



Limits of Computation

22 - New Computing Paradigms
Bernhard Reus



The story so far

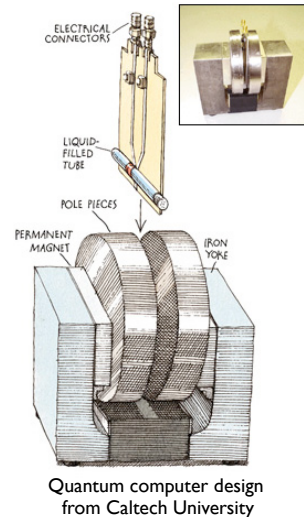
- we don't know whether $P = NP$
- we don't know any polynomial time solutions for **NP**-complete problems
- we have seen there are ways to try to negotiate ones ways around **NP**-completeness usually giving up the idea that one always gets good results (for large inputs)



Getting around infeasibility?

THIS TIME

- using natural phenomena as notion of computation...
- ... going “very very small”:
- The emerging fields of
 - *DNA computing*
 - *Quantum computing*



Harness Natural
Phenomena “in the
small”
molecular / atomic level



Molecular (DNA) computing



Some factoids

- Every human cell contains almost two meters of DNA strand rolled up into a small ball, i.e. a nucleus, of 5 micrometers
- *“DNA replication is a truly amazing biological phenomenon. The polymerase enzymes... do make mistakes at a rate of about 1 per every 100,000 nucleotides. That might not seem like much, until you consider how much DNA a cell has. In humans, with our 6 billion base pairs in each diploid cell, that would amount to about 120,000 mistakes every time a cell divides! Fortunately, cells have evolved highly sophisticated means of fixing most, but not all, of those mistakes.”*

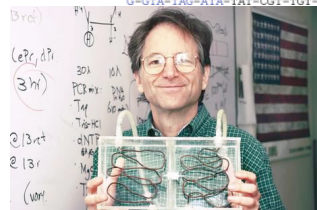
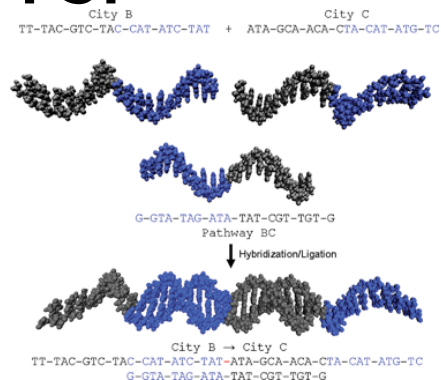


biocomputer
wetware computer

DNA computing TSP

- *Leonard Adleman* started the field 1994 using DNA to find a solution for TSP with 7 cities (later others managed up to 70 cities)
- encoded graph with DNA, computation via enzymes or catalytic DNA
- parallelisation in “molecular soup” happens naturally (e.g. polymerase chain reaction for copying DNA)

meanwhile also other NP-complete problems have been solved by DNA like SAT



L. Adleman
with his DNA
“computer”

<http://www.usc.edu/uscnnews/stories/7881.html>



DNA (molecular) computing

- enormous potential as DNA computing uses:
 - 1 billion times less energy
 - 1 trillion times less space
 - can be faster but to what extent?
- than conventional computing
- self-assembly possible (!)
- “in vitro” – “in vivo”: programming smart drugs
- “Liquid Logic”
 - **molecular DNA version of logic gates and circuits**
 - **Microsoft Research Cambridge** also very active, eg Programming Language for DNA computing simulators etc.

In January 2013 part of an audio file of Martin Luther Kings’ speech was stored in DNA “digital storage” among other things
in March 2013 a biological transistor was created

... the border between computing and biology is vanishing fast, and the process of hijacking the information-processing potential of DNA to build logic circuits has only just begun.

[The Economist, Technology Quarterly: Q1 2012g, 03/03/2012]



DNA computing disadvantage

- Can't solve **NP**-complete problems in polynomial time as we have the same issue as with parallel processors: we'd need bathtubs full of DNA
- Simple operations may take hours (biochemical processes) so DNA computing never useful for every-day computing
- Error rates in DNA replication.
- Not universally programmable!



DNA computing challenges

- **Accuracy:** *Extracting the right solutions* (strands) from the molecular “soup” (with longer strands the probability for errors increases).
- **Reliability:** there are sometimes errors in pairings of DNA strands itself.
- **High cost** regarding the time it takes to set up the experiment.
- One still needs a **Lab**.



