Why Quantum Computers Cannot Work and How

Gil Kalai
Institute of Mathematics
Hebrew University of Jerusalem
and Department of Mathematics
Yale University

February 22, 2013

Quantum Information Seminar, MIT, February 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 $C(logn)^3$ 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.

Quantum computers (cont.)

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 general-purpose quantum computers to fail. The challenge is to understand the systematic laws for this dependence. (Of course, within the framework of quantum probability.)

This lecture:

- Part I: Noise, quantum fault tolerance, and the "trivial flaw".
- Part II: Why topological quantum computing cannot shortcut traditional quantum fault tolerance.
- Part III: My conjectures.
- Part IV: Smoothed Lindblad evolutions
- Part V: Various conceptual issues from my debate with Aram Harrow.

Part I: 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.

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?
- Isn't the feasibility of quantum computers a direct consequence of quantum mechanics?

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 "trivial flaw"

The "trivial flaw"

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.

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.

What the big deal then?

Suppose that you accept that indeed the "trivial flaw" can be devastating, and may cause quantum computers to fail even well below the classical computational threshold. (Namely, that even general noiseless single-qubit and double-qubit evolutions can never be created.) This may account to some complicated nonlinear effect within quantum physics but 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 even well below the classical computational threshold. (Namely, that even general noiseless single-qubit and double-qubit evolutions can never be created.) This may account to some complicated nonlinear effect within quantum physics but will it have any additional interest?

If you ask Michel Dyakonov, the answer is negative, and he compares it to what could be learned from failing to teach a horse to speak. If you ask Scott Aaronson this will a moment comperable only to one or two events in the history of science. In my view, there are good reasons to think that finding principles explaining the failure of QCs (even of restricted scope, and certainly general) will be a big deal (but not quite as big as Scott thinks).

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."

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

Part II: Why topological quantum computing cannot shortcut the need for "traditional" quantum fault tolerance

Topological quantum computers

The idea: Using ordinary experimental processes to construct highly stable qubits based on non commutative anyons.

From a 2002 paper by Freedman, Kitaev, Larsen, and Wang: The chief advantage of anyonic computation would be physical error correction: An error rate scaling like $e^{-\alpha\ell}$, where ℓ is a length scale, and α is some positive constant. In contrast, the "presumptive" qubit-model of quantum computation, which repairs errors combinatorically, requires a fantastically low initial error rate (about 10^{-4}) before computation can be stabilized.

Why "weapon-graded" qubits based on anyons will not work

The argument against this idea: Ordinary experimental methods can be modeled by noisy quantum computers which do not carry the quantum-fault tolerance apparatus. For such noisy quantum computers the state of an encoded qubit will involve a (substantial) mixture with undesired codewords.

This will prevent highly stable qubits based on anyons.

Caveats and remarks

Caveats and remarks

1. This is an argument, not a mathematical proof.

Caveats and remarks

1. This is an argument, not a mathematical proof.
2. Even as such, the notions involved should be put on much more formal grounds (and this is what my work is about).

Caveats and remarks

1. This is an argument, not a mathematical proof.
2. Even as such, the notions involved should be put on much more formal grounds (and this is what my work is about).
3. This is not an argument against the usefulness of surface codes and other ideas from topological quantum computing in traditional implementations of QC. (This is a very promising direction!)

Caveats and remarks

1. This is an argument, not a mathematical proof.
2. Even as such, the notions involved should be put on much more formal grounds (and this is what my work is about).
3. This is not an argument against the usefulness of surface codes and other ideas from topological quantum computing in traditional implementations of QC. (This is a very promising direction!)
4. This argument should be "confronted" with the detailed ideas of creating stable qubits based on anyons.

Caveats and remarks

1. This is an argument, not a mathematical proof.
2. Even as such, the notions involved should be put on much more formal grounds (and this is what my work is about).
3. This is not an argument against the usefulness of surface codes and other ideas from topological quantum computing in traditional implementations of QC. (This is a very promising direction!)
4. This argument should be "confronted" with the detailed ideas of creating stable qubits based on anyons.
5. A similar argument applies to measurement-based computation based on cluster states, and may apply to various forms of adiabatic computation, photon-machines etc.

Caveats and remarks

1. This is an argument, not a mathematical proof.
2. Even as such, the notions involved should be put on much more formal grounds (and this is what my work is about).
3. This is not an argument against the usefulness of surface codes and other ideas from topological quantum computing in traditional implementations of QC. (This is a very promising direction!)
4. This argument should be "confronted" with the detailed ideas of creating stable qubits based on anyons.
5. A similar argument applies to measurement-based computation based on cluster states, and may apply to various forms of adiabatic computation, photon-machines etc.
6. The arguments for why QCs cannot be built altogether are weaker. Here we have an actual argument and for the general case we have only a viable alternative to the common point of view.

