Non-classical computing, feasible versus infeasible

Lewis Mackenzie & Paul Cockshott, University of Glasgow

Greg Michaelson, Heriot-Watt University

Introduction

- **Fundamental limits to computing established by Turing in 1930s**
  - halting problem: can't tell if arbitrary Turing Machine terminates
  - all subsequent bases for computing equivalent to TMs
- **Variety of proposals for *hyper-* or *super-Turing* computing**
  - logical challenges
  - physical challenges

- **Logical challenges**
  - alleged restrictions to TMs
    - e.g. interaction machines more powerful as TM tape cannot change – why not?
  - alleged emergence from combined theories
    - e.g. $ calculus = process algebra + cost

functions derived from von Neumann/Morgenstern

utility theory

Introduction

- **Physical challenges**
  - rely on having available some sort of ***actualised*** infinity
  - functions are TM computable if they required finite resources in terms of time and space
  - TM tape ***potentially*** infinite length but always finite at any given stage of computation
- **no good reason to suppose that we do or can ever have access to infinite resources.**

Introduction

- **Feasible non-classical computing must be finite and in accordance with physical laws.**
- **If we assume the currently known general laws are universal we can place bounds on what such devices can ever do.**
- **General physical bounds may only be approached in highly exotic scenarios.**

Physical Limits to Computation

- **Any physical system governed by mathematical laws that determine its evolution in time can be viewed as a computer.**
- **Such a "computer" only of practical use if a mechanism is available to manipulate initial conditions and retrieve results.**
- **e.g. Lloyd et al suggest using black holes as extreme quantum computing devices**
  - at present no theory governing the temporal evolution of black holes is known
  - the technology required to program them and read results may never be invented.

Processing Speed Limits

- **Margolus & Levitin showed that quantum theory limits the speed at which elementary operations can be performed.**
- **In this context an elementary operation is one which moves a system from one quantum state to an orthogonal one (for example, flipping a qubit).**
- **Margolus-Levitin theorem, using the energy-time uncertainty relation, shows that system with energy E above its ground state can perform at most**

$$\frac{2E}{\pi\hbar} \text{ operations/second}$$

- **This limit depends only on the total energy available to the system .**

Processing Speed Limits

- **If system performs multiple operations concurrently, E is divided up and each operation takes longer.**
- **Parallelism gains nothing in terms of speed. Degree to which it makes sense to use concurrency depends on physical extent of system.**
- **However, the more extensive the system, the greater the parallelism required to exploit its resources, due to communication constraints imposed by finite speed of light.**
- **For a 1kg system this translates into an upper bound of about 10^{51} ops/sec, (assuming all rest mass converted to energy)**

Processing Speed Limits

- **If system performs multiple operations concurrently, E is divided up and each operation takes longer.**
- **Parallelism gains nothing in terms of speed. Degree to which it makes sense to use concurrency depends on physical extent of system.**
- **However, the more extensive the system, the greater the parallelism required to exploit its resources, due to communication constraints imposed by finite speed of light.**
- **For a 1kg system this translates into an upper bound of about 10^{51} ops/sec, (assuming all rest mass converted to energy)**

Information Content Limits

- **Physics also bounds maximum information (entropy) content of a system.**
- **Holographic Bound (Susskind, 1995): no object can have higher entropy than a black hole whose event horizon bounds it & the entropy of such a black hole depends only on the *area* of the horizon (*not* the volume).**
- **Universal Entropy Bound (Beckenstein, 1981): any system of rest energy E contained in a volume of space of radius R has entropy no greater than:**

$$S_B = \frac{2\pi RE}{\hbar c}$$

Example: for system of volume 1 litre and mass 1kg we have:

$$S_B \approx 10^{43} \text{ bits}$$

Limits of the Universe

- **Lloyd (2002) uses this reasoning to estimate the computational capacity of the universe.**
- **All current evidence suggests the universe is finite in space and time.**
- **Using current estimates of resources available, Lloyd projects that:**
  - the universe has an information storage capacity of 1090 bits (excluding the postulated “dark energy”);
  - the universe is capable of no more than 10106 single bit ops/sec;
  - The universe has conducted no more than the equivalent of 10123 such operations since its creation 1010 years ago.
  - These numbers are very large but they suggest a final limit on what can ever be achieved using computers.

