Quantum Computation: Introduction

Ronald de Wolf

Centrum Wiskunde & Informatica

From classical physics to quantum

- Classical physics: Developed over centuries (Archimedes, Newton, Maxwell)
- Objects have well-defined properties, independent of how they are measured
- Quantum mechanics: First half of 20th century (Planck, Einstein, Bohr, Schrödinger, Heisenberg)
- One of our best physical theories,
  never been contradicted by experiment
- Not just in the lab: 1/3 of our GDP depends on quantum
- Many “weird” effects:

  superposition, interference, entanglement

Quantum computers

- Current computers (in theory and practice) are based on classical physics
- Feynman, Benioff ($\pm$1982):

  What about quantum mechanical computers?

  Can we use those weird effects for useful computation?
- Deutsch ('85): universal quantum Turing machine
- Peter Shor: efficient algorithm for factoring ('94)
- Since then: fast growing field
  1. can we build it?
  2. what can it do?
- We focus on second question: quantum algorithms

Overview of the course

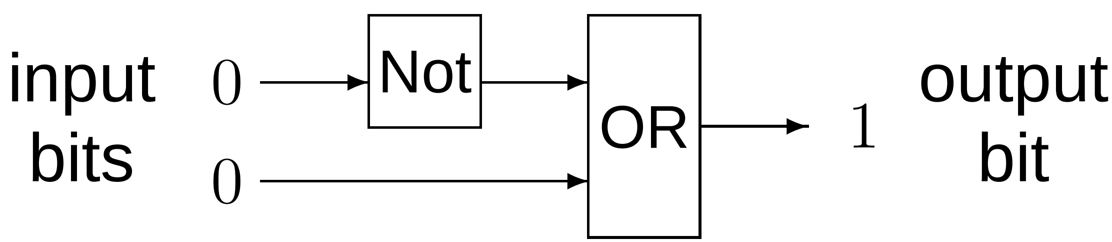
- Quantum computation: introduction (today)
- Quantum computation: main algorithms
- Quantum communication

Overview of this lecture

- What are classical algorithms?
- What are quantum algorithms?
- Simple quantum algorithms:
  - Deutsch-Jozsa
  - Simon

Classical algorithms

- Operate on bits
- Two main models: Turing machines, Boolean circuits
- Circuits are easier to generalize to quantum
- Directed acyclic graph of AND, OR, NOT gates
- Starting nodes: n input bits, additional workspace
- This computes some function by evaluating all gates



- Efficient computation: polynomial-size circuits

From classical to quantum

- bits $\longrightarrow$ qubits
- AND/OR/NOT gates $\longrightarrow$ unitary quantum gates
- classical circuit $\longrightarrow$ quantum circuit
- reading the output bit $\longrightarrow$ measuring final state

Recap of linear algebra 1

- Vector space V over field $\mathbb{F}$: set of objects such that
  1. $v, w \in V \Rightarrow v + w \in V$ (closed under addition)
  2. $v \in V, a \in \mathbb{F} \Rightarrow av \in V$ (closed u. scalar multiplication)

  Think: $V = \mathbb{C}^d$, $v = (v_1, \ldots, v_d)^T$, basis $\{e_1, \ldots, e_d\}$
- Inner product: $\langle v|w\rangle = \sum_{i=1}^{d} v_i^* w_i$
- Orthogonal: $\langle v|w\rangle = 0$
- Norm: $\| v \| = \sqrt{\langle v|v\rangle} = \sqrt{\sum_{i=1}^{d} |v_i|^2}$
- Unit vector: norm 1

Recap of linear algebra 2

- Linear transformation $A : V \to W$
  1. $u, v \in V \Rightarrow A(u + v) = A(u) + A(v)$
  2. $v \in V, a \in \mathbb{F} \Rightarrow A(av) = aA(v)$

  Think: $V = W = \mathbb{C}^d$, A is $d \times d$ matrix
- A is Hermitian if $A = A^*$ (conjugate transpose)
- A is unitary if $A^{-1} = A^*$

  Equivalent:
  A is norm-preserving,
  columns of A are orthonormal

Recap of linear algebra 3

- Tensor product of matrices:

$$A \otimes B = \begin{pmatrix} A_{11}B & \cdots & A_{1d'}B \\ & \ddots & \\ A_{d1}B & \cdots & A_{dd'}B \end{pmatrix}$$

