

Quantum Computer Algorithms

Source: <http://sci.tech-archive.net/Archive/sci.physics.research/2004-09/0345.html>

From: David Tweed (dtweed_at_inf.ed.ac.uk)

Date: 09/23/04

Date: Thu, 23 Sep 2004 09:46:54 +0000 (UTC)

Google is your friend:

http://www.fact-index.com/q/qu/quantum_computer.html

has answers to most of your detailed questions.

However, I'll take a stab at answering your first question, because I'm not aware of any web-source which gives an overview before jumping in to details. It's basically a rehash of part of David Deutsch's "The Fabric of Reality".

>How does QC relate to CC?

One way to look at this is historically: Turing (& other people like Church who turned out to be working on the foundations of computability theory) were trying to find some way of analysing what sorts of "information processing" was possible in the physical world in a way that whilst clearly physically realizable (in an idealized limiting case of infinite resources) whilst abstracting away as many inconsequential physical details as possible. (I'm trying to avoid the phrase computability here because the mathematical notion of computability was more an outcome of the investigation rather than a motivation for it.) So the Turing machine is a sort of machine built using the elementary physical operations are making marks on tape, moving the tape and changing internal state (where these operations behave as in classical physics). Algorithmics relates to what information processing can be done with these operations and the relative execution time (in terms of numbers of operations). It turns out that of most of the various fundamental models of computation, the sets of physical operations enable both the same information processing and the same execution times, which arguably is what makes algorithmics such an effective subject to study. (Imagine if what you could compute and/or dramatic changes in asymptotic execution time differed from computing device to computing device...)

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". Our current best quantum mechanical

models of physics say it's possible build elementary physical operations of computation that manipulate entangled superpositions of states according to the exact rules of quantum mechanics for sets of states which are arbitrary size. (You can debate the experimental/theoretical justification for such hypotheses.) As I understand it (AIUI), this quantum mechanics based model of physical computation doesn't change the fundamental range of what information processing is possible (that is, what is computable) but does have some sequences of quantum operations (algorithms) which produce the same result as classical algorithms but with a smaller asymptotic execution time. However, AIUI it's not the case that all classical algorithms can be converted to quantum algorithms which have asymptotically lower execution times, and there's no small description of how quantum complexity theory relates to all the various classical complexity classes, and indeed many open questions about how they relate.

So quantum computing is what classical computing would be, except you use quantum mechanical physics and all its possibilities in your elementary physical operations rather than classical physics. The question of what changes occur to algorithms depends whether you can relate something about your problem to an operation with different quantum and classical time complexities: appropriately expressed the idea behind Shor's algorithm works on a quantum or classical computer, but its because of superpositions & the quantum fourier transforms different asymptotic complexity the algorithm has different time complexities in QC and CC. It's not just convertability of algorithms between CC and QC but also how the complexity changes.

Hopefully this high level overview will make the more detailed stuff on the web more approachable.

__cheers, dave_____

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