Stories from Quantum Computing

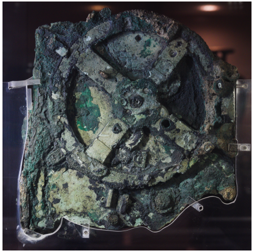
Viktória Nemkin

2025. 06. 03.

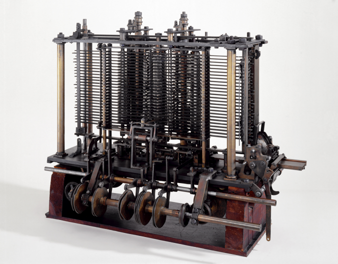
What is computing?

Stonehenge? (solstices)

Abacus

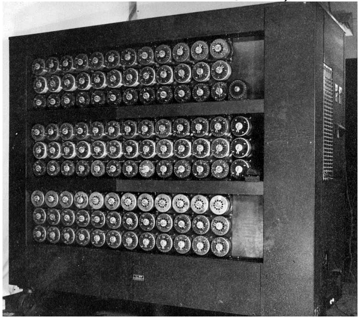


Antikythera mechanism (analogue astronomical computer)

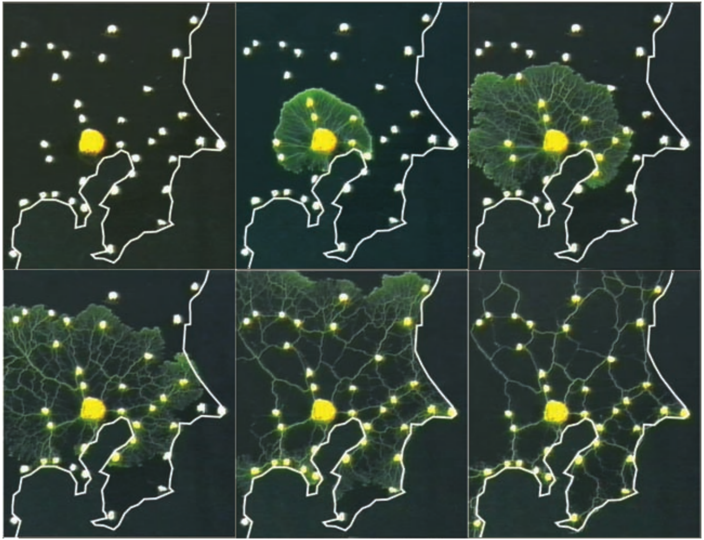


Babbage's Analytical engine (mechanical calculations)

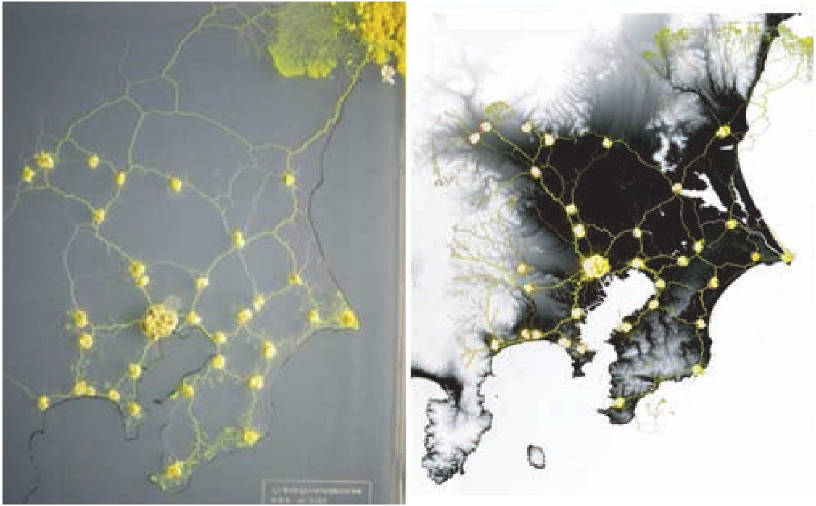
Hollerith's Tabulating machine (1890 US Census)



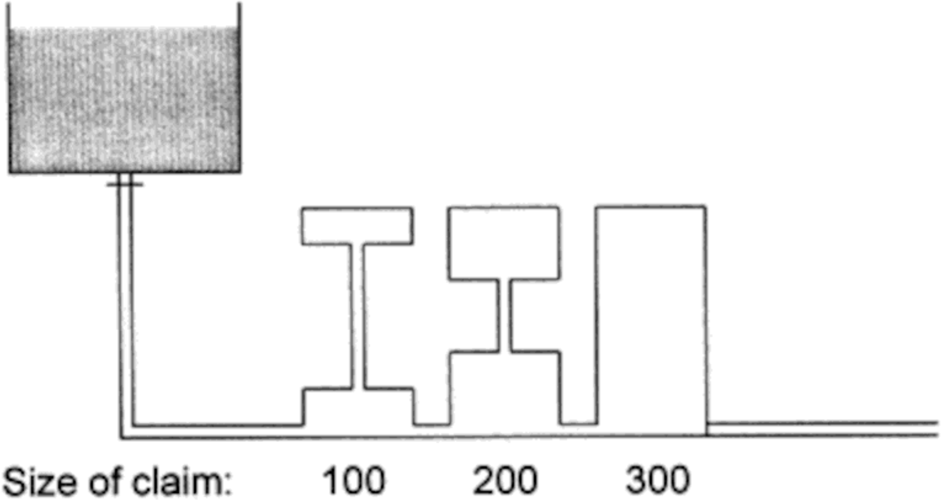
Turing's Bombe (breaking Enigma)



