Why Quantum Computers Cannot Work

Gil Kalai
Hebrew University of Jerusalem and Yale University

Department of Mathematics, U. Cal, Davis, October 2013.

Quantum computers

Quantum computers are hypothetical devices based on quantum physics that can out-perform classical computers. A famous algorithm by Peter Shor shows that quantum computers can factor an integer n in $C(log n)^3$ steps. The study of quantum computation and information is a remarkable interdisciplinary endeavor which involves several areas of physics, computer science, chemistry, engineering and mathematics.

The question if quantum computer are realistic is one of the most fascinating and clear-cut scientific problems of our time, and my work is geared toward a negative answer. The main concern from the start was that quantum systems are inherently noisy; we cannot accurately control them, and we cannot accurately describe them. To overcome this difficulty, a fascinating notion of quantum error-correction and a remarkable theory of quantum fault-tolerance were developed.

The debate on quantum computers

What makes it still hard to believe that superior quantum computers can be built is that building universal quantum computers represents a completely new reality in terms of controlled and observed quantum evolutions, and also a new computational complexity reality. What makes it hard to believe that quantum computers cannot be built is that this may require profoundly new insights in the understanding of quantum mechanical systems (including in regimes where people do not expect such new insights.)

Why quantum computers cannot work

Here is my explanation for why (fault-tolerant) quantum computers cannot be built:

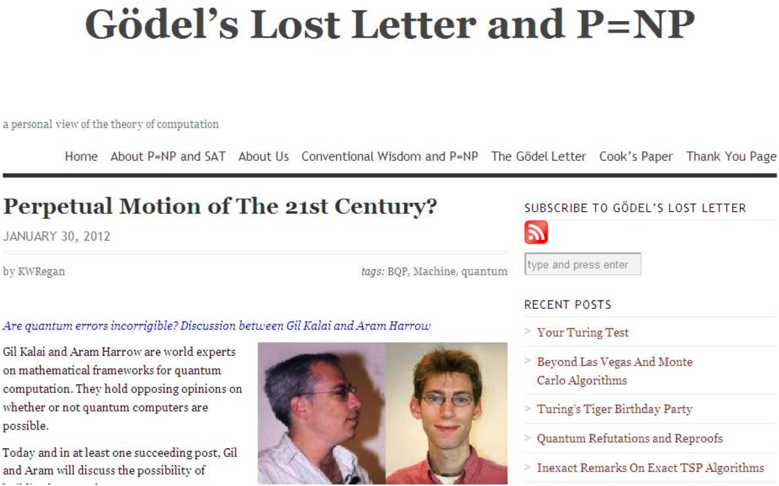
Quantum systems based on special-purpose quantum devices are subject to noise which systematically depends on the quantum evolution of the system; this dependence reflects dependence of the noise on the quantum device, and the dependence of the quantum device on the quantum evolution it is performing. Here, " a quantum device" refers both to human-made and to natural devices. This systematic dependence causes error-rate for general-purpose quantum computers to scale up.

The mathematical challenge is to understand the systematic laws for this dependence. (Of course, within the framework of quantum mechanics.)

Debate !

From the end of January 2012 until November 2012 Aram Harrow, a brilliant researcher in quantum information and computation from the University of Washington, Seattle (Now M.I.T) and I were engaged in a public academic debate regarding this question. The debate was hosted on Dick Lipton and Ken Regan's blog "Gödel's Lost Letter and P=NP." Further discussions with Peter Shor and Aram Harrow on "smoothed Lindblad evolutions" took place on my blog.

Debate !



Gödel's Lost Letter and P=NP

a personal view of the theory of computation

Home About P=NP and SAT About Us Conventional Wisdom and P=NP The Gödel Letter Cook's Paper Thank You Page

Perpetual Motion of The 21st Century?

JANUARY 30, 2012

by KWRegan

tags: BQP, Machine, quantum

Are quantum errors incorrigible? Discussion between Gil Kalai and Aram Harrow

Gil Kalai and Aram Harrow are world experts on mathematical frameworks for quantum computation. They hold opposing opinions on whether or not quantum computers are possible.

