Quantum computing, and why it's exciting!

Iain Stewart, Dept. of Computing, Imperial College, London SW7 2AZ, U.K.

Tuesday 28th July 2009
(with some post-talk corrections and improvements)

Quick summary - how to decide whether quantum computing is for you!

- If you're interested in **speed**...
  - you should be "cautiously interested" in quantum computing
  - it speeds up *a select few* things enormously over the "state of the art"...
  - ...but *most* general-purpose computing tasks apparently get little, if any, speedup - you have to "strike lucky"
- If you're interested in **cryptography**...
  - you should "unfortunately"(!) feel obliged to keep an eye on quantum computing
  - it *ruins* large swathes of classical cryptography...
  - but then *offers* "quantum cryptography" as a partial replacement!
- If you're interested in **modelling physical systems**...
  - quantum computing has fascinating potential for modelling
  - time and again, modellers have to "cheat" with the quantum aspects of what they're modelling
  - quantum computing offers the chance to be honest with those aspects
    - to get them *right* for our actual world; and
    - even to explore the impact of *different parameters* (particle charges, mass ratios, etc.) than those of our world!
- If you're interested in **distributed "grid computing"**...

Quick summary, cont'd.

- If you're interested in **distributed "grid computing"**...
  - you should suddenly be *very* interested in quantum computing!
  - some recent developments may have great potential for grid computing
  - a "quantum grid" will, it seems, allow *perfect obfuscation* of what data - and even what algorithm! - one grid user (Alice) is asking another (Bob) to handle on her behalf
    - ∗ even *Bob* can't tell what Alice's requests "really mean"!
  - thus, whole new communities (users with highly sensitive or private data and/or tasks) might learn to stop worrying and love the grid!

Why is there such a thing as “quantum computing” anyway?

- Take a subsystem of the world, put it in a box (even just in your imagination!), and call it a “computer”
- What can it compute?
- Answer: whatever **physics** permits it to compute!
- The various “classical” computing models - the Turing machine, the cellular automaton, etc. - make implicit assumptions about what the stuff of our world can do
  - a read/write head can move around and view/change a strip of tape - that sort of thing
- But the stuff of our actual, quantum world can do *more!*
  - it can go into a “superposition” of states, *each* of which can be something like a classical state of *the whole machine*
  - it can become “entangled” with other stuff far away, such that no classical “pre-agreement” instructions (“in circumstances X, you do this, and I’ll do that...”) can mimic *what the distributed entangled stuff actually does*
- Quantum computing is what you get when you ask “what can I compute with stuff which has such extra capability?”
  - and of course, how fast, with what resource usage, etc.

General-purpose computing - some limited speedup possible

- For the specialised computations of *cryptography* and *modelling physical systems*, quantum computing can offer huge speedups - more about those cases later
- But what about general-purpose computing?
- A large fraction of today's computing power goes on Knuth's two S's: *sorting* and *searching*
- Quantum computing so far offers no speedup for *sorting*...
- ...but **Lov Grover** discovered around 1996 that quantum *searching* through N items can be done in $\sqrt{N}$ time!
- The small print:
  - the entire database being searched has to be stored in quantum memory
  - the "time" expression above refers to *abstract sequential steps*
  - it seems likely a quantum machine's "clock cycle" will, at least initially, be slower than mature classical technology
- Even so: a database with 1,000,000,000 items can be searched 30,000 times "logically faster" - so even with a clock cycle 1,000 times *slower*, that's 30 times faster in real time!
- Grover's search algorithm also works for search through *candidate solutions* to an optimisation problem or the like
  - ...and it only needs whatever quantum memory the act of testing *one* candidate solution requires!
- Thus optimal paths, circuits etc. can be found in roughly the square root of the classical time (for example, taking 1,000,000,000 quantum steps to search through 1,000,000,000,000,000,000 candidate solutions)
- This is **not** a reduction from exponential to polynomial...
- ...but it may still be of value in many particular cases!

Cryptography - a death... and an awkward rebirth?

