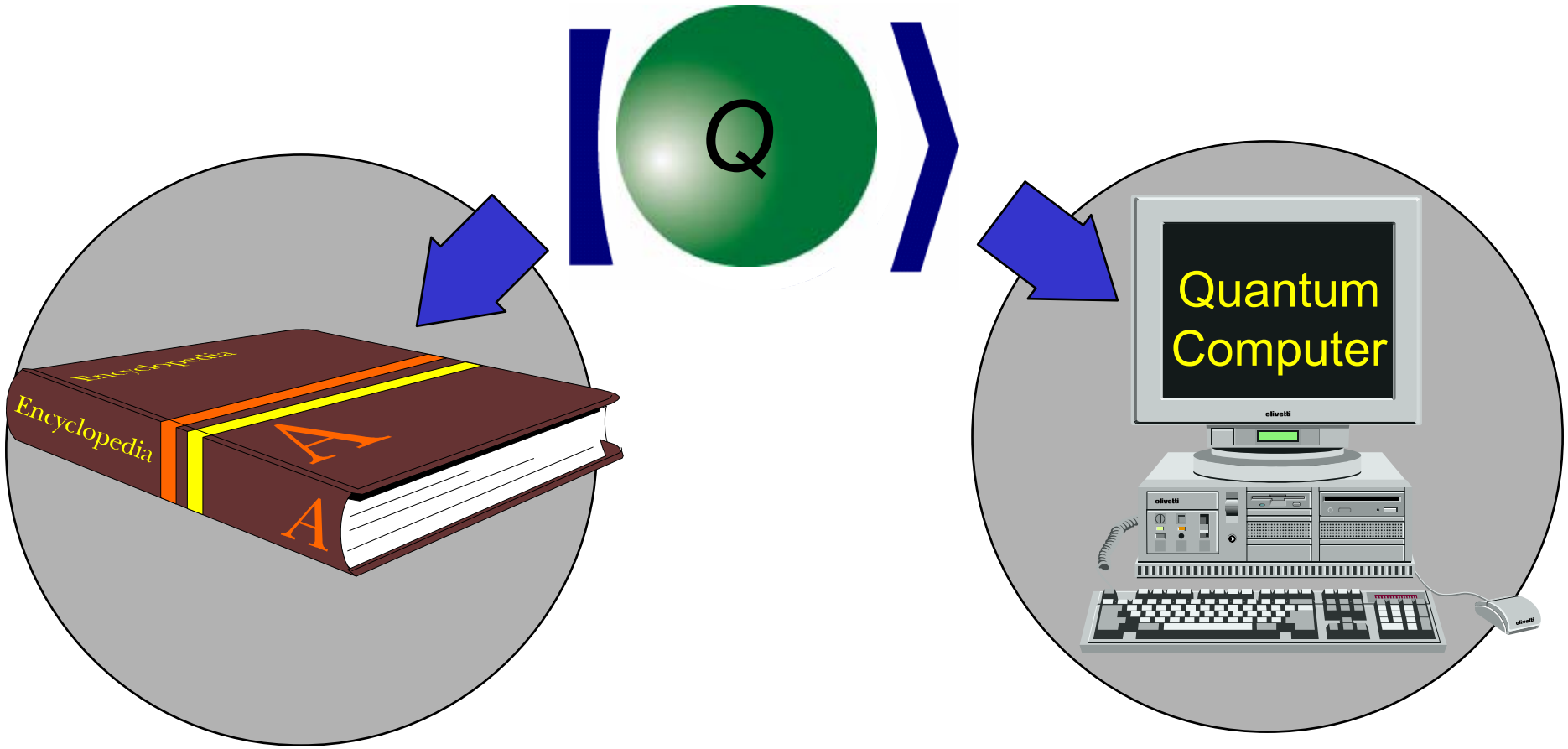
Quantum Computation and the Future of Physics



Institute for Quantum Information

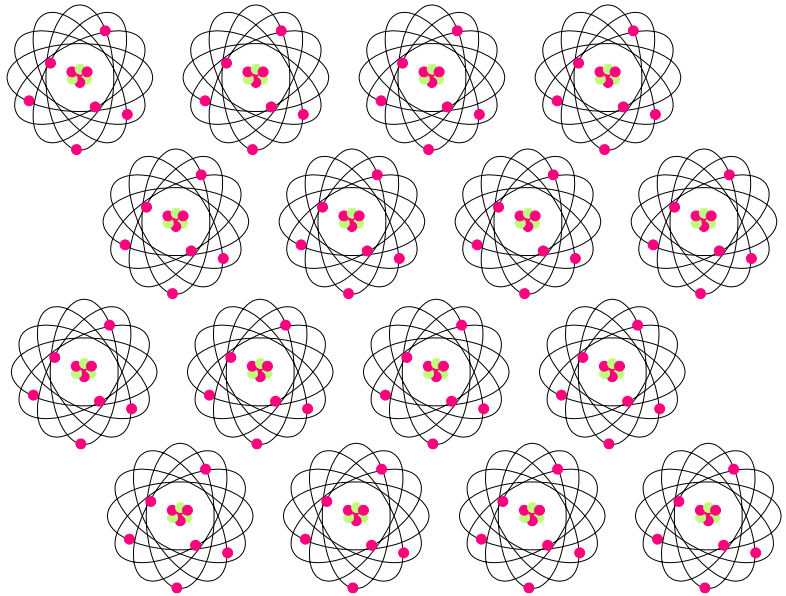
John Preskill, Caltech
10 May 2002
http://www.iqi.caltech.edu/

THEORY OF COMPUTATION & THE SCIENCES

"where can the`lens' provided by theoretical CS be a useful tool in other fields?"

What can the study of *quantum* computation and quantum information tell us about ***physics***?

The *Quantum* Century



Though quantum theory is 100 years old, there are profound aspects of the difference between quantum and classical systems that we have begun to understand in just the past few years.

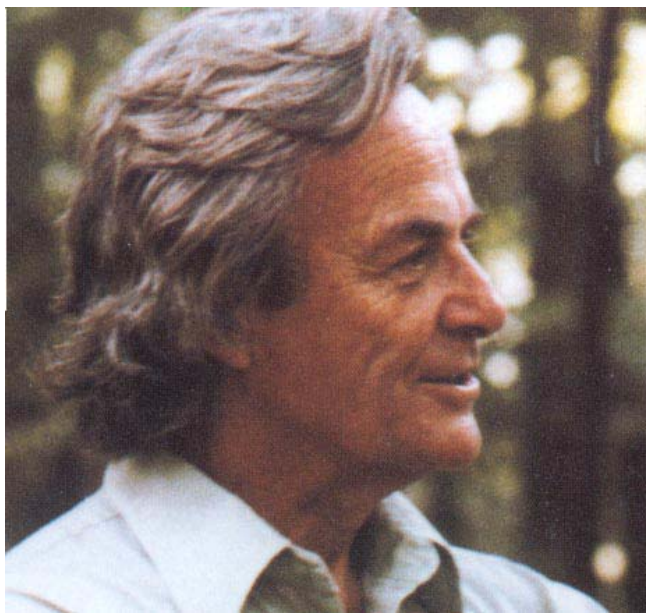
Theoretical Quantum Information Science

is driven by ...

Three ***Great*** Ideas:

1) Quantum Computation
2) Quantum Cryptography
3) Quantum Error Correction

(1) Quantum Computation

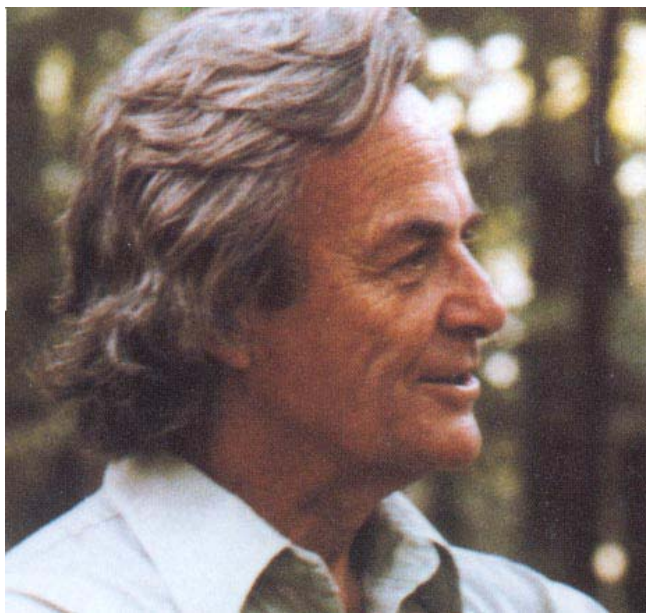


Feynman ‘81

Deutsch ‘85

Shor ‘94

A computer that operates on quantum states can perform tasks that are beyond the capability of any conceivable classical computer.



Feynman ‘81

Deutsch ‘85

Shor ‘94

Finding Prime Factors

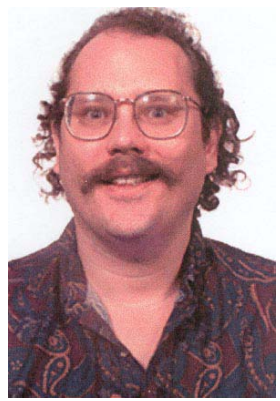
1807082088687
4048059516561
6440590556627
8102516769401
3491701270214
5005666254024
4048387341127
5908123033717
8188796656318
2013214880557

