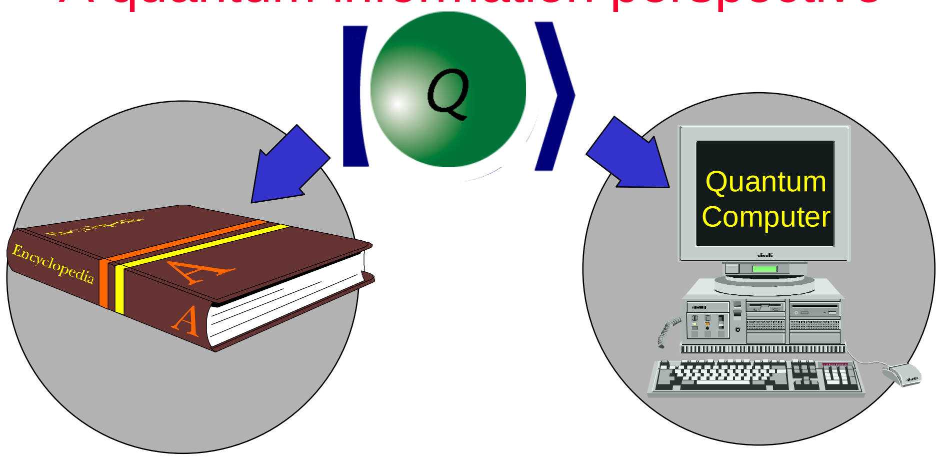
How more is different: A quantum information perspective



Institute for Quantum Information

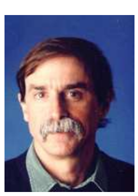
Sponsored by the NSF

John Preskill, Caltech
23 May 2003
http://www.iqi.caltech.edu/

Quantum Achievements


Shor


Bennett


Wineland

- Algorithms: polynomial-time factoring algorithm, based on the fast quantum Fourier transform.
- Cryptography: unconditionally secure quantum key distribution.
- Error correction: robust quantum computation, overcoming the pervasive effects of decoherence.
- Hardware: working prototypes for quantum key distribution; coherent quantum gates in small-scale devices.

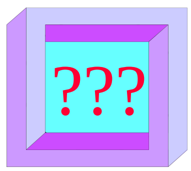
Quantum Challenges


Hallgren


Gottesman


Kitaev

- Algorithms: exponential speedups beyond the abelian hidden subgroup problem.
- Cryptography: quantum enhancements of other cryptographic tasks.
- Error correction: *physically* robust quantum memory.
- Hardware: toward scalable devices.

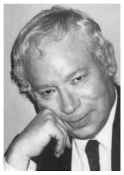


Theoretical Quantum Information Science

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?

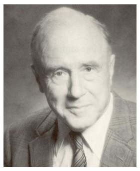


Weinberg

• “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?)

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 computationally more powerful than quantum field theory? Is physics *computable*?

• “More is different.” What are the robust universal properties of phases of matter? Can there be a “final theory” of condensed matter? Are there a finite number of classes of collective quantum phenomenon that can be explored with reasonable resources?

• “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*?

Themes of quantum information science

1) Quantum Computation
2) Quantum Cryptography
3) Quantum Entanglement
4) Quantum Error Correction
5) Quantum Hardware

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

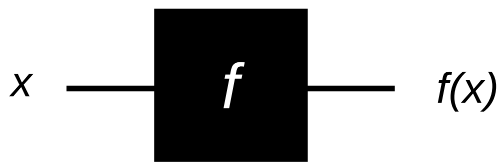
×

4553449864673
5972188403686
8972744088643
5630126320506
9600999044599


Shor ‘94

Black Box model (= oracle model)

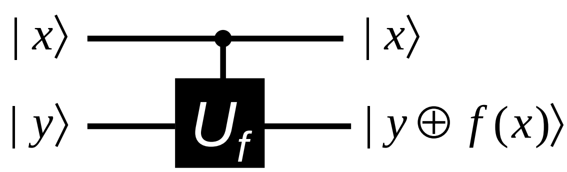
The black box computes a function



Our task is to determine what the box is doing, as efficiently as possible. The “black box complexity’’ (or “oracle complexity’’) of the problem is the minimum number of “queries’’ to the box that will allow us to determine the function (or some property of the function).

Quantum Black Box model

The black box performs a unitary transformation



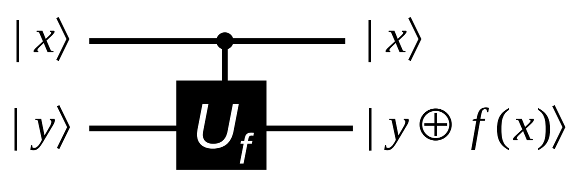
Again, we want to find *f.* We can submit to the box either classical queries (computational basis states $|x, y\rangle$) or quantum queries (general states). Claim: with quantum queries, in some cases we can solve the problem with an *exponential speedup* relative to what can be achieved with only classical queries.

Hidden subgroup problem

The function $f: G \rightarrow X$
is *constant and distinct* on the cosets of the subgroup $H \subseteq G$.

The problem is to find the generator(s) of the "hidden subgroup" H. This problem is hard (classically) if the number of cosets is exponentially large.

Claim: the hidden subgroup problem can be solved efficiently in the quantum black box model for any finitely generated abelian group G (e.g., in time polylog($|G/H|$).



Hidden subgroup problem

Claim: the hidden subgroup problem can be solved efficiently in the quantum black box model for any finitely generated abelian group G.

This is so because the quantum Fourier transform can be implemented efficiently (time polylog($|G|$) on a quantum computer. Hence:

$$|0\rangle \otimes |0\rangle \xrightarrow{F.T.} \sum_{x \in G} |x\rangle \otimes |0\rangle \xrightarrow{f} \sum_{x \in G} |x\rangle \otimes |f(x)\rangle$$

$$\xrightarrow{\text{measure}} \sum_{x \in H} |x + x_0\rangle \otimes |f(x_0)\rangle \xrightarrow{F.T.^{-1}} \sum_{y \in H^{\perp}} (phase)|y\rangle$$

We determine the group H by finding its *dual* (or reciprocal) group $H^{\perp}$.

Hidden subgroup problem

Example: finding the period of a function $f:\mathbf{Z}\to\mathbf{Z}$
Then:

$$f(x+r)=f(x) \quad \text{or} \quad H=r\mathbf{Z}\subseteq G=\mathbf{Z}.$$

This is the problem solved by Shor ('94) which is related to the factoring problem by a number-theoretic classical reduction.

(We can't really Fourier transform over $\mathbf{Z}$, but it suffices to consider $\mathbf{Z}/n\mathbf{Z}$ for $n=\text{poly}(r)$.)

Most known cases in which a quantum computer achieves an exponential speedup relative to a classical computer involve using the quantum Fourier transform to solve a (finitely-generated) abelian hidden subgroup problem.