“I believe things like DNA computing will eventually lead the way to a ‘molecular revolution,’ which ultimately will have a very dramatic effect on the world.”

Leonard Adleman 1995



Organic Computing

“wet computer in a living organism or even cell”



Abstract Model

- **Chemical Reaction Networks** are abstract models abstracting away from concrete chemistry
- using integer counts of molecules (of various types) in a well-mixed solution and describe reactions via rules involving quantities of molecules
- rule execution is chemical reaction; no control over order of “execution”
- complexity: linear is slow, need logarithmic complexity due to large number of molecules.

13



Synthetic Biology

- use biological processes to simulate e.g. digital computers
- building transistors (transcriptors) using flow of RNA polymerase (enzyme that produces RNA transcripts)
- since many of those processes are not (yet) fully understood there is a lack of design principles

14



Synthetic Chemistry

- use chemistry as assembly language
- DNA is still used (but this is more of an “accident”)
- implement CRNs with help of so-called join and fork gates that consume input signals and produce output signal
- DNA strand displacement used to implement this



Quantum Computing



Going really small...

- A field effect transistor on a chip from 2015 was 14 nanometer wide
- This is the width of a hair – divided by 5,000
- Quantum effects: electrons can “tunnel” through thin layers and this “leakage” causes unwanted currents...
- Problem for very small transistors and a limit to Moore’s Law of ever decreasing sizes of transistors on microchips.

17

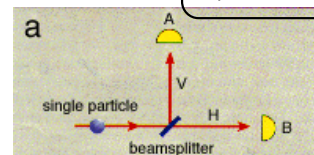


Quantum Computing

- **BIG IDEA:** introduced 1980/81 by Yuri Manin and Richard Feynman

use *quantum mechanics* (interference)

- *Duality: wave vs particle*;
appears only close to atomic scale!



photon particle detected with equal probability at A **and** B (and not as expected either A or B)

- Quantum bit state can be 0 and 1 *at the same time*.

qubit =
quantum bit

So n qubits can express 2^n states simultaneously (superposition); operations need to work on all those states at the same time.

- When we observe results though, the state space collapses into one.

massive parallelisation

18



Quantum Bits

- Quantum bits are probability vectors with a 2-norm.
- States of qubits are unit vectors in the two-dimensional space of complex numbers.
- Operations on qubits must preserve this (maths!)
- Complexity class: **BQP (bounded error quantum polynomial time)** using quantum turing machines (using quantum states)

19



Quantum Factorisation

- *Peter Shor (now MIT) published an algorithm that uses quantum superposition to factorise primes in polynomial time on a (theoretical) quantum computer. (1994)*
- Shook the computing world, (and computer manufacturers)



Peter W Shor

so with a quantum computer one could possibly crack all public key encryption!

20



Grover's Algorithm

- Search Algorithm in unordered list. Can normally only be done in $O(n)$.
- Grover's Algorithm can do it (superposition) in $O(\sqrt{n})$
- This shows “brute force” on a Quantum Computer gives a *quadratic* speed-up but most likely won't help us solve **NP**-complete problems in polynomial time.
- So (please remember this):

21



“A Quantum Computer is
NOT like a massively-
parallel classical computer.”

Scott Aaronson, MIT

22



Quantum Computing

- Note that we can *simulate* a quantum computation on a common machine (so Church-Turing thesis is not violated) but with exponential loss of time.
- Quantum computers may be able to search through all possible solutions of an optimisation problem by *superposition* and thus might squash the *Cook-Karp thesis*! But we carefully used the term “sequential models” in Cook’s thesis so that is still fine 😊.
- Quantum computers are still SciFi but *quantum cryptography* is already in use to safely transmit keys!



Quantum Challenges

- Challenges (current research):
 - building quantum *gates*, computer hardware
 - in particular “interference (entanglement) of quantum states with environment”: *decoherence*
 - quantum *algorithmics* needed that can make use of *superposition* of inputs and *superposition* of outputs
 - design *quantum programming languages*




February 2014

Quantum computers are still SciFi – or are they?

A company's claim that they built a 512 qubit quantum machine is disputed by the renowned IEEE.

