Quantum Computing - The Next Generation of Computing Technology

Ian Glendinning

October 24, 2000

Outline

- Introduction
- Qubits and Quantum Gates
- Applications and Algorithms
- Building a Quantum Computer
- State of the Art and Future Prospects
- Deeper Implications
- Conclusion

Introduction

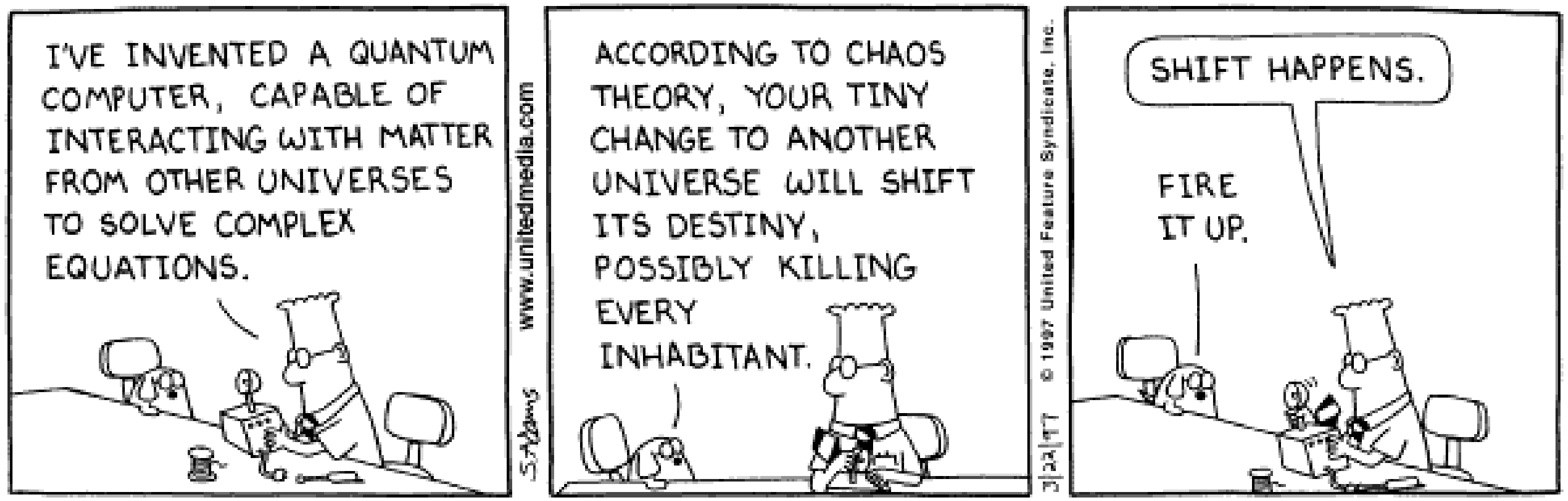
- What is Quantum Computing?
  - A fundamentally new mode of information processing that can be performed only by harnessing physical phenomena unique to quantum mechanics
- What is Quantum Mechanics?
  - The deepest theory of physics; the framework within which all other current theories, except the general theory of relativity, are formulated

Introduction

- What makes quantum computers different from classical computers?
  - Binary data is represented by a two-state quantum system, e.g. electron spin or photon polarization
  - Information stored in a 2-state quantum system is called a *qubit* and its values are labelled $|0>$ and $|1>$
  - Unlike a classical bit, which can only have the value 0 or 1, a qubit can be in a *superposition* of the states $|0>$ and $|1>$
  - It can be thought of as exisiting in two different universes!

Introduction

- Dilbert on Quantum Computing



Introduction

- What makes quantum computers so exciting?
  - Operations on qubits effectively act on both the values $|0>$ and $|1>$ at the same time: Quantum Parallelism
  - A register with L qubits can be in a superposition of 2^L states
  - Operations can be performed on all 2^L states simultaneously
  - That's what I call *really* high performance computing!
- Where's the catch?
  - Decoherence: quantum states are usually microscopic systems, sensitive to interference from their environment

Qubits and Quantum Gates

A qubit may take on any value:

$$\alpha|0> + \beta|1>$$

where α and β are complex numbers.

