of Computation



Looking inside a pottery kiln

by its own glow

by external light



Why study the thermodynamics of computing and the theory of reversible computing?

- Practice for quantum computing

- Improving the thermodynamic efficiency of today's computers, where heat dissipation is a serious problem.

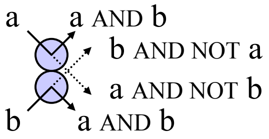
- Understanding ultimate limits and scaling of computation and, by extension, self-organization

I. Classification of Computers from thermodynamic viewpoint

A. Irreversible

B. Reversible

1.Ballistic (e.g. Billiard ball model)



2. Brownian (e.g. RNA polymerase)

3. Intermediate (like walk on a 1d lattice with mean free path >1)

II. Errors and the thermodynamics of error correction in Brownian computers

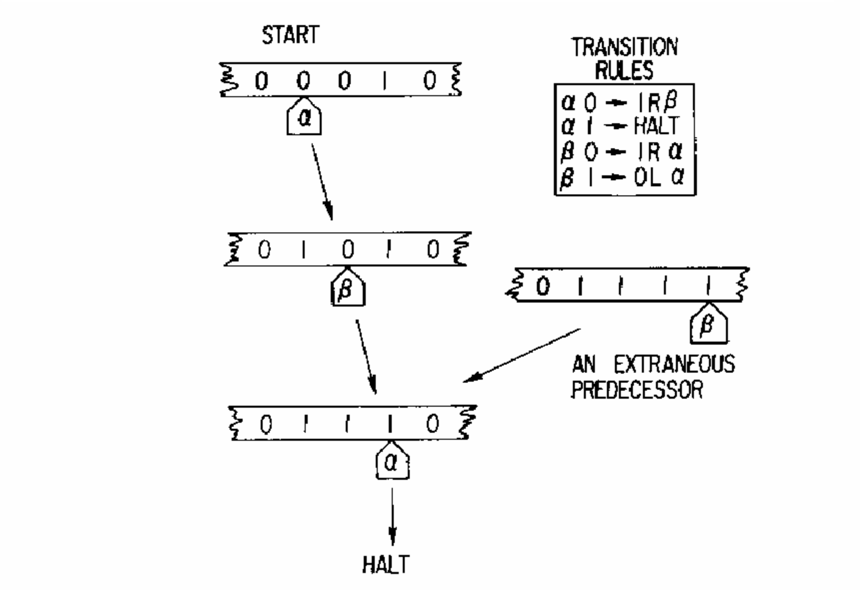
- How can an arbitrary computation be performed reversibly, and how much overhead (extra time and/or space) is required to do so?

- RNA polymerase, a natural reversible computer.*

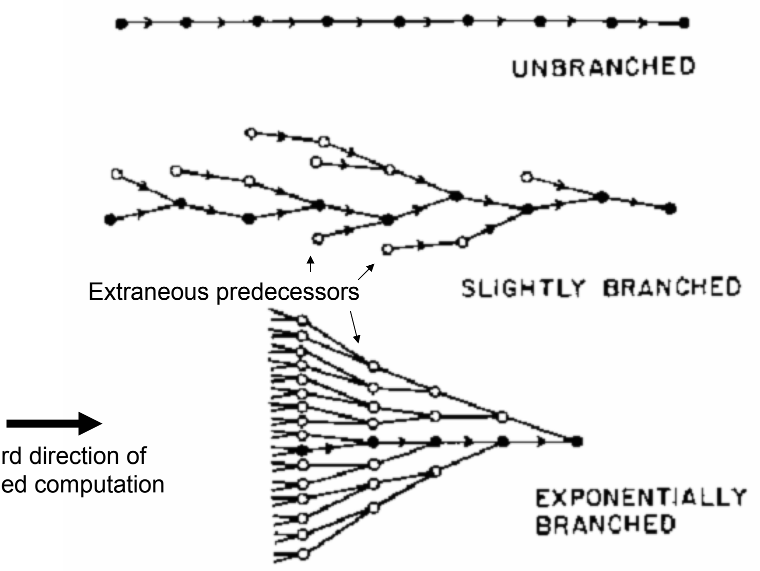
- Thermodynamic cost of error correction. Proofreading in DNA polymerase, and dissipation error tradeoff in a simplified model thereof.

- Ultimate scalability of computing with regard to heat removal and error correction.