Quantum algorithm for Pell's equation

Hallgren

What are the integer solutions *(x,y)* to:

$$x^2 - d\,y^2 = 1$$

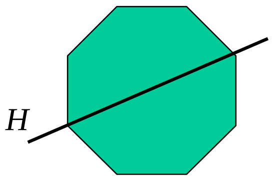
where *d* is an integer that is not a perfect square?

This problem has been studied for over 1000 years, and seems to be more difficult than factoring, in that the best known classical algorithm for Pell's equation is exponentially slower than the best known classical algorithm for factoring: $O(\exp(\log d)^{1/2})$). Sean Hallgren's (2002) quantum algorithm solves it in time O(polylog *d*), breaking a proposed cryptosystem based on the presumed hardness of solving Pell's equation.

Hallgren's algorithm extends the solution of the hidden subgroup problem to an abelian group that is not finitely generated (finding an irrational period of a function on real numbers).

Dihedral Hidden Subgroup Problem

Kuperberg '03



The hidden subgroup is a two element group *H*, generated by a reflection, of the dihedral group D_N, where $N=2^n$. There are many such subgroups, related by conjugation, that are hard to distinguish.

There are two one-dimensional irreps that can reveal a bit of information about the "slope" of the subgroup *H*. These are very unlikely to occur when we measure after doing the Fourier transform. But we can fuse two two-dimensional irreps…

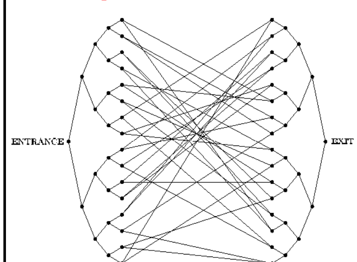
$$V_k \otimes V_l = V_{k+l} \oplus V_{k-l}$$

and "steer" the outcome toward the irreps that provide useful information.

The speedup is from the classical time $2^{O(n)}$ to quantum time $2^{O(\sqrt{n})}$. Can it be improved to *Poly(n)* ?

Finding the shortest vector on a lattice (a problem with cryptographic applications) can be reduced to solving the dihedral hidden subgroup problem.

Exponential speedup by quantum walk



Childs, Cleve, Deotto, Farhi, Gutmann & Spielman '02

Two trees are connected with a random cycle. There are 2^n nodes, labeled with randomly assigned $2n$-bit strings. If queried with a valid name of a node, the oracle responds with the names of the adjacent nodes. The label of the entrance is given. The problem is to find the name of the exit.

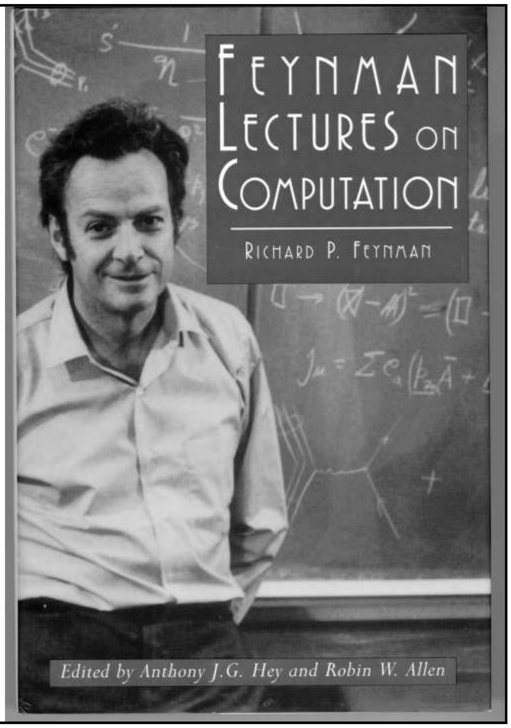
Classically, this problem is hard. (Classical diffusion carries you to the center, away from the exit.)

Quantumly, the oracle is an operator that can be invoked to simulate a Hamiltonian that couples adjacent sites. A uniform superposition of all nodes in a column is preserved by the Schrödinger evolution. The exit (but not a path through the graph). can be found efficiently

Random walks on graphs have many applications in classical algorithms, and this example shows that quantum walks can enhance computational power. But are there less contrived problems with such speedups?

"The rule of simulation that I would like to have is that the number of computer elements required to simulate a large physical system is only proportional to the space-time volume of the physical system"

R. P. Feynman, "Simulating Physics with Computers" (1981).



Simulation of a quantum phase transition:
a tunable and nearly perfect (optical) lattice!

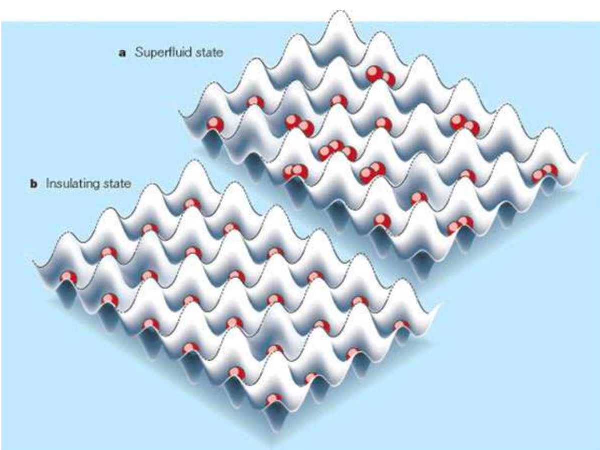


Figure 1 A quantum phase transition in an ultracold gas. By using a web of laser beams to create an energy landscape of mountains and valleys (an optical lattice), Greiner *et al.*[1] can reversibly switch a gas of rubidium atoms from a superfluid to an insulating phase. **a,** At a temperature of 10 nanokelvin or less the rubidium atoms share the same quantum state and are in a superfluid phase, in which they can move freely between valleys. **b,** By increasing the intensity of the laser beams in the optical lattice, the researchers force the gas into an insulating phase, in which each atom is trapped in an individual valley. Such control is vital to most proposals for building a quantum computer.

Jaksch

Zoller

M. Greiner, O. Mandel, T. Esslinger, T. W. Hänsch, and I. Block, "Quantum phase transition from a superfluid to a Mott insulator in a gas of ultracold atoms," *Nature* 415, 39-44 (2002).

Simulation of a quantum phase transition:
a tunable and nearly perfect (optical) lattice!

