Summary of Quantum Mechanics
From Classical to Quantum Computing

• Boolean circuits
• Reversible computing
• Quantum computing
GOALS

• Construct a quantum model for computation
• Relate the quantum model of computation to the classical one
• Point out the differences between classical and quantum computing
• Show that classical computations can be done on a quantum computer
Boolean Circuits

A mathematical model for classical computing

Thursday, 19 April 12
**Boolean Circuits**

- Any function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ can be computed using a small fixed set of **boolean gates**
**Boolean Circuits**

- Any function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ can be computed using a small fixed set of boolean gates.
- Each gate corresponds to some boolean function.
Boolean Circuits

- Any function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ can be computed using a small fixed set of boolean gates.
- Each gate corresponds to some boolean function.
- A network of boolean gates is called a boolean circuit.
Boolean Circuits

- Any function $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$ can be computed using a small fixed set of boolean gates
- This fixed set of boolean gates is called a universal set of gates
**Boolean Circuits**

- Any function \( f : \{0, 1\}^n \rightarrow \{0, 1\}^m \) can be computed using a small **fixed set** of boolean gates.
- This **fixed set** of boolean gates is called a **universal set of gates**.
- There exists more than one **universal set of gates**.

![Boolean gates](image)
Boolean Circuits

- Any function \( f : \{0, 1\}^n \to \{0, 1\}^m \) can be computed using a small **fixed set of boolean gates**
- This **fixed set** of boolean gates is called a **universal set of gates**
- There exists more than one **universal set of gates**
Boolean Circuits

- Any function \( f : \{0, 1\}^n \to \{0, 1\}^m \) can be computed using a small **fixed set** of boolean gates
- This **fixed set** of boolean gates is called a **universal set of gates**
- There exists more than one **universal set of gates**

\[
\begin{align*}
\text{AND: } a \land b \\
\text{NOT: } \neg a \\
\text{OR: } a \lor b \\
\text{NAND: } \neg(a \land b)
\end{align*}
\]
Boolean Circuits

• Any function \( f : \{0, 1\}^n \rightarrow \{0, 1\}^m \) can be computed using a small **fixed set** of boolean gates

• This **fixed set** of boolean gates is called a **universal set of gates**

• There exists more than one **universal set of gates**
**Boolean Circuits**

- Boolean circuits are **irreversible**
- In general, we cannot recover the input to a boolean circuit from its output
- Quantum operators are **reversible**
- A quantum analog to the boolean circuits should therefore be **reversible**
Reversible Classical Computing
Reversible Classical Computing

- Unitary evolution is reversible (for every U, there exists U dagger)
- Hence quantum computing is going to be reversible
Two bit boolean gates are not enough
At least three bit gates are required
A universal reversible gate is the Toffoli gate
Reversible Functions

- We can use the Toffoli gate to simulate a NAND gate
- Hence every boolean circuit can be represented as a reversible circuit consisting of only Toffoli gates

\[ 1 \oplus (a \land b) = \neg (a \land b) \]
Reversible Functions

- We can use the Toffoli gate to simulate a NAND gate
- Hence every boolean circuit can be represented as a reversible circuit consisting of only Toffoli gates
- It also turns out, that the Toffoli gate acts as a **unitary operator**

\[
1 \oplus (a \land b) = \neg (a \land b)
\]
Quantum Circuits

A mathematical model for quantum computing
The quantum analogues of \textit{bits} are \textit{qubits}
Quantum Circuits

- **qubits** are represented as **wires** in the quantum circuit model
Quantum Circuits

- **qubits** are represented as **wires** in the quantum circuit model
- **unitary operators** acting on the **qubits** are represented as **quantum gates**
Quantum Circuits

- **qubits** are represented as **wires** in the quantum circuit model.
- **unitary operators** acting on the **qubits** are represented as **quantum gates**.
- **gates** can act on multiple qubits.

![Quantum Circuit Diagram]

Thursday, 19 April 12
Quantum Circuits

- qubits are represented as wires in the quantum circuit model
- unitary operators acting on the qubits are represented as quantum gates
- gates can act on multiple qubits
Quantum Circuits

- **qubits** are represented as **wires** in the quantum circuit model

- **unitary operators** acting on the **qubits** are represented as **quantum gates**

- **gates** can act on multiple qubits
We could use any unitary gate in this model
This would be an unrealistic model
In practice, not every unitary is implementable
What is the smallest set of universal gates?
Quantum Toffoli

- The Toffoli gate implements a unitary operator
- As we can use every unitary operator in quantum computing, we can use Toffoli as a quantum gate.
Quantum Toffoli

- The Toffoli gate implements a unitary operator.
- As we can use every unitary operator in quantum computing, we can use Toffoli as a quantum gate.

\[
\begin{align*}
\text{a} & \quad \rightarrow \quad \text{a} \\
\text{b} & \quad \rightarrow \quad \text{b} \\
\text{c} & \quad \rightarrow \quad \text{c} \oplus (a \land \text{b})
\end{align*}
\]
Quantum Toffoli

• The Toffoli gate implements a unitary operator
• As we can use every unitary operator in quantum computing, we can use Toffoli as a quantum gate.

\[ a \quad \quad \quad \quad a \]
\[ b \quad \quad \quad \quad b \]
\[ c \quad \quad \quad \quad c \oplus ( a \land b ) \]

• Therefore we can implement any classical computation on a quantum computer
• What about probabilistic computations?
Quantum Toffoli

- The Toffoli gate implements a unitary operator
- As we can use every unitary operator in quantum computing, we can use Toffoli as a quantum gate.
- It turns out that Toffoli is “too much” for performing reversible classical computing on quantum computers
Quantum Toffoli

- The Toffoli gate implements a unitary operator.
- As we can use every unitary operator in quantum computing, we can use Toffoli as a quantum gate.
- It turns out that Toffoli is “too much” for performing reversible classical computing on quantum computers.
Decomposing Toffoli

- The more qubits a gate acts on, the harder it is to implement in the real world
- Two qubit gates is hard to implement, three qubit ones is extremely difficult
Universal Set of Quantum Gates

- Theoretically a completely universal set of gates is not needed if we are interested in building a quantum computer for a single algorithm.