Why?

- **Analogue computers suggest infinitely accurate computation. Quantum computers have qubits parameterised by real numbers and also seem to imply infinite computation.**
- **Why is this potential not realisable?**
- **Answer seems to lie in the nature of our fundamental theory of nature.**
- **The limit theorems are all based on quantum mechanics.**

Why?

- All observational data about the real world is gathered through quantum measurement.
- Perhaps objective reality performs “computations” of infinite precision but, if so, we cannot access them.
- What we call a “physical system” is in fact a quantum-mediated “image” of some element of underlying ontology.
- The laws of physics are laws governing the quantum interaction between the observer and the world.

Geometry and computers

- **Current machines are 2D surfaces for good reason**
  - 1 free dimension needed to get rid of heat
  - 1 free dimension needed to print the design during manufacture. Printing along a 3d dimension allows the simultaneous transmission of design information.
- **Viable new classes of computers are likely to remain 2D for these reasons.**

Computers and Simulators

- **A general purpose computer is a physical subsystem that can be made to emulate the behaviour of a large class of other systems.**
- **In principle a computer can simulate any physical system to an arbitrary degree of accuracy given enough time and memory.**
- **At the birth of a technology it is often easier to build special purpose simulators than general purpose ones.**

Possible classes of simulators

- **Quantum simulators**
  - Less general than quantum computers
- **General purpose analogue simulators**
  - Large scale versions of the analogue computer on a chip
- **General purpose digital symulators**
  - Von Neuman machines –classical computing
  - General purpose logic arrays

Quantum simulators

- Feynman observed that quantum mechanics was inherently hard to simulate on digital computers
- The digital representation of a quantum system grows as the tensor product of the basis states of its components.
- Thus for *n* subsystems each with two basis states, we have a state space of 2^n . The matrix operator, then requires a storage space of 2^{2n} and each evolution step is of the same order.
- Feynman proposed to simulate a given quantum system **A** with another quantum system **B** .
- One to one mapping between the states and dynamics of the two quantum systems, superposition of states in **B** can then linearly simulate the superposition of states in **A**

Quantum Digital Computers

- **Most practical effort on quantum circuit model: computationally equivalent to Deutsch's Quantum Turing Machine.**
- **More recent alternatives (adiabatic, topological quantum models) are computationally equivalent.**
- **Circuit model relies on a sequence of unitary transformations, or quantum gates, applied to a register of qubits.**
- **Transformations are ordered by quantum wires (particle transfers or unitary time evolution).**

Quantum Digital Computers

- **Multiple input gates cause qubits to be entangled.**
- **Eventually quantum circuit produces output which can be subjected to a quantum measurement.**
- **Idea is to design circuit to implement logic of some desired computation.**
- **Power from parallelism in entanglement but...**
- **...quantum measurement is inherently non-deterministic so correct answer occurs, only with a certain probability.**
- **In general multiple runs are required.**

Quantum Algorithms

- **Any classical algorithm can be simulated but not necessarily with speed up.**
- **Most celebrated quantum algorithm is Shor's quantum factoring algorithm**
- **Finds prime factors of an integer in polynomial time.**
- **Exponentially faster than any known classical technique.**
- **Other algorithms are known (e.g. Grover's search) but relatively few.**

Quantum Algorithms

- **Quantum algorithms are hard to design.**
  - No proof that quantum computers can solve NP complete problems.
  - Shor has expressed pessimism. Points out that it can be shown that a quantum computer cannot search a space of size N in less than $O(\sqrt{N})$ time.
  - Some claims have been made for possible quantum solutions to NP complete problems but no such claim has stood up to scrutiny.
- **If reliable quantum computers can be built they will give significant advantages in some important algorithms but there is no evidence that they will have hyper-computational capabilities.**