Turing machine, illustrating logical irreversibility



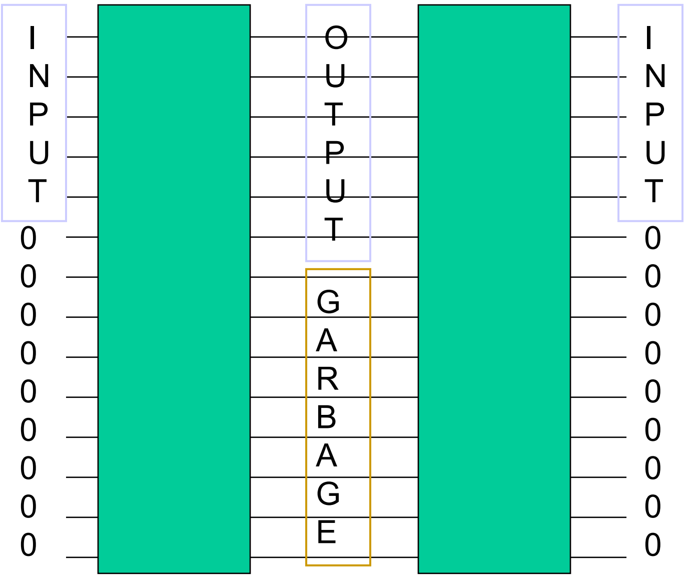
Kinds of computation graph



Extraneous predecessors

Forward direction of
Intended computation

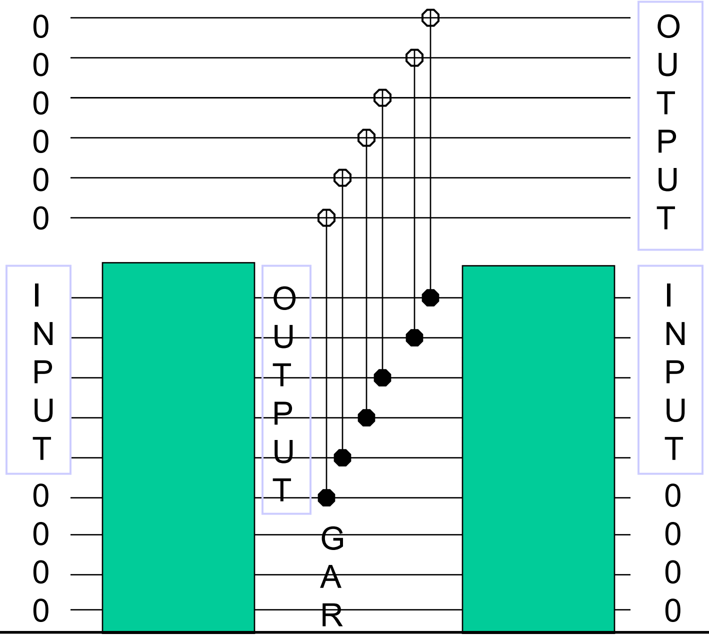
Time-Efficient Space-Inefficient reversible simulation of an irreversible computation


INPUT
0 0 0 0 0 0 0 0 0

OUTPUT
GARBAGE

INPUT
0 0 0 0 0 0 0 0 0

Using CNOTs to copy output before undoing computation

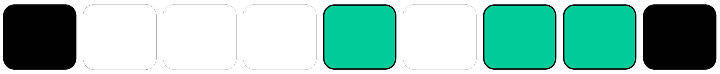


Another view of the Time-efficient, space-inefficient simulation

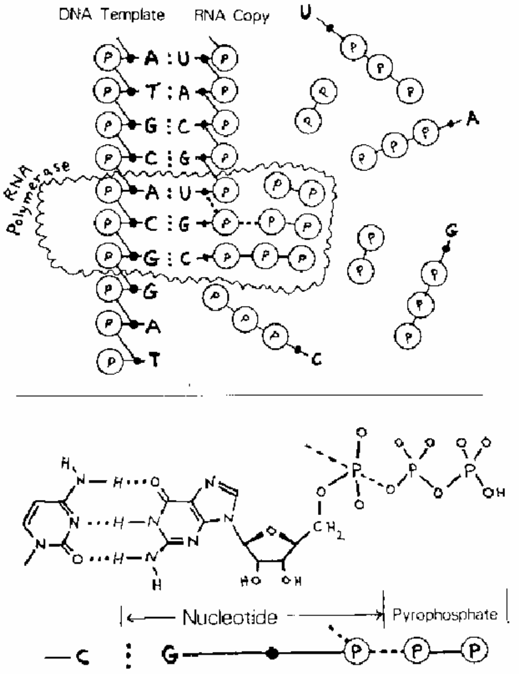
T steps of irreversible computation are simulated in 2T steps of reversible computation, using O(T) extra memory for temporary storage of intermediate results.

Like laying down a row of stepping stones to cross a river, then removing them. A stepping stone may be placed or removed only when its predecessor is present.

Trading time for space: By doing and undoing steps in a hierarchical manner, $T=2^m$ steps of irreversible computation can be simulated in 3^m reversible steps using O(m) temporary intermediate storage.

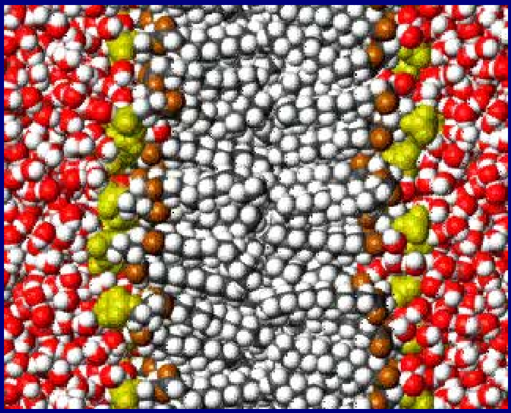


More generally, this type of argument shows that for all $\varepsilon > 0$, an irreversible computation using time T and space S can be reversibly simulated in time $\propto T^{1+\varepsilon}$ and space $\propto S \log T$. A still more space-efficient simulation runs in exponential time and linear space.



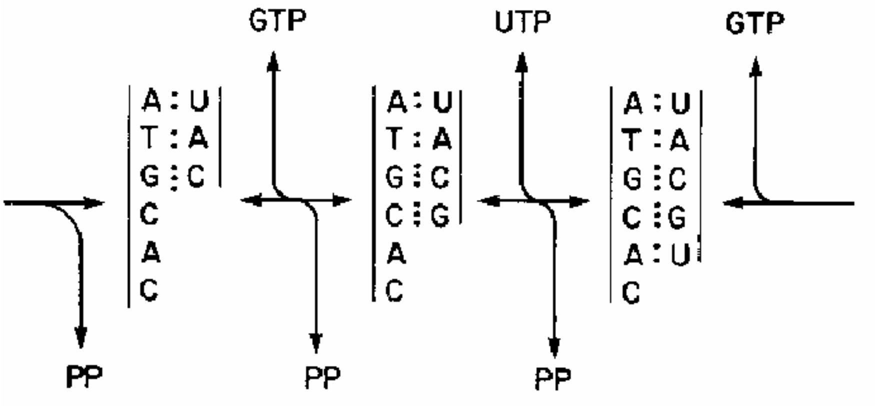
RNA Polymerase may be viewed as a reversible tape-copying Turing machine. The chemical reaction is reversible, but in vivo it is driven forward by removal of PP.