IEEE = Institute of Electrical and Electronics Engineers
(large professional organisation)



Follow on: [f](#) [t](#) [in](#) [+](#) [m](#)

Engineering Topics • Special Reports • Blogs • Multimedia

Tech Talk | Computing | Hardware

D-Wave's Quantum Computing Claim Disputed Again

By Jeremy Hsu
Posted 10 Feb 2014 | 20:01 GMT

[Share](#) | [Email](#) | [Print](#)

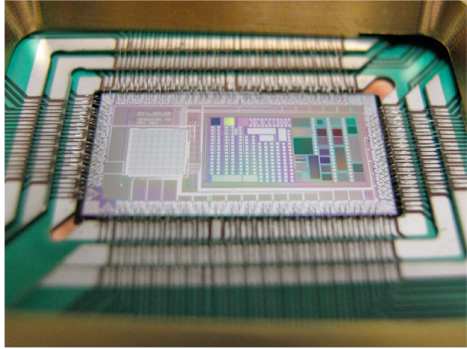


Photo: D-Wave Systems

The strongest scientific evidence for D-Wave's claim to have built commercial quantum computers just got weaker. A new paper finds that classical computing can explain the performance patterns of D-Wave's machines just as well as quantum computing can—a result that undermines crucial support for D-Wave's claim from a previous study.

25



2019

D-Wave has shipped 2,048 qubit quantum machines.

Allegedly, Google and NASA have bought such a system.

Only for optimisation problems. Uses “quantum annealing”.

NATURE | NEWS

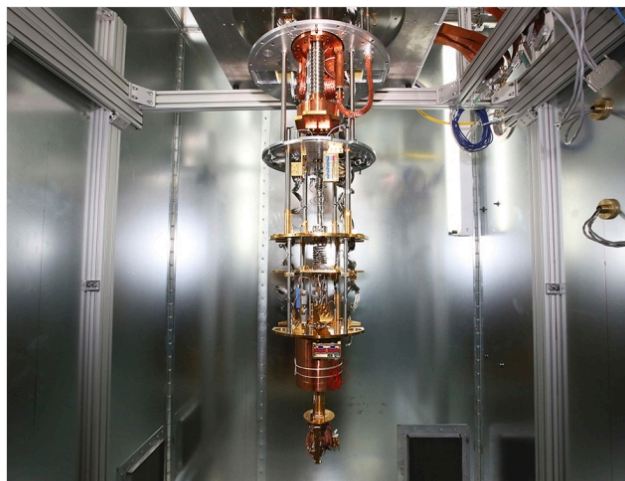
D-Wave upgrade: How scientists are using the world's most controversial quantum computer

Scepticism surrounds the ultimate potential of D-wave machines, but researchers are already finding uses for them.

Elizabeth Gibney

24 January 2017

[PDF](#) [Rights & Permissions](#)



Kim Stalknecht/The New York Times/vyevins

D-Wave's latest processor has 2,000 qubits — far surpassing the capacity of previous models.

26



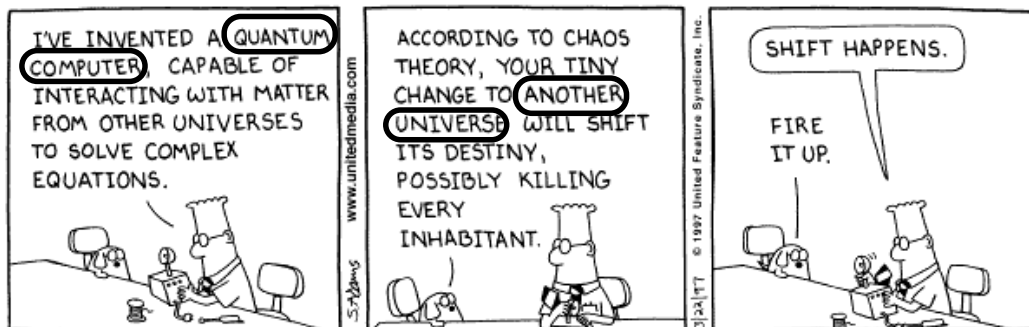
Now there's a thought...

- *David Deutsch* uses *Shor's algorithm* as argument for the existence of parallel universes:
- Quantum-Factorisation of a 200 digit number would require many more resources than atoms exist in the universe, so there must be parallel universes in which the quantum computation takes place. We just observe one (our) universe.

27



To boldly go...



Copyright © 1997 United Feature Syndicate, Inc.
Redistribution in whole or in part prohibited

in the computability course of the **future**, will the quantum computer be “the computer” and will the machines we use today be to them what Turing Machines are for us today?

28



to boldly
go...



THE END

© 2008-20. Bernhard Reus, University of Sussex