=

3968599945959
7454290161126
1628837860675
7644911281006
4832555157243

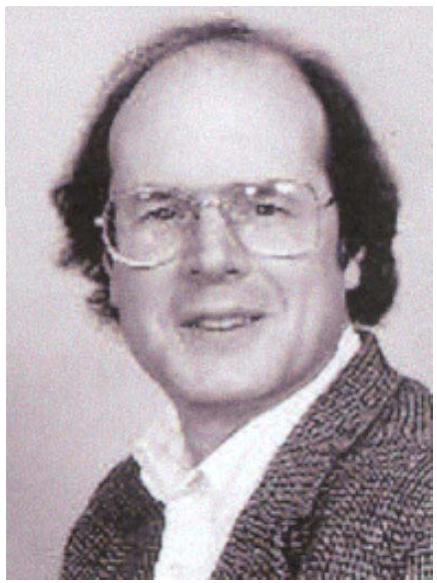
×

4553449864673
5972188403686
8972744088643
5630126320506
9600999044599

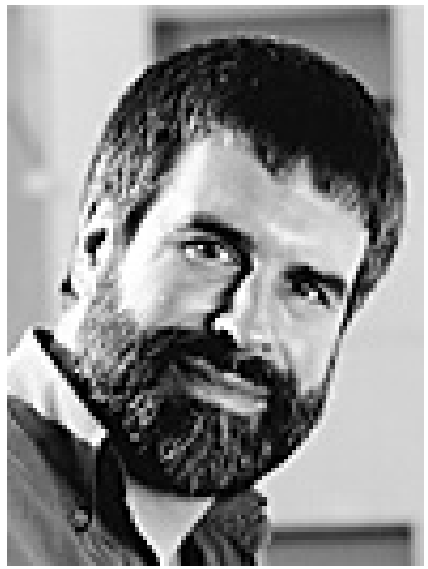


Shor ‘94

(2) Quantum Cryptography

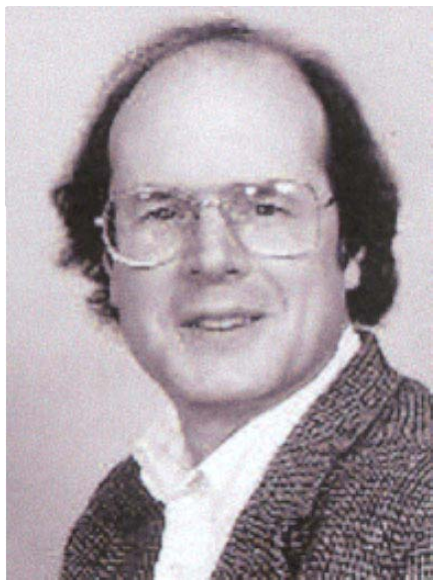


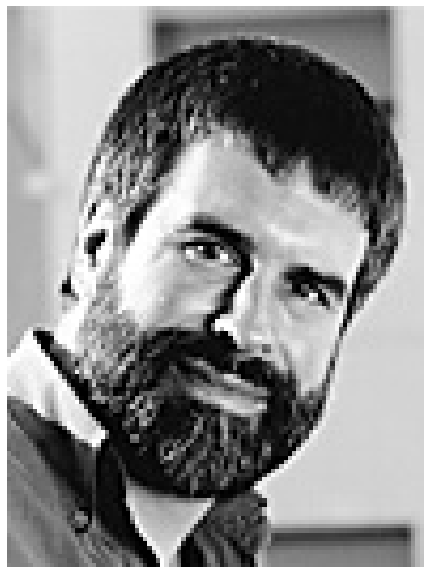
Bennett



Brassard ’84

Eavesdropping on quantum information can be detected; key distribution via quantum states is *unconditionally* secure.





Bennett Brassard ’84

Quantum Cryptography

Alice

Eve

Bob

Privacy is founded on principles of fundamental physics, not the assumption that eavesdropping requires a difficult computation. Gathering information about a quantum state unavoidably disturbs the state.

Quantum Error Correction

Shor ‘95

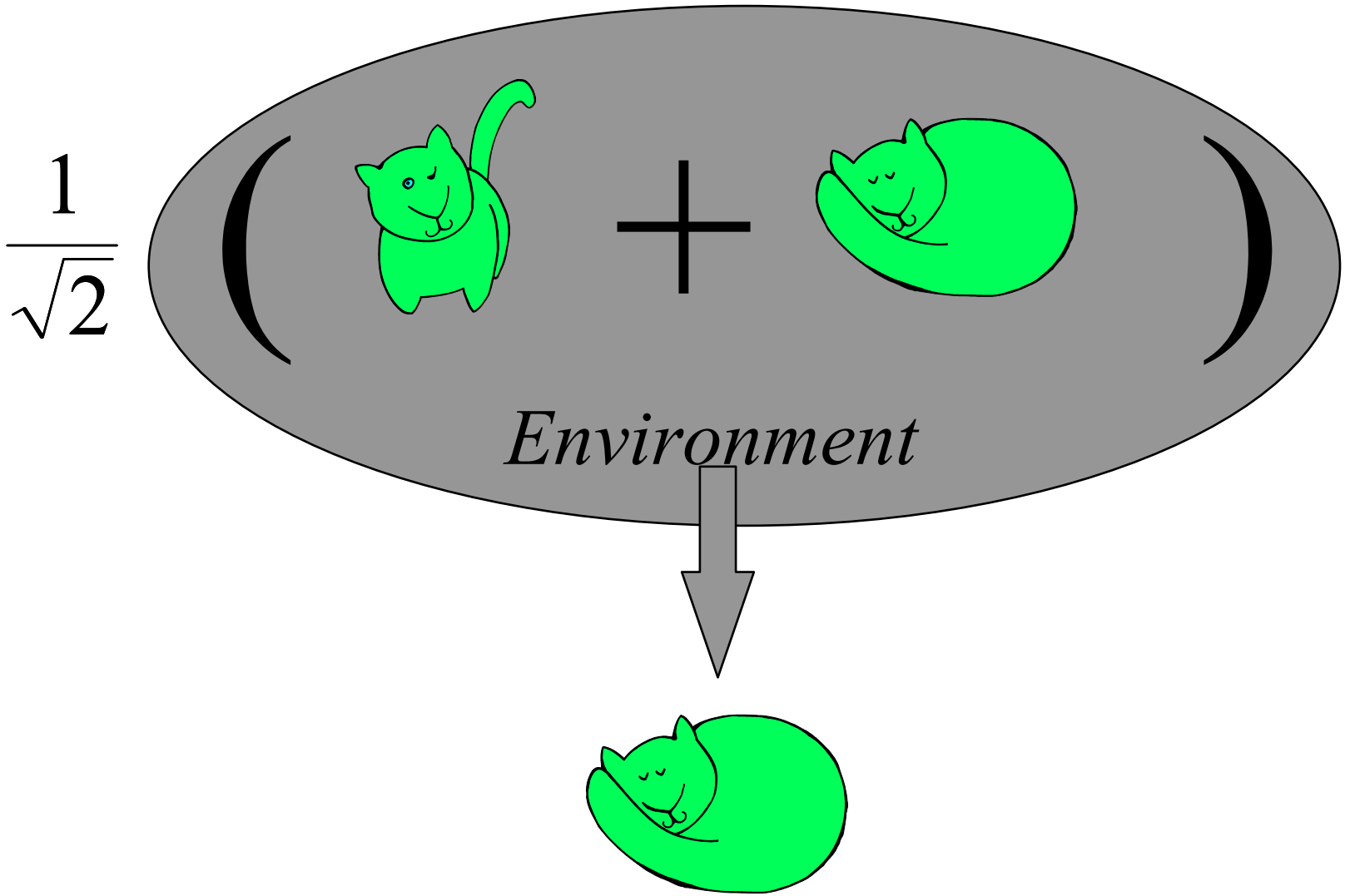
Steane ‘95

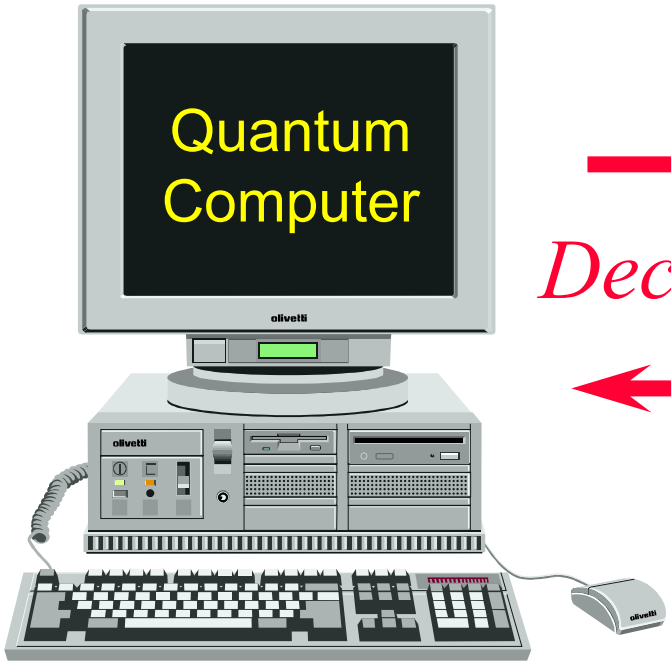
Quantum information can be protected, and processed fault-tolerantly.

Shor ‘95

Steane ‘95

Decoherence





Decoherence

Environment

ERROR!

If quantum information is cleverly encoded, it *can* be protected from decoherence and other potential sources of error. Intricate quantum systems *can* be accurately controlled.

Theoretical Quantum Information Science

Three ***Great*** Ideas:

1) Quantum Computation
2) Quantum Cryptography
3) Quantum Error Correction

The computer scientists seem to be setting the agenda ….
What problems do physicists usually grapple with?

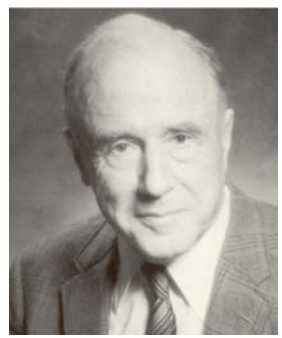
Challenges in theoretical (quantum) physics?

Weinberg

• "Dreams of a final theory." What theory describes the fundamental constituents of matter and their interactions? (What *computational model* is realized in Nature?)

Anderson

• "More is different." What emergent collective phenomena can arise in condensed matter? (What is the potential *complexity* of quantum many-body systems?)



Wheeler

• "How come the quantum?" *Why* do the rules of quantum mechanics apply to Nature? (Is *everything* information?)

Dreams of a final theory I. The standard model

Weinberg

We have a spectacularly successful model of the strong, weak, and electromagnetic interactions, describing matter down to 10^{-16} cm. But ...

- QCD. Does quantum chromodynamics correctly predict the properties of the strongly interacting particles, and can we compute those predictions? [Quark confinement, spontaneous, chiral symmetry breaking, hadron masses, ..]
- Gauge group. *Why* the gauge symmetry $SU(3)_{strong}$ X $[SU(2)$ X $U(1)]_{electroweak}$?
- Parameters. For example, the mass spectrum (and mixing angles) of quarks and leptons. [$m_{top}/m_{electron} \sim 3$ X 10^{-6} .]
- Heirarchy. *Why* $m_{weak}/m_{Planck} \sim 10^{-17}$?
- Supersymmetry. Does it exist, and is it experimentally accessible? How and why is it broken?
- Neutrino Mass. A vestige of physics beyond the standard model, at $\sim 10^{-24}$ cm.

Dreams of a final theory II. Quantum gravity

Weinberg

General relativity is a spectacularly successful model of gravitational interactions at accessible distances. But …

• Quantum gravity model. Is there a quantum theory that consistently describes large quantum fluctuations of spacetime geometry at "arbitrarily short distances"? Is it string theory / M theory? [M = mystery, mother, membrane, matrix, …]

• What *is* string theory / M theory? "Nonperturbative" formulation, with spacetime as an emergent property.

• Dimensionality. Why 3 + 1 spacetime dimensions?

• Cosmological Constant. What does the vacuum weigh?
Why $\rho_{vac}/\rho_{Planck} \sim 10^{-122}$?

• Cosmology. How and why did the universe begin?

• Black holes. Do they *destroy* quantum information? Is quantum gravity "unitary"?

• Predictability. Is physics an *environmental* science? To what extent are the fundamental laws determined by the "final" theory?

More is different: Quantum many-body theory

Anderson

What collective phenomena arise when quantum fluctuations are large? [For example, systems composed of "strongly correlated electrons" such that the elementary excitations do not resemble electrons.]

• Phases. What phases of matter are possible at zero temperture? What physical properties are robust (invariant under small changes in the Hamiltonian)? What are the (universal) properties of the transitions between the phases? [What are the possible manifestations of *many-particle quantum entanglement*?]