The chaotic world of Brownian motion, illustrated by a molecular dynamics movie of a synthetic lipid bilayer (middle) in water (left and right)



dilauryl phosphatidyl ethanolamine in water

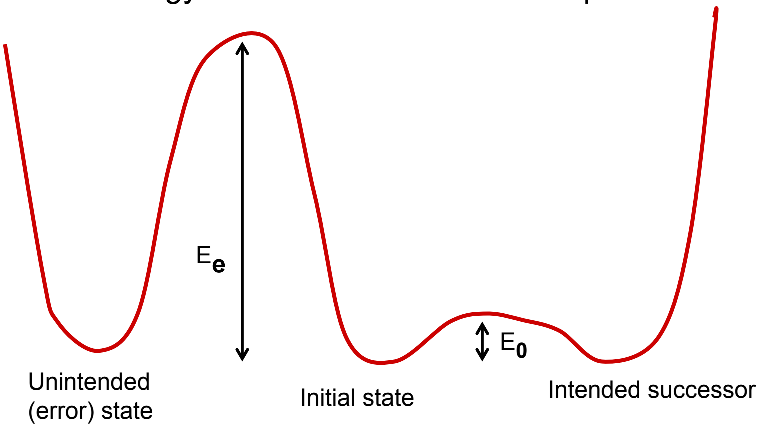
http://www.pc.chemie.tu-darmstadt.de/research/molcad/movie.shtml



. RNA polymerase reaction viewed as a one-dimensional random walk.

In vitro, by adjusting PP vs XTP concentrations, the copying can be made to drift forward or backward while dissipating < kT dissipation per step.

Potential Energy Surface for Brownian Computer

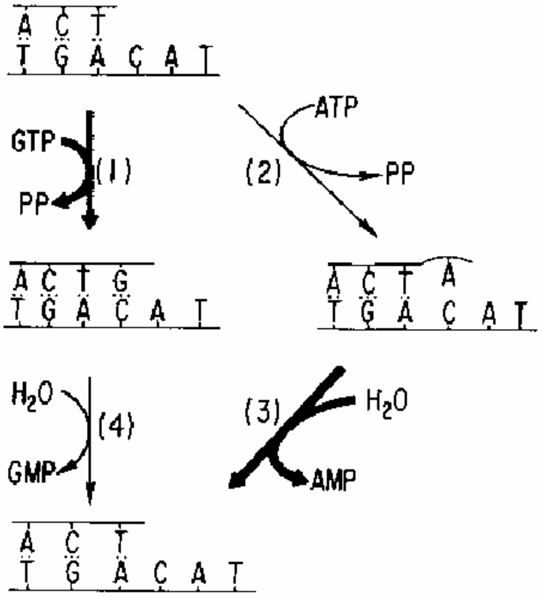


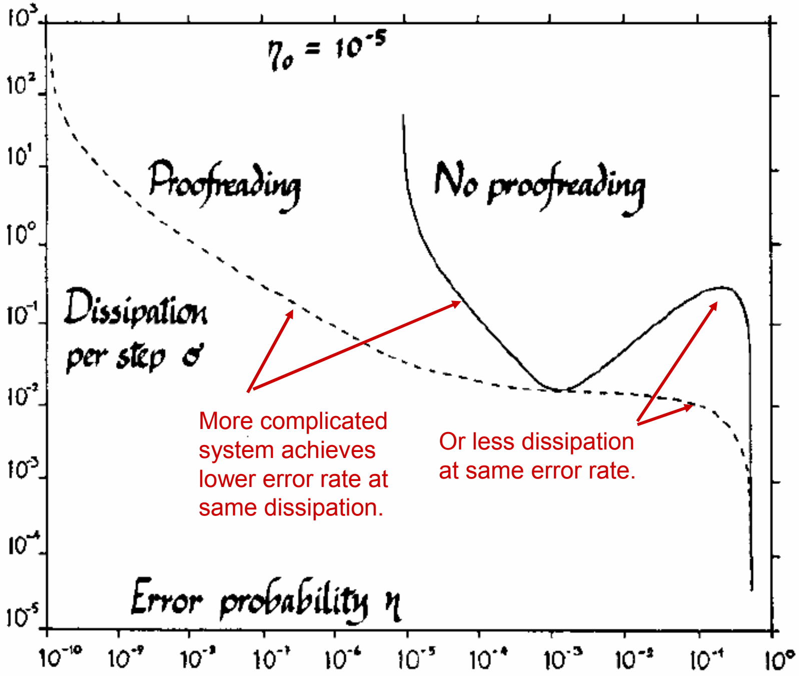
Error probability per step approx. exp [(E_0 -E_e) / kT]

Even when a computation is programmed reversibly, errors will occur, and by Landauer's principle energy must be dissipated to correct them.

Proofreading in DNA Replication for higher accuracy

Polymerase (1) tries to insert correct base, but occasionally (2) makes an error. Exonuclease (3) tries to remove errors, but occasionally (4) removes correct bases. When both reactions are driven hard forward the error rate is the product of their individual error rates.

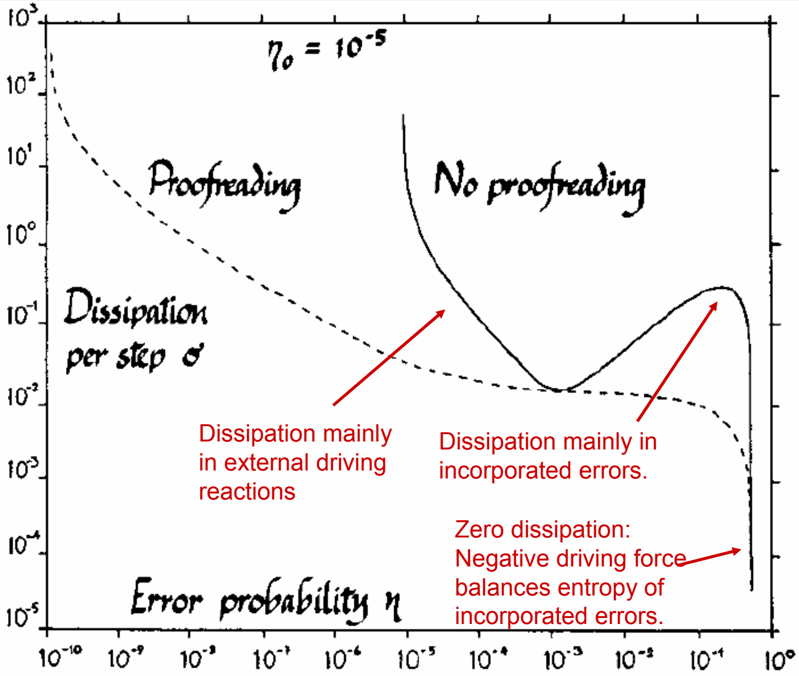




More complicated system achieves lower error rate at same dissipation.