Topological quantum computers (cont.)

How does nature know what anyonic state we try to create so it can foil us?

Topological quantum computers (cont.)

How does nature know what anyonic state we try to create so it can foil us?

In a recent experiment Moti Heiblum tried to create interference between certain fractionally-charged microparticles, and when this failed he concluded that this is not possible because additional zero-charged microparticles must be created. How does nature know what Moti was trying to do?

Topological quantum computers (cont.)

How does nature know what anyonic state we try to create so it can foil us?

In a recent experiment Moti Heiblum tried to create interference between certain fractionally-charged microparticles, and when this failed he concluded that this is not possible because additional zero-charged microparticles must be created. How does nature know what Moti was trying to do?

These questions are meaningless in this context.

Part III: My conjectures:

Conjecture 1: No quantum error-correction

My first post described my conjectures regarding how noisy quantum computers *really* behave. Starting with

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 2: The strong principle of noise

Conjecture 2: (The strong principle of noise): Quantum systems are inherently noisy with respect to every Hilbert space used in their description; in other words, it is impossible to find noiseless quantum subsystem embedded in a noisy system.

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.

(This is a conjecture about appropriate modeling of noisy quantum computation.)

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 VI: 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 and allow some added atom at 0.)

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 and allow some added atom at 0.)

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 Kuperberg and I showed that FTQC is possible.

Smoothed-in-time Lindblad evolution

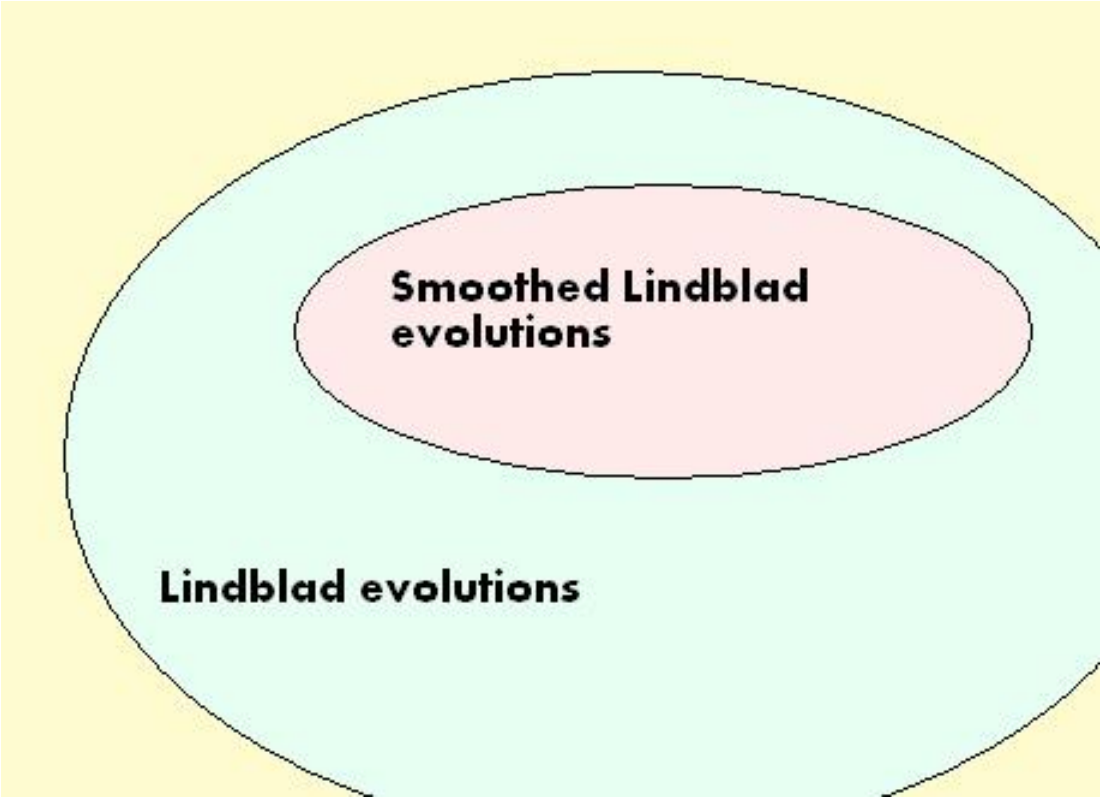


Figure: 1. Smoothed Lindblad evolutions are a restricted subclass of the class of all Lindblad evolutions

Smoothed-in-time Lindblad evolution

Two questions:

1. (Lukas Svec): How can I say that these SLE 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 SLE 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 SLE 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. Hint: remember the "trivial flaw."