Today and in at least one succeeding post, Gil and Aram will discuss the possibility of

SUBSCRIBE TO GÖDEL'S LOST LETTER

type and press enter

RECENT POSTS

- Your Turing Test
- Beyond Las Vegas And Monte Carlo Algorithms
- Turing's Tiger Birthday Party
- Quantum Refutations and Reproofs
- Inexact Remarks On Exact TSP Algorithms

This lecture:

- Part I: Quantum computers
- Part II: Noise, quantum fault tolerance, and the "trivial flaw".
- Part III: My conjectures.
- Part IV: Smoothed Lindblad evolutions
- Part V: A few conceptual issues from my debate with Aram Harrow. Conclusion.
- Encore: If times allow: relation to BKS-noise sensitivity, topological quantum computing, BosonSampling,...

Part I: Quantum Computers

What is a computer? (A circuit model)

We have *n* bits of memory, each one can be in two states '0' and '1'.

At every computer cycle we can perform a gate on one or two bits. We need three types of gates AND OR and NOT.

What is a qubit

A qubit is a piece of quantum memory. The state of a qubit can be described by a unit vector in a 2-dimensional complex Hilbert space $\mathcal{H}$.
We assume that a basis of $\mathcal{H}$ consists of the two vectors $|0\rangle$ and $|1\rangle$.
So the qubit's state has the form $a|0\rangle + b|1\rangle$, where $|a|^2 + |b|^2 = 1$.

A qubit can be *measured* and this will give a probabilistic bit which is '0' with probability $|a|^2$ and '1' with probability $|b|^2$.

What is a quantum computer

The memory consists of *n* qubits. The state of the computer is a unit vector in the tensor product of all the 2-dimensional Hilbert spaces corresponding to the qubits.
We can perform "gates" on one or two qubits. There is a small list of gates needed for universal quantum computing. A gate is a unitary transformation acting on the corresponding 2- or 4-dimensional Hilbert space..
The state of the entire computer can be measured and this gives a probability distribution on 0-1 vectors of length *n*.

Part II: Noise, quantum fault tolerance, and the ”trivial flaw”

Concerns about noise

The main concern regarding quantum-computer feasibility is that quantum systems are inherently noisy. This concern was put forward in the mid-90s by Landauer, Unruh, and others.

We can think about noise modeling and analysis, error modeling and analysis, and risk modeling and analysis, as different notions for the same thing. For quantum systems, leak of information amounts to noise and this is often referred to as "decoherence."

Noisy quantum systems

The early concern that quantum systems are inherently noisy raised several questions:

- Why are quantum systems noisy?
- What is the nature and magnitude of the noise?
- Can we reduce via engineering the noise level per qubit to be $1/poly(n)$?
- Isn't it the case that the whole universe manifests a pure quantum evolution?
- Isn't noise (and pure evolutions) just a subjective matter?

These and other arguments led several researchers to regard noise (even before quantum error-correction and certainly after) as an engineering issue which has no roots in fundamental physics.

Quantum error-correction and FTQC

The theory of quantum error correction and fault-tolerant quantum computation (FTQC) and, in particular, the *threshold theorem*, which asserts that under certain conditions FTQC is possible, provide strong support for the possibility of building quantum computers.

FTQC allows to embed via quantum error correction a noiseless universal quantum computer inside a noisy quantum computer. (The overheads in time and space are rather small.)

Clarification: In this lecture **noiseless** means "noiseless for all practical purposes". (The probability of errors is negligible.)

The quantum fault-tolerance barrier

Quantum fault-tolerance represents a major phase-transition for noisy quantum systems. The main purpose of my work is to draw formally and generally the “quantum fault-tolerance barrier” between noisy quantum systems without quantum fault-tolerance and noisy quantum systems with quantum fault-tolerance.

The quantum fault-tolerance barrier

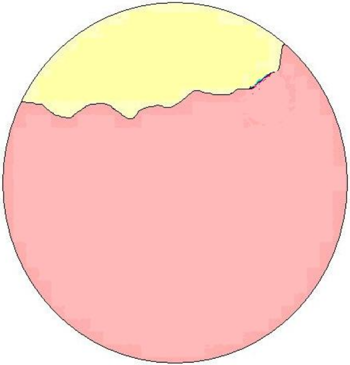


Figure: 1. The barrier between quantum systems with quantum fault-tolerance and quantum systems without quantum fault-tolerance

The "trivial flaw"

Ignoring the possibility that quantum evolutions (human-made and natural alike) require special-purpose devices whose physical properties depend systematically on the evolution they perform.