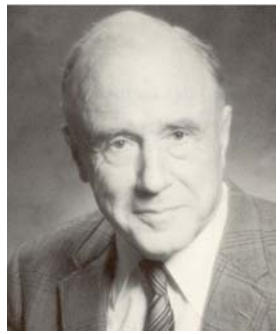
Examples:

• High-temperature superconductivity. What microscopic mechanism explains the properties of the high-T_c cuprates?

• Quantum Hall systems. What phases can be realized by a highly correlated two-dimensional gas of highly mobile electrons in a strong magnetic field?

• Mesoscopic physics. How do electrons behave in very small conducting devices?

How come the quantum?



Wheeler

Apart from the quest for the ultimate building blocks and what can be built from them (and receiving far less attention from most practicing physicists) is the issue: can we gain a deeper understanding of the *foundations* of quantum theory?

- Interpretation. What is a "wave function"? Does it describe intrinsic properties of a system or what one knows about a system? What is the role of the "observer"?

- Measurement. What is a "measurement"? Is there a fundamental distinction between a measurement and "unitary evolution"? Is the outcome of a measurement truly random?

- New foundations? If quantum mechanics is flawed, what is the alternative? If it is not flawed, can we understand why it must be the way it is?

- Quantum/classical interface. How does "classical" behavior emerge from a quantum system? Can we identify a sharp boundary between quantum and classical behavior?

- Quantum information. Are the foundations more transparent when expressed in an information-theoretical framework?

Challenges in theoretical (quantum) physics?

- "Dreams of a final theory." What theory describes the fundamental constituents of matter and their interactions? (What *computational model* is realized in Nature?)
- "More is different." What emergent collective phenomena can arise in condensed matter? (What is the potential *complexity* of quantum many-body systems?)
- "How come the quantum?" *Why* do the rules of quantum mechanics apply to Nature? (Is *everything* information?)

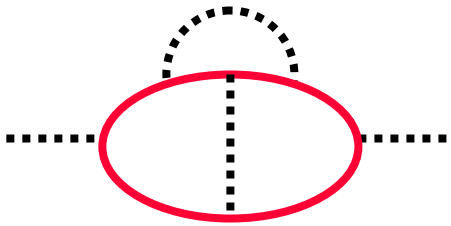
What (if anything) do these challenges have to do with (quantum) computation? How might computational concepts illuminate the big questions at the core of physics?

Universality: the most important idea in physics

Wilson

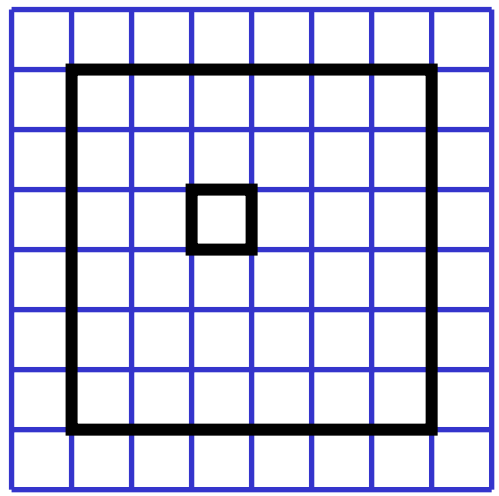
A case study: 30 years ago Ken Wilson was unusually "computational" among physicists. He wondered how to simulate quantum field theory on a computer, which helped lead him to a fruitful answer to the question: What *is* quantum field theory?

His insights launched new analytic and computational methods for exploring the properties of systems governed by large thermal or quantum fluctuations.

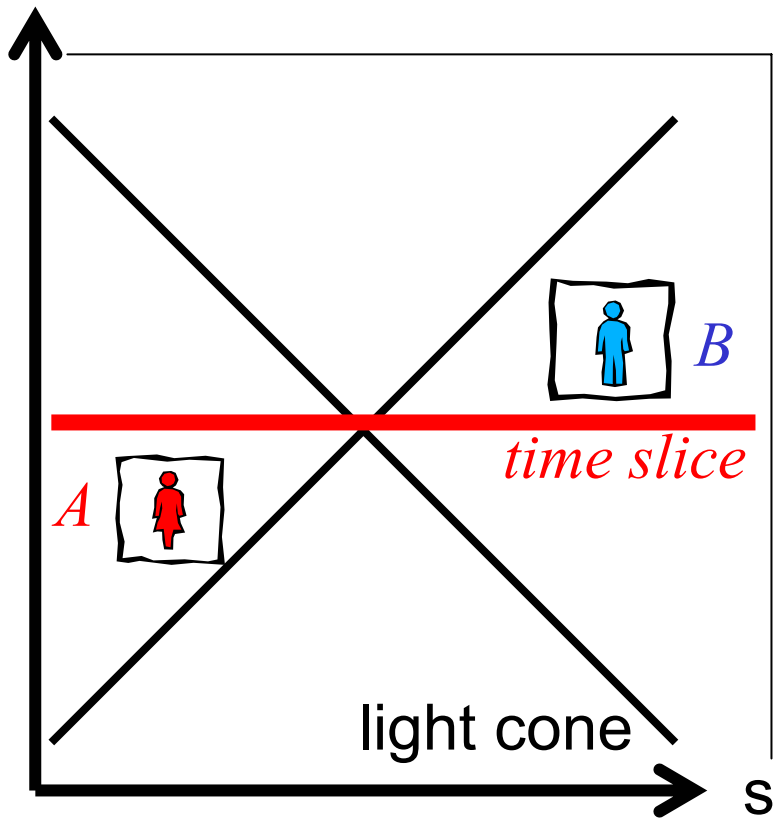


Before Wilson, calculations in quantum field theory were usually perturbative, organized as a power series expansion in powers of Planck's constant $\hbar$ (Feynman diagram expansion).

Wilson recognized that in many settings it is more instructive to organize the theory *scale by scale*. We can integrate out the effects of quantum fluctuations at short distance scales, and incorporate these effects into our description of physics at longer distance scales ("renormalization group").



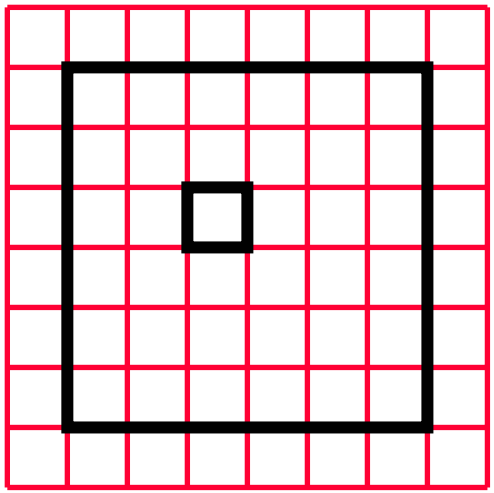
Quantum field theory



(Relativistic) quantum field theory is *local*. Fields associate *observables* with open regions of spacetime. Observables *A* and *B* supported in spacelike separated regions *commute*, to assure that a measurement of *A* has no influence on *B*. Furthermore, the dynamics of the observables is governed by a Hamiltonian that couples together only *neighboring* degrees of freedom.

It is difficult to construct a theory that is consistent with both the principles of quantum mechanics and the principles of special relativity. Therefore quantum field theories are highly constrained. They are built on the notion that the algebra of observables should have *a natural decomposition as a tensor product of subsystems*, where each subsystem is highly localized. This structure should be reflected in a computational model that purports to describe Nature.

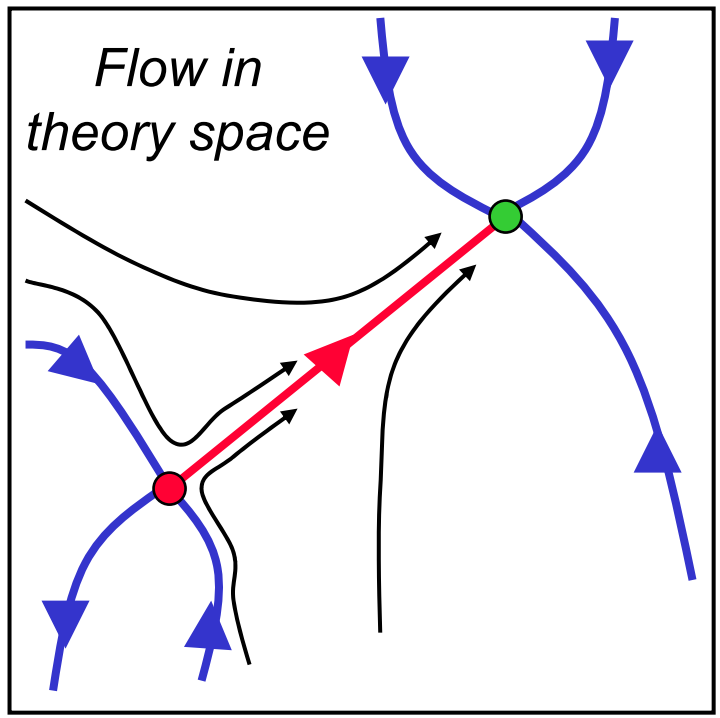
Universality: the most important idea in physics



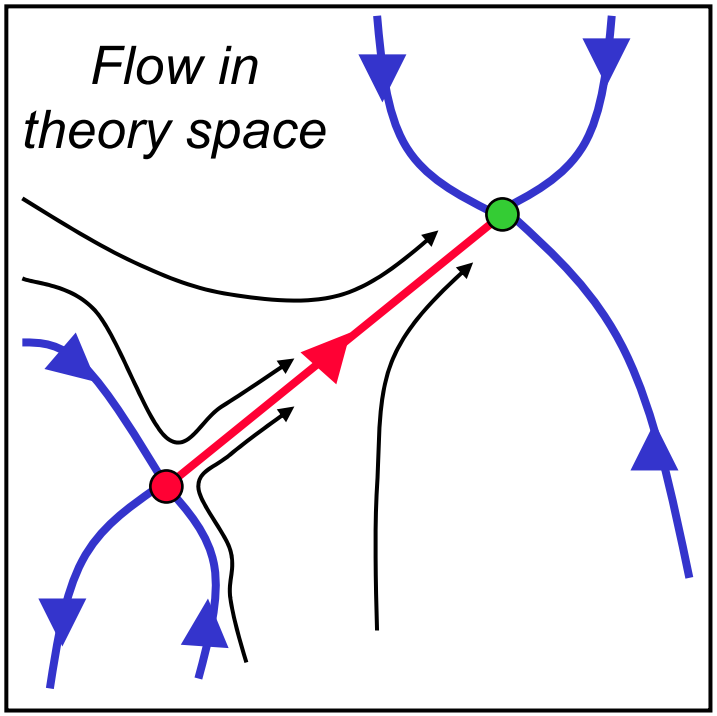
Wilson

Correlations of quantum fields are governed by a probability distribution for field histories in space and (imaginary) time. Fields can be defined on a very fine lattice in spacetime. Predicted properties of processes with characteristic distance scale large compared to the lattice spacing can be derived from an *effective field theory* for long wavelengths obtained by averaging over the short wavelength modes.

