Lecture 1
Introduction to quantum computing

January 9, 2020

The Moore Law

	Intel First Production
1999	180 nm
2001	130 nm
2003	90 nm
2005	65 nm
2007	45 nm
2009	32 nm
2011	22 nm
2014	14 nm
2016	~~10 nm~~
2017	~~10 nm~~
2018	10 nm?
2019	10 nm!

- miniaturization reaches levels where quantum effects become non-negligible. Suppress them or exploit them ?

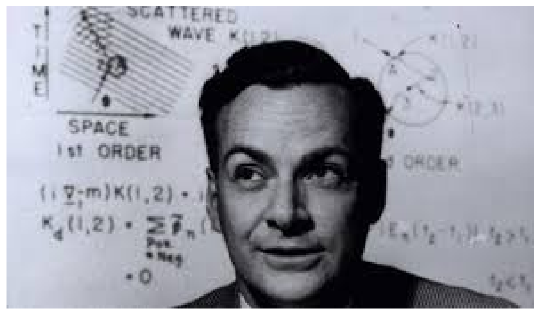
Genesis of quantum computing

Feynman 1981

"Can quantum systems be probabilistically simulated by a classical computer?
[. . .] The answer is almost certainly, No!"

$\Rightarrow$ use quantum systems to simulate quantum systems!

$\Rightarrow$ birth of quantum simulation



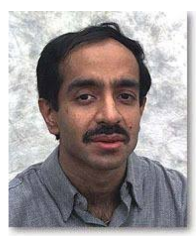
Deutsch 1985 : Foundations of quantum computation

The early algorithms

Shor 1994

- Solves the discrete logarithm and factoring problem in polynomial time with a quantum computer
- breaks almost all cryptosystems used in practice nowadays
- Crypto community worried about this a few years ago
- end of 2017 : NIST has launched a competition for standardizing public-key cryptography that is resistant to a quantum computer

Grover 1996 : search for a particular element in a list of size n in $O(\sqrt{n})$

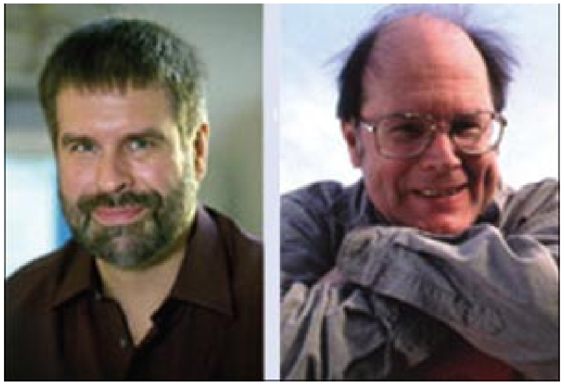


Quantum cryptography

Bennett-Brassard 1984

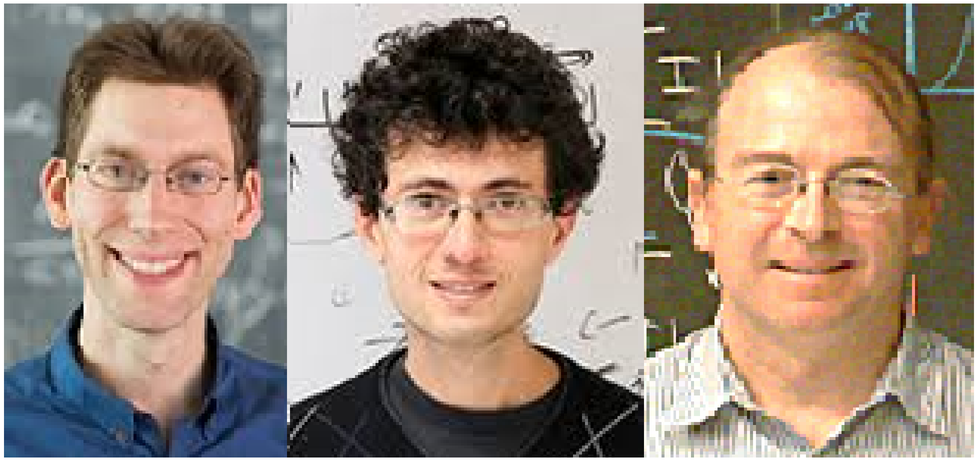
Quantum protocol for key exchange

- is already implemented
- "unconditional security" : security only relies on the validity of the laws of quantum physics and not on computational assumptions



Slow progress in quantum computing ?