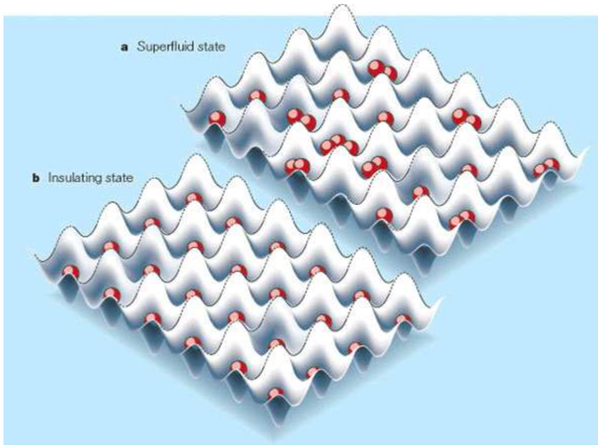


Figure 1 A quantum phase transition in an ultracold gas. By using a web of laser beams to create an energy landscape of mountains and valleys (an optical lattice), Greiner *et al.*[1] can reversibly switch a gas of rubidium atoms from a superfluid to an insulating phase. **a**, At a temperature of 10 nanokelvin or less the rubidium atoms share the same quantum state and are in a superfluid phase, in which they can move freely between valleys. **b**, By increasing the intensity of the laser beams in the optical lattice, the researchers force the gas into an insulating phase, in which each atom is trapped in an individual valley. Such control is vital to most proposals for building a quantum computer.

The quantum computer can be an important tool for investigating the properties of quantum many-body systems and exotic materials.

Adiabatic Quantum Computation

Farhi, Gutman, Goldstone & Sipser (2000) ..

An NP-hard problem: Find the ground state of an Ising spin glass on a three-dimensional cubic lattice.

$$H_{\text{problem}} = -\sum_{\langle ij\rangle} J_{ij}\sigma_i\sigma_j\ , \quad \sigma_i = \pm 1$$

An "instance" of the problem is specified by

$$\{J_{ij}\}, \quad J_{ij} = \begin{cases} +1 & \text{(ferromagnetic)} \\ -1 & \text{(antiferromag)} \end{cases}$$

Geometrically, domain walls terminate at frustrated 1-cycles; the ground state is a 2-surface of minimal area with a specified 1-dimensional boundary.

Can we find the ground state by simulated annealing? Unfortunately, there are many local minima of the energy for typical hard instances, so the equilibration time is exponentially long...

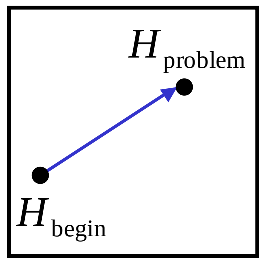
Adiabatic Quantum Computation

Perhaps a quantum algorithm can "tunnel" through barriers to find the global minimum more efficiently than a classical search. For example, we can find the ground state via adiabatic evolution:

$$i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle , \quad H(t) = \tilde{H}(t/T) ,$$

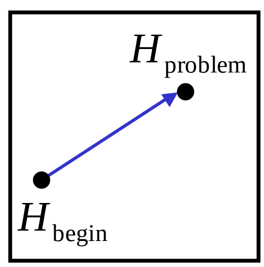
$$\tilde{H}(s) = (1-s)H_{\text{begin}} + s H_{\text{problem}} , \quad s \in [0,1] .$$

The beginning Hamiltonian could be a large magnetic field pointing in the transverse (x) direction, with a simple ground state. If the "run time" T is long enough, the system remains in the ground state with high probability, and we can read out the Ising ground state by measuring all spins along the z-axis.



Adiabatic Quantum Computation

The run time T is determined by the *minimum gap* Δ encountered as the Hamiltonian varies between H_{begin} and H_{problem}: the probability of successfully finding the ground state is appreciable provided that…



$$T \; ? \; \frac{\left\| \frac{d}{ds} H(s) \right\|_{\max}}{\Delta^2} \quad \text{where} \quad \Delta = \min_{s\in[0,1]} \left(E_1(s) - E_0(s) \right)$$

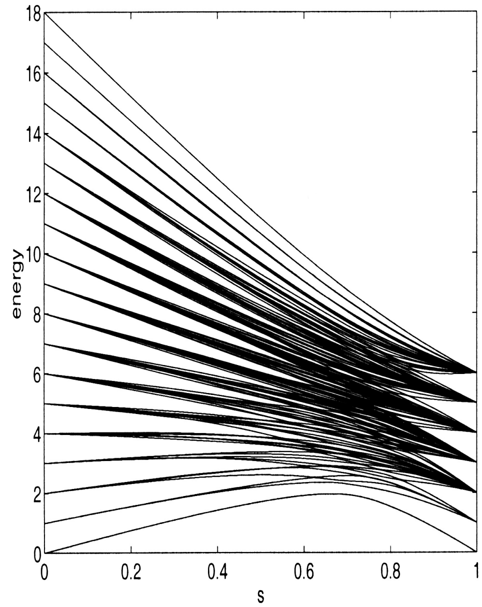
Thus, if $\Delta > 1/\text{poly}(n)$ then the adiabatic algorithm is efficient,

while if $\Delta < \exp\left(-cn\right)$ then it is inefficient.

Note that Hamiltonian evolution can be simulated efficiently on a "garden variety" quantum computer, so if the quantum adiabatic algorithm works, we can run it on any quantum computer.

Adiabatic Quantum Computation

An H_{problem} that encodes the solution to an NP-complete satisfiability problem (“exact cover”) has been studied by Farhi *et al*. For input size up to ~10 bits, $H(s)$ can be diagonalized numerically. Although typical spacings in the spectrum become very small for intermediate values of s, the gap between ground and first excited states remains large for all s.

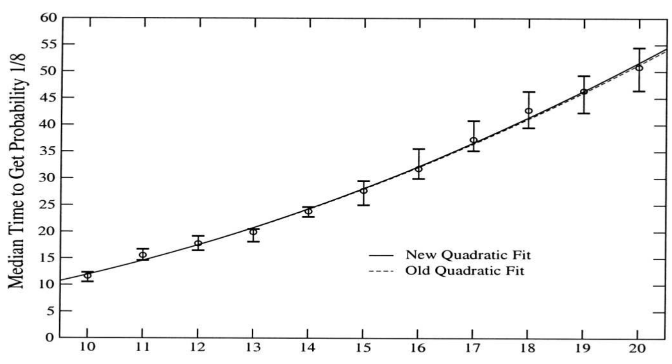


Adiabatic Quantum Computation

For input size up to n=20 bits, the Schrödinger equation with

$$H(t) = (1 - t/T)\,H_{\text{begin}} + \left(t/T\right)H_{\text{problem}}$$

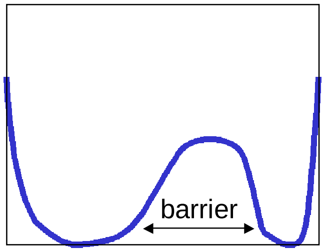
has been integrated numerically. The time T needed to find the ground state with fixed success probability in typical “hard instances” (where the ground state is unique) seems to rise quadratically with the input size:



Adiabatic Quantum Computation

Analytically, van Dam *et al.* (2002) have observed that there are particular types of problem Hamiltonians (*high-valence* formulas in which all triplets of bits are coupled together) for which the gap *does* become exponentially small.