In the "far infrared" (at long distance scales), the infinite-dimensional space of theories collapses to a submanifold of low dimension. While microscopic theories come in many varieties, all make the same predictions for long-distance physics, depending on just a few parameters. Hence "universality."



Universality: the most important idea in physics



Wilson

The far-infrared behavior is dominated by *scale-invariant* theories ("conformal field theories"), or by the flow from one CFT to another. The flow seems to be a *gradient* flow --- it runs downhill from "more information" (about the microscopic theory) to "less information." Can this information-theoretic interpretation of the flow be made more precise?

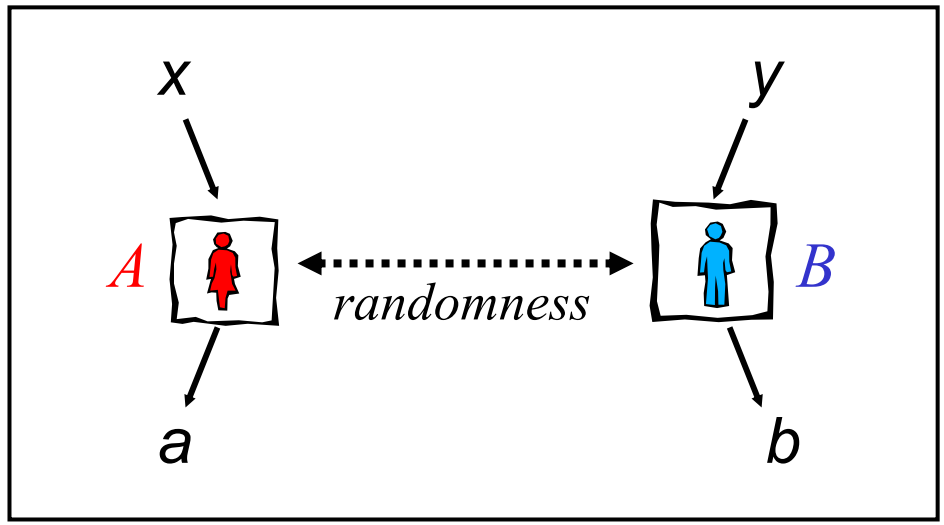
Universality is a two-edged sword. On the one hand, *it makes physics possible.* We can understand e.g. the electronic structure of atoms (10^{-8} cm) without knowing the details of the right theory of quantum gravity (10^{-33} cm) .

On the other hand, theories of very-short-distance physics are *hard to test experimentally:* the effects of physics at distance scale L_{short} are suppressed in experiments at energy scale hc/L_{long} by powers of L_{short} / L_{long}.

Quantum entanglement: a subtle revision of locality

Alice and Bob share an indefinite amount of randomness, each has an input bit (*x* for Alice, *y* for Bob), and each is to produce an output bit (*a* for Alice, *b* for Bob) Their goal is to choose outputs such that:

$$a \oplus b = x \wedge y$$



Then, averaged over input bits,

$P_{\text{success}} \leq 3/4 = .75$ (a *Bell inequality*).

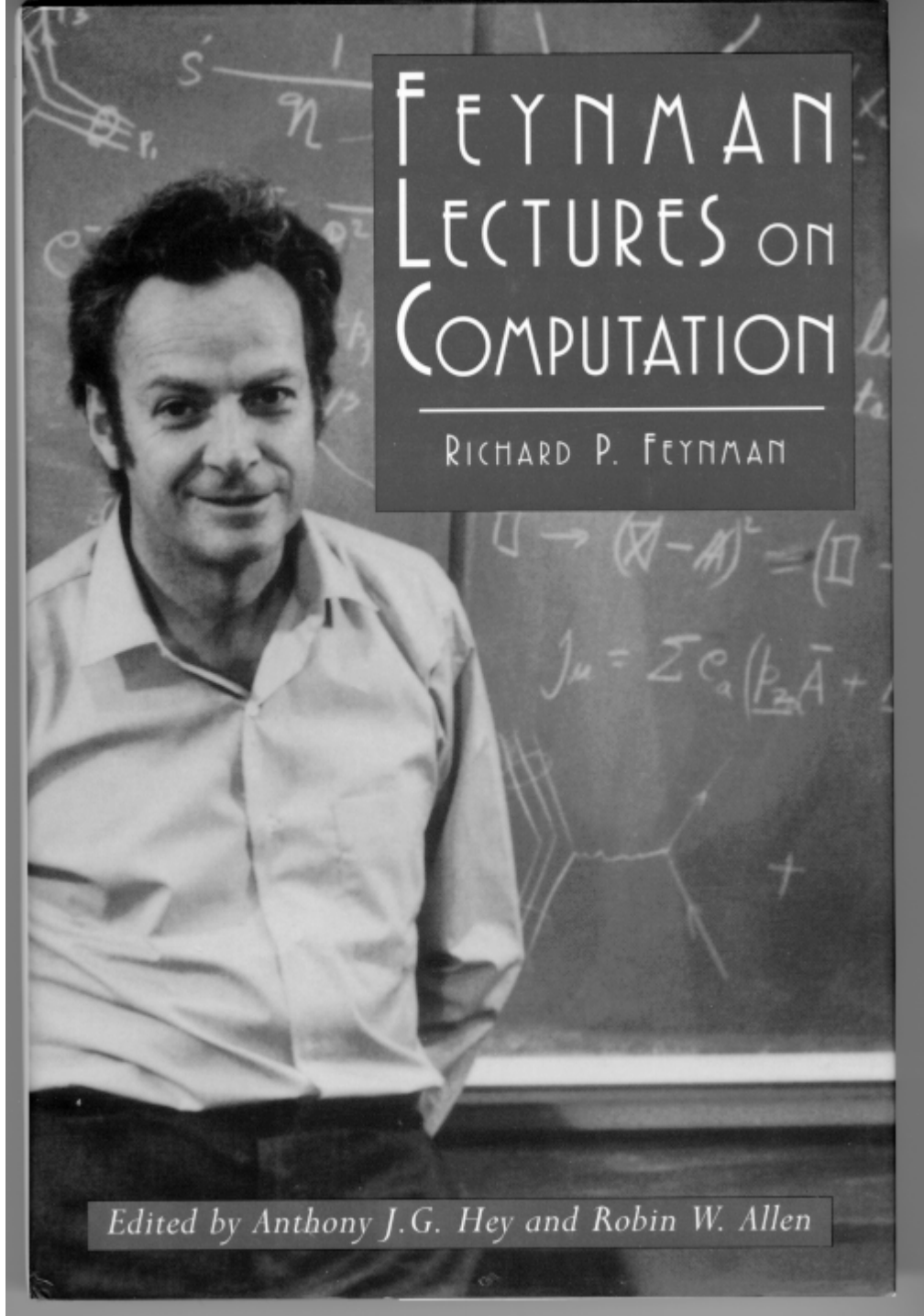
But if Alice and Bob share an *entangled* pair of quantum bits ("qubits"), then

$$P_{\text{success}} = \frac{1}{2} + \frac{1}{2\sqrt{2}} = .853$$ is achievable.

The classical communication cost of simulating the correlations of *n* pairs of qubits is $O(2^n)$. Entanglement is a *powerful resource*.

For one typical state of n qubits, we would need $O(2^n)$ bits to give a complete *classical* description of all the *quantum* correlations among the n qubits.

Therefore, to simulate a quantum computer with a classical computer seems to require exponential resources --- the quantum computer is intrinsically more powerful.



Quantum computer: the model

(1) Hilbert space of *n* qubits: $\mathfrak{H} = \left(\mathbb{C}^{2^n} \right)$

spanned by

$$|x\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle, \; x \in \{0,1\}^n$$

Important: the Hilbert space is equipped with a natural tensor-product decomposition into subsystems.

$$\mathbb{C}^{2^n} = \underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}}$$

Physically, this decomposition arises from spatial locality. Elementary operations ("quantum gates") that act on a small number of qubits (independent of *n)* are "easy;" operations that act on many qubits (increasing with *n*) are "hard."

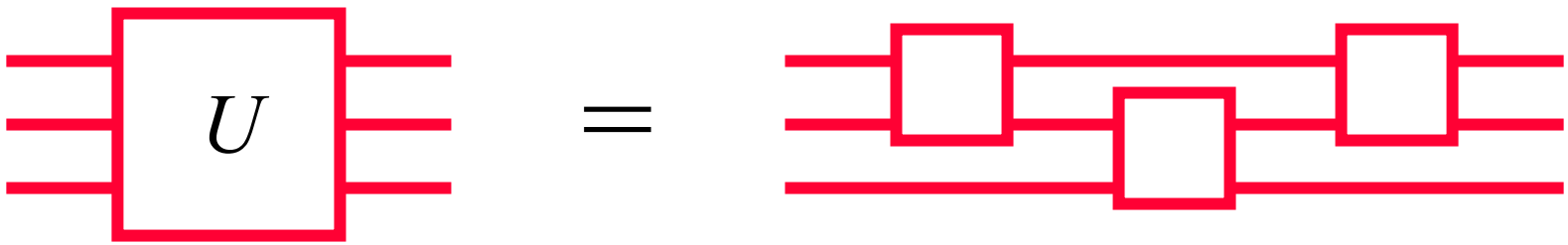
(2) Initial state: $|000\ldots0\rangle = |0\rangle^{\otimes n}$

Quantum computer: the model

(3) A finite set of fundamental quantum gates:

$$\{U_1, U_2, U_3, \ldots U_{n_G}\}$$

Each gate is a unitary transformation acting on a bounded number of qubits. The gates form a universal set: arbitrary unitary transformations can be constructed, to any specified accuracy, as a quantum circuit constructed from the gates:



(Universal gates are generic.)

Important: One universal set of gates can simulate another efficiently, so there is a notion of complexity that is independent of the details of the quantum hardware.

Quantum computer: the model

(4) Classical control:

The construction of a quantum circuit is directed by a classical computer, *i.e.,* a Turing machine. (We're not interested in what a quantum circuit can do unless the circuit can be designed efficiently by a classical machine.)

(5) Readout:

At the end of the quantum computation, we read out the result by measuring σ_z , *i.e.*, projecting onto the basis $\{|0\rangle, |1\rangle\}$

(We don't want to hide computational power in the ability to perform difficult measurements.)