Or less dissipation at same error rate.

Fig. 3. Dissipation per digit copied, with and without proofreading.



Dissipation mainly in external driving reactions

Dissipation mainly in incorporated errors.

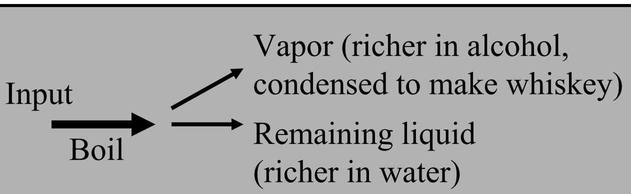
Zero dissipation: Negative driving force balances entropy of incorporated errors.

Fig. 3. Dissipation per digit copied, with and without proofreading.

For any given hardware environment, e.g. CMOS, DNA polymerase, there will be some tradeoff among dissipation, error, and computation rate. More complicated hardware might reduce the error, and/or increase the amount of computation done per unit energy dissipated.

This tradeoff is largely unexplored, except by engineers.

Simple Distillation

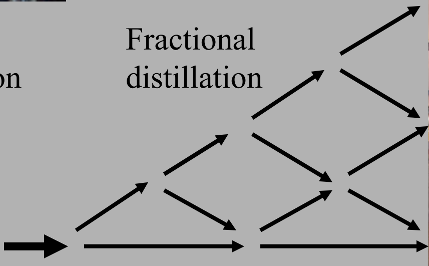


Input

Boil

Vapor (richer in alcohol, condensed to make whiskey)

Remaining liquid (richer in water)

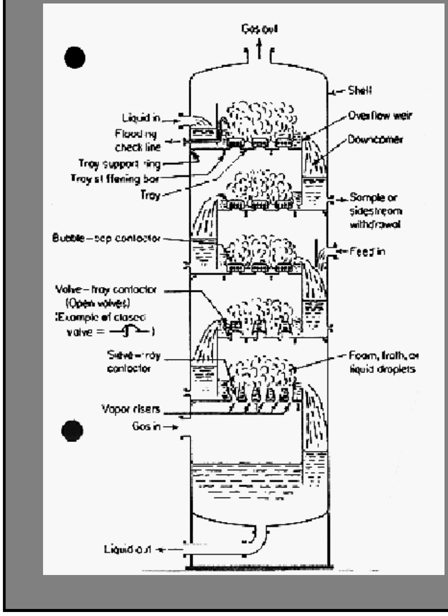


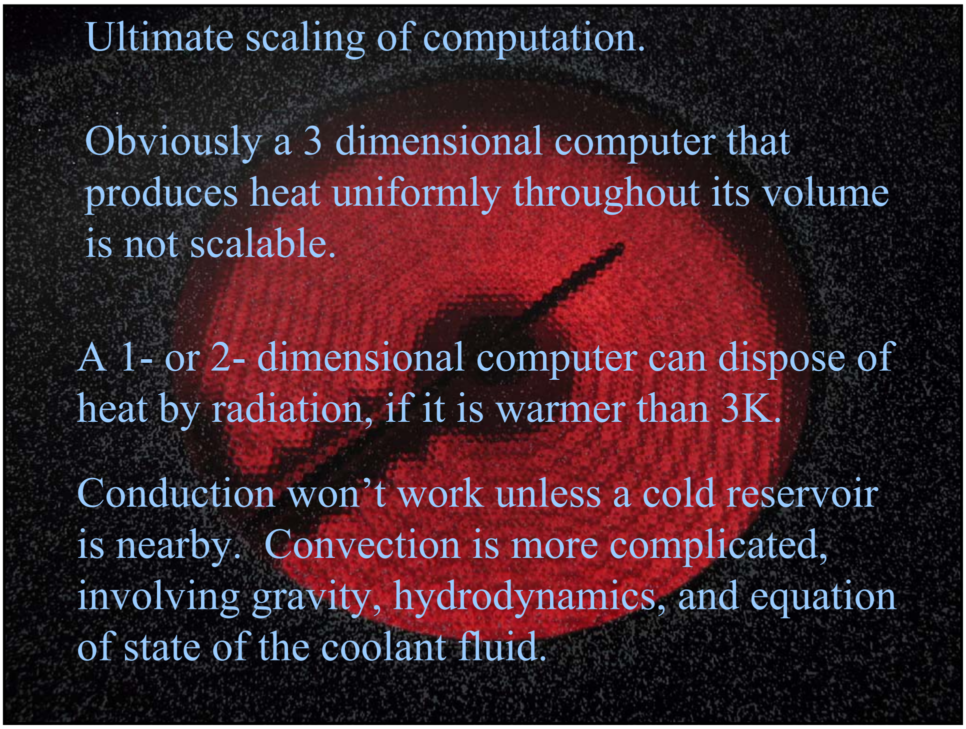
Fractional distillation

Input

Can approach ideal efficiency in the limit of zero speed:
Reversible: mixture separation cost = −free energy of mixing.
Real stills operate less efficiency but at finite speed.

