Introduction to Quantum Computing

Group 5
(represented by Steffen Maass)

Mathematische Fakultät
Technische Universität Berlin

Scientific Computing, January 20

Outline

State of a Quantum Computer

Bit: classical two-state system

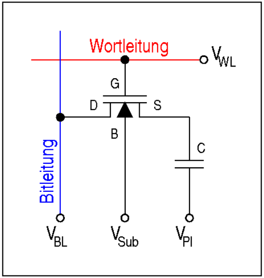


Figure: Circuit of a DRAM memory cell, CC BY 3.0, via Wikimedia Commons

Qubit: quantum mechanical two-state system

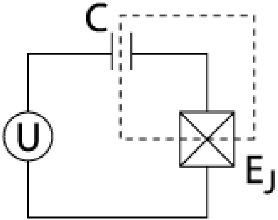


Figure: Circuit of Cooper-pair box, CC BY 3.0, via Wikimedia Commons

Quantum Register

A quantum computer operates on a quantum register that holds the state of a quantum system with several qubits.

State of a Single Qubit

- **state space**: 2-dimensional complex Hilbert space $\mathcal{H}$
- **basis states**: orthonormal vectors $|0\rangle$ and $|1\rangle$
  (e.g. eigenstates of an energy operator)

State of a Single Qubit

- **state space**: 2-dimensional complex Hilbert space $\mathcal{H}$
- **basis states**: orthonormal vectors $|0\rangle$ and $|1\rangle$
  (e.g. eigenstates of an energy operator)
- general state is a **superposition** of the basis states:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathcal{H} \qquad \alpha, \beta \in \mathbf{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$

State of a Single Qubit

- **state space**: 2-dimensional complex Hilbert space $\mathcal{H}$
- **basis states**: orthonormal vectors $|0\rangle$ and $|1\rangle$
  (e.g. eigenstates of an energy operator)
- general state is a **superposition** of the basis states:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \in \mathcal{H} \qquad \alpha, \beta \in \mathbf{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$

- **probabilistic interpretation**:
  $|\alpha|^2$ probability that (after measuring) the qubit is in basis state $|0\rangle$
  $|\beta|^2$ probability that (after measuring) the qubit is in basis state $|1\rangle$

System of Qubits: Entanglement

The state of a q-qubit register is described by unit vectors in the tensor product of the state spaces of the individual qubits

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_q$$

System of Qubits: Entanglement

The state of a q-qubit register is described by unit vectors in the tensor product of the state spaces of the individual qubits

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_q$$

Standard Basis for state space of a 2-qubit register

$$|0\rangle \otimes |0\rangle = |00\rangle, \quad |0\rangle \otimes |1\rangle = |01\rangle, \quad |1\rangle \otimes |0\rangle = |10\rangle, \quad |1\rangle \otimes |1\rangle = |11\rangle$$

System of Qubits: Entanglement

The state of a q-qubit register is described by unit vectors in the tensor product of the state spaces of the individual qubits

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_q$$

Standard Basis for state space of a 2-qubit register

$$|0\rangle \otimes |0\rangle = |00\rangle, \quad |0\rangle \otimes |1\rangle = |01\rangle, \quad |1\rangle \otimes |0\rangle = |10\rangle, \quad |1\rangle \otimes |1\rangle = |11\rangle$$

Example of a 2-qubit register:

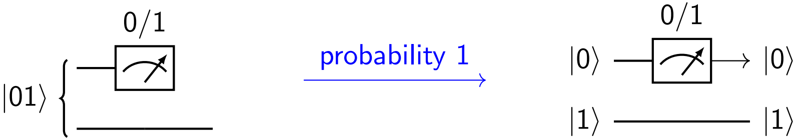
$$|\psi\rangle = \begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix} \in \mathbf{C}^4 \cong \quad \frac{1}{\sqrt{3}}|01\rangle + \frac{\sqrt{2}}{\sqrt{3}}|10\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$$

Entangled States

Not every state is a pure state, i.e. can be written as $|\psi_1\rangle \otimes \ldots \otimes |\psi_q\rangle$.