For general-purpose quantum devices, the possibility for quantum fault-tolerance reduces essentially to a single parameter, and modeling general-purpose devices is much too narrow to deal with the issue of scalability.

This flaw does not mean that QCs cannot be built, but only that many arguments and intuitions for why QCs can be built are incorrect. It also means that this possible dependence should be studied carefully.

The "Trivial Flaw"

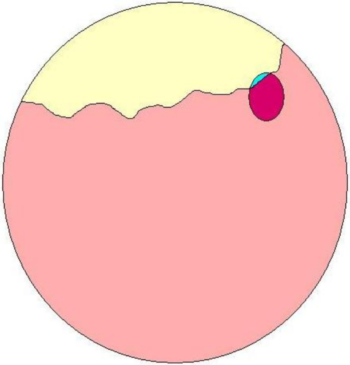


Figure: 2. General-purpose quantum computing devices form a very restricted subclass of special-purpose quantum devices.

The "trivial flaw:" FAQ

Q: Does the connection between the evolution and the noise in violation of QM linearity or other basic physics principles?
A: No

Q: But current noise models do account for some relations between the noise and the evolution,
A: Correct! they account for that in a very limited way which is based on the general-purpose quantum device description.

The ”trivial flaw:” FAQ (cont.)

Q: Do you claim that each device can perform only a single evolution?
A: No. The systematic relations between evolution and errors through a device should apply to all available evolutions for the device.
Q: But qubits and quantum gates are not imaginary, their quality is steadily improved, several plans for putting them together for having universal quantum computers, or highly stable qubits based on quantum error-correction are on their way!

Part III: My conjectures:

My first post in the debate with Aram Harrow described my conjectures regarding how noisy quantum computers *really* behave. These conjectures attempt to describe formally the quantum-fault tolerance barrier. Some of them describe the simplest distinctions between my modeling and the standard ones for one and two qubits. Other conjectures apply to very general quantum systems.

Note: These are not mathematical conjectures but conjectures about appropriate mathematical modeling of noisy quantum systems.

Conjecture 1: No quantum error-correction for a single qubit

Conjecture 1: (No quantum error-correction): In every implementation of quantum error-correcting codes with one encoded qubit, the probability of not getting the intended qubit is at least some $\delta > 0$, independently of the number of qubits used for encoding.

Ordinary models assume the existence of some small δ for the individual qubit-errors and reduces the amount of noise for the encoded qubit exponentially via quantum fault-tolerance.

Conjecture 3: Two qubits behavior

A noisy quantum computer is subject to error with the property that information leaks for two substantially entangled qubits have a substantial positive correlation.

Conjecture 4: Error synchronization

In any noisy quantum computer in a highly entangled state there will be a strong effect of error synchronization.

How to express these conjectures mathematically and one reduction

I found that the best way to express error-synchronization (Conj. 4) and positive correlation for information leaks (Conj. 3) is by the expansion to product of Pauli operators.

We need a stronger form of Conjecture 3 where “entanglement” is replaced by a measure of expected entanglement based on (separably) measuring the other qubits in an arbitrary way.
Theorem: This strong form of Conjecture 3 implies Conjecture 4.

Sure/Shor separators, smoothed Lindblad evolutions, rate

"Sure/Shor separator:" The only realistic approximately-pure quantum evolutions are approximately bounded depth. This conjecture largely goes back to Unruh. (The notion of Sure/Shor separator was suggested by Aaronson.)

Smoothed Lindblad equations: "Detrimental" noise that cannot be avoided (and cause quantum fault-tolerance to fail) can be described in terms of "smoothed Lindblad evolutions".

A conjecture regarding rate: The rate of noise at time interval $[s,t]$ is bounded below by a noncommutativity measure for (projections in the) the algebra spanned by unitaries expressing the evolution in the time-intervals $[s,t]$.

Part IV: How to model un-suppressed noise accumulation?

Smoothed Lindblad evolution

We start with a unitary evolution at time-interval [0,1]. $U_{s,t}$ is a unitary operator describing the change from time s to time t.

