Second WAW Quantum Computing Introductory Talk

Michael Epping
Peter Ken Schuhmacher

– based on talks of the HPC Seminar –

Quantum Computing Group
High-Performance Computing
Institute for Software Technology

November 3rd, 2021

DLR

Outline

How to build a quantum computer

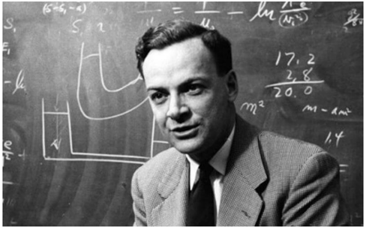
State of Development

What Quantum Computers can do

And what they can’t

Original Idea

- Challenge: the Hilbert space dimension of a quantum system scales **exponentially** with the number of particles
  - ⇝ Simulation of quantum systems is hard for classical computing machines
- Solution: Use the exponentially large Hilbert space of quantum systems as a **resource** for computing



"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."

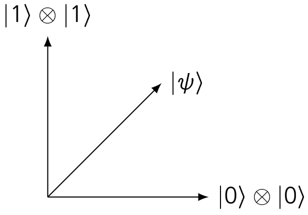
Richard Feynman, "Simulating Physics with Computers", 1st conf. on Phys. and Comp., MIT (1981)

Superposition

- Single qubit basis: $|0\rangle$, $|1\rangle$
- Composite system via tensor product.
  Basis: $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$, …
- Superposition-principle introduces "intermediate" states, e.g.

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right)$$

- $|\psi\rangle \neq |\phi\rangle \otimes |\chi\rangle \rightsquigarrow$ *entanglement*



DiVincenzo's Criteria

Requirements for quantum computers[1]:

1. scalable
2. initializable
3. low noise
4. a universal set of gates
5. readout

[1] D.P. DiVincenzo, The Physical Implementation of Quantum Computation, Fortschr. Phys. **48**: 771-783 (2000)

Quantum Error Correction (QEC)

- Quantum information is prone to noise.
- Any noise can be decomposed into:
  1. bit-flips $|0\rangle \mapsto |1\rangle, |1\rangle \mapsto |0\rangle$
  2. phase-flips $|0\rangle \mapsto |0\rangle, |1\rangle \mapsto -|1\rangle$
- It's not possible to copy quantum states (No-Cloning-Theorem)!
- Create redundancy via entangled multi-qubit states, e.g.

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \alpha|000\rangle + \beta|111\rangle$$

- We need five qubits to correct both error types.

Threshold Theorem

- Error correction is implemented via noisy gates.
- Increasing the code size improves the capabilities, but requires more gates.
- There is a threshold gate fidelity for where more error correction helps.
- High fidelities (e.g. 99.99%) with many qubits (e.g. 10^6) enable arbitrary long computation.

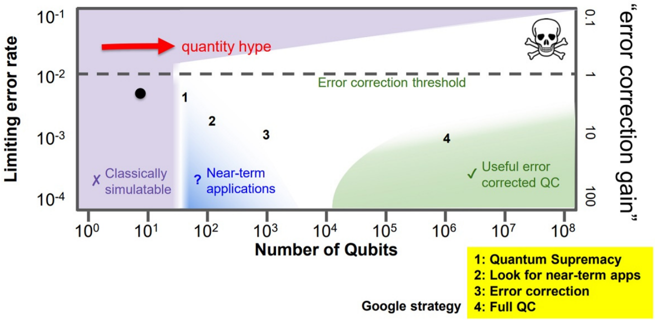


Image: Google (Martinis group)

How to build a quantum computer

State of Development

What Quantum Computers can do

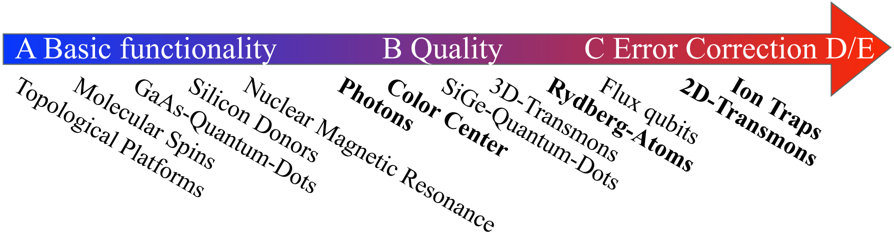
And what they can’t

Development Levels[1]