- A few years ago the only algorithms giving a quantum speedup were
  - Shor's algorithm
  - Grover's algorithm
  - variants/generalizations (quantum walks...)
- Then in 2009 came the HHL (Harrow, Hassidim, Lloyd) algorithm



The HHL algorithm and its "exponential speedup"

Problem

Input: an $n \times n$ complex matrix $\mathbf{A}$, $\mathbf{b} \in \mathbb{C}^n$

Output: a solution $\mathbf{x} \in \mathbb{C}^n$ of $\mathbf{Ax} = \mathbf{b}$.

Complexity

- Classically $\Omega(n^2)$
- Quantumly (HHL) $O(\log n)$ (under certain restrictions)

HHL, the fine prints

Assumes that

- $\mathbf{b}$ is given as a quantum state $\mathbf{b} = \sum_i b_i |i\rangle$
- $\mathbf{A}$ is sparse and well conditioned

Then HHL outputs a quantum state $|x\rangle = \sum_i x_i |i\rangle$ in time polynomial in s (sparsity of the matrix) and κ (condition number) and logarithmic in n

First use in machine learning for recommendation systems Kerenidis, Prakash (2016)

Recommendation system

Problem

An unknown (hidden) $m \times n$ binary matrix $\mathbf{P}$ modelling customers preferences and $\mathbf{P}$ is of low rank k. For a customer i one should output columns j such that it is likely that $P_{ij} = 1$.

- Quantum algorithm based on HHL that is of complexity $O(\text{poly}(k)\text{polylog}(mn))$ (we do not use all the entries of $\mathbf{P}$!)

The big issue : decoherence

- Qubits are very fragile and interfere quickly with the environment: decoherence
- Quantum gates are noisy themselves
- Needs quantum fault tolerant architectures
- This can be done in principle by using quantum error correcting codes

Theorem 1. [Aharonov, Ben-Or, 1997] *Quantum computation is possible provided the noise is sufficiently low (below some constant, say 1%)*

The cost of fault tolerance

- Intel, IBM and Google have now quantum devices with $50 - 70$ imperfect qubits and gates
- Fault tolerant architectures produce "good enough" qubits from imperfect qubits and gates
- Shor's algorithm for breaking RSA-1024
  - requires about few 10^3 "good enough" qubits
  - current quantum fault tolerant architectures do this with the help of $10^7 - 10^9$ imperfect qubits

What's next

- Quantum sensing
- NISQ: Noisy Intermediate Scale Quantum computing, computing with 100's of imperfect qubits by using low depth quantum circuits
  - solve combinatorial optimization problems with hybrid classical/quantum algorithms for instance
    1. quantum processor prepares a quantum state
    2. measure it
    3. process the result classically
    4. instructs how to modify the quantum state preparation
    5. repeat until convergence
  - quantum chemistry: find low-energy states of (large) molecules

Classical bit

- Classical bit $b \in \{0,1\}$
- Probabilistic bit $\mathcal{P} = \begin{pmatrix} p \\ q \end{pmatrix} \in [0,1]^2$ and $p + q = 1$

$$
\begin{aligned}
p &\stackrel{\text{def}}{=} \mathbf{Prob}(b = 0) \\
q &\stackrel{\text{def}}{=} \mathbf{Prob}(b = 1)
\end{aligned}
$$

- Evolution:

$$
\begin{aligned}
\begin{pmatrix} p \\ q \end{pmatrix} \rightarrow \begin{pmatrix} p' \\ q' \end{pmatrix} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p \\ q \end{pmatrix} \text{ where} \\
a + c &= 1 \\
b + d &= 1
\end{aligned}
$$

probabilistic computation: multiplication by a stochastic matrix

The qubit

- qubit: element $|\psi\rangle$ of $\mathbb{C}^2$ of (euclidean) norm 1

$$\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \; |\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle, \text{ where } |\alpha|^2 + |\beta|^2 = 1$$

- Measurement: probabilistic orthogonal projection.