Next we consider a general Lindblad evolution obtained by adding noise expressed infinitesimally at time t by E_t.

We replace E_t by the weighted average of $U_{s,t}E_sU_{s,t}^{-1}$ over all times s with respect to a positive kernel $K(t-s)$. (We can just assume that K is Gaussian.)

Smoothed Lindblad evolution

We start with a unitary evolution at time-interval [0,1]. $U_{s,t}$ is a unitary operator describing the change from time s to time t.

Next we consider a general Lindblad evolution obtained by adding noise expressed infinitesimally at time t by E_t.

We replace E_t by the weighted average of $U_{s,t}E_sU_{s,t}^{-1}$ over all times s with respect to a positive kernel $K(t-s)$. (We can just assume that K is Gaussian.)

Important point: $K(x)$ is positive on [-1,1] and we average over all $s \in [0,1]$. If the smoothing depends only on the past Greg Kuperberg and I showed that FTQC is possible.

The work with Kuperberg

If the smoothing depends only on the past Greg Kuperberg and I showed that FTQC is possible.
Imagine a circuit model for quantum computation. As usual, a circuit is an acyclic directed graph in which each edge represents a bit or a qubit, and vertex is labelled by one element from a fixed set of gates. Now, normally the edges are all bits for a classical circuit, and all qubits for a quantum circuit. However, it is entirely reasonable to have a mixed circuit in which some edges are bits and some are qubits, and then also mixed gates.

The work with Kuperberg: ”Preventing quantum computation requires time travel” (cont.)

Theorem (K. and Kuperberg): It is possible to build quantum-universal circuits in which the maximum length of a directed path of qubit edges is bounded. Moreover, this can be done with a constant factor of overhead

One corollary of this theorem is that if the smoothing depends only on the past then FTQC is possible. Greg's interpretation is described in the title of the slide.

The work with Kuperberg: "Preventing quantum computation requires time travel" (cont.)

Theorem (K. and Kuperberg): It is possible to build quantum-universal circuits in which the maximum length of a directed path of qubit edges is bounded. Moreover, this can be done with a constant factor of overhead

One corollary of this theorem is that if the smoothing depends only on the past then FTQC is possible. Greg's interpretation is described in the title of the slide. Greg's mistake is...

The work with Kuperberg: ”Preventing quantum computation requires time travel” (cont.)

Theorem (K. and Kuperberg): It is possible to build quantum-universal circuits in which the maximum length of a directed path of qubit edges is bounded. Moreover, this can be done with a constant factor of overhead

One corollary of this theorem is that if the smoothing depends only on the past then FTQC is possible. Greg's interpretation is described in the title of the slide. Greg's mistake is... the *trivial flaw*. The causality structure is much different for special-purpose devices.

Smoothed-in-time Lindblad evolution

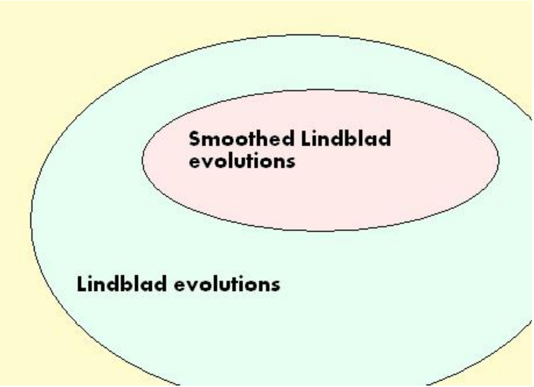


Figure: 3. Smoothed Lindblad evolutions are a restricted subclass of the class of all Lindblad evolutions

Smoothed-in-time Lindblad evolution

Two questions:

1. (Lukas Svec): How can I say that these Smoothed Lindblad evolutions are subclasses of all Lindblad evolutions when they have "memory"?

Smoothed-in-time Lindblad evolution

Two questions:
1. (Lukas Svec): How can I say that these Smoothed Lindblad evolutions are subclasses of all Lindblad evolutions when they have "memory"?

2. Isn't this smoothing "into the future" violating causality?

Smoothed-in-time Lindblad evolution

Two questions:
1. (Lukas Svec): How can I say that these Smoothed Lindblad evolutions are subclasses of all Lindblad evolutions when they have ”memory”?