- **Level A: Basic functionality**
  ≥ 2 qubits, gate operations, readout
- **Level B: Quality**
  Gate error rates below error correction threshold
- **Level C: Quantum Error Correction**
  Quantum error correction helps
- **Level D: Fault-tolerant operations**
  Fully error corrected universal gates
- **Level E: Algorithms**
  Complex algorithms have been executed

[1] F.K. Wilhelm *et. al.*, Entwicklungsstand Quantencomputer, BSI Studie 283 (2020)

Hardware Platforms: State of Development



State of Development[1]

[1] F.K. Wilhelm *et. al.*, Entwicklungsstand Quantencomputer, BSI Studie 283 (2020)

Photons

- Qubits based on non-classical states of light: Single photons, Multi-photon squeezed states, ...
- Circuits are waveguides integrated into micro-chips.
- Gates are formed by Beam splitters, phase shifters, interferometers and more.
- Pro: No cooling, easily integrates with networks
- Con: Difficult interaction, photon loss

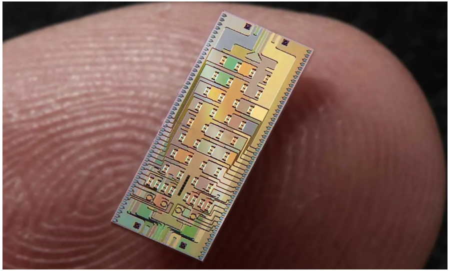


Image: Xanadu

Nitrogen-Vacancy-Centers

- The NV-center is a charged defect in diamond.
- The electron spin forms the qubit.
- The spin is read via photoluminescence.
- Pro: Long lifetime.
- Con: Each center has different characteristics.

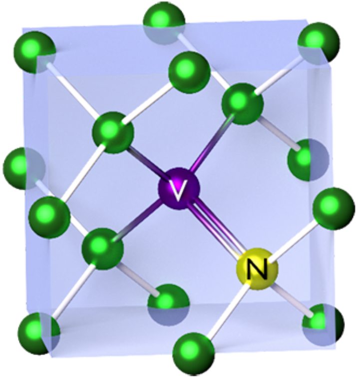


Image: Wikipedia

Rydberg-Atoms

- Rydberg-Atoms are highly excited Atoms, with larger diameter.
- They can be trapped in optical lattices.
- Multi-qubit gates via strong interaction with neighbours.
- Pro: Many qubits
- Con: Lower gate fidelities, atom loss

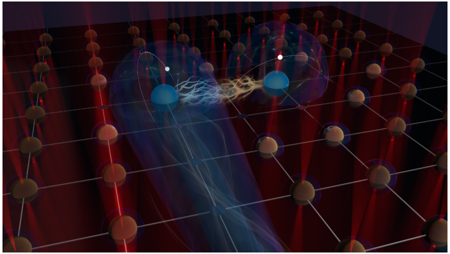


Image: University of Stuttgart

Superconducting Qubits

- Macroscopic (μm) circuits, e.g. rings or junctions
- Cooled to low temperatures ($\lesssim 100\text{mK}$)
- Commercial front-runner (IBM, Google, ...)
- Pro: Established manufacturing, scalable
- Con: Cryogenic cooling, noise, different qubits

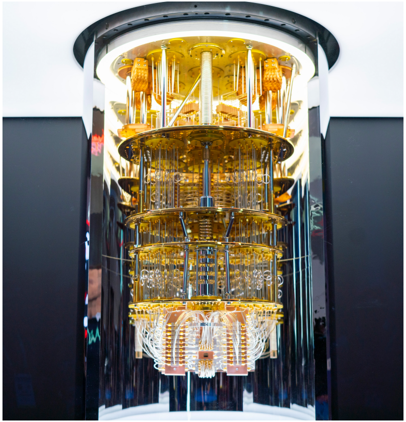


Image: Fraunhofer

Ion Traps

- Charged atoms are trapped in a time-dependent electromagnetic field.
- The qubit states are atomic levels.
- Qubits interact via motion.
- Pro: Low noise, multi-qubit interactions
- Con: Difficult scaling, ion loss