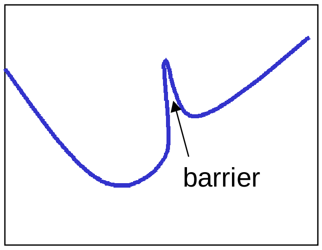
The small gap arises because there is a classical degeneracy, and the classical ground states are separated by a large barrier.



It is not clear whether this behavior is a generic feature when minimizing the problem Hamiltonian is hard classically. Might the quantum adiabatic algorithm be able to solve the *typical hard instances* of NP-complete problems?

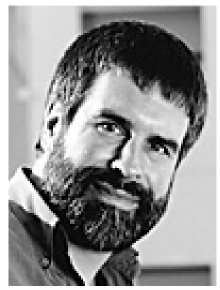
Adiabatic Quantum Computation

In some cases, a potential barrier that would foil e.g. simulated annealing can be easily penetrated by quantum tunneling. The adiabatic algorithm is harder to tool than a local classical search.



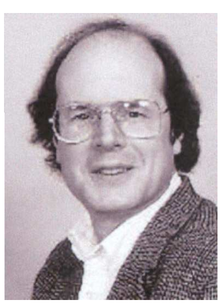
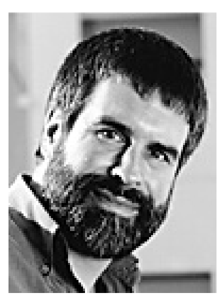
Recently, Aharonov, van Dam, Kempe, Landau, Lloyd & Regev (2003) have announced that adiabatic evolution with a local Hamiltonian is as powerful as the standard model of quantum computation (nearest-neighbor interactions in two dimensions among five-dimensional particles). Thus, in a sense the study of the power of quantum computing has been reduced to the study of spectral gaps!

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

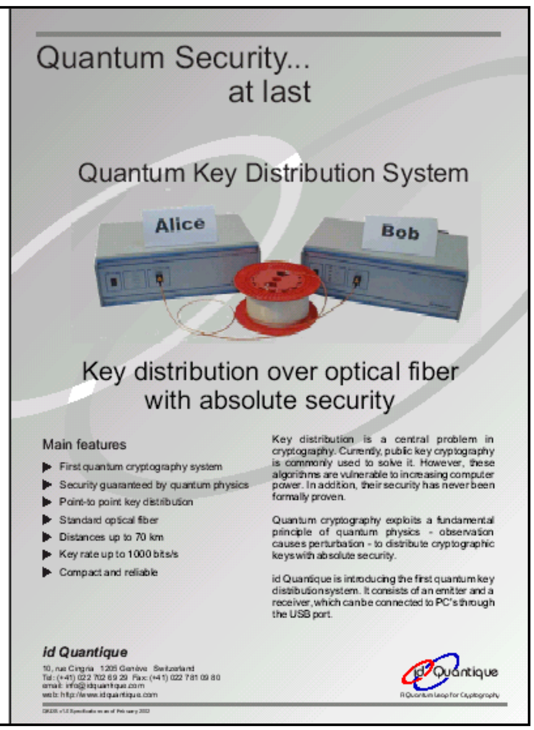
Eve

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.

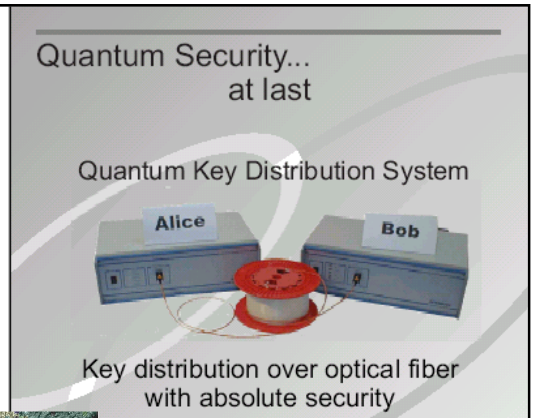
QKD for sale!

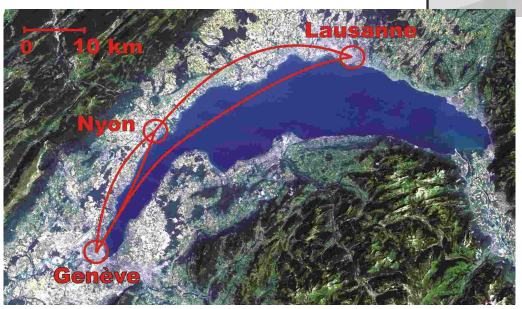
"Plug and play" quantum key distribution is *commercially available*:



QKD for sale!

"Plug and play" quantum key distribution is *commercially available*:

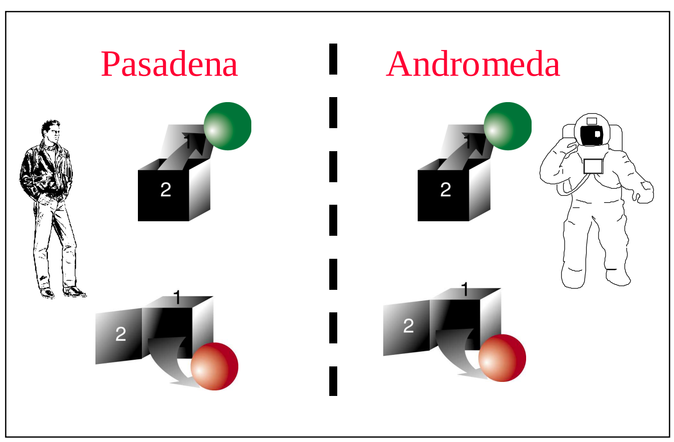




BB84 QKD has been achieved through a 67 km optical fiber under Lake Geneva.

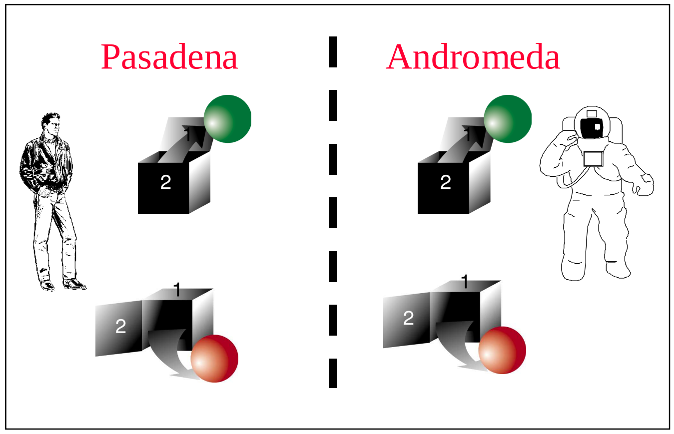
Quantum Entanglement

Bell '64



Quantum information can be *nonlocal*; quantum correlations are a stronger resource than classical correlations.