2. Isn’t this smoothing ”into the future” violating causality?

Answers: 1. No memory, 2. no causality violation. Remember the ”trivial flaw,” the evolution and the consequences on errors are “wired in” the device. The evolution is not a variable.

The Smoothed Lindblad evolution conjecture

Conjecture: Every realistic noisy quantum system includes a noise-component well approximated by a smoothed Lindblad evolution.

A correlation description of "smoothed component of noise": The noise E_t at time t has significant correlation with $U_{s,t} E_s U^*_{s,t}$.

The conjecture and FAQ

My conjecture is that an “SLE” component of noise exists for every realistic quantum system, and this property draws the quantum fault-tolerance barrier.

A frequently asked question: What is the physical reason for that?

The conjecture and FAQ

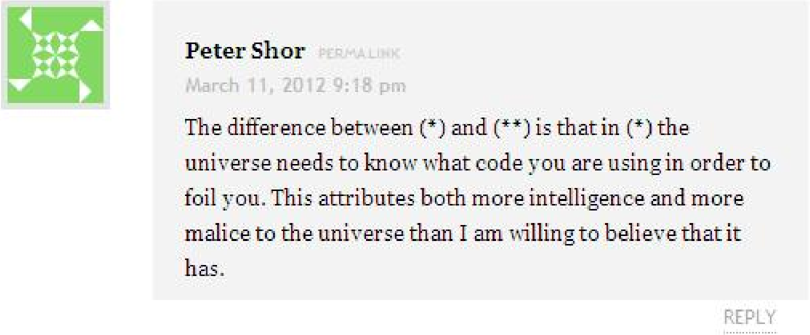
My conjecture is that an “SLE” component of noise exists for every realistic quantum system, and this property draws the quantum fault-tolerance barrier.

A frequently asked question: What is the physical reason for that?

(Incomplete) answer: The model of quantum computers is a huge abstraction putting together under the same roof many different systems. The SLE noise is also a major abstraction and the specific physical reasons for it will depend on the implementation.

Part V: Some conceptual points raised in the debate by Aram and others

The discussion



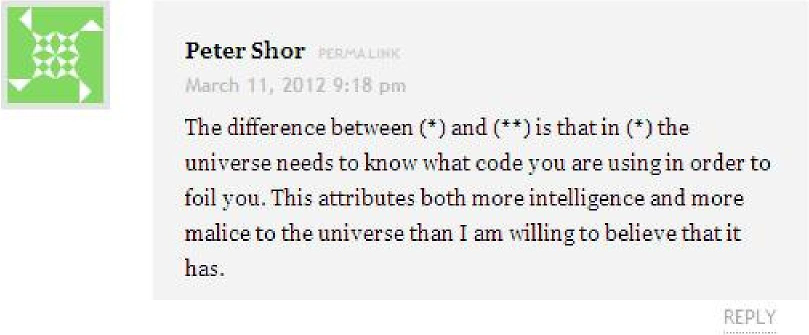
Peter Shor PERMALINK

March 11, 2012 9:18 pm

The difference between (*) and (**) is that in (*) the universe needs to know what code you are using in order to foil you. This attributes both more intelligence and more malice to the universe than I am willing to believe that it has.

Peter: It takes too much malice and intelligence for nature to detect and intercept the quantum error-correcting codes.

The discussion



Peter Shor PERMALINK

March 11, 2012 9:18 pm

The difference between (*) and (**) is that in (*) the universe needs to know what code you are using in order to foil you. This attributes both more intelligence and more malice to the universe than I am willing to believe that it has.

