

Rasetti: Quantum Computers based on TQFT

Source: <http://sci.tech-archive.net/Archive/sci.physics.research/2005-03/0518.html>

From: Urs Schreiber (*Urs.Schreiber_at_uni-essen.de*)

Date: 03/22/05

Date: Tue, 22 Mar 2005 08:23:03 +0000 (UTC)

M. Rasetti is a theorist from Torino university. He says he is working on trying to figure out if quantum computation (QC) is fundamentally stronger than classical Turing-like computations. In other words, if QC can solve problems which are not in P in polynomial time.

I know that there is a meme floating around some brains which says that if you had a quantum system governed by a Hamiltonian whose discrete eigenvalues are a sufficiently hard to compute function of the integers you could, by measuring these eigenvalues in a suitably prepared system, essentially compute this function and hence solve not-P problems in polynomial time.

This argument I always found rather less than convincing. It suffices to note that by precisely the same argument you could claim that a classical analog computer may compute NP problems easily: Just partition classical phase space into a denumerable number of subsets and pick a system whose energy is a non-computable function of the ordinal associated to each such subset. Up to some smoothness issues this is precisely the analogous idea as above — and clearly not a reasonable way to get a stronger-than-classical computer.

What Rasetti is talking about sounds much more sophisticated — though in the end it seems to reduce to more or less the above argument. Or does it?

So the idea is that there may be more types of quantum computers than currently considered in the standard literature. In particular, so Rasetti's idea, using systems that have to be described by quantum *field* theory one might be able to (in principle) construct new and more powerful types of quantum computers.

This idea apparently goes back to Michael Friedman, who first proposed that non-abelian topological quantum field theories might exhibit features necessary so support a model of computation capable of solving not-P problems in polynomial time?

Apparently Friedman, Kitaev and Wang in particular proposed that Chern-Simons theory is a promising candidate.

I have not yet managed to talk to Rasetti and ask him some questions about his work, but if I understood correctly what he said in a talk the idea is this:

The computation of non-abelian holonomy as well as that of Jones polynomials is not in P. Since the observables of CS theory are precisely these quantities all we have to do is to set up a system which is governed by CS theory, somehow prepare it to be in a given knot state and then observe its observables. Since these will be not-P functions of these knots, we effectively have an analog quantum computer which computes not-P problems easily.

Does that make sense? Isn't it precisely the same idea as mentioned at the very beginning, that given any system whose observables are a not-P function of its states it superficially looks like a device that computes not-P problems in polynomial time.

I have the feeling that something is wrong here.

I also feel that there should be a high-brow theoretical answer for what is wrong or why this is not wrong and am surprised that among QC-theorists there apparently is no clarity about this.

So for me the conclusion of Rasetti's talk is currently just that if you are willing to be interested in systems whose observables are non-P functions of their states, then some quantum field theories in general and Chern-Simons theory in particular suggest themselves as laboratories since they do enjoy this property naturally.

It seems to me that the issue here is related to the general question in as much we want to regard analog computers as computers when it comes to complexity issues. I am not a computation theorist so what I am saying here will sound crude to those who are, but let me say it anyway:

Clearly when talking about computational complexity one has to remove analog computers from the picture somehow. For instance protein folding is a famous hard problem. It remains hard, even though I can figure out how a protein folds easily by just synthesizing it and seeing how it folds. That's an analog computation and I bet it scales linearly with the size of the protein. You might rather want to call it an experiment, though.

And that's the point, I think. It's an experiment rather than a computation. And the same is true for the Chern-Simons computer proposed by Rasetti et al. They propose to make experiments in field theory and regard the measurement of the outcome as a calculation.

For practical purposes that may be fine. If I really want to know the value of some Jones polynomial and I really find it easier to come up with a system governed by CS theory, prepare it suitably and measure

its observables somehow with sufficient accuracy, than to compute the polynomial on a digital computer up to that accuracy then that's fine I guess.

But

a) this has little to do with quantum computation and is all about analog computers, and

b) it does hence not show that quantum computers are inherently more powerful than classical ones.

I assume the problem is related to the fact that we really want to study _universal_ computers, not just special-purpose ones. I believe the problem is to figure out if a _universal_ quantum computer is more powerful than the universal Turing machine.

(This message is also available at <http://golem.ph.utexas.edu/string/archives/000534.html>)