Practical Fractional Stills



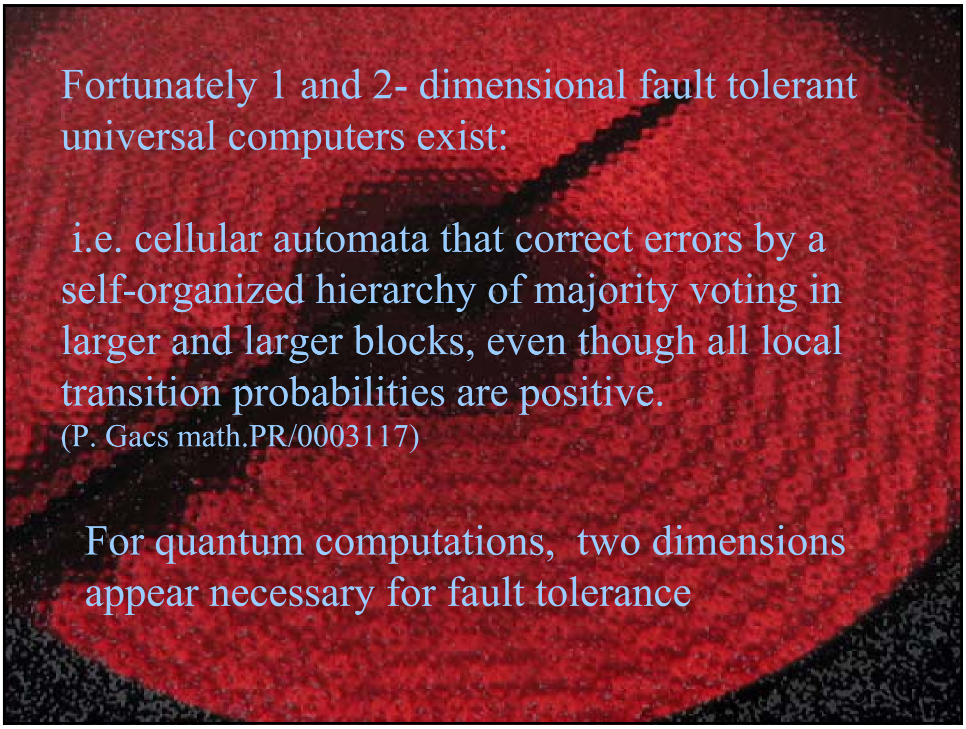


Ultimate scaling of computation.

Obviously a 3 dimensional computer that produces heat uniformly throughout its volume is not scalable.

A 1- or 2- dimensional computer can dispose of heat by radiation, if it is warmer than 3K.

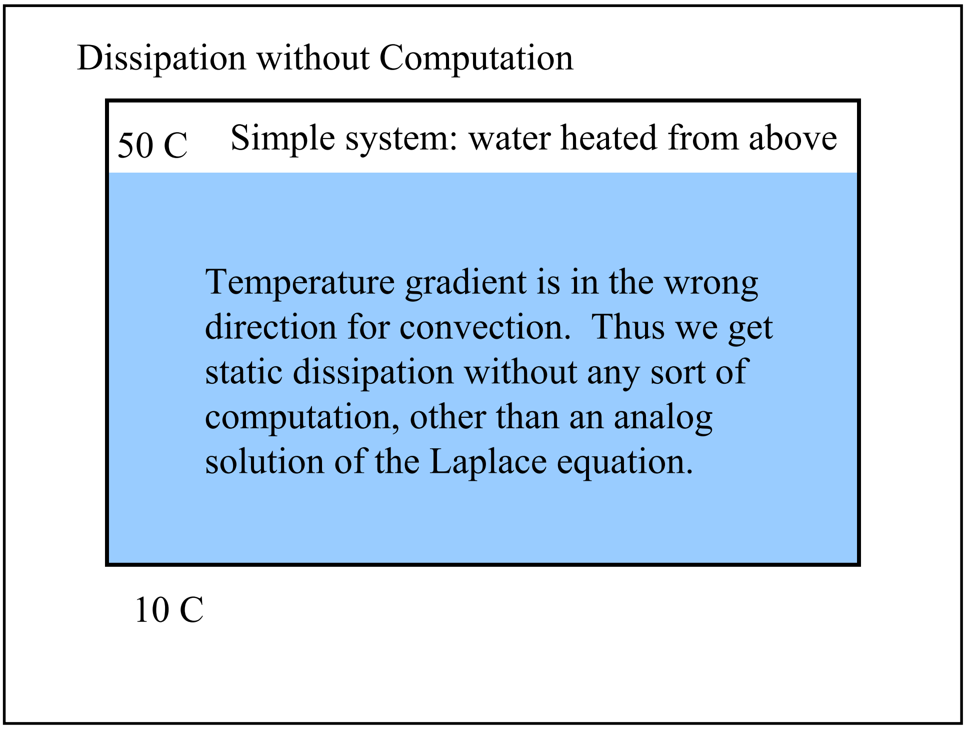
Conduction won’t work unless a cold reservoir is nearby. Convection is more complicated, involving gravity, hydrodynamics, and equation of state of the coolant fluid.



Fortunately 1 and 2- dimensional fault tolerant universal computers exist:

i.e. cellular automata that correct errors by a self-organized hierarchy of majority voting in larger and larger blocks, even though all local transition probabilities are positive.
(P. Gacs math.PR/0003117)

For quantum computations, two dimensions appear necessary for fault tolerance



Dissipation without Computation

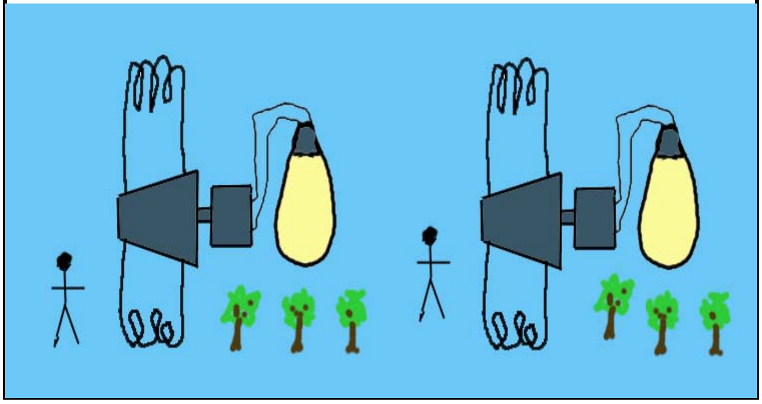
50 C Simple system: water heated from above

Temperature gradient is in the wrong direction for convection. Thus we get static dissipation without any sort of computation, other than an analog solution of the Laplace equation.