- Special case: vectors $\begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ \vdots \\ b_e \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_d b_e \end{pmatrix}$

- Tensor product $V \otimes W$ of spaces V and W:
take basis $\{v_1 \ldots, v_d\}$ for V, basis $\{w_1, \ldots, w_e\}$ for W,
then $V \otimes W =$ span$\{v_i \otimes w_j : 1 \leq i \leq d, 1 \leq j \leq e\}$
Note: dimension of $V \otimes W$ is $d \cdot e$

Quantum bits

- Classical bit: value 0 or value 1
- Basis states of a 2-dimensional vector space:

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

- Qubit: superposition $\alpha_0|0\rangle + \alpha_1|1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \in \mathbb{C}^2$
- We require $|\alpha_0|^2 + |\alpha_1|^2 = 1$
- Examples: $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
  $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}e^{i\pi/4}|1\rangle$
  $\sin(\alpha)|0\rangle + \cos(\alpha)|1\rangle$

More qubits

- Two qubits: tensor product space, with 4 basis vectors

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

- Abbreviate $|a\rangle \otimes |b\rangle = |a\rangle|b\rangle = |a, b\rangle = |ab\rangle$
- 2-qubit state: $|\phi\rangle = \sum_{x \in \{0,1\}^2} \alpha_x |x\rangle \in \mathbb{C}^4$
- Example: EPR-pair: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ (entangled)
- n-qubit state: $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \in \mathbb{C}^{2^n}$

Quantum states and dynamics

- n-qubit state $|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle = \begin{pmatrix} \alpha_{0\ldots0} \\ \vdots \\ \alpha_{1\ldots1} \end{pmatrix} \in \mathbb{C}^{2^n}$

- *Informally*: we are in all 2^n basis states simultaneously
- *Formally*: $|\phi\rangle$ is a unit vector in 2^n-dimensional space

- Two kinds of quantum operations on $|\phi\rangle$:

  1. Unitary transform of the amplitude-vector
  2. Measurement

Measurement

- Measuring quantum state $|\phi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$ gives $|x\rangle$ with probability $|\alpha_x|^2$; state collapses to $|x\rangle$
- Note: probabilities sum to 1 because $|\phi\rangle$ is a unit vector
- We can also measure part of a state.
  The state then collapses to the part that is "consistent" with the measurement outcome
- Example: measure 2nd register of $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle$
  gives $|a\rangle$ with probability $\frac{|\{x: f(x)=a\}|}{2^n}$;
  State collapses to $\frac{1}{\sqrt{|\{x : f(x) = a\}|}} \sum_{x: f(x)=a} |x\rangle|a\rangle$

Quantum gate: unitary on 1 or 2 qubits

- 1-qubit NOT gate: $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
- 1-qubit Hadamard gate: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
- 1-qubit $\pi/4$-gate: $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$
- 2-qubit controlled-NOT: $C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Example: fun with Hadamard

- $H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$

  Measurement gives $|0\rangle$ or $|1\rangle$ with probability 1/2
- $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle$

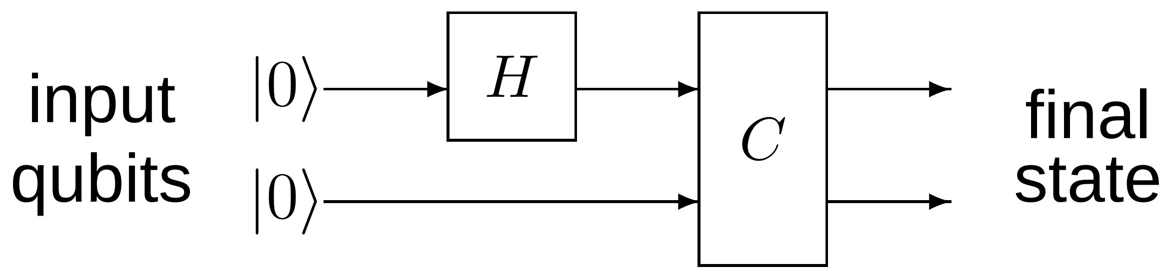
  Measurement gives $|0\rangle$ or $|1\rangle$ with probability 1/2
- We can get interference:

  $$H|+\rangle = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle$$

  $$H|-\rangle = |1\rangle$$
- Hadamard on n qubits: $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y}|y\rangle$