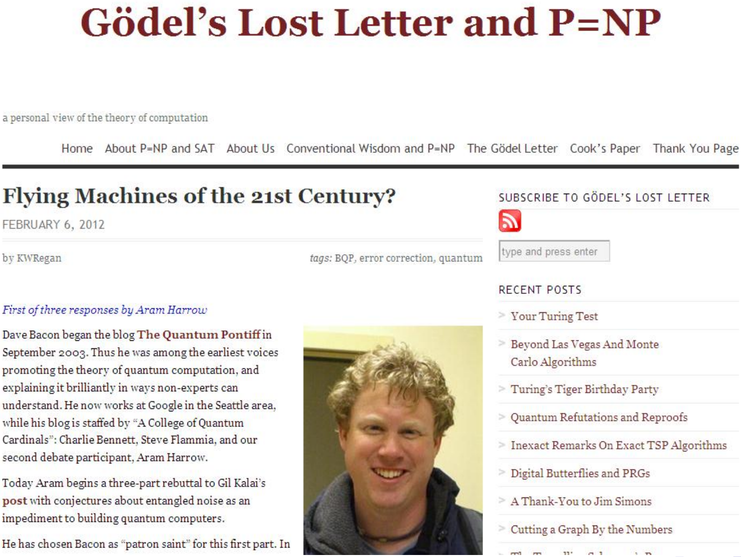
Peter: It takes too much malice and intelligence for nature to detect and intercept the quantum error-correcting codes.

Response: The trivial flaw again- if every quantum code requires a special device to create, no malice or intelligence is needed.

Other objections

- **Aram Harrow:** If quantum fault-tolerance is impossible why classical fault-tolerance possible?
- **Aram:** We can redefine the quantum system to include the environment/noise.
- **Cris Moore:** Skepticism of quantum computers means skepticism of quantum mechanics
- **Joe Fitzsimons's:** Blind computation
- **John Preskill:** A general model where the threshold theorem holds.
- **Joe:** A 2-locality argument. More generally, the conjecture are in conflict with the principle of locality.

(Aram's first post:) Why classical computers are possible?



Gödel's Lost Letter and P=NP

a personal view of the theory of computation

Flying Machines of the 21st Century?

FEBRUARY 6, 2012

by KWRegan

tags: BQP, error correction, quantum

First of three responses by Aram Harrow

Dave Bacon began the blog **The Quantum Pontiff** in September 2003. Thus he was among the earliest voices promoting the theory of quantum computation, and explaining it brilliantly in ways non-experts can understand. He now works at Google in the Seattle area, while his blog is staffed by "A College of Quantum Cardinals": Charlie Bennett, Steve Flammia, and our second debate participant, Aram Harrow.

Today Aram begins a three-part rebuttal to Gil Kalai's **post** with conjectures about entangled noise as an impediment to building quantum computers.

He has chosen Bacon as "patron saint" for this first part. In

SUBSCRIBE TO GÖDEL'S LOST LETTER

RECENT POSTS

- Your Turing Test
- Beyond Las Vegas And Monte Carlo Algorithms
- Turing's Tiger Birthday Party
- Quantum Refutations and Reproofs
- Inexact Remarks On Exact TSP Algorithms
- Digital Butterflies and PRGs
- A Thank-You to Jim Simons
- Cutting a Graph By the Numbers

Classical computing devices

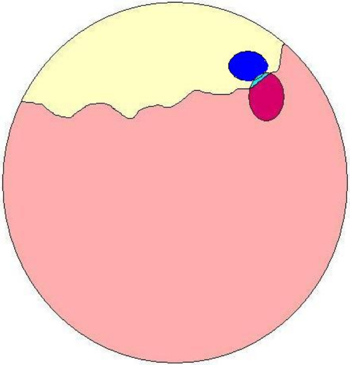


Figure: 3. General-purpose classical computers are special-purpose quantum devices.

If computationally superior quantum computers are not possible does it mean that, in principle, classical computation suffices to simulate any physical process?

If computationally superior quantum computers are not possible does it mean that, in principle, classical computation suffices to simulate any physical process?

The short answer is: Yes.

Does impossibility of QC means breakdown of QM?

The short answer is: No!

What the big deal then?

Suppose that you accept that indeed the ”trivial flaw” can be devastating, and may cause quantum computers to fail. Will it have any additional interest?

What the big deal then?

Suppose that you accept that indeed the ”trivial flaw” can be devastating, and may cause quantum computers to fail. Will it have any additional interest?

Analogy: What was Lord Kelvin's mistake in dating the earth? (He was off by a factor of 50.)

What the big deal then?

Suppose that you accept that indeed the ”trivial flaw” can be devastating, and may cause quantum computers to fail. Will it have any additional interest?

Analogy: What was Lord Kelvin’s mistake in dating the earth? (He was off by a factor of 50.)