10 C

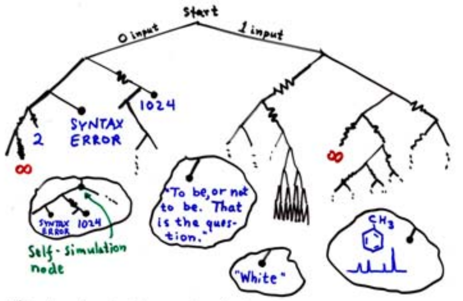
Dissipation-error Tradeoff for Computation

50 C But if the water has impurities



10 C Turbine civilization can maintain and repair itself, do universal computation.

Monkey randomly supplies input to a universal binary computer, might get it to do any computation. (chaitin 1975)



The input-output graph of this or any other universal computer is a microcosm of all cause-effect relations that can be demonstrated by deductive logic or numerical simulation

The awesome power of the notion of Computational Universality suggests a complementary thesis

It from Bit: Physics is Informational

Dynamics should be viewed as computation

Physics should be seen as a branch of mathematics, aiming to develop a mathematical model of all possible worlds wherein our own world can be seen as typical

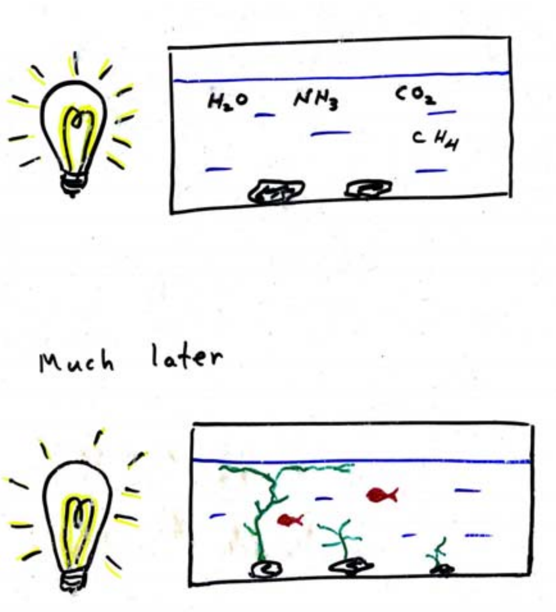
Anthropic Principle

We are (merely) thoughts in the mind of God

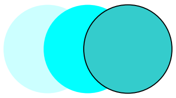
What is the difference between complex dynamics (like our universe seems to have) and simple dynamics (like that of a free particle or harmonic oscillator)?

Can mathematical physics, in particular quantum mechanics, give a non-anthropocentric, non-circular explanation of this difference?

Complex



Simple



Given a Hamiltonian, how do we decide whether it represents complex dynamics or simple dynamics?

Simple answer: We cannot, because any Hamiltonian represents a trivial evolution of its energy eigenstates. In Schumacher's words, "Hilbert space is too smooth" to distinguish one state from another, or one unitary evolution from another.

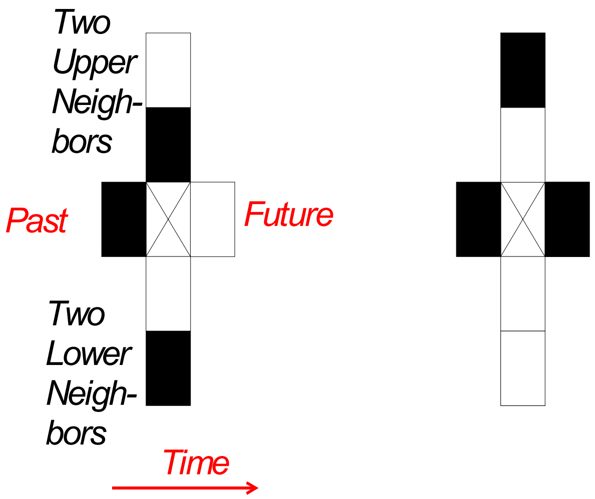
Besides the Hamiltonian, what else do we need to know/specify to separate simple from complex dynamics?

- A preferred basis (probably more than we need)
- A factorization of the Hilbert space into subsystems (probably this is enough). But where we get this factorization from is another question we won't discuss here.

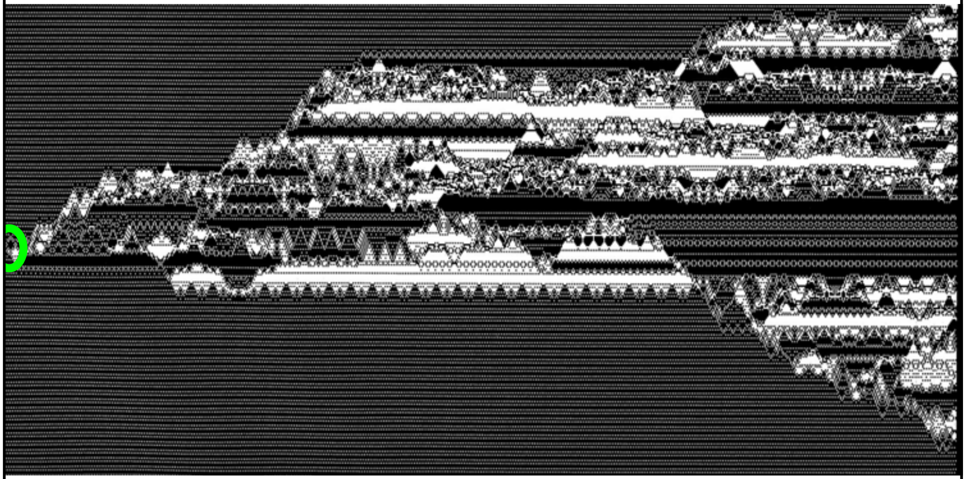
What is complexity? Can we give a nonanthropocentric definition?

What is the difference between a complex state and complex dynamics?

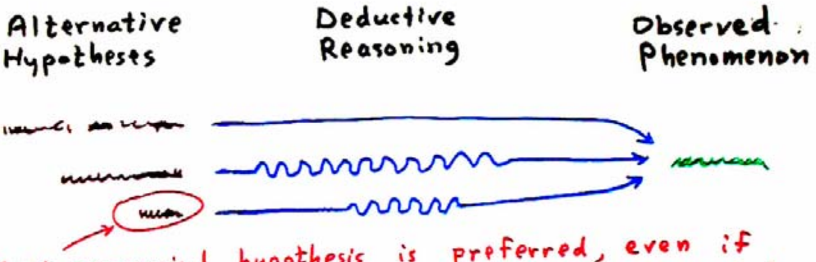
These questions can be posed in the simpler arena of classical discrete reversible dynamics (eg cellular automata)