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

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

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

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

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
- Digital Butterflies and PRGs
- A Thank-You to Jim Simons
- Cutting a Graph By the Numbers

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

"The first reason I'm skeptical about Gil's conjectures is that... Gil questions the independence assumption of errors. But if highly correlated errors routinely struck computers, then they would also be a problem for classical computers. Quantum mechanics describes everything, including classical computers. If quantum computers suffer massively correlated errors with non-negligible probability, then so must classical computers, be they Pentiums or abacuses (or DNA, or human memory)."

This is a central problem, that I discuss in my papers. To a large extent my formal conjectures duck this issue. I think that we did gain some insight on the distinction between classical and quantum error correction and the special role of the "repetition mechanism" for robust classical information to emerge but there is more to do. This distinction should be interesting to QC believers as well.

Aram's third post: Two thought experiments

Gödel's Lost Letter and P=NP

a personal view of the theory of computation

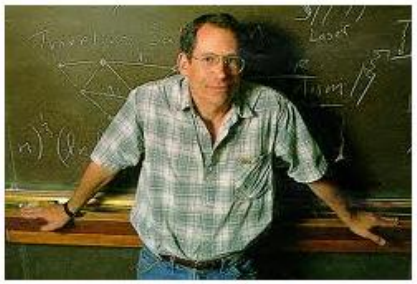
Home | About P=NP and SAT | About Us | Conventional Wisdom and P=NP | The Gödel Letter | Cook's Paper | Thank You Page

The Quantum Super-PAC

MARCH 5, 2012

by KWRegan | *tags:* BQP, Machine, quantum, randomness

What unlimited contributions might buy you in power



John Preskill is no stranger to high finance in physics. In 1997 he made a famous **bet** against Stephen Hawking and Kip Thorne relating to the **black hole information paradox**. Hawking conceded the bet in 2004, but Thorne has yet to agree. The prize was an encyclopedia of the winner's choice, which for Preskill was *Total Baseball: The Ultimate Baseball Encyclopedia*.

Today we present the third of three installments of Aram Harrow's initial response to Gil Kalai's

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
- Digital Butterflies and PRGs

Third post: Aram's second thought experiment - redefine the QC!

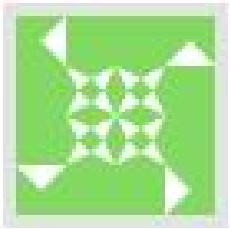
An even more imaginary quantum computer... provides another thought experiment that refutes Gil's conjectures. Imagine a large quantum computer with a high rate of noise. The experimenter attempts to create entanglement between qubits, and can indeed apply the entangling operations, but this entanglement almost immediately disappears because of noise from the environment. So far uncontroversial.

But what does it mean that the entanglement disappears because of noise? The Schrödinger equation says that the state of the entire universe changes unitarily. How can entanglement disappear in such a model? This is an old problem in the interpretation of quantum mechanics. The key is a principle commonly called "going to the church of the larger Hilbert space."

Third post: Aram's second thought experiment - redefine the QC! (cont.)

Any noisy quantum process can be modeled as a unitary interaction with the environment, followed by discarding [formally, tracing-out] the qubits of the environment. That is to say, unitary evolution only appears noisy because it involves systems, such as photons heading away at the speed of light, that are out of our control. This picture offers a way to resolve the problem of noise in quantum computers, albeit one that wont yield any practical computational speedups. We simply redefine what we call the "computer" to include all of the qubits in the environment that interact with it. This gives us a quantum computer that is definitely in a pure, highly entangled state, performing calculations that we have no idea how to simulate in sub-exponential time.

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.

REPLY

Other objections

- **Cris Moore:** Skepticism of quantum computers means skepticism of quantum mechanics
- **Joe Fitzsimons's:** Blind computation
- **Peter Shor:** It takes too much malice and intelligence for nature to detect and intercept that quantum error correcting codes.
- **John Preskill:** A general model where the threshold theorem holds.
- **Joe:** A 2-locality argument.

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

The relevance of non linear and chaotic behavior of classical systems

This issue was raised in the debate by Robert Alicki (and also by Michel Dyakonov). (I racall discussing it long ago with Tali Tishby.) This is a direction I did not pursue and I believe it is very relevant.

Does impossibility of QC means breakdown of QM?

The short answer is: No?

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.)

Can You Hear the Shape of a Quantum Computer?

JUNE 20, 2012

by KWRegan *tags:* BQP, fault-tolerance, Mark Kac,

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.

Reasons to disbelieve: 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
- State and evolutions can 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

Quantum computers and quantum mechanics

Failure of fault-tolerant quantum computations can be supported by quantum mechanics. This issue touches on profound questions regarding higher levels of physical laws and physical theories which are based on quantum mechanics. The crux of matter is the nature of approximations in quantum physics.

Thank you very much!