A *measurement* of the state of the qubit will always yield either $|0>$ or $|1>$, with a probability of $|\alpha|^2$ for $|0>$ and $|\beta|^2$ for $|1>$

Since the probability that the qubit is observed to be in some state must be one, it follows that:

$$|\alpha|^2 + |\beta|^2 = 1$$

Qubits and Quantum Gates

This property, and therefore the probability interpretation, is preserved under transformation by any *unitary* operator, defined by:

$$U^*U = 1$$

A quantum state may be transformed into a new quantum state by a unitary operator, and we can define quantum analogues of logical operators, such as the NOT operator:

$$U_{NOT}|1> = |0>$$
$$U_{NOT}|0> = -|1>$$

where the phase is for consistency of interpretation with a spin 1/2 particle, corresponding to a 180° spin rotation

Qubits and Quantum Gates

We can perform more general computations than on classical bits; unitary operations on linear combinations of states:

$$U_{NOT}\frac{1}{\sqrt{2}}(|1> + |0>) = \frac{1}{\sqrt{2}}(|0> - |1>)$$

and operations with no classical analogue, e.g. Deutsch's 'square root of NOT':

$$(U_{SRN})^2 = U_{NOT}$$
$$U_{SRN}|1> = \frac{1}{\sqrt{2}}(|1> + |0>)$$
$$U_{SRN}|0> = \frac{1}{\sqrt{2}}(-|1> + |0>)$$

which physically corresponds to a 90° spin rotation.

Qubits and Quantum Gates

So far we have considered a single qubit, represented by, say an electron's spin. By considering multiparticle systems we can construct quantum registers. An n-bit register may be written as:

$$|1> \otimes |1> \cdots \otimes |1> \equiv |11 \ldots 1>$$

and applying our SRN (or Hadamard) transformation to this state, we generate a superposition of all 2^n states:

$$U_{SRN} \otimes U_{SRN} \cdots \otimes U_{SRN} |11 \ldots 1>$$

Applications and Algorithms

The most important applications currently known are:

- Cryptography: perfectly secure communication
- Simulating quantum-mechanical systems efficiently
- Factorising large numbers very rapidly (Shor's algorithm)
- Searching, especially algorithmic searching (Grover's algorithm)

But who knows what else will be discovered...

Grover's Algorithm

The problem: search a database with N names in a random order for the phone number of a friend. Classically this would require on average $N/2$ steps.

Grover's algorithm can search a quantum database in $O(N^{1/2})$ steps.

Formulate as a system with 2^L states, $S_1, S_2 \ldots S_N$. We want S_m.

1. Start with L qubit register in state
   $|0 >= |00\ldots 0 >$
2. Apply Hadamard transformation to generate a superposition of all possible states

$$U_H|00\ldots> = \frac{1}{2^{L/2}}(|0> + |1>)^L = \frac{1}{2^{L/2}}\sum_{n=0}^{2^L-1}|n>$$

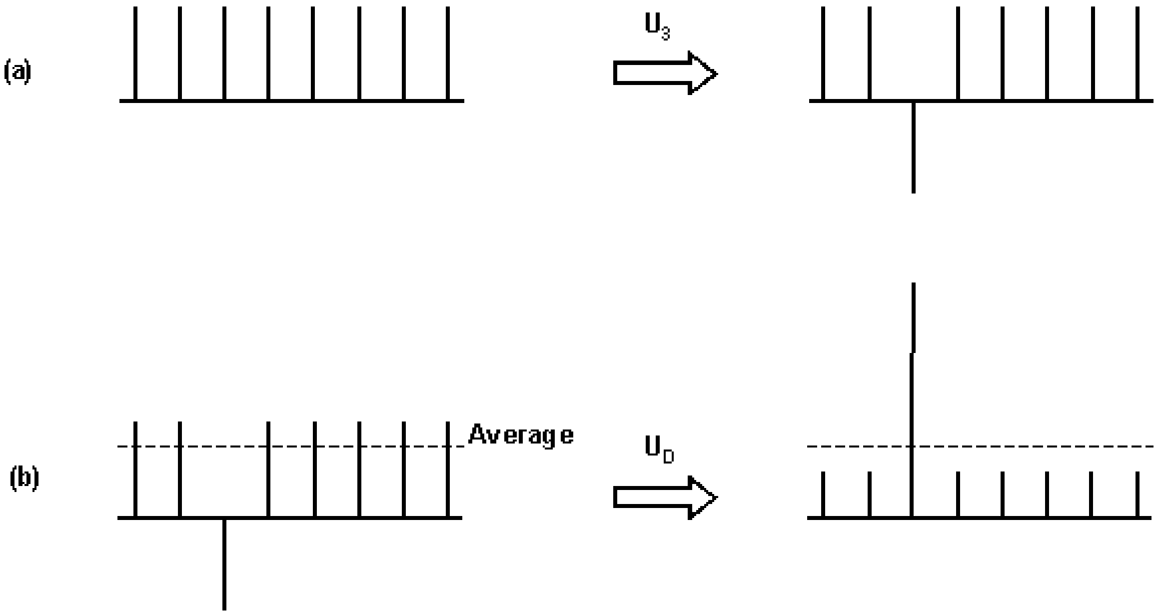
3. DO FOR $O(N^{1/2})$ TIMES
   (a) Apply the operator U_m defined by
   $U_m|n> = -|n>$ for $n = m$
   $U_m|n> = |n>$ otherwise
   (b) Apply Grover's 'diffusion' operator
   $U_D = U_H U_0 U_H$
4. END DO
5. Measurement yields state S_m with probability of at least $1/2$