Tero, Takagi, Saigusa, Ito, Bebber, Fricker, Yumiki, Kobayashi, Nakagaki. 2010.
Rules for biologically inspired adaptive network design. *Science*, 327(5964), 439–442.



Tero, Takagi, Saigusa, Ito, Bebber, Fricker, Yumiki, Kobayashi, Nakagaki. 2010.
Rules for biologically inspired adaptive network design. *Science*, 327(5964), 439–442.



Kaminski. 2000. **'Hydraulic' rationing.** *Mathematical Social Sciences*, 40(2), 131–155.

What is computation?

- Doesn't need electricity.
- Doesn't need mechanical parts.
- Doesn't need a central authority.

What is computation?

- Doesn't need electricity.
- Doesn't need mechanical parts.
- Doesn't need a central authority.

Computation is:

- a natural (physical, biological) system
- evolving according to the laws of nature
- where the final result can be meaningfully interpreted.

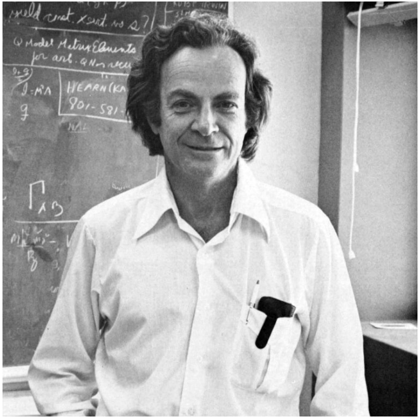
Susan Stepney
(unconventional computing)

Stepney, S. (2008). **The neglected pillar of material computation.** *Physica D: Nonlinear Phenomena*, 237(9), 1157–1164.

Simulating quantum mechanical systems

Simulating quantum physics

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."



Richard Feynman

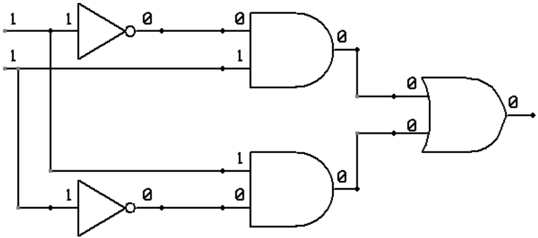
Feynman. 1982. **Simulating physics with computers.** *International Journal of Theoretical Physics*, 21(6–7), 467–488.

Quantum computers

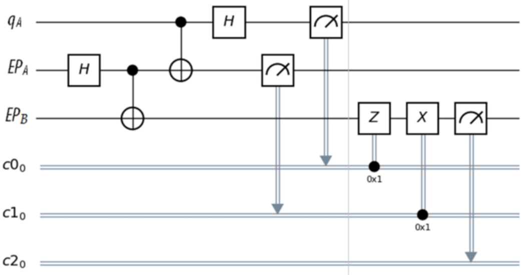
Any computer that uses quantum mechanical phenomena to compute.

Gate-based systems

- similar to logic circuits: wires and gates
- superconducting, trapped ions, photonic, etc.
- e.g. IBM, Google



classical logic circuit

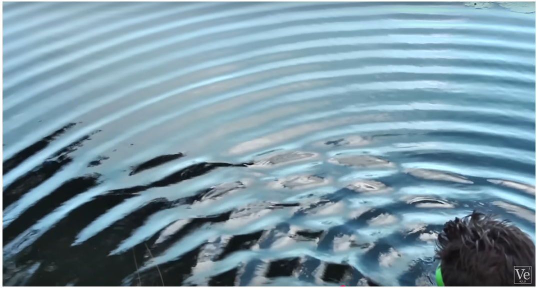


quantum circuit

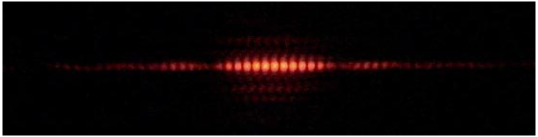
- but! superposition

Superposition

- Young's double-slit experiment



waves on water from two sources



interference, even for a single particle

Exponentially many options

- classical bit = 0 or 1
- quantum bit ≈ probability distribution of 0 and 1, but with complex numbers, length is 1

$$[q] = a \cdot [0] + b \cdot [1] \qquad a, b \in \mathbb{C}, \qquad |a|^2 + |b|^2 = 1$$