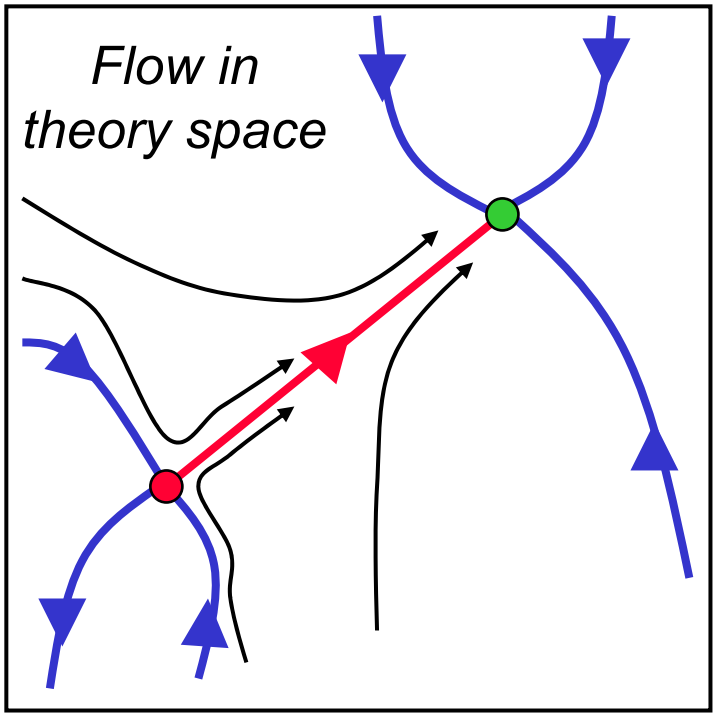
Quantum computer: the model

(1) *n* qubits
(2) initial state
(3) quantum gates
(4) classical control
(5) readout

Clearly, the model can be simulated by a classical computer with access to a random number generator. But there is an exponential slowdown, since the simulation involves matrices of exponential size.

The quantum computer might solve efficiently some problems that can't be solved efficiently by a classical computer. ("Efficiently" means that the number of quantum gates = polynomial of the number of bits of input to the problem.)

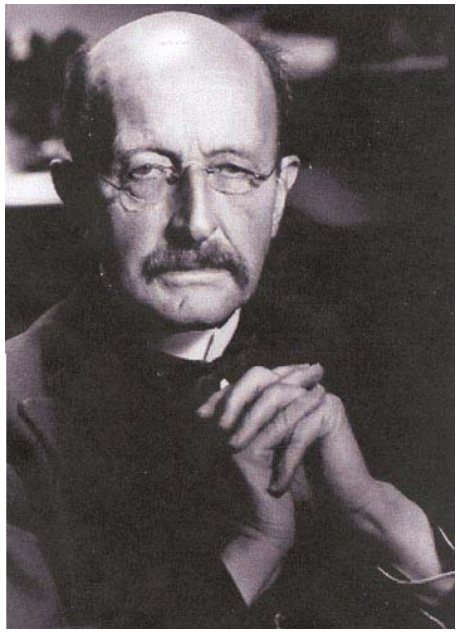
Computational power of local quantum field theory



Universality: in a *local* quantum field theory, physical processes with characteristic distance scale L (energy scale hc/L) can be modeled by a theory on a lattice with lattice spacing a --- corrections due to the lattice cutoff are suppressed by powers of a/L.

Therefore, a "garden-variety" quantum computer can model quantum field theory efficiently, if the "size of the input" to the problem is (say) the volume being simulated in lattice units.

The quantum field computer has very-short-wavelength modes at its disposal, a potentially powerful resource. But if the input and output are encoded in modes of wavelength L, then in a local field theory, all physical effects of the short-wavelength modes can be incorporated into a few parameters of the *effective* field theory, which has no short-wavelength modes and is easy to simulate (on a *quantum* computer).



PARADOX!

When the theories we use to describe Nature lead to unacceptable or self-contradictory conclusions, we are faced with a great challenge and a great opportunity….

Planck 1900

"*The ultraviolet catastrophe.*"

Classical electromagnetic theory and statistical mechanics predict that in thermal equilibrium the electromagnetic field in a cavity stores an infinite amount of energy.

The end of classical physics!

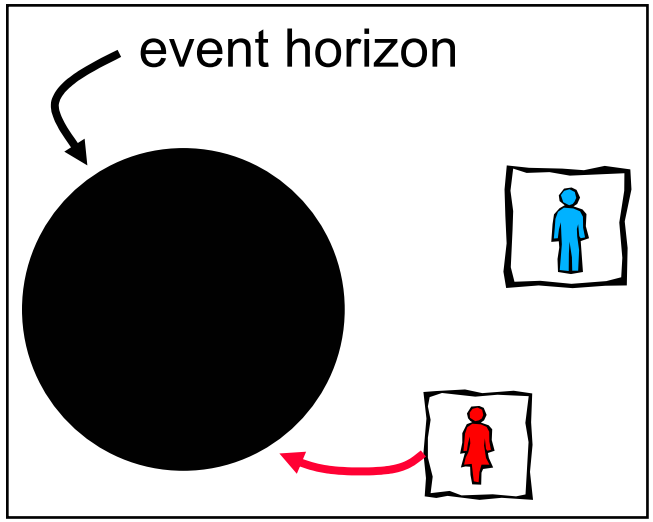
Hawking 1975

"*The information loss puzzle.*"

Classical gravitation theory and quantum field theory on curved spacetime predict that the formation and subsequent complete evaporation of a black hole cannot be unitary.

The end of quantum field theory?

Black Hole

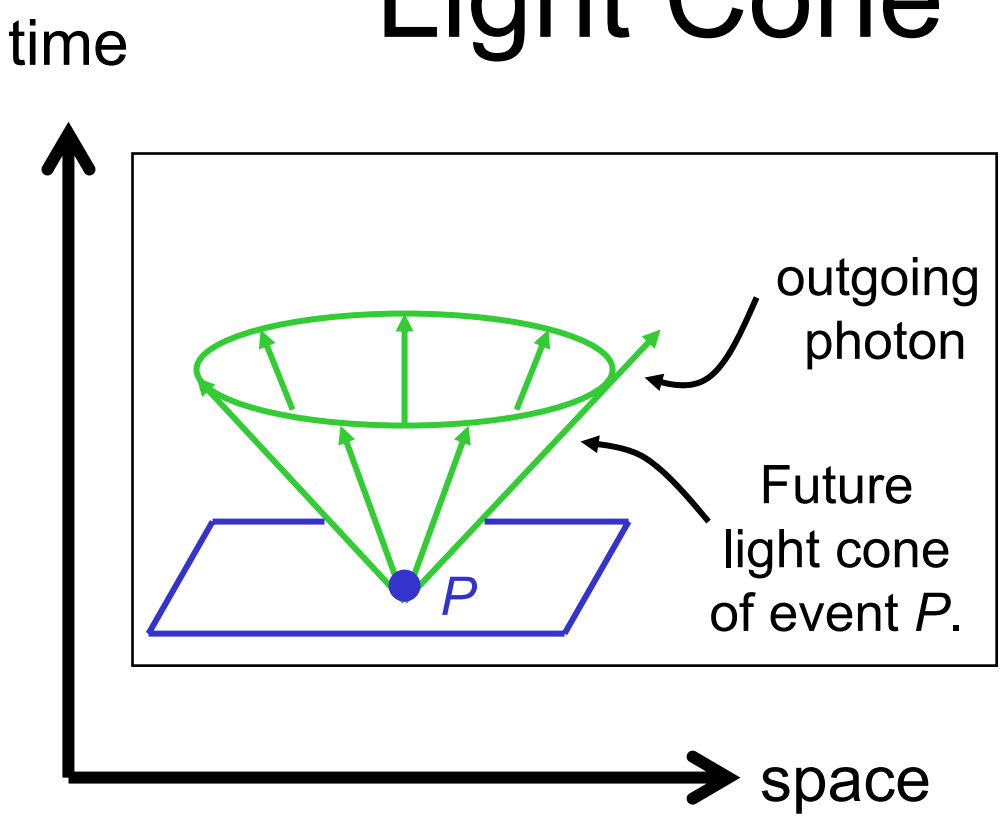


Classically, a black hole is a very simple object (it has “no hair”) composed of pure spacetime geometry.

If Alice crosses the event horizon of a black hole, she will never be able to return to or communicate with Bob, who remains outside.

To understand the event horizon better, consider the concept of a light cone. Imagine a light source that emits a flash (the spacetime event *P*). The flash travels outward as a spherical shell expanding at light speed. Plotted as a function of time, the expanding shell defines a cone, the future light cone of *P*. All events that can be influenced by *P* lie inside its future lightcone.

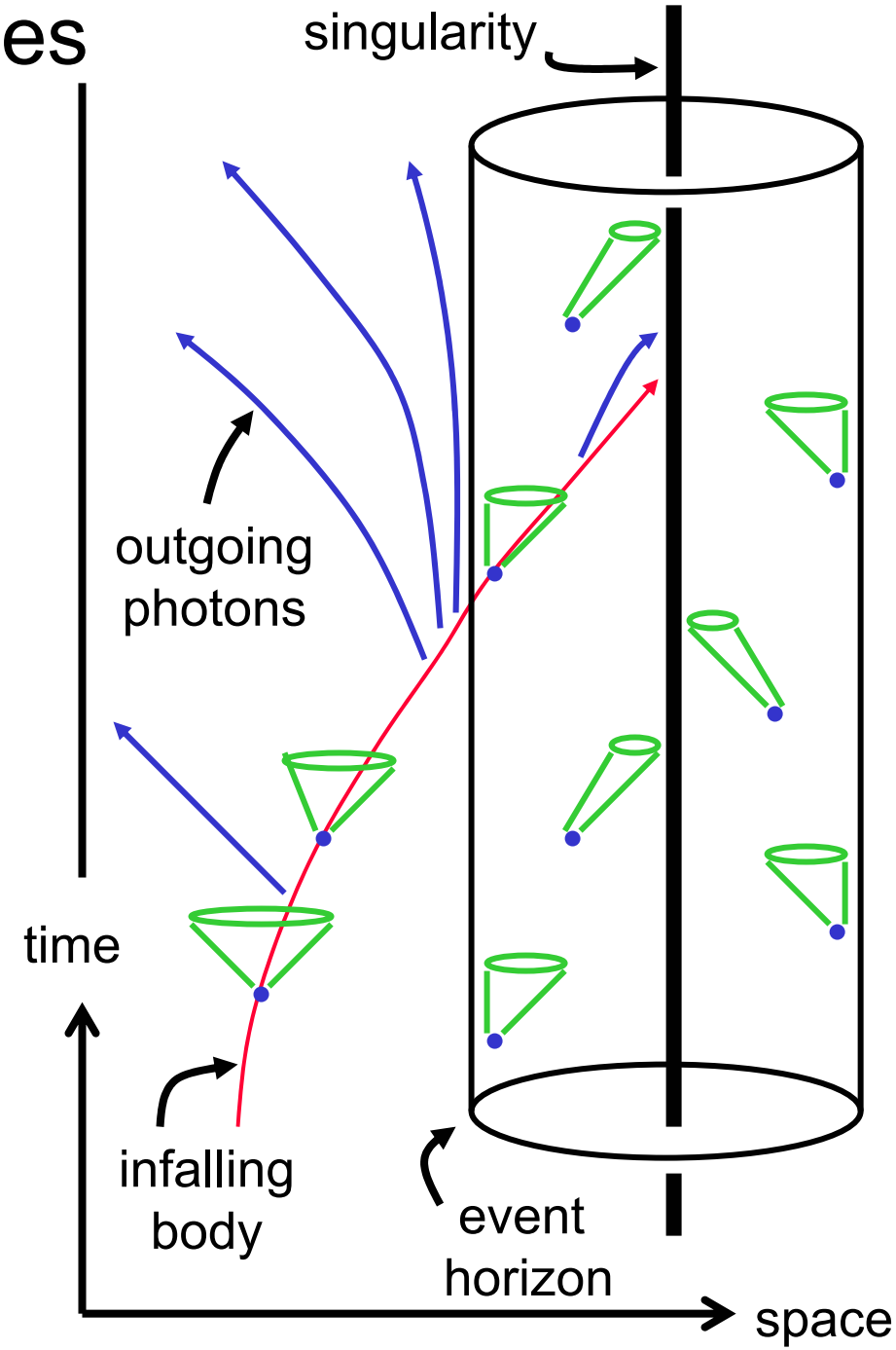
Light Cone



Tipping of the light cones

We find by solving the Einstein field equations that the lightcones tip inward as one approaches the black hole. The future light cone of a point inside the horizon lies entirely inside the horizon. Any signal emitted from a point inside the horizon necessarily travels more deeply into the black hole.

