

# Re: Quantum Computer Algorithms

**Source:** <http://sci.tech-archive.net/Archive/sci.physics.research/2004-09/0468.html>

---

**From:** David Tweed ([dtweed\\_at\\_inf.ed.ac.uk](mailto:dtweed_at_inf.ed.ac.uk))

**Date:** 09/28/04

Date: Tue, 28 Sep 2004 07:28:29 +0000 (UTC)

frisbieinstein@yahoo.com (Patrick Powers) wrote

> However, David Deutsch (one of the pioneers of QC) has a neat line about

> how when building the Turing machine model "Turing thought he understood

> the physics of marks on tape works".

|

| I don't agree.

|

| Computations proved by Turing to be impossible would still be impossible on a quantum computer because solution brings contradiction.

I tried (in my typical broken English :-)) to point out later in that paragraph that the what is computable does not change between classical and quantum computers, it's that sometimes (to the best of our current knowledge) asymptotic execution time of algorithms for solving problems differs between classical and quantum algorithms. But the real point I was trying to make is that computability theory is often (at least from what I've seen) presented as an entirely mathematical notion, whereas it's more of the form

GIVEN THAT you can do these things in the physical world (physics)  
THEN building up with these elements these things are possible, these aren't, if you had an oracle which could.... then ..., etc (mathematics)

i.e., it's sort of a tower of mathematics built upon some foundations which come from physics. The quote about Turing thinking he understood the physics of marks on tape is supposed to show that you might have to re-evaluate the scope of physical 'information processing' afresh if your idea of what's physically possible changes. (As originally mentioned, turns out the shift from classical to quantum doesn't change what's computable, but does change some asymptotic complexities. And there are certainly people trying to come up with some example of a physical operation which changes what's computable, eg,

<http://portal.acm.org/citation.cfm?id=1011190>

although I'm unqualified to rate whether these ideas are sensible or not.)

|The sort of computations that a quantum computer is meant for are  
|those believed to be in NP. An informal definition is a puzzle that  
|is too expensive to solve, but the solution if known can be verified  
|easily. The classic example is factoring certain composite numbers.

|Turing did consider such problems. In his terminology, these can be  
|solved by a "nondeterministic computation." This confusing term means  
|that while searching for a solution somehow the correct choice is  
|always made. If you think about it, you will see that this is very  
|much the same as the definition of NP.

I've only a passing knowledge of quantum computation, but it's not clear to me that nondeterministic computation is precisely how quantum computation differs from classical computation. In particular, I can't point at some element of Shor's algorithm and say 'aha: that step is a non-deterministic computation', where non-deterministic is used the in computer sense of 'magically making the correct choice at some point'. (There are certainly elements there that I can relate to the classical computational notion of probabilistic computation.) I'd certainly be interested in a brief, readable reference (paper or web) that clarified the relation between non-deterministic & quantum computation.

Incidentally, it's not obvious to me why easy verifiability need be important for quantum computer algorithms? And certainly most minimisation problems are easy to state yet solutions don't come with any simple property to verify that a solution is a global minimum. And there's some work on function minimisation using quantum computing:

[www.iqc.ca/seminar/abstracts/081103.html](http://www.iqc.ca/seminar/abstracts/081103.html)

|So now we have uncomputable problems, which cannot be solved, and NP  
|problems, which a quantum computer could do. There are classes of  
|problems in between, solvable but not by a quantum computer.  
|Typically these are competitive games: since there is a competitor  
|with free will, there is no effective way to verify a purported best  
|strategy. So, harder than NP.

This bit loses me.

--

\_\_cheers, dave\_\_\_\_\_  
[www.inf.ed.ac.uk/people/staff/David\\_Tweed.html](http://www.inf.ed.ac.uk/people/staff/David_Tweed.html)  
tel: +44 131 651 3447 fax: +44 131 651 3435  
X wrote a book about this, which Y was carrying around for  
a long time with little discernible effect -- John Baez