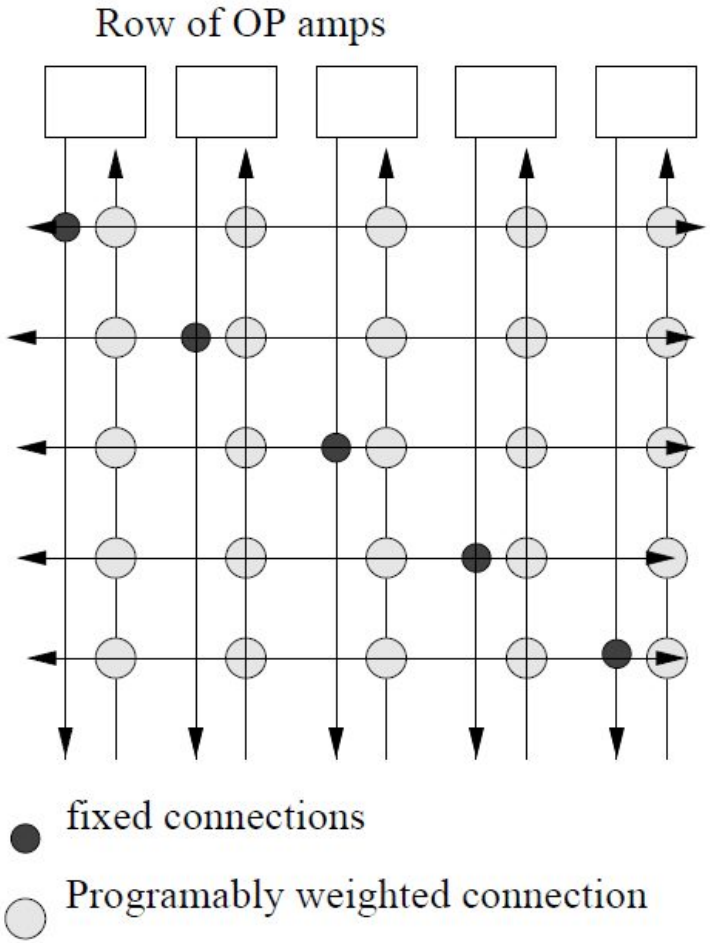
Building Quantum Computers

- **Quantum computers need to maintain entanglement of qubits long enough to allow computation to complete.**
- **Enemy is decoherence: quantum entanglement with the environment.**
- **Even limited decoherence causes errors: bounding errors is a major challenge.**
- **Several implementation technologies are being researched: winner is unclear yet.**

Building Quantum Computers

- **DiVincenzo (2000) has listed the technological requirements:**
  - Scalable system with well characterised qubits
  - Ability to initialise qubits
  - Long decoherence times
  - Universal set of implementable quantum gates
  - Qubit specific measuring capability
- **These remain significant challenges.**
- **Other avenues than the circuit model may prove fruitful. Work is also being done on adiabatic and topological approaches (the latter is claimed to be more resistant to decoherence).**

General purpose analogue simulator chip



- **Can in principle simulate any system described by differential equations**
- **Area grows as square of number of variables**
- **Chips of this sort do actually exist, but not widely used**