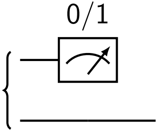
Measurement Gates

The measurement of a basis state is similar to classical measurements:



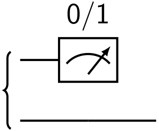
Measurement Gates: Example

$$\frac{1}{\sqrt{3}}|01\rangle + \frac{\sqrt{2}}{\sqrt{3}}|10\rangle \sim \begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$



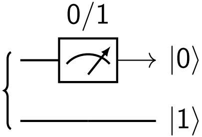
Measurement Gates: Example

$$\frac{1}{\sqrt{3}}\left|01\right\rangle + \frac{\sqrt{2}}{\sqrt{3}}\left|10\right\rangle \sim \begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$



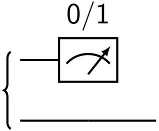
probability 1/3

$$\begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$



Measurement Gates: Example

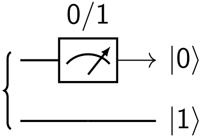
$$\frac{1}{\sqrt{3}}|01\rangle + \frac{\sqrt{2}}{\sqrt{3}}|10\rangle \sim \begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$



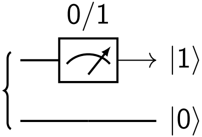
probability 1/3

probability 2/3

$$\begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$

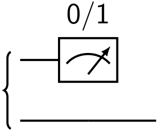


$$\begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$



Measurement Gates: Example

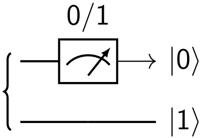
$$\frac{1}{\sqrt{3}}|01\rangle + \frac{\sqrt{2}}{\sqrt{3}}|10\rangle \sim \begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$



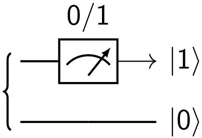
probability 1/3

probability 2/3

$$\begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$



$$\begin{bmatrix} 0 \\ 1/\sqrt{3} \\ \sqrt{2}/\sqrt{3} \\ 0 \end{bmatrix}$$



Entangled Qubits

If the first qubit is measured to be 0 then the second qubit will be in state 1 after the measurement almost surely.

Operations on the State

Unitary Operators

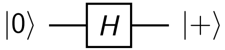
An operation applied by a quantum computer with q qubits, also called a gate, is a unitary operator $U \in \mathbf{C}^{2^q \times 2^q}$.

Operations on the State

Unitary Operators

An operation applied by a quantum computer with q qubits, also called a gate, is a unitary operator $U \in \mathbf{C}^{2^q \times 2^q}$.

- Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

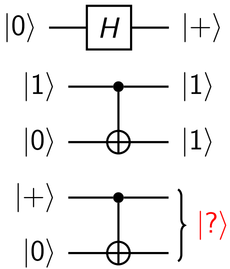


Operations on the State

Unitary Operators

An operation applied by a quantum computer with q qubits, also called a gate, is a unitary operator $U \in \mathbf{C}^{2^q \times 2^q}$.

- Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- CNOT gate $C_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

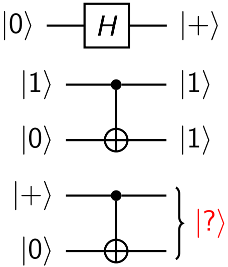


Operations on the State

Unitary Operators

An operation applied by a quantum computer with q qubits, also called a gate, is a unitary operator $U \in \mathbf{C}^{2^q \times 2^q}$.

- Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- CNOT gate $C_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
- $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

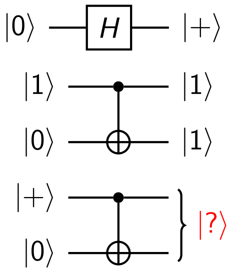


Operations on the State

Unitary Operators

An operation applied by a quantum computer with q qubits, also called a gate, is a unitary operator $U \in \mathbf{C}^{2^q \times 2^q}$.

- Hadamard gate $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
- CNOT gate $C_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
- $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$



Universal Set of Gates

By composing H, T, and CNOT gates every gate (unitary operator) can be arbitrarily well approximated.

