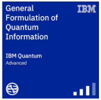
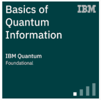
Quantum Computation and Information
The Basics

Dr. Thorsten Hehn





Outline

Definition

Definition

- Quantum Computation
    - is an emerging field of computer science and engineering
    - uses the principles of quantum-mechanical systems for computation
    - can solve certain complex problems beyond the ability of the most powerful classical computers
- Quantum Information
    - Information-processing operations using quantum-mechanical systems

Quantum Computation

- ... shall not replace classical computation and classical information

Quantum Computation

- ... shall not replace classical computation and classical information
- ... will augment and run in parallel to classical computing

Remark

Interaction of QPU and CPU

- Quantum Error Correction: syndrome measurement on quantum system
- Inference of most likely error pattern on classical CPU

Quantum Computation

- ... shall not replace classical computation and classical information
- ... will augment and run in parallel to classical computing
- ... has specialized powers and was engineered for niche, mathematical problems

Remark

Scott Aaronson's Space Shuttle Analogy

- A space shuttle was built for a specialized problem
- It is over-engineered and too expensive for everyday tasks
- Driving a space shuttle to the grocery store $\leftrightarrow$ Browsing the web on a quantum computer

Key Properties: Superposition and Entanglement

Key Properties

- Key Property 1: Superposition
- Key Property 2: Entanglement

Bra-ket Notation by Dirac

Basis states:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$\langle 0| = |0\rangle^H = \begin{pmatrix} 1 & 0 \end{pmatrix}, \quad \langle 1| = |1\rangle^H = \begin{pmatrix} 0 & 1 \end{pmatrix}$$

Well-known vector-calculus rules apply:

$$\begin{aligned} \langle 0| \, |0\rangle &= \begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1 \\ |0\rangle \, \langle 0| &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \end{aligned}$$

Key Property 1: Superposition

- Classical Bits take values from $\Sigma = \{0, 1\}$
- Qubits can (initially) be represented by state vectors of the form $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $\alpha, \beta \in \mathbb{C}$, and $|\alpha|^2 + |\beta|^2 = 1$.
- Key property for performance gains

Formal definition: A quantum state is said to be in a superposition (with respect to a chosen orthonormal basis) if it is a nontrivial linear combination of two or more basis states: $|\phi\rangle = \sum_i c_i |\psi_i\rangle$, where ψ_i are the basis states and $\sum_i |c_i|^2 = 1$ holds.

Examples:

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |\phi_2\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$$

$$|\phi_3\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1+i}{2}|1\rangle, \quad |\phi_4\rangle = \frac{-i}{\sqrt{2}}|0\rangle + \frac{3+4i}{\sqrt{50}}|1\rangle$$

Key Property 1: Superposition

- The qubit is not simultaneously in both basis states, but in only one state (linear combination of basis states).
- Measuring $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ in the basis $|0\rangle, |1\rangle$
  - yields 0 with probability $|\alpha|^2$
  - yields 1 with probability $|\beta|^2$.
- Before performing a measurement, we can use the superposition state $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ to perform calculcations. Example: performing a not-operation on ϕ yields $|\overline{\phi}\rangle = \alpha |1\rangle + \beta |0\rangle$

Key Property 2: Entanglement

Definition: A composite quantum state describes the joint state of two or more qubits.

Definition: A composite quantum state is entangled if it is not separable, i.e., cannot be expressed as a tensor product of quantum states of its individual subsystems.

Example: The Bell State $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle),\ \forall \alpha, \beta, \gamma, \delta$$

Key Property 2: Entanglement

- Key property for information transmission and teleportation
- Entaglement is stronger than classical correlation as it operates on multiple bases
- Entanglement does not rely on hidden variables, proof given by Bell Experiment.
  - Intuition: Bell experiment uses CHSH Game to show that entanglement beats the maximum possible correlation. Assume that the pre-agreed player strategy represents the hidden variables.
  - Consequence: qubits provide randomness without reliance on hidden variables (QRNG $\geq$ RNG $>$ PRNG).

