Quantum Computational Models

GC7: Journeys in Non-Classical Computation

Sam L. Braunstein, Susan Stepney

Non-Standard Computation Group
Department of Computer Science
University of York
bit commitment protocols

- classical bit commitment
  - cryptographic techniques to lock up the committed bit in tamperproof wrappers
- quantum impossibility
  - entangle to “committed” qubit with another outside the box
  - rotate this other bit, to change the “committed” bit, at a later date
- special relativity to the rescue!
  - split the information onto two paths
  - light travel times restrict the operators that can be applied
  - after-commitment rotations take time, and can be detected
error correction

• classical
  - repetition, and multiple copies

• quantum
  - "no cloning theorem" \implies no copying \implies no quantum error correction??

• no, because there's a different classical formulation
  - correlations of multibit states
  - this can be generalised to the quantum case
  - quantum error correction is possible
the problem of linearity

- consider a quantum program $P$ that takes an unknown amount of time to execute on input states $|\Psi_1\rangle$ and $|\Psi_2\rangle$
- linearity describes it running on a superposition of input states $P(\alpha|\Psi_1\rangle + \beta|\Psi_2\rangle)$
- given the unknown running times, we currently have no idea how to construct a circuit for $P$ to maintain coherency
- this seems to imply
  - no if statements (two branches with different running times)?
  - no general recursion?
  - no general subroutines?
there is often a number of different ways of formulating computational problems classically.

- classically equivalent results
- some of these generalise naturally to the quantum domain, but some do not

example:

- classical recursion (multiple function application) does not generalise, because of the unknown time for each call:
- "fixed point" reformulation seems to generalise more naturally
GC7 and non-classical physics

- the underlying laws of physics affect computation and information theory
- quantum computation is very different from classical computation
- quantum investigations can lead to new computational theories
- and can also shed light on the underlying classical theories
the proposed journey

- to investigate various classically equivalent models of computations
  - discover which ones generalise to the quantum domain
    - leading to powerful new quantum computational models
    - deeper understanding of the various classical formulations
  - or, discover that none of them do!
    - requirement for genuinely novel quantum paradigms

- to understand classically possible, but quantumly impossible, protocols
  - when, and why, isn’t classical a subset of quantum?
  - assumptions of decoherence, and when they break down