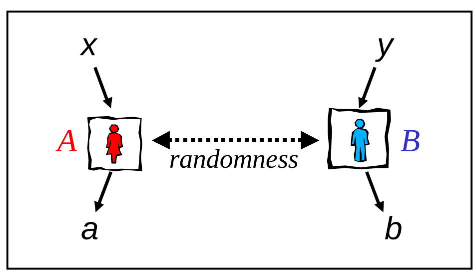
Bell '64



Quantum entanglement

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*).

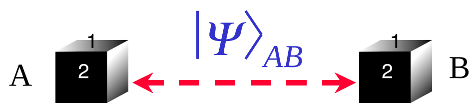
But if Alice and Bob share an *entangled* pair of quantum bits ("qubits"), then

$$P_{\text{success}} = \frac{1}{2} + \frac{1}{2\sqrt{2}} = .854$$ is achievable.

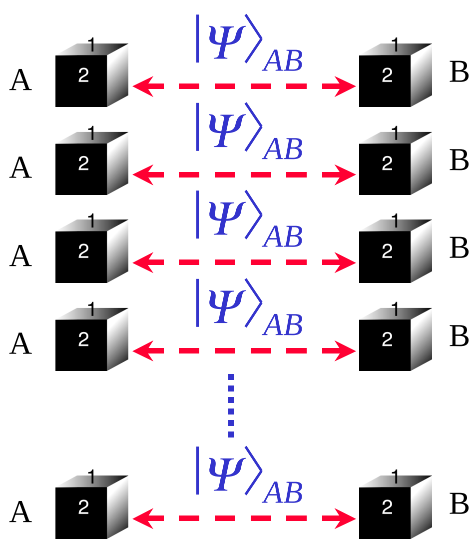
Bipartite Pure-State Entanglement

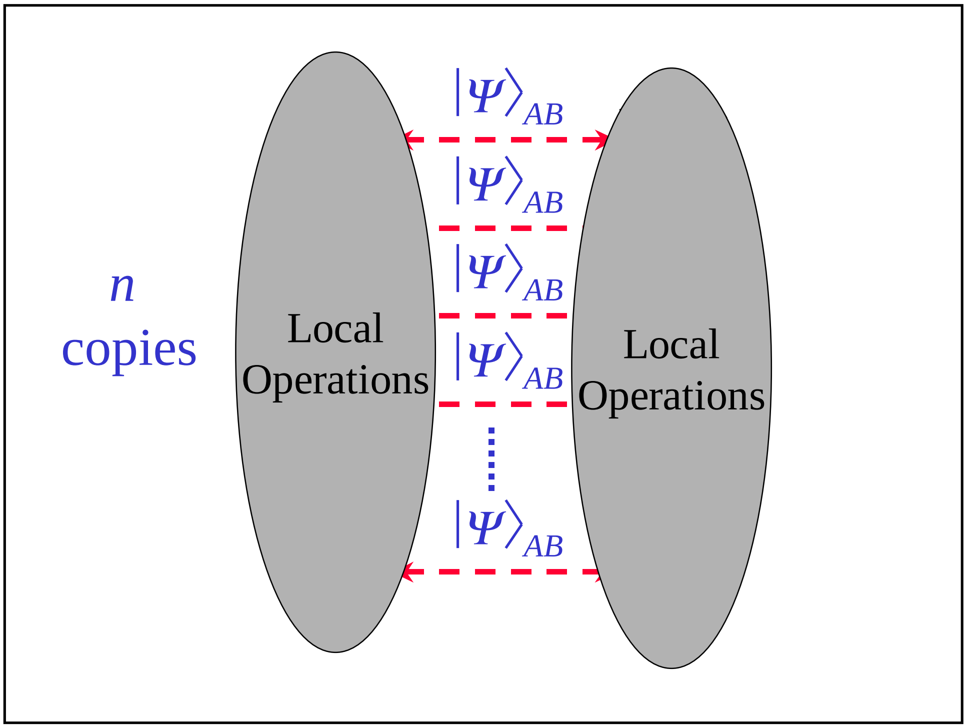
How to characterize it and quantify it, for *pure* states.

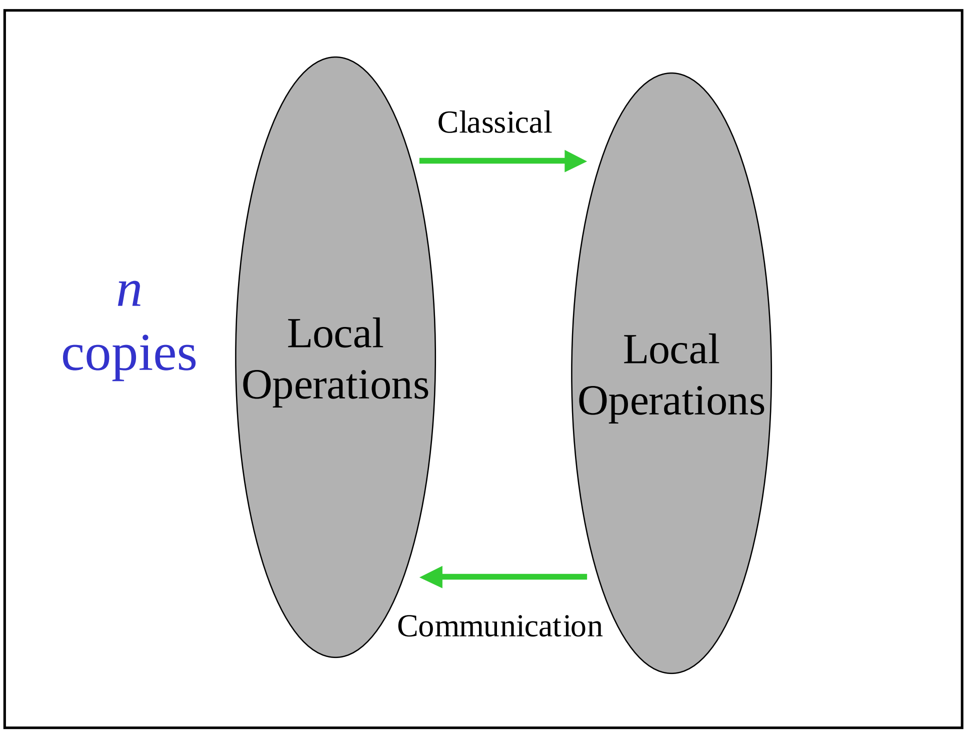
Cf., two qubits:



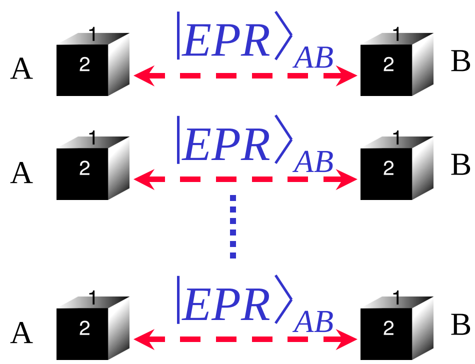
n
copies




$|\Psi\rangle_{AB}$
$|\Psi\rangle_{AB}$
$|\Psi\rangle_{AB}$
$|\Psi\rangle_{AB}$
$|\Psi\rangle_{AB}$
n copies
Local Operations
Local Operations


n copies
Local Operations
Local Operations
Classical
Communication

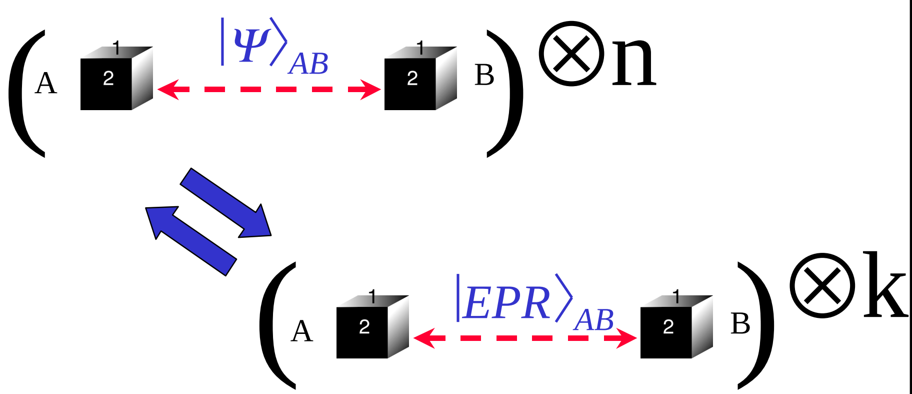
$k_{\max}$ copies $(k_{\max} \leq n)$



$$\left(|EPR\rangle = \left(|00\rangle - |11\rangle \right) / \sqrt{2} \right)$$

$$D = \lim_{n\to\infty} \left(\frac{k_{\max}}{n} \right) = S(\rho_A)\,, \quad S(\rho) = -tr\,\rho \log_2 \rho$$

Bennett, *et al*.... '95



Two party pure-state entanglement can be converted to a standard currency (EPR pairs) … *and* back again.

$$E = \lim_{n\to\infty} \left(\frac{k_{\min}}{n} \right) = S(\rho_A)\,, \quad S(\rho) = -tr\,\rho \log_2 \rho$$

Mixed state quantum entanglement

A separable state can be prepared by two distantly separated parties who perform *local operations and classical communication (LOCC)*:

Werner

$$\rho = \sum_i p_i \left(|\alpha_i\rangle\langle\alpha_i|\right)_A \otimes \left(|\beta_i\rangle\langle\beta_i|\right)_B$$

An *inseparable* state is entangled. Entangled pure states always violate Bell inequalities, but entangled mixed states sometimes admit a local hidden variable description. For example, the two-qubit state

$$\rho = F\,(\text{singlet}) + (1-F)\,(\text{uniform triplet})$$

is entangled for $F > ½$, but it is Bell-inequality violating only for $F > 5/8$ (Werner '89).

Quantifying mixed state quantum entanglement

Bennett, DiVincenzo, Smolin, Wootters '96

As with pure states, we can quantify the entanglement of a bipartite mixed state ρ in terms of the minimal asymptotic *cost* in Bell pairs needed to make a copy of ρ :

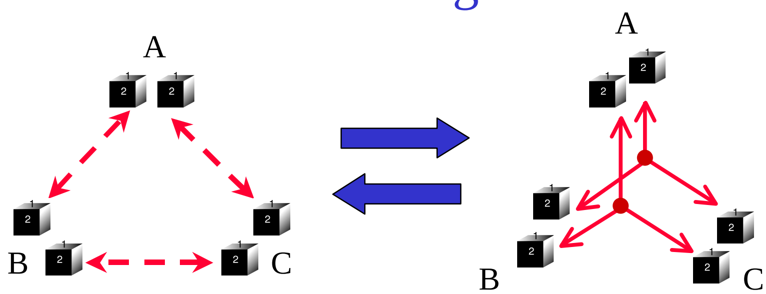
$$\text{entanglement cost: } E(\rho) \equiv \lim_{n\to\infty} \frac{k_{\min}}{n}$$

An alternative measure is the maximal number of Bells pairs that can be *distilled* asymptotically from each copy of ρ :

$$\text{distillable entanglement: } D(\rho) \equiv \lim_{n\to\infty} \frac{k_{\max}}{n}$$

For pure states *E=D*, but for some mixed states $E > D$ (asymptotic irreversibility of entanglement transformations). This is not surprising (information is discarded during the preparation of the state), but it was surprisingly difficult to prove (Vidal & Cirac '02). There are even states with *D=0* and $E > 0$ (bound entanglement, Horodecki '97). Although bound entanglement is not distillable, it may not be useless …

What about 3 (or more) part pure-state entanglement?



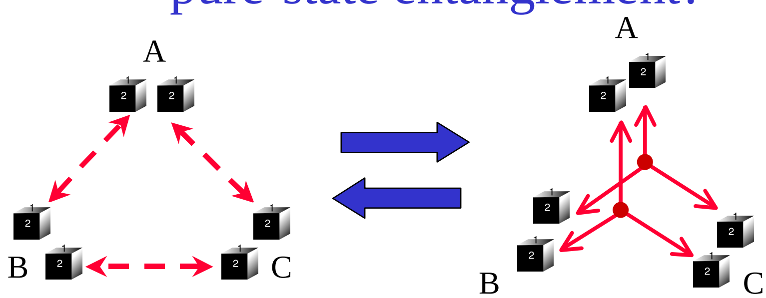
3 EPR pairs

$$|\phi^+\rangle = (\,|00\rangle - |11\rangle\,)/\sqrt{2}$$

2 “cat” (GHZ) states

$$|\psi\rangle = (\,|000\rangle - |111\rangle\,)/\sqrt{2}$$

But what about 3 (or more) part pure-state entanglement?



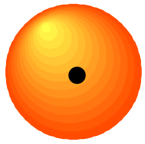
3 EPR pairs

2 “cat” (GHZ) states

These are not (asymptotically) interchangeable (Linden et al. ’00)
Furthermore, EPR and GHZ states alone do not suffice for reversible generation of other three-party pure states (Acin et al. ’02).

True *n*-particle entanglement exists for all *n*.

The separable ball



Gurvits & Barnum ‘03

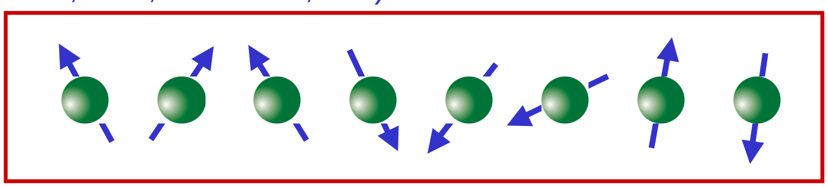
For a state of *m* systems, each with dimension *d*, how large is the maximal ball of separable states centered at the uniform density operator?

