Copyright Warning

Curtin
University of Technology

Theoretical Foundations of Computer Science 300

Lecture 10

Other Computing Models

Curtin University of Technology

Outline

- Other Architectures
- Quantum Computing
- Biological Computing

Curtin University of Technology

Assessment Criteria

- **None**. The material in this lecture is not assessable.

Curtin University of Technology

Determinism

- The Decidability and Complexity discussed in this unit so far apply to deterministic Turing Machines only.
- Non-Deterministic Turing Machines are used as a way of testing for membership of NP.
- There are a number of computational models under development that aren't adequately modeled by the DTM or the NTM.

Alternatives

- Quantum Computing – using Quantum uncertainty to generate something similar to non-determinism.
- DNA Computing – using the DNA in strands of viruses to encode and solve problems
- And there's many others, including photonic (light-based) computers and even living computers (made of leech parts!).

Curtin University of Technology

And then there was…

- There are also some unusual implementations of the Turing Machine.

- One implementation, using cards and rules from the game Magic: the Gathering is described on a link in Blackboard.

- Another implementation is a working Turing Machine built entirely out of Lego!

The Lego TM

- Not only is it build out of Lego, it doesn't use electricity.

- The first 2 or so minutes explain what you already know. The rest talks about the machine.

  http://www.youtube.com/watch?v=KrNTmOSVW-U

- But now, on to something more serious ... I carefully won't mention the computer circuits utilizing billiard balls!

Curtin University of Technology

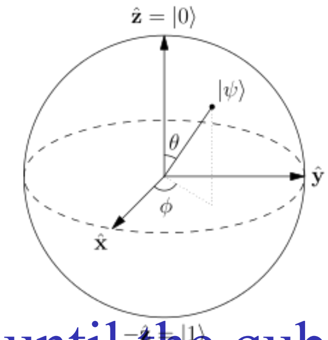
QUANTUM COMPUTING

The Quantum Turing Machine

QTM = DTM ?

It’s a little (qu)bit different

- Normal computers store information using bits
  - ➢ Bits take a value of either 0 or 1
  - ➢ Their value is always known and can always be examined



- A Quantum computer uses qubits:
  - ➢ A qbit also takes on a value of either 0 or 1
  - ➢ However the value of a qubit isn’t determined until the qubit is collapsed – at that point either a 0 or a 1 is observed
  - ➢ The important fact is that *before* collapse, the qubit has a value of both 0 and 1 – this is called Quantum superposition
  - ➢ Because it has both values, we can effectively check both possibilities at once.

Curtin University of Technology

PhD Movie

- This movie is a short introduction to quantum computing.
- From www.youtube.com/watch?v=T2DXrs0OpHU

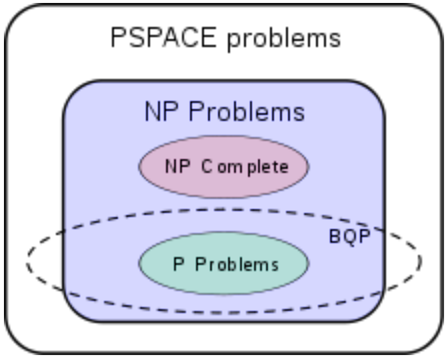
Applications

- Because quantum computers can try a large number of possibilities at once, they make a number of problems easier to solve.
- Any problem in NP can be solved in polynomial time by a NTM – but it is a little uncertain whether this holds for a QTM!
- However QTM have been shown to be very useful for specific applications:
  - ➢ Several types of optimization
  - ➢ RSA decryption

Curtin University of Technology

What problems CAN a QTM solve?

- There is a difference of opinion.
  - ➢ The general opinion, as presented in the PhD video clip, is that a QTM is similar in power to a NTM
  - ➢ A fairly strong body of research suggests that it is not true, but that QTMs instead have their own category of problems that they can solve in polynomial time – BQP
  - ➢ The extent of BQP is not known, but it is believed that it does **not** include any NP-complete problems



QTM with post-selection

- A model of a QTM with post-selection has been proposed.
  - ➢ post-selection means putting conditions on probability

- This model has been shown to be equivalent in power to complexity class PP
  - ➢ PP is a probabilistic complexity class that includes problems such as SAT
  - ➢ In fact, PP includes all of NP, and thus all of NP-C!
  - ➢ The QTM with post-selection can thus solve all NP-complete problems in polynomial time. Theoretically.

Curtin University of Technology

Classical vs Quantum (the Hype)

To factor a 2048-bit number:

- a classical algorithm would :
  - ➢ require a server farm covering 1/4 of the land in North America
  - ➢ cost a million-trillion dollars
  - ➢ consume 100,000 times the current energy output of the entire world
    - – This is the equivalent of using the world's supply of fossil fuels in a single day
  - ➢ take 10 years
- a quantum algorithm using current technology would:
  - ➢ require 10 trillion times less energy (at 10 megawatts)
  - ➢ cost ~100 billion dollars at current prices
  - ➢ finish in just 16 hours.
- However, please note that the “current technology” part is not elaborated upon.

Curtin University of Technology

So…?

- How powerful are quantum computers, really?

- The answer is going to depend on:
  - what sort of quantum computers we're talking about
  - whether not it's actually feasible to build practical quantum computers

- There are currently no quantum computers known to exist that are of a decent size (more than 10 qubits) and truly general.