- quantum register (3 qubits)

$$[q] = a_0[000] + a_1[001] + a_2[010] + a_3[011] + a_4[100] + a_5[101] + a_6[110] + a_7[111]$$

$$a_i \in \mathbb{C} \qquad \sum_i |a_i|^2 = 1$$

- a_i = complex probability amplitudes
- state vector of the system $[q]$:

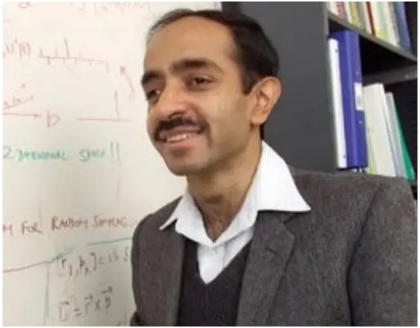
$$[q] = (a_0, a_1, \ldots, a_7)$$

Parallel computation?

- operation = matrix multiplication (unitary matrices)
- problem: we can't see the state
- measurement: destructive, one result only
- classically hard (NP-hard) problems = parallel computation $\rightarrow$ polynomial solver :(

Grover's algorithm

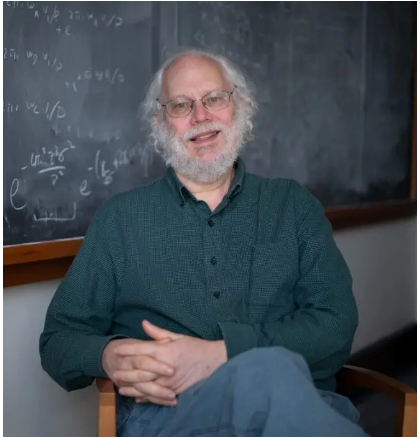
- needs: a unitary matrix describing the desired states (model your constraints)
- does: "cleans" bad amplitudes from the register
- price: n qubits in $\approx \sqrt{2^n}$
  - vs classical bruteforce in $\approx 2^n$ steps
- uses: rotation toward the "cleaned" vector in 2^n dimensional space
  - and probably magic too



Grover. 1996. **A fast quantum mechanical algorithm for database search.** *Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC)*, 212–219.

Selling quantum: Shor's algorithm

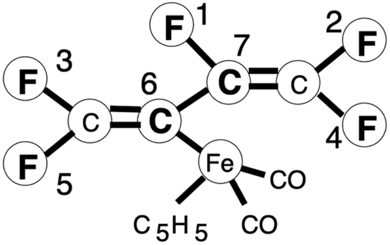
- does: integer factorization
- classically hard
- price: **exponential speedup** over classically known methods
- cryptography in danger
- everyone starts building quantum computers



Shor. 1994. **Algorithms for quantum computation: Discrete logarithms and factoring.** *Proceedings 35th Annual Symposium on Foundations of Computer Science (FOCS)*, 124–134.

Molecular quantum computer

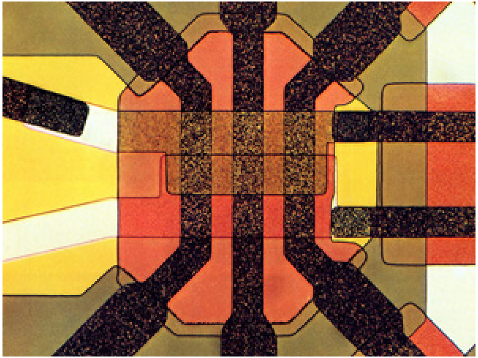
- NMR = nuclear magnetic resonance
- qubits = magnetic spin states of atomic nuclei in molecules + oscillating electromagnetic field → superposition
- same tech as in MRI (magnetic resonance imaging)
- IBM chemists *designed* molecule, 7 qubits
- demonstrated factoring $15 = 3 \cdot 5$ with Shor
  - issue: scaling (21)
  - later: true quantumness is debated



Vandersypen, Steffen, Breyta, Yannoni, Sherwood, Chuang. 2001. **Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.** *Nature*, 414(6866), 883–887.

Superconduction-based gated quantum computers

- IBM: superconducting research since 1950s (cryoton memory, Josephson-junctions) $\rightarrow$ cheap semiconductors beat them
- 2000s: reboot for quantum
- Josephson-junction based qubits
- challenges: noise + time before collapse



Quantum computing today

- in the cloud, 500 qubits
- **IBM**: superconducting, Qiskit
- **Google Sycamore**: superconducting, quantum supremacy (?)
- **IonQ, Quantinuum**: trapped ion
- **PsiQuantum** photonic qubits

We need more, useful algorithms!