The unfortunate astronaut who enters the black hole is unavoidably drawn to the singularity, a region of enormous gravitational forces that tear him apart.



Black hole radiance

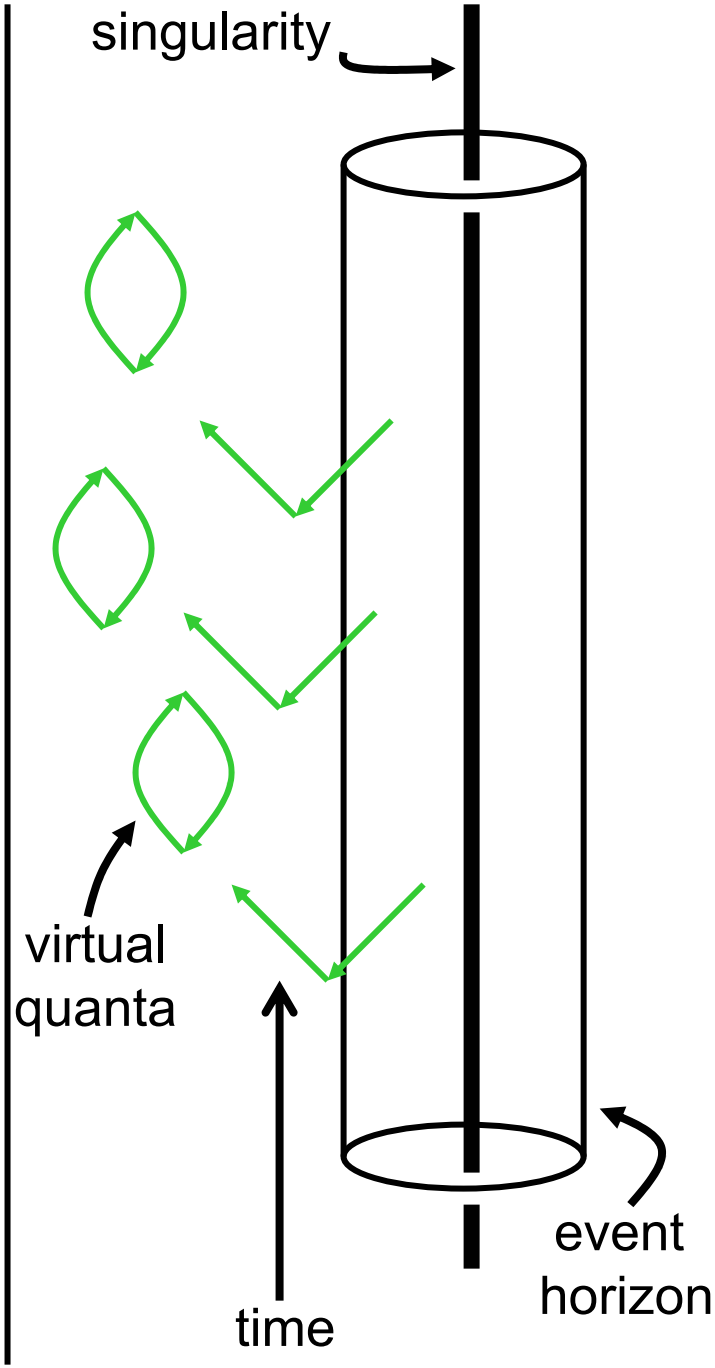
Classically, nothing can escape from a black hole, but quantumly, black holes *radiate*.

Quantum fluctuations in the vacuum continually create pairs of virtual particles, which then reannihilate. But if one member of the pair ducks behind the event horizon, the other escapes.

To an observer far away, the black hole seems to be a source of featureless thermal radiation with wavelength comparable to the black hole radius:

$$k_B T_{\text{black hole}} = \hbar c / 4\pi R_{\text{black hole}}$$

Since the radiation really arises from quantum fluctuations just outside the horizon, its properties don't depend on how the black hole was formed.



Black hole entropy

Integrating $TdS = dE$, we find from

$$k_B T_{\text{black hole}} = \hbar c / 4\pi R_{\text{black hole}}$$

and

$$E = Mc^2 = \left(c^4 / 2G\right) R_{\text{black hole}}$$

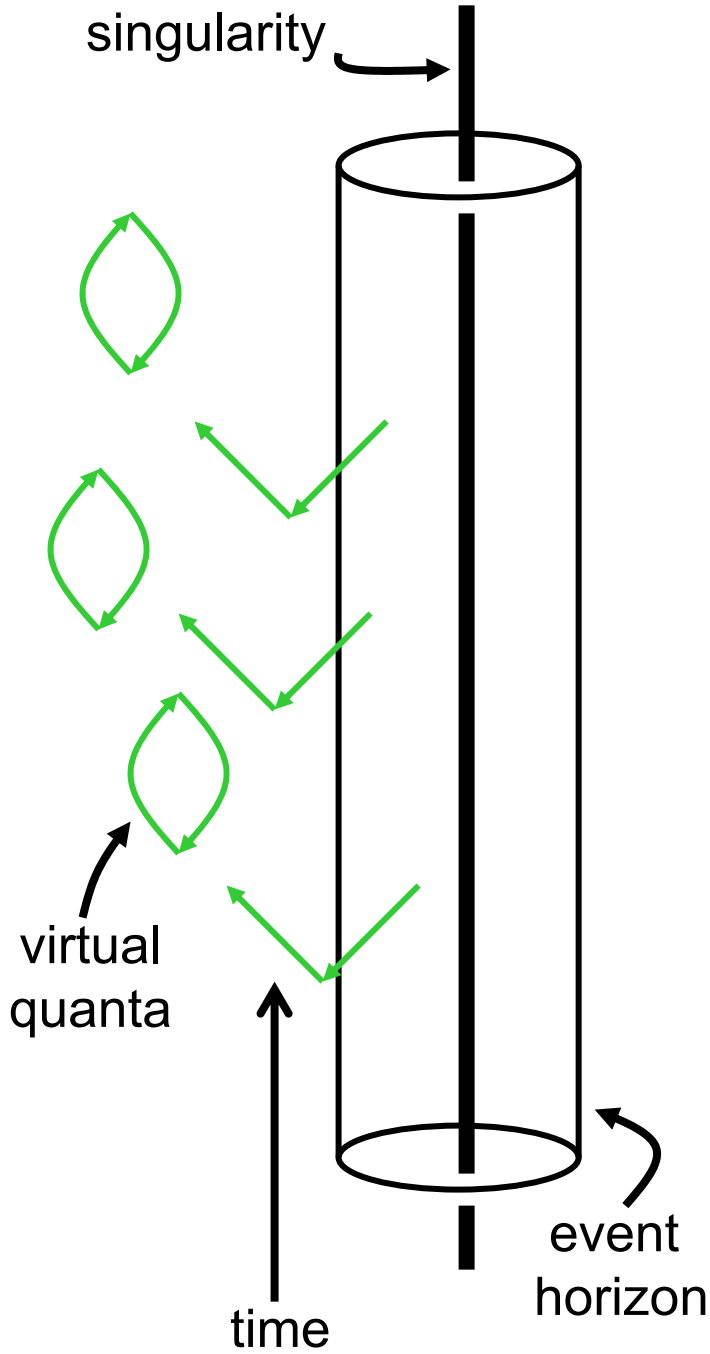
that

$$S_{\text{black hole}} = \frac{1}{4} \frac{Area}{L^2_{\text{Planck}}}$$

where

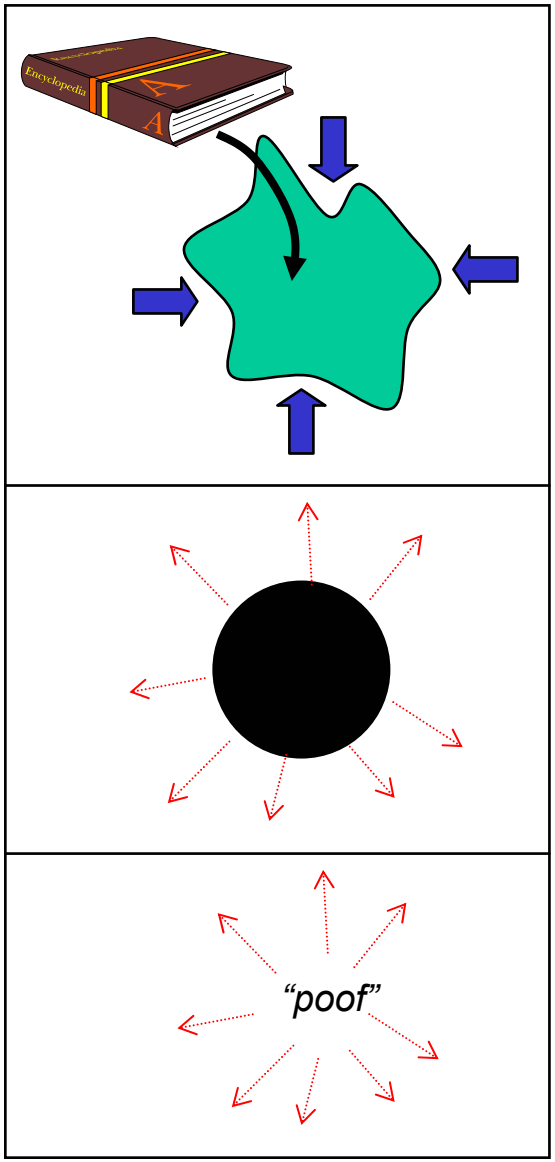
$$L_{\text{Planck}} = \left(\hbar G / c^3\right)^{1/2} = 10^{-33}\,\text{cm}$$

Strangely, black holes seem to be both very simple (have no hair), and yet also very complex (have enormous entropy, e.g., 10^{78} for a solar mass).



Black hole evaporation

Suppose we prepare a quantum state, encoding some information, as pressureless dust on the brink of gravitational collapse.



It collapses, and begins to emit Hawking radiation. This radiation is featureless, not dependent on the information encoded in original collapsing body.

Eventually, all the mass is radiated away, and the black hole disappears. What happened to the information?

Other hot bodies emit thermal radiation. Such processes are *thermodynamically* irreversible but not *microscopically* irreversible.