Quantum circuits

- Circuit of gates transforms input state to final state



- Viewed as a big unitary: $C(H \otimes I)$
- Final state: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, an EPR-pair
- Measure specific qubit of final state to obtain output
- H, T, C gates can approximate any n-qubit unitary
- Efficient quantum computation: polynomial-size circuit

Quantum parallelism

- Suppose classical algorithm computes $f : \{0,1\}^n \to \{0,1\}^m$
- Then quantum circuit $U : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$ can compute f on all inputs simultaneously!

$$U\left(\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle\right)=\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

- This contains all 2^n function values!
- But observing gives only one random $|x\rangle|f(x)\rangle$
- All other information will be lost
- More tricks needed for successful quantum computation

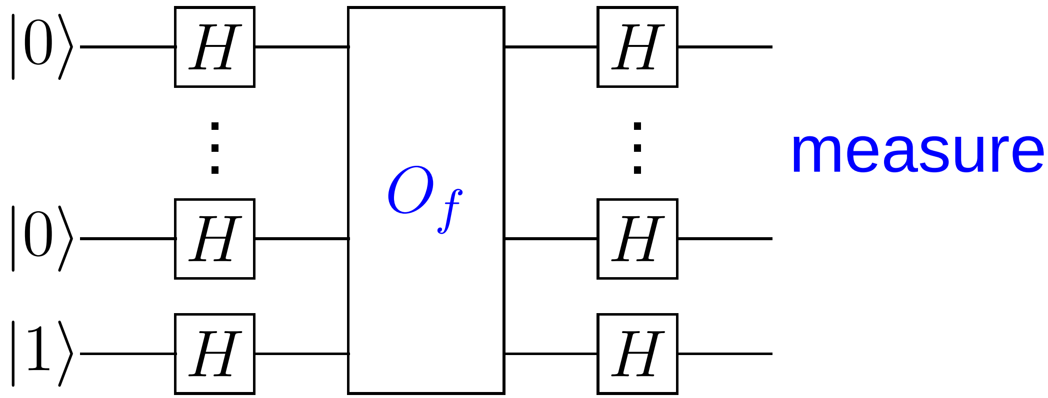
Deutsch-Jozsa problem

- Given: function $f : \{0,1\}^n \to \{0,1\}$ (2^n bits), s.t.
(1) $f(x) = 0$ for all x (constant), or
(2) $f(x) = 0$ for $\frac{1}{2} \cdot 2^n$ of the x's (balanced)
- Question: is f constant or balanced?

- Classically: need at least $\frac{1}{2} \cdot 2^n + 1$ steps ("queries" to f)
- Quantumly: $O(n)$ gates suffice, and only 1 query

- Query: application of unitary $O_f : |x, 0\rangle \mapsto |x, f(x)\rangle$
- More generally: $O_f : |x, b\rangle \mapsto |x, b \oplus f(x)\rangle$ ($b \in \{0,1\}$)
- Note: $O_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

Deutsch-Jozsa algorithm



- Starting state: $|\underbrace{0\ldots0}_{n}\rangle|1\rangle$
- After first Hadamards: $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|-\rangle$
- Make one query: $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle|-\rangle$
- Forget about the $|-\rangle$

Deutsch-Jozsa (continued)

- After second Hadamard:

$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y} |y\rangle$$

- $\alpha_{0\ldots0} = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} = \begin{cases} 1 & \text{if constant} \\ 0 & \text{if balanced} \end{cases}$

- Measurement gives right answer with certainty

- Big quantum-classical separation. . .