Quantum Circuits: Black-Box Search

Problem: Find the unique binary string satisfying a given property.

x	000	001	010	011	100	101	110	111
$f(x)$	0	0	0	0	0	0	1	0

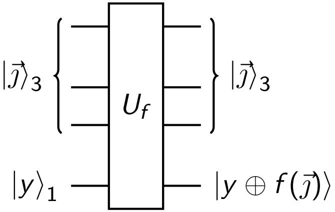


Figure: Quantum circuit treated as black box

Typical way to implement a binary function; recall that all operations are reversible

Quantum Circuits: Black-Box Search

Problem: Find the unique binary string satisfying a given property.

x	000	001	010	011	100	101	110	111
$f(x)$	0	0	0	0	0	0	1	0

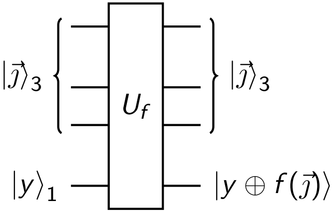


Figure: Quantum circuit treated as black box

Typical way to implement a binary function; recall that all operations are reversible

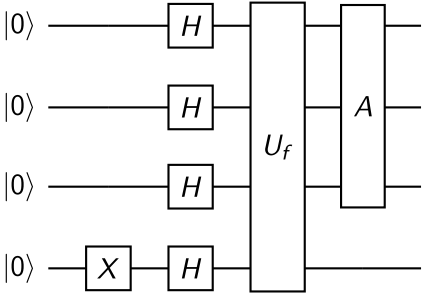


Figure: Basic Circuit in Grover's Algorithm

Grover's Algorithm

1. **Initialization:**

$$\sum_{\vec{\jmath}\in\{0,1\}^3} \frac{1}{\sqrt{8}} |\vec{\jmath}\rangle \otimes |-\rangle$$

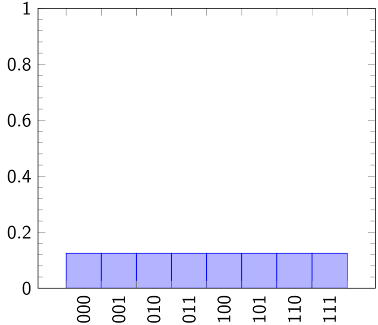


Figure: Probability interpretation of the state

1. **Initialization:**
$$\sum_{\vec{\jmath}\in\{0,1\}^3} \frac{1}{\sqrt{8}} |\vec{\jmath}\rangle \otimes |-\rangle$$
2. **Black-Box:**

$$\left(-\frac{1}{\sqrt{8}} |110\rangle + \sum_{\substack{\vec{\jmath}\in\{0,1\}^3 \\ \vec{\jmath}\neq 110}} \frac{1}{\sqrt{8}} |\vec{\jmath}\rangle \right) \otimes |-\rangle$$

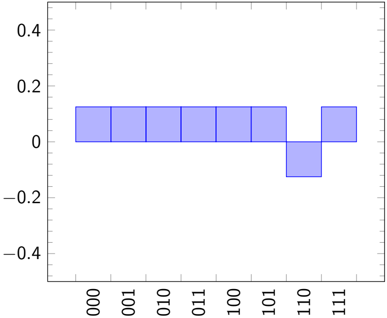


Figure: Probability interpretation of the state

Grover's Algorithm

1. **Initialization:**
$$\sum_{\vec{\jmath}\in\{0,1\}^3} \frac{1}{\sqrt{8}} |\vec{\jmath}\rangle \otimes |-\rangle$$
2. **Black-Box:**
$$\left(-\frac{1}{\sqrt{8}} |110\rangle + \sum_{\substack{\vec{\jmath}\in\{0,1\}^3 \\ \vec{\jmath}\neq 110}} \frac{1}{\sqrt{8}} |\vec{\jmath}\rangle \right) \otimes |-\rangle$$
3. **Inversion about the Average:**
$$\left(\frac{5}{2\sqrt{8}} |110\rangle + \sum_{\substack{\vec{\jmath}\in\{0,1\}^3 \\ \vec{\jmath}\neq 110}} \frac{1}{2\sqrt{8}} |\vec{\jmath}\rangle \right) \otimes |-\rangle$$

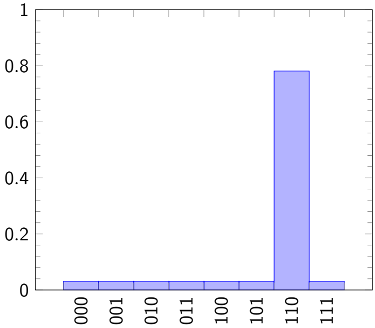


Figure: Probability interpretation of the state

Grover's Algorithm: Complexity

Classically, the best that can be done is randomly sample the function f on the binary strings. Therefore, $\Omega(2^n)$ queries are needed to guarantee a large probability of success.