Key Property 2: Entanglement

Thought experiment:

- Alice and Bob own an entangled qubit pair.
- Alice takes a rocket to Mars and measures her qubit in the $|0\rangle, |1\rangle$ basis. The result is 0.
- Bob's measurement (in the same basis) is guaranteed to result to 0.
- Question: did we observe an event exceeding the speed of light?

Key Property 2: Entanglement

Thought experiment:

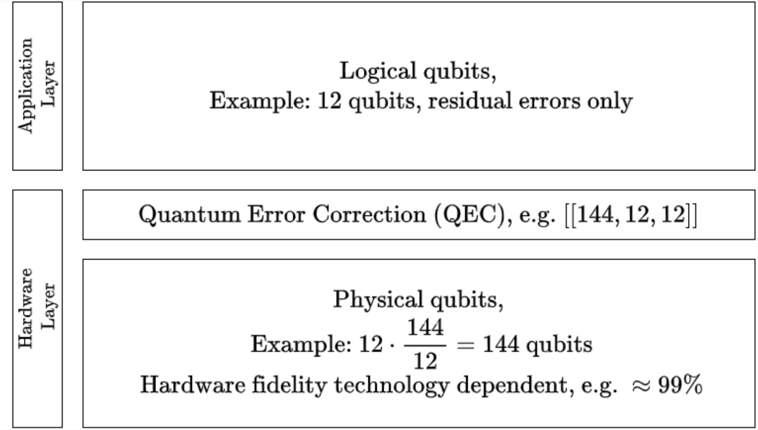
- Alice and Bob own an entangled qubit pair.
- Alice takes a rocket to Mars and measures her qubit in the $|0\rangle, |1\rangle$ basis. The result is 0.
- Bob's measurement (in the same basis) is guaranteed to result to 0.
- Question: did we observe an event exceeding the speed of light?
- Answer: no, as Bob is not aware of the change and statistics on his qubit do not change. He needs to be informed about the event on Alice's side through classical communication.

Quantum Computing Technologies

Leading Quantum Computing Technologies

	Trapped Ion	**Superconducting**	**Neutral Atoms**
Qubit	Charged atoms	Supercond. circuits	Neutral atoms
Confinement	Electromtrap	–	Optical tweezers
Temperature	Vacuum	~ 10 mK	Vacuum
Control	Laser pulses	Microwave pulses	Laser pulses
Gate speed	Slow	**Very fast**	Medium–fast
Gate fidelity	**Very High**	High	High
Connectivity	All-to-all	Local	Reconfigurable
Companies	IonQ, Quantinuum	IBM, Google	Infleqtion, QuEra

Logical and Physical qubits



Note: the example is based on IBM's $[[144, 12, 12]]$ Gross code with a nomincal rate of $\frac{12}{144}$. Actual hardware implementation requires additional qubits, e.g. ancilla qubits for syndrome extraction.

Quantum Hardware: Where are we today?

Commercial implementation (as of August 2026):

- Superconducting qubits: up to ≈ 150 physical qubits at $\approx 99.88\%$ two-qubit gate fidelity.
- Trapped-ion qubits: up to ≈ 100 physical qubits at $\approx 99.9\%$ two-qubit gate fidelity.

Consequence: implementation of mid- to large-scale algorithms, e.g. Shor's, not yet possible.

Fields of Application

Fields of Application

- Explore nature - Engine of new discoveries
  - Simulate quantum systems
  - Life science and medical research: simulation of cells and docking behaviors for drug discovery
  - Chemistry and materials design
  - Battery and photovoltaics simulations
- Speedup in unstructured search
  - Database applications
- Solve complex problems
  - Transportation and logistics
  - Network optimization
- Cryptanalysis
- Possibly modest gains in AI applications

Quantum Industry Overview

Quantum Industry Overview

Big Players

- Alphabet / Google
- Microsoft
- IBM

Quantum Pure Play

- IonQ
- D-Wave
- Quantinuum
- Rigetti
- Quantum Computing
- Infleqtion
- QuEra
- EU:
  Pasqal, Alice&Bob, IQM