The “pseudo-pure state” $$(1-\varepsilon)\frac{I}{d^m}+\varepsilon(pure)$$

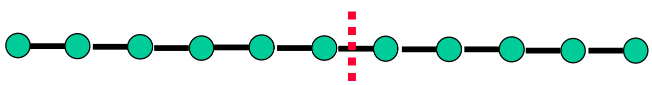
is separable for $\varepsilon \leq 2^{-(m/2-1)}/d^m$

Thus, pseudo-pure states prepared using room-temperature liquid-state NMR are separable for $m < 23$ qubits.

How “quantum” is NMR quantum information processing (Caves, Knill, Laflamme, etc.)?



Efficient classical simulation of quantum systems with bounded entanglement



Vidal

Consider the quantum state of *n* qubits, expanded in the standard basis:

$$|\psi\rangle = \sum_{i_i \ldots i_n} c_{i_1 \ldots i_n} |i_1 \ldots i_n\rangle$$

There are 2^n terms. But suppose the Schmidt rank is less than χ for all ways of dividing the system into two parts. Then by *iterating* the Schmidt decomposition, we arrive at a much more succinct description:

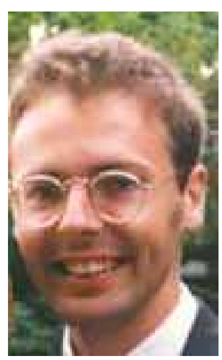
$$c_{i_1 \ldots i_n} = \sum_{\alpha_1 \ldots \alpha_{n-1}} \Gamma^{[1]i_1}_{\alpha_1} \lambda^{[1]}_{\alpha_1} \Gamma^{[2]i_2}_{\alpha_1\alpha_2} \lambda^{[2]}_{\alpha_2} \Gamma^{[3]i_3}_{\alpha_2\alpha_3} \ldots \Gamma^{[n-1]i_{n-1}}_{\alpha_{n-2}\alpha_{n-1}} \lambda^{[n-1]}_{\alpha_{n-1}} \Gamma^{[n]i_n}_{\alpha_{n-1}}$$

There are *n-1* Schmidt vectors (the λ_α’s), each with at most χ components, and at most $2n\,\chi^2$ parameters for the Γ’s. We can easily update these quantities in a simulation of a circuit of quantum gates (Vidal, quant-ph/0301063, Cf, also Jozsa & Linden ’02)! For example, we can simulate a spin chain with a finite correlation length (or even a critical chain).

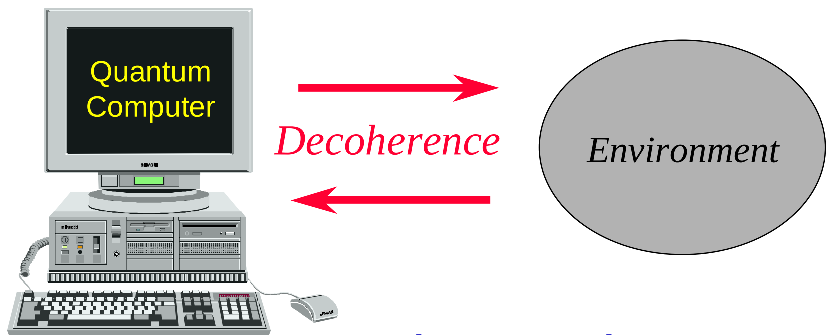
Quantum
Error Correction

Shor '95 Steane '95

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



Shor '95 Steane '95



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.

Errors

The most general type of error acting on n qubits can be expressed as a unitary transformation acting on the qubits and their environment:

$$U: |\psi\rangle \otimes |0\rangle_E \rightarrow \sum_a E_a |\psi\rangle \otimes |a\rangle_E$$

The states $|a\rangle_E$ of the environment are neither normalized nor mutually orthogonal. The operators $\{E_a\}$ are a basis for operators acting on n qubits, conveniently chosen to be "Pauli operators": $\{I, X, Y, Z\}^{\otimes n}$,

where

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

The errors could be "unitary errors" if $|a\rangle_E = C_a |0\rangle_E$ or decoherence errors if the states of the environment are mutually orthogonal.

Errors

$$U : |\psi\rangle \otimes |0\rangle_E \rightarrow \sum_a E_a |\psi\rangle \otimes |a\rangle_E$$

Our objective is to recover the (unknown) state $|\psi\rangle$ of the quantum computer. We can't expect to succeed for arbitrary errors, but we might succeed if the errors are of a restricted type. In fact, since the interactions with the environment are *local*, it is reasonable to expect that the errors are not too strongly correlated.

Define the "weight" w of a Pauli operator to be the number of qubits on which it acts nontrivially; that is $X,Y,$ or Z is applied to w of the qubits, and I is applied to n-w qubits. If errors are weakly correlated (and rare), then Pauli operators E_a with large weight have small amplitude $\mathrm{P}|a\rangle_E\,\mathrm{P}$.

Quantum error-correcting code

We won't be able to correct all errors of weight up to t for arbitrary states $|\psi\rangle \in \mathrm{H}_{n \text{ qubits}}$. But perhaps we can succeed for states contained in a *code subspace* of the full Hilbert space,

$$\mathrm{H}_{\text{code}} \in \mathrm{H}_{n \text{ qubits}}.$$

If the code subspace has dimension 2^k, then we say that k encoded qubits are embedded in the block of n qubits.

How can such a code be constructed? It will *suffice* if

$$\left\{E_a \mathrm{H}_{\text{code}}, \quad E_a \in \left\{\text{Pauli operators of weight} \leq t\right\}\right\}$$

are mutually orthogonal.

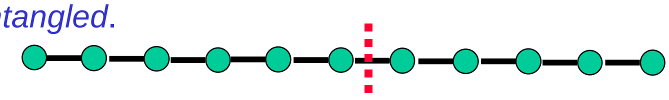
If so, then it is possible in principle to perform an (incomplete) orthogonal measurement that determines the error $\boldsymbol{E_a}$ (without revealing any information about the encoded state). We recover by applying the unitary transformation $\boldsymbol{E_a}^{\dagger}$.

Quantum error-correcting codes and entanglement

"Nondegenerate" quantum error-correcting code that corrects t errors in a block of n qubits:

$$E_a \mathrm{H}_{\mathrm{code}} \perp \mathrm{H}_{\mathrm{code}}, \quad \text{for} \quad E_a \in \{\text{Pauli operators of weight} \le 2t\}$$

The expectation value of E_a vanishes in the code space, so that the density operator of any $2t$ qubits (if we trace out the remaining n-$2t$) is random. The states in the code space are *profoundly entangled*.