Curtin
University of Technology

State of the Art

- Currently, quantum computing is more theoretical than practical (as far as the public knows).
- General quantum computing is only possible with a small number of qubits (6 or so).
- A large-scale quantum chip (512 qubit) is commercially available and has been shown to match world leading super computers
  - The comparison isn't entirely fair since the quantum computer is not general while the other computers were
  - Only quantum annealing is possible

Google's Quantum Computer

http://www.youtube.com/watch?v=CMdHDHEuOUE#t=368

- This video is referred to in an article that discusses Google using the quantum computer to:
  - optimize Android
  - solve game trees faster than conventional computers
  - develop quantum machine learning applications for devices such as mobile phones
  - improve blink detection for Google Glass
  - "generate algorithms faster than the entire Google datacentre"!

Curtin University of Technology

Other Work

- A recent (March 2013) breakthrough at Yale has possibly shown one more step to true quantum computing.

- The Yale scientists that they were able to isolate a qubit, but they cannot yet control the quantum collapse.

- The paper is here:

http://www.nature.com/nature/journal/v495/n7440/full/nature11902.html

Curtin University of Technology

Other Work

- In Germany, work has been done on using electromagnetic fields to enclose qubits.

- Results have been presented demonstrating multi-qubit systems.

- A useful thesis can be found here:

http://edoc.ub.uni-muenchen.de/16099/1/Viehmann_Oliver.pdf

Curtin University of Technology

Quantum Turing Machine

- Was proposed by David Deutsch in 1985.

- There are some interesting points raised with this:
  - A QTM never actually 'halts', but rather signals that is has completed the computation by setting a chosen qubit to 1
  - The state of a QTM is a unit vector in a state space
  - The tape position changes by only 1 space for each step
  - Every action taken by the QTM is reversible – and the paper discusses how this can also apply to the classical model
  - The model uses a matrix as it's transition function and changes state using matrix multiplication

QTM vs NTM

- A QTM can be considered to be in multiple states at once. The same is true for a NTM.

- So what is the difference?

- According to the QTM model, a QTM has a certain probability of being in each state, while a NTM actually IS in all appropriate states.

- So it comes to who is correct:
  - ➢ if the other scientists are correct, QTM ≅ NTM
  - ➢ if the computer theorists are correct, a QTM only has a polynomial speedup compared to a NTM
    - – On the bright side, with post-selection we again get QTM ≅ NTM

Curtin University of Technology

DNA COMPUTING

Parallel Computing in a Test Tube

What is DNA computing?

- The short answer – computation using encoding of information into DNA.

- The long answer (from work by Adleman):
  - Strands of DNA in enzymes are used to construct the biological equivalent of logic gates
  - The molecules are mixed in a test tube, causing DNA strands to combine. Within a few seconds, fairly much every possible combination has occurred.
  - Eliminate the strands that do not represent solutions through chemical means
  - Decode the answer(s).

Curtin University of Technology

DNA Logic

- Logic gates built of DNA don’t use electricity.
- Instead, they are sections of DNA that latch on to and combine other DNA in an appropriate manner.
- For example a DNA AND gate links two other DNA strands in sequence

Curtin University of Technology

The Beginnings

- The Adleman method was designed as a proof of concept.
- The initial problem solved was finding a Hamiltonian Circuit through 7 cities.
- Solving the problem took seconds on the first try, but encoding and decoding took days.

Curtin
University of Technology

Progress

- Since then, DNA computing has been used to build the equivalent of TMs.
- Work has been done to see what problems it is suited for.
- Experiments with different molecules are ongoing.
- One problem that has a suggested solution is the Bounded Post Correspondence Problem
  - ➢ It requires a lot of manual set up and analysis

Curtin University of Technology

Progress

- Recently (March 2013) researchers stored all of the following in DNA:
  - ➢ Shakespeare's sonnets (text)
  - ➢ Scholarly paper (PDF)
  - ➢ A colour photograph (JPEG)
  - ➢ A part of Martin Luther King's speech (MP3)
- The files (total size around 750kB) were stored in the contents of a small test tube.
- The coding process includes an index and error correction.

DNA Storage Video

- http://www.youtube.com/watch?v=RmXJtKYdhT8

- Listen out for the estimate of the cost per MB.

Curtin University of Technology

The Advantages of DNA Computing

- Huge memory space
  - 1L of water can contain enough DNA for around 10^{19} bytes.
  - That's about 9,094,947 TB!

- Massively parallel
  - It is possible to perform operations on all of this data in parallel
  - The potential speed of computation is around 10^{14} operations per second
  - By comparison, the current fastest computer (as of June 2013) is around 3.4×10^{16} flops.

Curtin University of Technology

The Down Side

- At this stage, the DNA sequences must be set up using a rather slow process.

- Reading the results is also slow and can be expensive.

- So, while running the actual algorithm may be fast, this speed is lost due to the slow and work-intensive job before and after the calculation.

Curtin University of Technology

ALTERNATIVE COMPUTING

The Rest

Optical Computing

- The primary aim is to replace electronic components with photonic components
  - That means, components that use light (photons).

- The first optics device was produced in 2003, but there has not been much progress.

- There is also work using photoluminescence
  - That means chemical light

Chemical Computing

- The use of chemical reactions to change the state of substances.
- Has some of the advantages of DNA computing
  - Appears to be massively parallel
- Not to be confused with the simulation of chemical and molecular reactions using computers that is also referred to as chemical computing.

Curtin University of Technology

Wetware

- Why try to simulate a brain with computers, when you can build a computer out of a brain?
- Normally called biological neural computing
- Involves growing artificial ‘brains’ our of living neurons taken from leeches
- One prototype exists that can perform simple arithmetic such as addition

(No, this is not a joke.)

Summary

- Other ways of computing are being developed.
- While they show promise, they are not yet ready to be fully deployed.
- It is important to keep abreast of developments in these fields in order to seize possible opportunities.
- Professional organizations are a good way to do this.

Curtin University of Technology