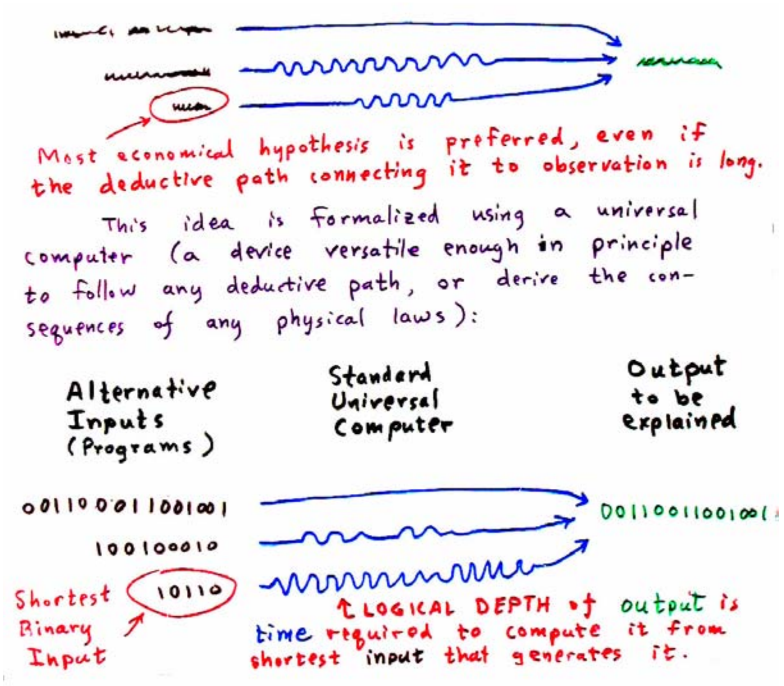
Two-state, range-2, deterministic Ising rule for a one dimensional cellular automaton. Future differs from past iff exactly two of the four neighbors are black at present.



In the philosophy of science, the principle of Occam's Razor directs us to choose the most economical hypothesis able to explain a given body of observed phenomena.



Most economical hypothesis is preferred, even if the deductive path connecting it to observation is long.

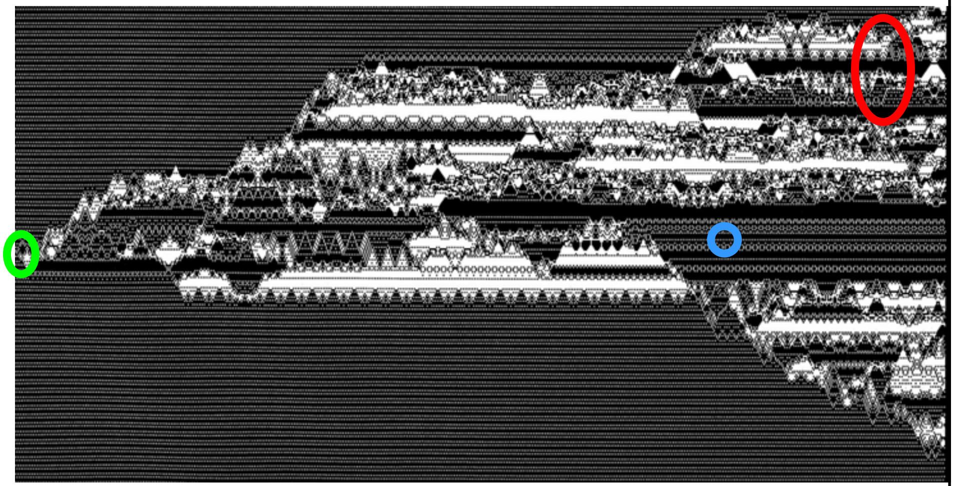


Most economical hypothesis is preferred, even if the deductive path connecting it to observation is long.

This idea is formalized using a universal computer (a device versatile enough in principle to follow any deductive path, or derive the consequences of any physical laws):

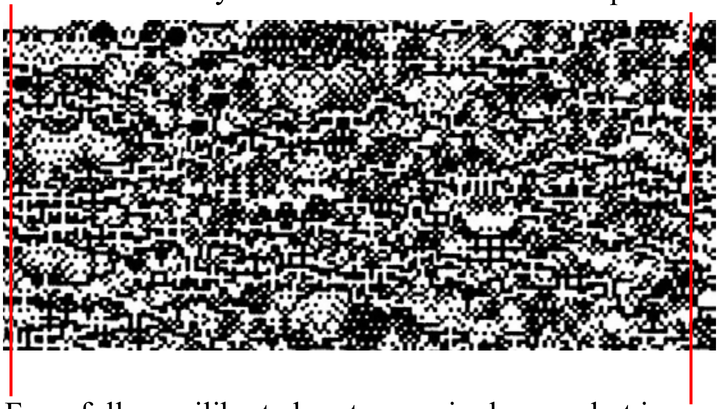
Alternative Inputs (Programs)
Standard Universal Computer
Output to be explained
001100011001001
100100010
10110
00110011001001
Shortest Binary Input

↑ LOGICAL DEPTH of output is time required to compute it from shortest input that generates it.



Thus red region is deep, because it is big enough to contain internal evidence of the complicated process leading to it. Blue region is shallow, because it is too small to contain such internal evidence.

Heat death: a world at thermal equilibrium is no fun.
Our world is only fun because it's still out of equilibrium.



For a fully equilibrated system, a single snapshot is typically random and hence shallow, but a pair of snapshots far apart in time, when taken together (as a single 2n bit string) can be deep if it contains evidence of a nontrivial intervening history.

From whose viewpoint can a quantum dynamics be recognized as complex?

