

comp.theory: Re: THIS STATEMENT HAS NO PROOF IN ANY SYSTEM = true or false?

Re: THIS STATEMENT HAS NO PROOF IN ANY SYSTEM = true or false?

Source: <http://coding.derkeiler.com/Archive/General/comp.theory/2005-02/0318.html>

From: Ralph Hartley (hartley_at_aic.nrl.navy.mil)

Date: 02/09/05

Date: Wed, 09 Feb 2005 13:13:20 -0500

examachine@gmail.com wrote:

> *Ralph Hartley wrote:*

>

>> *For any number n of connected qbits, and any acceptable error epsilon,*

>> *a classical machine can simulate the quantum one. But the*

>> *computational effort required grows with decreasing epsilon and grows*

>> *(almost certainly exponentially) with n .*

>

> *I haven't seen any proof of exponential speedup*

I said **almost** certainly. The status of $BPP \stackrel{?}{=} BQP$ (the big quantum complexity question) is almost exactly the same as $P \stackrel{?}{=} NP$. Strongly suspected to be true, but without much prospect of a proof.

There are oracle problems for which Quantum computation is provably exponentially faster. That essentially means that if Quantum computation does **not** provide an exponential speedup, that fact would be tough to prove.

> *which would just end all the troubles of computer science.*

It would not. The class of problems to which the speedup is expected to apply is very small (though some are economically important).

For example, it would **not** be expected to apply to all NP problems. Nor would it answer the $P \stackrel{?}{=} NP$ question.

Also, It is unknown if a practical device that takes advantage of the speedup can be built. I suspect it can, but there are people I respect who disagree.

> *Isn't it more likely that there is just a polynomial speedup? (Like quadratic)*

Only if there are (classical) polynomial algorithms for factoring and discrete logarithms. Both problems **are** polynomial on a Quantum computer, and both are strongly suspected **not** to be polynomial on a classical computer.

Re: THIS STATEMENT HAS NO PROOF IN ANY SYSTEM = true or false?

comp.theory: Re: THIS STATEMENT HAS NO PROOF IN ANY SYSTEM = true or false?

Quite a bit of effort has gone into *trying* to find polynomial algorithms for those problems. Modern crypto protocols would essentially collapse if one were found.

Ralph Hartley