Kelvin’s “trivial flaw” was to assume that heat conductance is the only mechanism for moving heat around.

What the big deal then?

Suppose that you accept that indeed the "trivial flaw" can be devastating, and may cause quantum computers to fail. Will it have any additional interest?

Analogy: What was Lord Kelvin's mistake in dating the earth? (He was off by a factor of 50.)

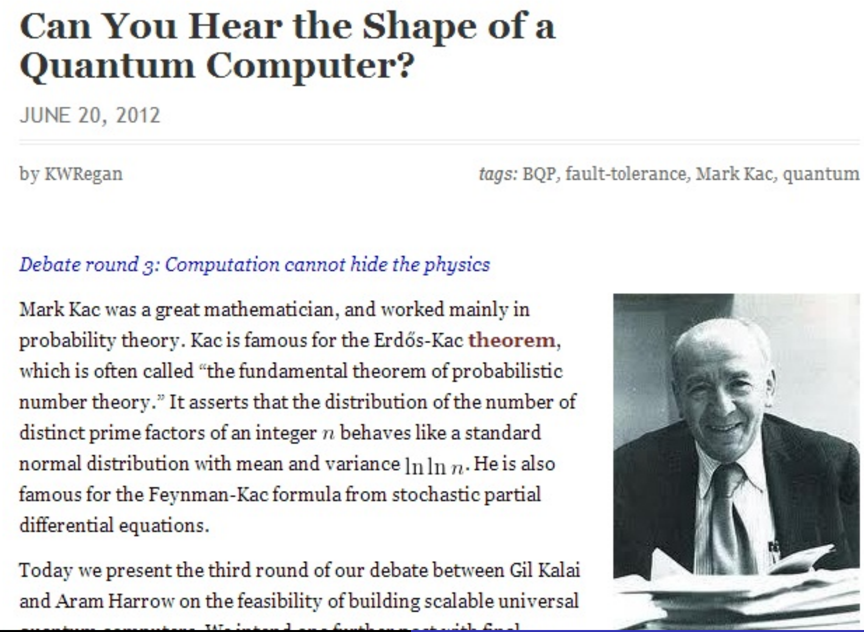
Kelvin's "trivial flaw" was to assume that heat conductance is the only mechanism for moving heat around.

But his mistake is also related to deeper issues. Kelvin dated the sun before dating the earth and there his estimates did not took into account nuclear relations - unknown at the time.

To what areas of physics are obstructions (or impossibility) of quantum error-correction relevant?

1. Thermodynamics.
2. Approximations/perturbation methods in various areas of quantum physics including quantum field theory.
3. Classical physics (!) (Possible connections with issues of quantum noise emerging from symplectic geometry, related to recent papers by Leonid Polterovich seems very interesting.)

Reasons to doubt



Can You Hear the Shape of a Quantum Computer?

JUNE 20, 2012

by KWRegan

tags: BQP, fault-tolerance, Mark Kac, quantum

Debate round 3: Computation cannot hide the physics

Mark Kac was a great mathematician, and worked mainly in probability theory. Kac is famous for the Erdős-Kac **theorem**, which is often called "the fundamental theorem of probabilistic number theory." It asserts that the distribution of the number of distinct prime factors of an integer n behaves like a standard normal distribution with mean and variance $\ln \ln n$. He is also famous for the Feynman-Kac formula from stochastic partial differential equations.

Today we present the third round of our debate between Gil Kalai and Aram Harrow on the feasibility of building scalable universal

Reasons to doubt: How quantum computers will change the physical reality

- A universal machine for creating quantum states and evolutions could be built.
- Complicated states and evolutions never encountered before could be created
- States and evolutions could be constructed on arbitrary geometry
- Emulated quantum evolutions could always be time-reversed
- The noise of (approximately pure) quantum states will not respect symmetries of the state but rather depends on a computational basis
- Factoring will become easy

Summary

Quantum fault-tolerance represents a major phase-transition for noisy quantum systems. Finding the appropriate mathematical tools to model and understand the nature of this phase transition - *the quantum fault-tolerance barrier,* is an important problem.

My expectation is that the ultimate triumph of quantum information theory will be in explaining why quantum computers cannot be built.

Thank you very much!

Recent project BKS noise sensitivity and AA BosonSampling