Complexity of Grover's algorithm

To maximize the probability of measuring the correct (marked) item, the optimal number of queries is approximately $\sqrt{2^n} = 2^{n/2}$.

Complexity Theory

- **Complexity Class** BPQ: Problems solvable in polynomial time by a quantum computer with bounded (and small) error probability.

Complexity Theory

- **Complexity Class** BPQ: Problems solvable in polynomial time by a quantum computer with bounded (and small) error probability.
- Every classical circuit can be efficiently simulated by a quantum circuit $\implies$ P $\subseteq$ BPQ

Complexity Theory

- **Complexity Class** BPQ: Problems solvable in polynomial time by a quantum computer with bounded (and small) error probability.
- Every classical circuit can be efficiently simulated by a quantum circuit $\implies$ P $\subseteq$ BPQ

Theorem (Bennett, Bernstein, Brassard, and Vazirani, 94)

Grover's algorithm uses assymptotically the minimal number of queries.

Corallary: There is no "brute force" quantum algorithm to solve NP-complete problems in polynomial time.

Complexity Theory

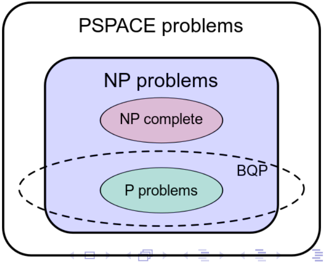
- **Complexity Class** BPQ: Problems solvable in polynomial time by a quantum computer with bounded (and small) error probability.
- Every classical circuit can be efficiently simulated by a quantum circuit $\implies$ P $\subseteq$ BPQ

Theorem (Bennett, Bernstein, Brassard, and Vazirani, 94)

Grover's algorithm uses assymptotically the minimal number of queries.

Corallary: There is no "brute force" quantum algorithm to solve NP-complete problems in polynomial time.

- Integer factorization is in BPQ (**Shor's algorithm**)
- Not knwon whether NP $\subset$ BPQ implies P $=$ NP



The Answer to the “Ultimate Question of Life, the Universe, and Everything”

The Answer to the "Ultimate Question of Life, the Universe, and Everything"

$$21 = 7 \cdot 3$$

Figure: IBM Research, CC BY 2.0, via Wikimedia Commons

The Answer to the "Ultimate Question of Life, the Universe, and Everything"

Preventing decoherence of the system of entangled qubits is challenging:

- cooled close to 0 °K
- placed into near vacuum environment
- shielded from electromagnetic radiation

$$21 = 7 \cdot 3$$

Figure: IBM Research, CC BY 2.0, via Wikimedia Commons

The Answer to the “Ultimate Question of Life, the Universe, and Everything”

Preventing decoherence of the system of entangled qubits is challenging:

- cooled close to 0 °K
- placed into near vacuum environment
- shielded from electromagnetic radiation

Details on the IBM System One at the Fraunhofer Center of Quantum Computing:

- 27 qubits
- coherence time: 100 μs
- 2 qubit gate error rate $\approx 1\%$
- operational time of a 2 qubit gate $\approx$ 500 ns

$$21 = 7 \cdot 3$$

Figure: IBM Research, CC BY 2.0, via Wikimedia Commons

References

[1] Scott Aaronson. "NP-complete Problems and Physical Reality". In: (2005). DOI: 10.48550/ARXIV.QUANT-PH/0502072. URL: https://arxiv.org/abs/quant-ph/0502072.

[2] Fraunhofer IAF. *Kompetenzzentrum Quantum Computing Baden-Würtemberg*. Last accessed 19 January 2023. 2022. URL: https://www.iaf.fraunhofer.de/de/netzwerker/KQC.html.

[3] Giacomo Nannicini. "An Introduction to Quantum Computing, Without the Physics". In: *CoRR* abs/1708.03684 (2017). arXiv: 1708.03684. URL: http://arxiv.org/abs/1708.03684.