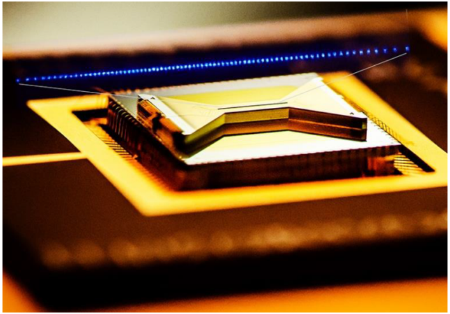


Image: IonQ

How to build a quantum computer

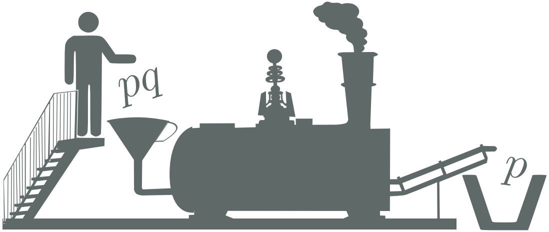
State of Development

What Quantum Computers can do

And what they can’t

The input-output-problem

- State preparation
  - can set all amplitudes in the state
  - may require exponentially many gates



- State tomography
  - unveils the 2^n complex amplitudes of the state
  - takes an exponential amount of measurements (and copies of the state!)

- good problems for quantum computers
  1. are difficult
  2. are specified by few parameters
  3. have a short answer (yes, no, few integers)

Grover search

- Every quantum operation acts linearly on all states in a superposition. For example:

$$G|\psi\rangle = \frac{1}{\sqrt{2}}(G|00\rangle + G|11\rangle)$$

- An oracle is a black box which marks solutions, e.g. $G|00\rangle = |00\rangle$, $G|11\rangle = -|11\rangle$.
- Grover (roughly): Start with uniform superposition, iteratively suppress unmarked states.
- For problems without structure:

  Classically try all $N = 2^n$ possible solutions $\mathcal{O}(N)$

  Grover $\mathcal{O}(\sqrt{N}) \rightsquigarrow$ quadratic speed-up. Known to be optimal.

Quantum Fourier transform (QFT)

- The QFT performs the discrete fourier transform on quantum amplitudes

$$|j\rangle \mapsto \sum_{k=0}^{2^n-1} \mathrm{e}^{2\pi \mathrm{i} jk/2^n} |k\rangle$$

- It uses $\mathcal{O}(n^2)$ gates, while Fast Fourier Transform (FFT) requires $\mathcal{O}(n2^n)$ gates
- Preparing and accessing amplitudes is difficult!
- QFT is a key component of many quantum algorithms:
  - Phase estimation
  - Period finding
  - Discrete logarithm and factorization
  - ...

How to build a quantum computer

State of Development

What Quantum Computers can do

And what they can’t

No-Signalling

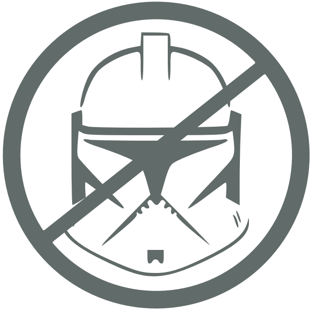
- Despite entanglement we can't communicate faster than light.
- Every quantum operation on Alice's subsystem only has no measurable effect on Bob's system.
- Useful: Any idea that violates no-signalling is unphysical.

No-Cloning

- It is impossible to copy an unknown quantum state:

$$|\varphi\rangle \not\longrightarrow |\varphi\rangle\,|\varphi\rangle$$

- Cloning would violate the no-signalling principle:
  The choice of measurement basis on one half of an entangled pair could be determined from the second half.
- No-cloning makes quantum error correction difficult.
- It enables quantum cryptography.



Thank you! Do you have questions?