Analogue cellular automata

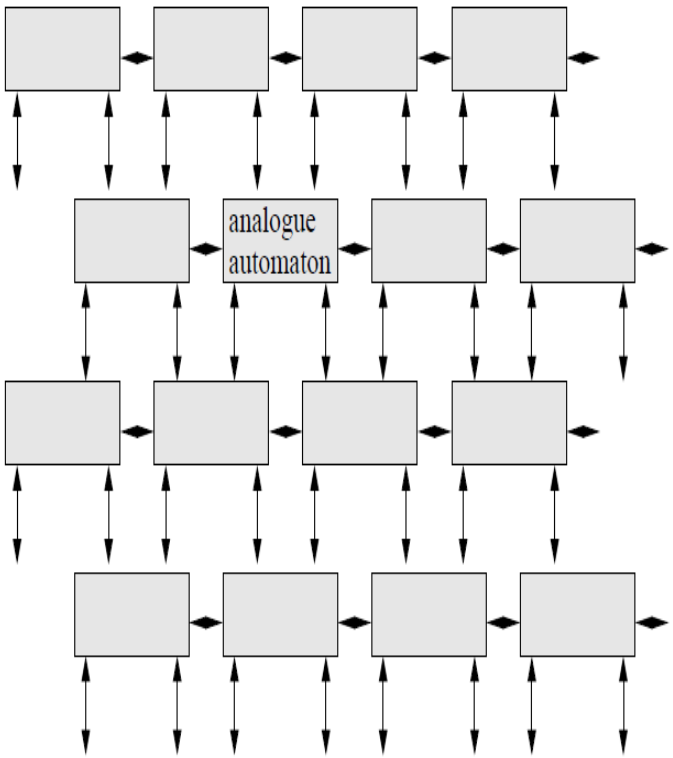
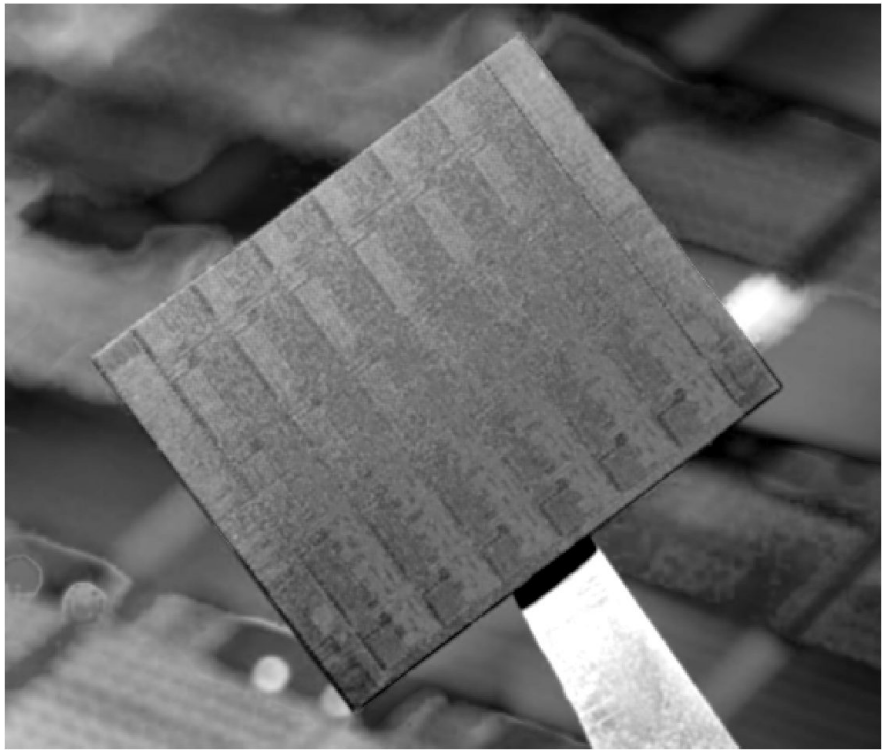


Figure 2: *Analogue automata on a hexagonal lattice on a chip*

- **Suitable for simulating any 2D manifold operating by local interactions**
- **Scales much better than the previous approach**
- **Can not handle 3 and higher dimensions**

What we are likely to get

- **Surfaces tiled with VN processors with local communication**
- **More general as simulators than previous systems.**
- **Time and memory muxing allows simulation > 2 dimensional manifolds**



Intel 48 core single chip cloud computer

Conclusions

- **Essential to continually challenge limits to current theories**
  - Maybe new mathematics/physics will unleash new models of computing
- **Right now, nowhere near practical limits of bounds of current maths & physics**
  - New models can still emerge from current theories
  - Vast challenges in building faster/smaller/energy efficient computers long before bounds are reached