Grover's Algorithm

This may appear cryptic, but the effect is is actually rather simple

- The diffusion operator corresponds to a reflection of all the amplitudes about their mean
- Because the sign of the amplitude we want has been reversed, it is amplified at the expense of the others

Grover's Algorithm



Building a Quantum Computer

Very primitive quantum computers have already been built

- Nuclear Magnetic Resonance (NMR)
- Ion traps
- Cavity Quantum Electrodynamics

It has been theoretically proven that quantum error correction is possible, so decoherence can be tackled.

State of the Art and Future Prospects

- State of the Art
  - The world's first 2-qubit quantum computer was developed in 1998 at University of California Berkeley)
  - The first 3-qubit quantum computer in 1999 at IBM-Almaden
  - The order-finding result announced in August 2000 by IBM-Almaden researcher Isaac Chuang is the most complex algorithm yet to be demonstrated by a quantum computer
  - It runs on a five bit NMR computer
  - Quantum Computer Emulator

– Quantum Compilers

Deeper Implications

- The Church-Turing hypothesis (that all 'natural' models of computation are equivalent to each other), was never proved
- Its analogue in the quantum theory of computation (the Turing Principle, that the universal quantum computer can simulate the behaviour of any finite physical system) was straightforwardly proved in Deutsch's 1985 paper
- A stronger result, namely that such simulations can always be performed in a time that is at most a polynomial function of the time taken for the physical evolution, has since been proved in the quantum case

Deeper Implications

- Performing any computation that provides a definite output is tantamount to proving that the observed output is one of the possible results of the given computation
- We can always translate such a proof into the proof of some mathematical theorem
- Henceforward, a proof must be regarded as a process – the computation itself, because quantum computers will prove theorems by methods that can never be checked step-by-step; if the steps for such a proof were printed out, the paper would fill the observable universe many times over

Deeper Implications

- The theory of quantum computation allows us to look at the question of consciousness from a new perspective, since every physical object can be regarded as a quantum computer and any physical process can be considered a computation
- The brain can therefore be regarded as a computer and consciousness as the result of a computation, and Deutsch's universality result means it must be possible to simulate conscious rational thought using a quantum computer
- Some believe that quantum computing could well be the key to cracking the problem of artificial intelligence but others disagree

Conclusion

- Quantum Computers can solve hard problems
  - A new classification of complexity has been erected
  - The class of problems for which quantum computers have a big adavantage remains to be characterized
- Quantum errors can be corrected
  - The effects of decoherence can be overcome
- Quantum hardware can be constructed
  - We are privileged to be witnessing the dawn of the age of coherent manipulation of information in the laboratory

Conclusion

- There is almost daily progress in developing ever more promising technologies for realising quantum computation and new quantum algorithms with various advantages over their classical counterparts.
- There is potential here for truly revolutionary innovation.

Conclusion

- Quantum Computing Limerick

  If the computers that you build are quantum,
  Then spies of all factions will want 'em.
  Our codes will all fail,
  And they'll read our email,
  Till we get crypto that's quantum, and daunt 'em.

  Jennifer and Peter Shor

- Further Information

  http://www.qubit.org/