- Much of today's (classical) cryptography depends on making an adversary's cracking efforts *too hard* to be practical
- The RSA public-key protocol, and various tweaks thereof, depend on a number theorist's old favourite classically hard task - *finding the factors* of a large integer
- **Peter Shor** discovered around 1993 that *factoring is easy* on a quantum computer!
  - polynomial time, compared with somewhat less than exponential time for the best currently known classical algorithm
- Thus, if quantum computing becomes cheap and ubiquitous, much of classical cryptography will be ruined
- *Quantum* cryptography - designed to be unbreakable even if an eavesdropper or other adversary has access to quantum computing power - does exist as a partial replacement
- It is, however, more generally cumbersome than classical cryptography
  - resources such as keys can't just be published and then used by any number of counterparties...
  - ...they need to be created, exchanged and consumed for each usage (just like classical one-time pad cryptography)
- So cryptography will still be *possible* in a ubiquitous quantum computing setting...
- ...but not quite as *user-friendly* as the cryptography we know today!

Simulating the world

- Probably the single most inspiring *scientific* usage of computing power has been **simulation**
- But there's a problem, which modellers have brushed under the carpet
- The quantum "stuff" of our world can casually go into vast, sprawling superpositions of states, which can interfere and entangle with each other in rich and complex ways
- The only known *fully honest* way a *classical* computer can mimic this is to wade through an exponential explosion of "versions" of the system being modelled
- This is hopeless for all but the tiniest quantum systems
- Time and again, modellers have to "cheat" with the quantum aspects of what they're modelling - they may for example notice some regularity in the way superpositions behave, which they hope(!) scales to larger systems
  - For example, in *ab initio* chemistry, approximations such as *atomic and molecular orbitals* have become so useful that many people - even some textbook writers! - have forgotten that *they don't actually exist* in a true many-electron solution!
- By "hacking" a classically computed scaled version of a purported regularity into a simulation, modellers can achieve tolerable accuracy in many cases...
- ...but at the cost of no longer honestly tracking what the system is doing in its own, quantum terms

Simulating the world, cont'd.

- Quantum computing has fascinating potential for modelling
- At least for many Hamiltonians (prescriptions for time evolution), a quantum computer will be able to keep up with the system being modelled
  - by sending *its own quantum stuff* into the same sort of sprawling superposition of "versions" that so quickly overwhelms a classical machine
- Such **quantum simulation** will likely cut the run-time of many, many simulation problems **all the way from exponential time to polynomial!**
  - chemical reactions - bond breaking and re-making in glorious detail
  - exotic material properties - superconductivity, superfluidity, etc.
  - some grand challenges for physics - quantum fields in the early universe (topological defects, etc) or other extreme environments
- But there's more...
- ...we can simulate things as they *could have been*, which history shows often gives great insight into the way they actually are!

Simulating counterfactual worlds - “journeys to elsewhy”

- Even with classical simulation, modellers enjoy varying things that our actual world (or our actual corner of the world) holds constant, or in advance of an anticipated change
  - Fancy simulating the climate with a different atmosphere? a hotter sun? farms instead of rainforests intercepting the incoming sunlight?
  - Fancy simulating planet formation with a different chemical cocktail than our actual early solar system?
  - ...and looking for planets elsewhere that resemble what you get?
- With quantum simulation, more radical “variant worlds” may become tractable
- Today’s physics throws up “constants” (particle charges, mass ratios, etc.) stuck at certain values, with no clear reason *why* those values are special
- Simulations of *alternative versions* of those values may help clarify whether and how our world’s actual values “stand out” in some sense in the landscape of competing alternatives
- Modellers are used to taking simulated journeys to else*where* or else*when* - “what will the solar system be like a billion years from now?” sort of thing
- Quantum simulation may offer us the scientific ride of a lifetime - **journeys to elsewhy!**
  - some limited “journeys to elsewhy” are possible even on classical hardware, but quantum simulation will likely greatly extend our range
- It might be a while coming, but: **Enjoy the ride!**

Distributed “grid computing” - a possible quantum revolution!