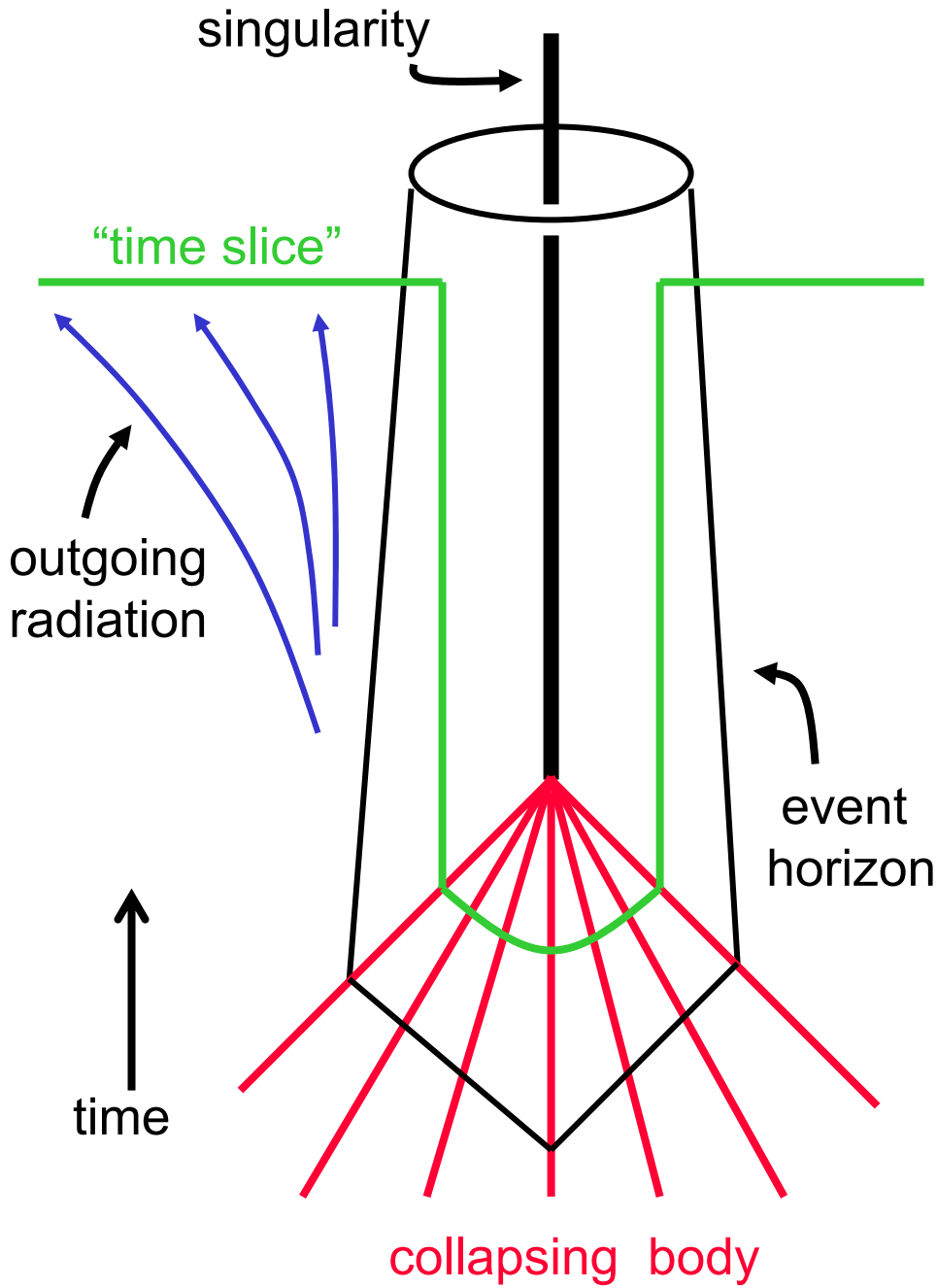
But a black hole is different than other hot bodies, because it has an event horizon. Does that mean that this process is microscopically irreversible, that the information is lost not just in practice but in principle?

Black hole: a quantum cloning machine?

Suppose that the information about the collapsing body is subtly encoded in correlations among the quanta in the Hawking radiation; the information is *thermalized*, not destroyed.

The green time slice crosses both the collapsing body behind the horizon and the radiation outside the horizon. *Thus the same information is in two places at the same time.*

A quantum cloning machine has operated, which is not allowed by the linearity of quantum mechanics.



Information loss PARADOX!

Hawking

General relativity, and quantum field theory on curved spacetime, lead to a violation of the principles of quantum theory ….

Accept that evolution need not be unitary?

- On what new foundations should physics stand?
- Information loss is highly *infectious*. Can we accommodate a little bit of information loss, and still understand the successes of quantum theory in ordinary processes?

Revise our notion of locality in spacetime?

- How should spacetime be described in a quantum theory of gravity?
- If the evaporation of a black hole involves a violation of our notion of locality, how do we explain the successes of relativistic causality in ordinary processes?

Whereas Stephen Hawking and Kip Thorne firmly believe that information swallowed by a black hole is forever hidden from the outside universe, and can never be revealed even as the black hole evaporates and completely disappears,

And whereas John Preskill firmly believes that a mechanism for the information to be released by the evaporating black hole must and will be found in the correct theory of quantum gravity,

Therefore Preskill offers, and Hawking/Thorne accept, a wager that:

When an initial pure quantum state undergoes gravitational collapse to form a black hole, the final state at the end of black hole evaporation will always be a pure quantum state.

The loser(s) will reward the winner(s) with an encyclopedia of the winner's choice, from which information can be recovered at will.

Stephen W. Hawking, Kip S. Thorne, John P. Preskill
Pasadena, California, 6 February 1997

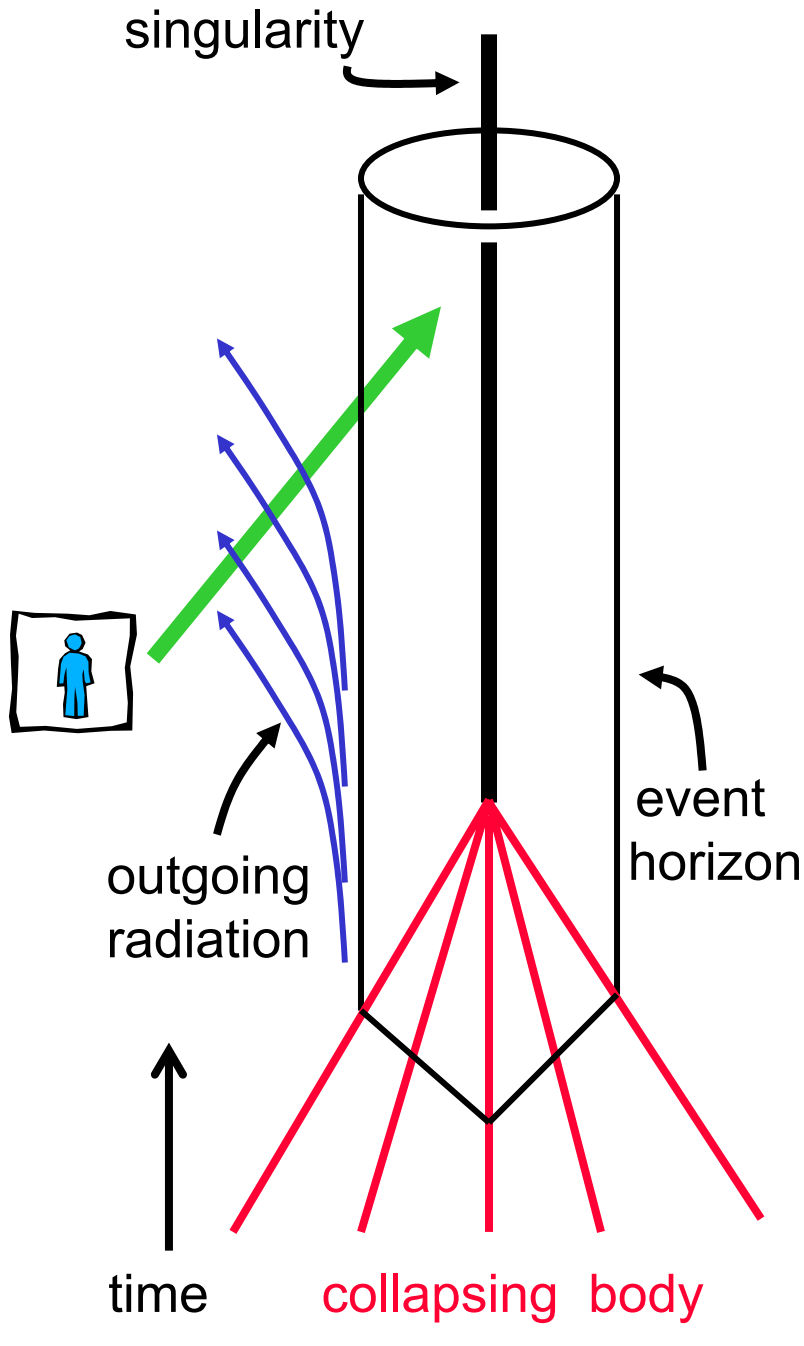
Black hole complementarity

An observer who reads the outgoing radiation concludes that the information must be erased as the collapsing body crosses the event horizon.

A freely falling observer who follows the collapsing body across the horizon knows otherwise.

But they can never compare notes…

Perhaps it is okay for quantum information to be copied, if no one can ever find out!