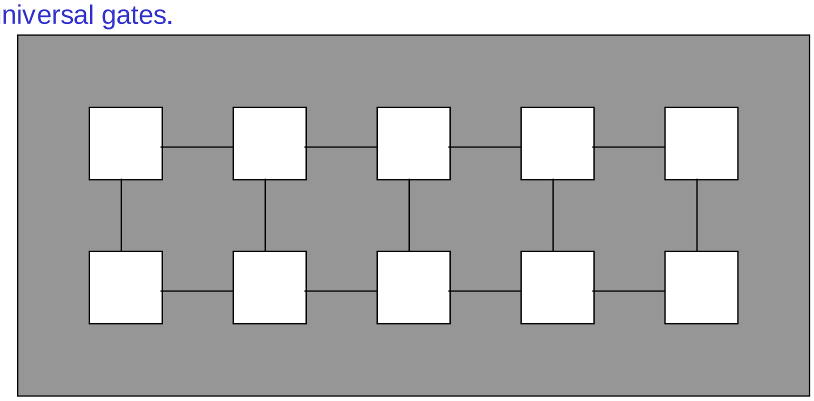


Maximally entangled states with n parts can be constructed such that the density operator of any k parts is random, for any k up to $n/2$. (But not for qubits: the dimension p of the parts is a prime number greater than n.) Such states are easily constructed with efficient quantum circuits, but cannot be an eigenstate of any local Hamiltonian (Haselgrove et al. '03).

Topological quantum memory

Kitaev '96

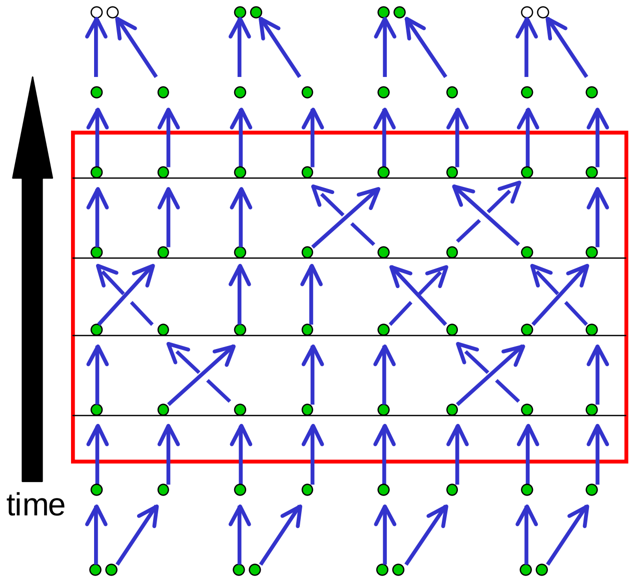
Qubits can reside in holes in a planar array, where the holes carry Z_2 charge or flux. Then the quantum memory is topologically stable, but nontopological couplings between holes are needed to complete a set of universal gates.



This scheme might be realizable in suitably designed Josephson-junction arrays, which have a phase that can be interpreted as a condensate of objects with charge $4e$. A hole in the array can carry charge $2e$ or flux $\Phi_0/2=2\pi/4e$.

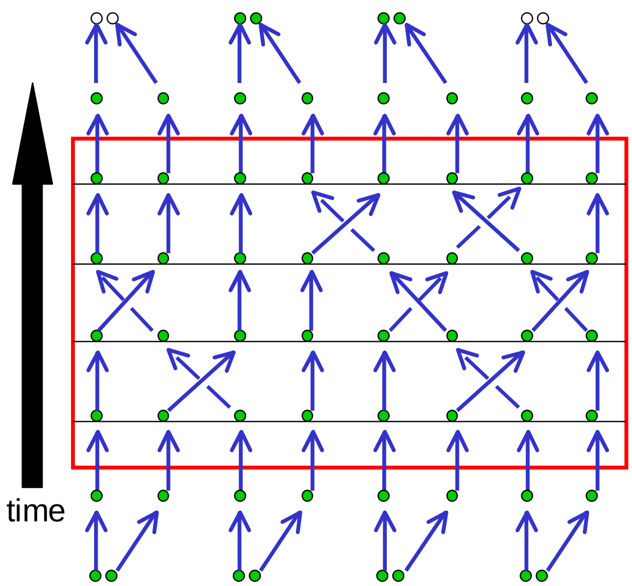
Ioffe et al. '02

Topological quantum computation (Kitaev '97)



Kitaev

Topological quantum computation (Kitaev '97)

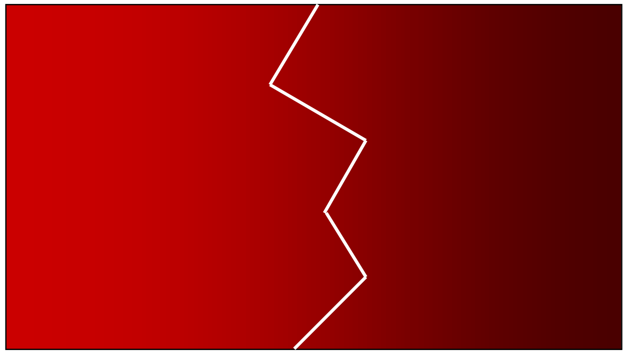


Physical fault tolerance with nonabelians:

uncontrolled exchange of quantum numbers will be rare if particles are widely separated, and thermal anyons are suppressed...

Quantum vs. Classical

Very Quantum



Very Classical

There is a sharp boundary between classical phase (efficiently simulable by a classical computer) and quantum phase (not efficiently simulable). For a quantum computer with a topological memory, it can be identified with the boundary between the *confinement phase* and the *superconducting phase* of a gauge theory with quenched randomness.

[Dennis, Kitaev, Landahl & Preskill '01; Wang, Harrington & Preskill '02]

Quantum Hardware

Kimble

Devoret

Two-level ions in a Paul trap, coupled to "phonons."

Two-level atoms in a high-finesse microcavity, strongly coupled to cavity modes of the electromagnetic field.

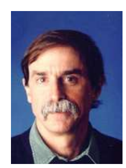
Charge in a Cooper-pair box; fluxons through a superconducting loop.

Electron spin (or charge) in quantum dots.

Bose condensates in optical lattices.

Nuclear spins in semiconductors, and in liquid state NMR.

Electrons floating on liquid He, etc.



Wineland

Blatt

The 2nd Quantum Century

• We just beginning to appreciate the surprisingly rich implications of the tensor product structure of Hilbert space, and of many-body quantum entanglement: Quantum algorithms, quantum error correction, etc.

• Progress in understanding the power of quantum computing is slow but steady. There are strong connections with the theory of spectral gaps in disordered quantum systems.

• We have learned a lot about bipartite quantum entanglement (pure and mixed). Less is understood about many-body entanglement, but there have been valuable insights.

• Future advances in our understanding of quantum computation and information will be closely linked to new insights about properties of quantum many-body systems and of quantum phase transitions.