- But the problem is efficiently solvable by bounded-error classical algorithm (query f at a few random x)

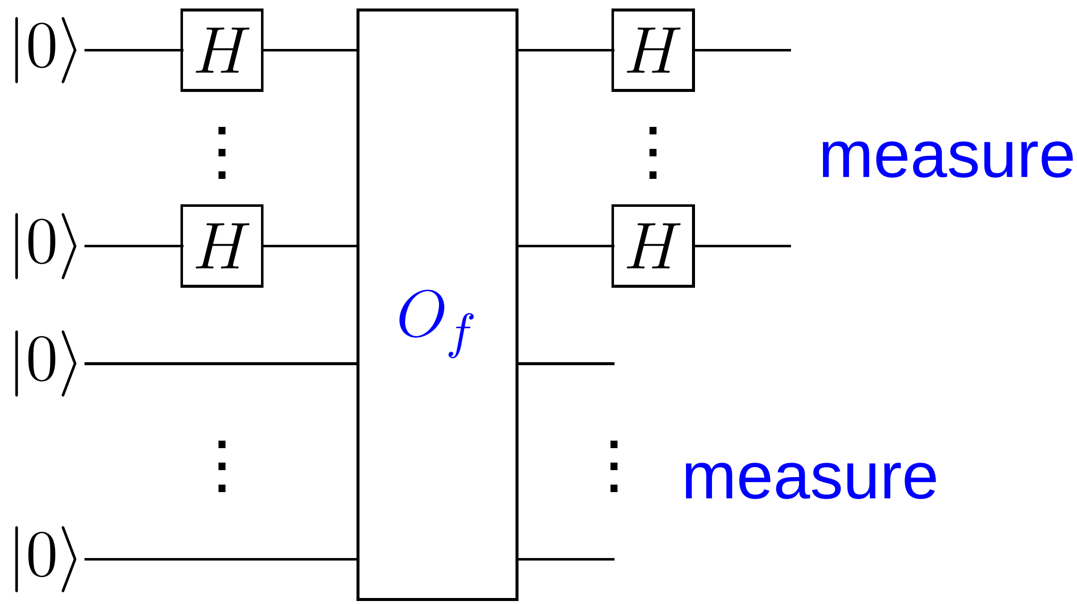
Simon's problem

- Given: function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ such that there exists $s \in \{0,1\}^n$ satisfying $f(x) = f(y)$ iff $x = y \oplus s$
- Note: if $s = 0^n$ then f is a permutation (1-1), otherwise f is a 2-1 function
- Question: is $s = 0^n$ or not

- Classically: need $\sqrt{2^n}$ queries for high success prob
- Quantumly: solve in $O(n)$ queries and $O(n^3)$ gates

- Quantum algorithm is exponentially better, even compared with classical bounded-error algorithms

Simon: quantum algorithm



- After H's and O_f: $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$
- Measure specific $f(x)$: 1st register $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)$
- After H's: $\frac{1}{\sqrt{2^{n+1}}} \left(\sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle + (-1)^{(x \oplus s) \cdot y} |y\rangle \right)$

Simon's algorithm (continued)

- First n qubits: $\frac{1}{\sqrt{2^{n+1}}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} (1 + (-1)^{s \cdot y}) |y\rangle$
- Note: $|y\rangle$ has non-zero amplitude iff $s \cdot y = 0$ mod 2
- Measure: get string $y \in \{0,1\}^n$ s.t. $s \cdot y = 0$ mod 2
- Repeat this $2n$ times, giving $y_1, \ldots, y_{2n}$, each with $s \cdot y_i = 0$ mod 2
- W.h.p. there are n linearly independent y's
- This system of linear equations $s \cdot y_i = 0$ mod 2 determines s (solve via Gaussian elimination)
- Quantum algorithm uses $O(n)$ queries and $O(n^3)$ gates

Classical lower bound

- Intuition: a classical algorithm can only query f at random points
- As long as it doesn't find a collision (x, y s.t. $f(x) = f(y)$) it cannot distinguish 1-1 from 2-1 functions
- For uniform 2-1 function and fixed x, y: $\Pr[f(x) = f(y)] \approx 1/2^n$
- With T queries, we have queried $\binom{T}{2}$ specific pairs

$$\Pr[\text{see a collision}] \leq \text{Exp}[\#\text{collisions}] \approx \binom{T}{2}\frac{1}{2^n} \approx \frac{T^2}{2^{n+1}}$$

- If $T \ll \sqrt{2^n}$ then algorithm can't distinguish 1-1 from 2-1
- Classical algorithm needs $\approx \sqrt{2^n}$ queries

Summary

- We introduced quantum mechanics
- We showed how to use it for computation:
  qubits, unitary gates, circuits, measurements
- Quantum algorithms can be better than classical (Deutsch-Jozsa and Simon)

- Next two lectures:
  - Main quantum algorithms: Shor and Grover
  - Quantum communication