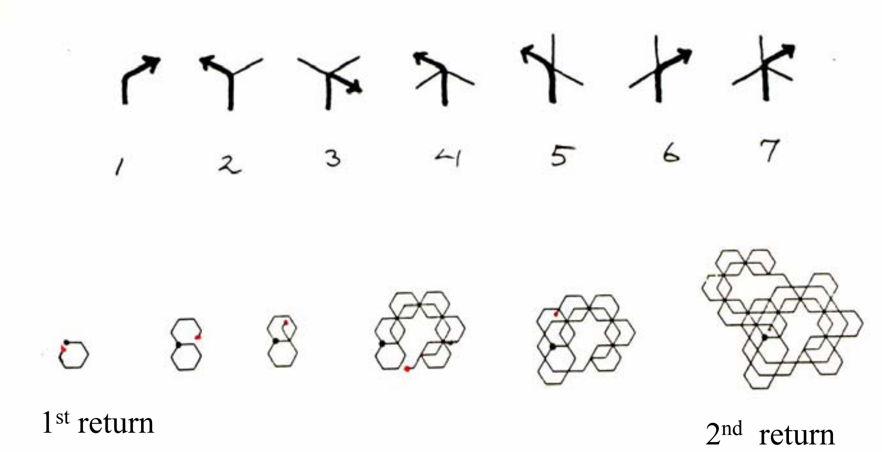
- The physicists standing outside the system and trying to look nonanthropocentrically at its Hamiltonian?

- The inhabitant of the world described by the Hamiltonian?

Classically, a reversible system needs to be out of equilibrium for its inhabitants to realize that it is complex. At equilibrium two-time correlations are needed, which cannot be seen by the inhabitant.

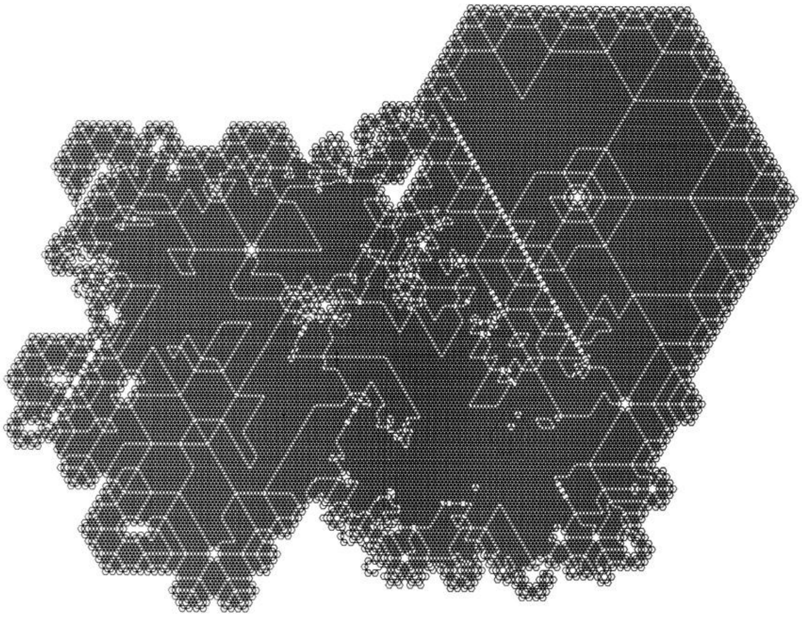
Other examples of Complexity

Patterson’s Worm crawls around on a triangular grid of streets according to fixed rules, marking its path as it goes. Six streets meet at each intersection, and it can never use the same street twice. On its third return to its birthplace there are no streets left, so it dies.

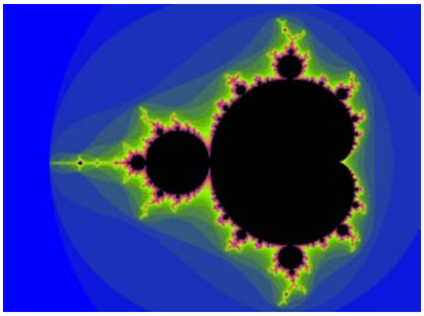


1st return

2nd return



Some Infinitely Complicated Objects:



The Mandelbrot Set

Borges’ Aleph, *a Microcosm of the physical world*

The Monkey Graph
The Input/Output Diagram of a general purpose digital computer, which can perform any computation and simulate any mathematically describable dynamical process, is a microcosm of all possible cause/effect relations

The Aleph's diameter was probably little more than an inch, but all space was there, actual and undiminished. Each thing (a mirror's face, let us say) was infinite things, since I distinctly saw it from every angle of the universe. I saw the teeming sea; I saw daybreak and nightfall;
I saw the multitudes of America...I saw in a backyard of Soler Street the same tiles that thirty years before I'd seen in the entrance of a house in Fray Bentos; I saw bunches of grapes, snow, tobacco, lodes of metal, steam; I saw convex equatorial deserts and each one of their grains of sand...I felt dizzy and wept, for my eyes had seen that secret and conjectured object whose name is common to all men but which no man has looked upon -- the unimaginable universe. ---J.L. Borges (much abridged)

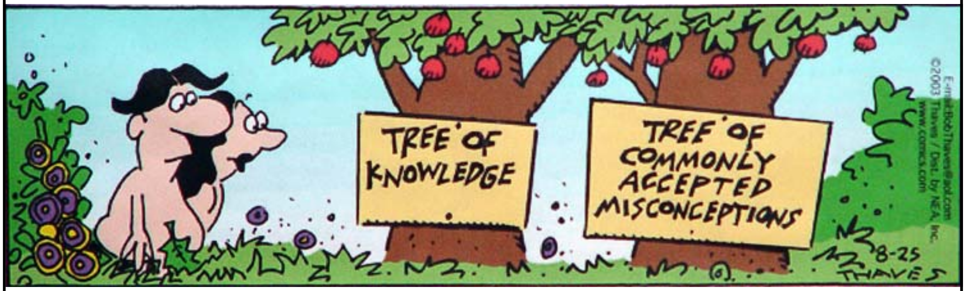
(the end)

Lipid bilayer MD dilaurylphosphatidylethanolamine
http://www.pc.chemie.tu-darmstadt.de/research/molcad/movie.shtml

Bennett, Charles H., "Dissipation-Error Tradeoff in Proofreading"
*BioSystems***11**, 85-91 (1979)

C.H. Bennett "The Thermodynamics of Computation-- a Review"
Internat. J. Theoret. Phys. **21**, pp. 905-940 (1982).

http://www.research/ibm.com/people/b/bennetc


TREE OF KNOWLEDGE
TREE OF COMMONLY ACCEPTED MISCONCEPTIONS
8-25
THAVES
E-mail:BobThaves@aol.com
©2003 Thaves / Dist. by NEA, Inc.
www.comics.com