- In recent years “grids” of computers, large and small, have started to emerge
- Even at a hobby level, people are taking to offering spare CPU cycles to help with various grand projects
  - SETI@home - the search for extraterrestrial signals
  - Einstein@Home - the search for gravity waves
  - Folding@home - simulations of how proteins fold into precise shapes
- The projects currently most successful in terms of sheer scale all have one thing in common: **non-sensitive data**
  - typically data which has already been made public as part of the general scientific endeavour
- But what about people wanting heavy crunching of **sensitive** data?
  - patient medical histories
  - banking transactions, buy/sell orders in markets
  - customer buying habits and preferences
- Patterns hidden in such data could greatly help with medical progress at one extreme of grandeur, or just general market efficiency and responsiveness at the other
- The agencies sitting on such data typically don’t want to acquire and manage vast tracts of computer hardware themselves
- They’d love to farm out such interesting tasks to “the grid”...
  - ...but they can’t! the data is precious and confidential!
- Encryption, sadly, is not the answer:
  - Alice: “if $x < y$...”
  - Bob: “Sorry, I can’t help you there - you’ve encrypted x and y!”

Quantum grid computing, cont'd.

- People have looked into lighter forms of obfuscation than full encryption, to let Bob do Alice's "if $x < y$..." or whatever, but (except in a few lucky cases like keyword search from a fixed repertoire) obfuscation light enough to let serious data-crunching go ahead is *so* light it's far too easy for Bob to figure out the sensitive data!
- **QUANTUM COMPUTING TO THE RESCUE!**
- In 2008, **Anne Broadbent**, **Joseph Fitzsimons** and **Elham Kashefi** announced a quantum grid computing protocol they call "universal blind quantum computation"
- With this protocol, if Alice hires Bob to perform a quantum computation on her behalf, only Bob needs a quantum computer - Alice can get away with a classical machine (to handle the required two-way data stream between her and Bob) and some simple quantum hardware (single-bit preparation and transmission) of the sort that exists today
- The level of obfuscation their protocol achieves is sensational:
  - not only Alice's data but *even her algorithm* is completely cryptographically hidden from Bob
  - Bob can make no sense of Alice's stream of either instructions or data, nor of any of the intermediate or final results he streams back to Alice, even if he uses further *quantum* computing power in his cracking efforts
  - any eavesdroppers - whether in league with Bob or not - can likewise learn nothing of Alice's algorithm, data or results
- If this still quite recent work stands up to scrutiny, it may come to be heralded as the "grid cleared for take-off" protocol
- Whole new communities - users with highly sensitive or private data and/or tasks - might learn to **stop worrying and love the grid!**

Waiting for quantum computing: the engineering challenge

- Will we see robust, reliable, scalable quantum computing any time soon?
- There are many candidate quantum architectures being explored, but one in particular seems very hopeful for scalability and practicality: **measurement-based quantum computing**
- A traditional "gate-based" quantum computation performs delicate quantum operations all through its lifetime
- In 2000, **Hans Briegel** and **Robert Raussendorf** discovered a class of quantum states - "cluster" states - with some remarkable properties
- A cluster state acts as a *universal starting state* for a new way of doing quantum computing
- You can be given a standard initial cluster state *before* deciding what quantum algorithm you feel like running...
- ...and you can then perform any quantum algorithm of your choice by performing **only measurements** (these being much easier to perform than full quantum gate operations) on the cluster state!
  - you may of course use *classical* computing power - your own brain, pencil and paper, any classical machine - to decide what measurements to perform next, given the outcomes so far
- Cluster states of a few bits have been prepared - the race to create decent-sized ones is on!
- There are many other proposed architectures, and many researchers are much more optimistic about at least one of them succeeding than was the case even a few years ago
- Thanks to the algorithms and protocols discussed earlier, there will be *many* people cheering them on! **WISH THEM LUCK!**
- **Thank you!**