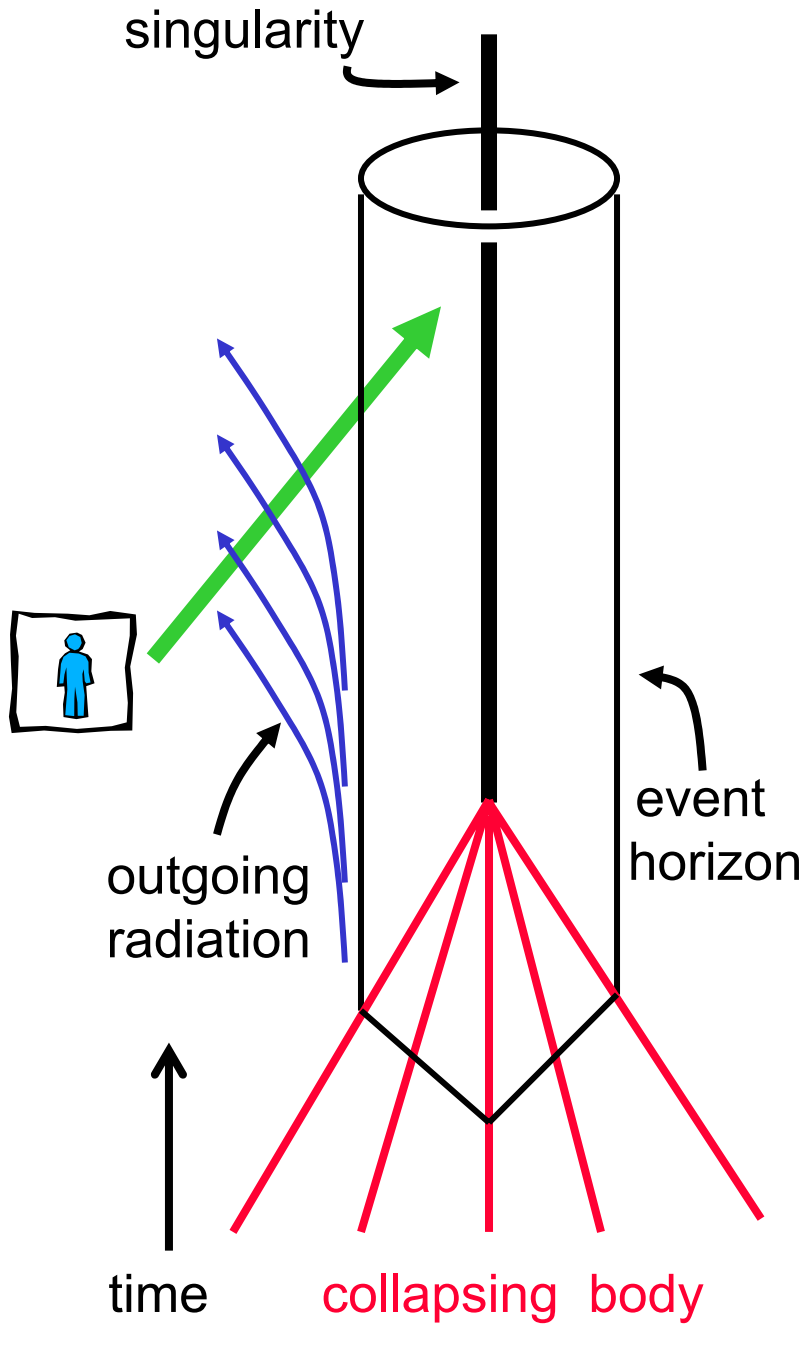
Black hole complementarity

The difficulty is reconciling the viewpoints of the two observers, so let's not even try. We'll be satisfied to find a consistent way for the "outside observer" to interpret what is happening.

From this viewpoint, since time "freezes" at the event horizon, the outgoing radiation seems to originate as modes of arbitrarily short wavelength stuck to the horizon. These carry no information.

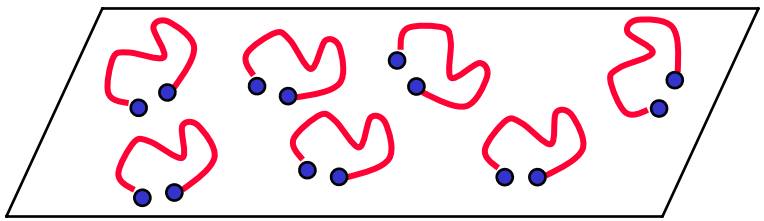
Perhaps in the *right* theory of quantum gravity, the amount of information stuck to the horizon is limited by the black hole entropy:

$$S_{\text{black hole}} = \frac{1}{4}\frac{Area}{L^2_{\text{Planck}}}$$



Counting states

There is a compelling candidate, still far from completely understood, for a quantum theory of gravity. In this theory, the fundamental dynamical objects are not (only) pointlike particles, but extended objects of various dimensionalities. Formerly know as *string theory*, it is now often called *M theory* [*M* = mystery, mother, membrane, matrix, …] to emphasize that strings are not the only fundamental entiities.

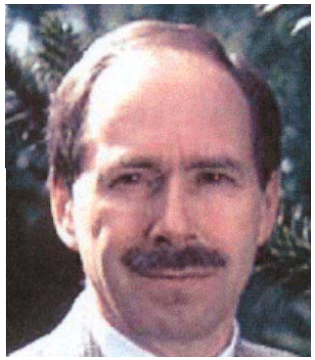


D-brane

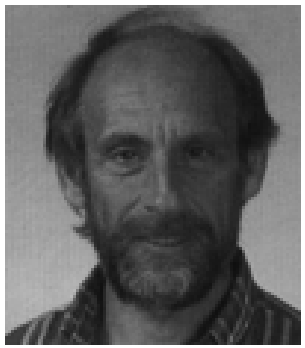
$$S_{\text{D-brane}} = \frac{1}{4}\frac{Area}{L^2_{\text{Planck}}}$$

Among the extended objects are *D-branes*, on which open strings can terminate. A *D*-brane provides a string-theoretic description of a black hole horizon, and its microscopic states can be counted. The state counting, in cases that can be analyzed, is consistent with the known black hole entropy.

The holographic principle

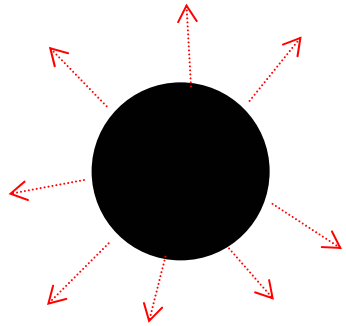


't Hooft



Susskind

The idea that information about a collapsing body can be stored at the event horizon may be a manifestation of a more general principle, for which there is growing evidence in *M* theory:



black hole

Information encoded in a region can, at least in principle, be read at the boundary of the region (the *holographic principle*).

The black hole entropy, proportional to the *area* of the boundary, is the maximum amount of information that can be stored.

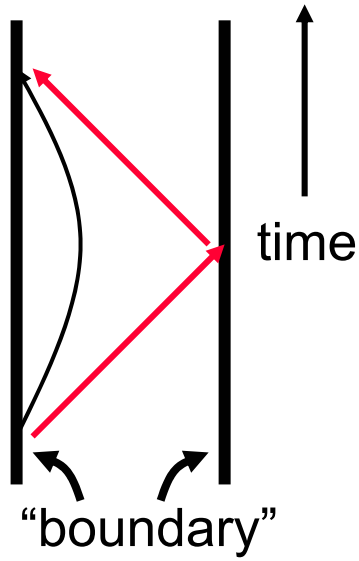
$$S = \frac{1}{4}\frac{Area}{L^2_{\text{Planck}}}$$

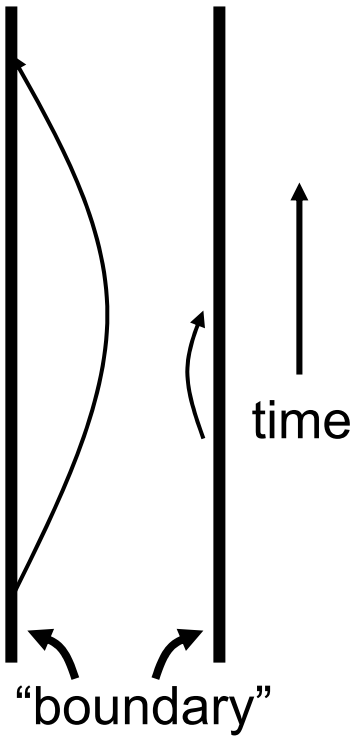
In a conventional quantum field theory, the number of degrees of freedom in a region is proportional to its *volume*. This counting seems to be profoundly *wrong*, an important hint that locality as realized in quantum field theory will not be a feature of a complete theory of Nature.

Maldacena

AdS-CFT Correspondence

Anti-de Sitter (AdS) space is a spacetime of constant negative curvature. Although the spatial slices are infinite, the spacetime has a boundary in the sense that light rays can reach infinity and return in a finite proper time.



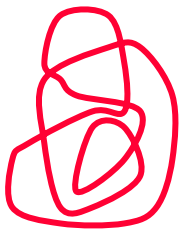


There is convincing evidence that string theory on five-dimensional AdS space can be described *exactly* using a (conformal) field theory (CFT) defined on the boundary of the spacetime --- a holographic description!

Furthermore, the AdS-CFT correspondence involves a remarkable *ultraviolet/infrared connection*: short distances on the "boundary" correspond to long distance in the "bulk". (Timelike geodesics that probe deeply into the bulk connect points that are far apart on the boundary.

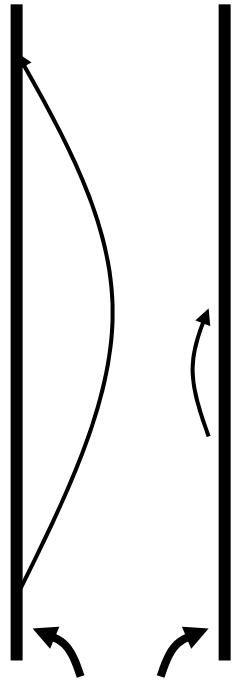
Ultraviolet-infrared connection

lower res



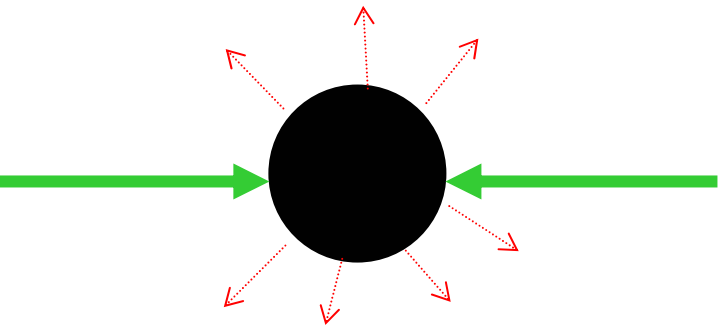
higher res

The ultraviolet/infrared connection has other manifestations in quantum gravity. For example, as we probe a string with better and better time resolution, the string seems to grow *longer*, because higher freqency modes contribute to its fluctuations.



"boundary"

And while in field theory, higher and higher energy collisions normally probe shorter and shorter distances, a sufficiently high energy collision produces a large black hole, which emits low energy quanta.



black hole

These unusual features provide further evidence that locality has a different status in quantum gravity than in quantum field theory.

What *is M* theory?

A general formulation of the theory is still elusive...

In one proposal (the matrix model), the theory is formulated in terms of very large (*N* X *N*) matrices X^a. The matrices (one for each space dimension, a=1,2,..,D-1) represent the positions of *N* pointlike objects called D0-branes.

$$H = \sum_{a=1}^{D-1} \sum_{i,j=1}^{N} \left(p_{ij}^{a} \right)^2 + \sum_{a,b=1}^{D-1} \sum_{i,j=1}^{N} \left(\left[X^a, X^b \right]_{ij} \right)^2 + \cdots$$

At low energies, the matrices all commute; their eigenvalues behave like normal spatial coordinates. Thus ordinary spacetime is an emergent concept in this model. But in the regime where quantum fluctuations in spacetime are strong, the full matrix structure (*noncommutative geometry*) must be retained…

Can a quantum computer simulate *M* theory efficiently? Perhaps not, because of M theory's inherent *nonlocality. E.g,* a quantum system described by *M* theory may have no natural tensor product decomposition into smaller systems. Thus, M theory may be a more powerful computational model!

What can the study of *quantum* computation and quantum information tell us about ***physics***?

- "Dreams of a final theory." Can computational approaches help us to answer "What is M theory?" How would we simulate M theory? Is M theory more powerful than quantum field theory? Is physics *computable*?

- "More is different." What are the robust properties of phases of matter? Can *quantum coding theory* illuminate this issue?

- "How come the quantum?" What *deformations* of quantum theory make sense? Can ideas about quantum error correction help us to understand why information loss (if it occurs) is not evident at low energies. Is quantum mechanics *attractive in the infrared limit*?