Measurement in the basis $\{|0\rangle, |1\rangle\}$:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \overset{\text{measure}}{\rightarrow} \begin{cases} |0\rangle & \text{with prob. } |\alpha|^2 \\ |1\rangle & \text{with prob. } |\beta|^2 \end{cases}$$

- Unitary evolution : $\mathbf{P} \in \mathbb{C}^{2\times 2}$ such that $\mathbf{P}^*\mathbf{P} = \mathbf{Id}$

$$|\psi\rangle \rightarrow \mathbf{P}\,|\psi\rangle$$

Note : the transformation is reversible

$$\begin{aligned} |\psi\rangle &\overset{\mathbf{P}}{\rightarrow} & |\psi'\rangle = \mathbf{P}\,|\psi\rangle \\ |\psi'\rangle &\overset{\mathbf{P}^*}{\rightarrow} & \mathbf{P}^*\,|\psi'\rangle = \mathbf{P}^*\mathbf{P}\,|\psi\rangle = |\psi\rangle\,. \end{aligned}$$

Examples of quantum gates

- The NOT gate (also called $\mathbf{X}$ gate)

$$
\begin{aligned}
|0\rangle &\stackrel{\text{NOT}}{\rightarrow} |1\rangle \\
|1\rangle &\stackrel{\text{NOT}}{\rightarrow} |0\rangle \\
|b\rangle &\stackrel{\text{NOT}}{\rightarrow} |1-b\rangle
\end{aligned}
$$

- The Hadamard gate

$$
\begin{aligned}
|0\rangle &\stackrel{\mathbf{H}}{\rightarrow} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|1\rangle &\stackrel{\mathbf{H}}{\rightarrow} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
|b\rangle &\stackrel{\mathbf{H}}{\rightarrow} \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{b}|1\rangle\right)
\end{aligned}
$$

Exercise

1. What is the effect of applying $\mathbf{H}$ to $|0\rangle$ and then measuring it ?
2. What is the effect of applying $\mathbf{H}$ twice to $|0\rangle$ and then measuring it ?
3. Show that there is no stochastic matrix $\mathbf{P}$ which when applied to 0, ie. to $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, simulates the effect of the Hadamard gate.
4. Give a quantum evolution (ie. a 2×2 unitary matrix) such that $\mathbf{P}^2$ is the NOT-gate
5. Does there exist a stochastic matrix $\mathbf{P}$ such that $\mathbf{P}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$?

Exercise

1. Give a quantum evolution $\mathbf{P}$ which satisfies for any $b \in \{0,1\}$

$$|b\rangle \quad \overset{\mathbf{P}}{\rightarrow}\overset{\text{meas.}}{\rightarrow} \quad \begin{cases} |0\rangle \text{ with prob. } 1/2 \\ |1\rangle \text{ with prob. } 1/2 \end{cases}$$

$$|b\rangle \quad \overset{\mathbf{P}}{\rightarrow}\overset{\mathbf{P}}{\rightarrow}\overset{\text{meas.}}{\rightarrow} \quad |b\rangle$$

2. Are there other solutions to this problem ?

Measurement in another basis

Orthonormal basis $\{|\psi_0\rangle, |\psi_1\rangle\}$, $\langle\psi_i|\psi_j\rangle = \delta_{ij}$

What we want

$$|\psi\rangle = \alpha|\psi_0\rangle + \beta|\psi_1\rangle \xrightarrow{\text{measure}(\psi_0,\psi_1)} \begin{cases} |\psi_0\rangle & \text{with prob. } |\alpha|^2 \\ |\psi_1\rangle & \text{with prob. } |\beta|^2 \end{cases}$$

Change of basis

$$\begin{aligned} |b\rangle &\xrightarrow{\mathbf{P}} |\psi_b\rangle \\ \mathbf{P} &= \begin{pmatrix} \langle 0|\psi_0\rangle & \langle 0|\psi_1\rangle \\ \langle 1|\psi_0\rangle & \langle 1|\psi_1\rangle \end{pmatrix} \end{aligned}$$

Realization

$$\rightarrow \boxed{\text{measure}(|\psi_0\rangle, |\psi_1\rangle)} \rightarrow\equiv\rightarrow \boxed{\mathbf{P}^*} \rightarrow \boxed{\text{measure}(|0\rangle, |1\rangle)} \rightarrow \boxed{\mathbf{P}} \rightarrow$$

The Deutsch-Josza problem

- Input: $f : \{0,1\}^n \to \{0,1\}$ either constant or balanced
- Output: 0 iff f is constant
- Constraint: f is a black-box
- Query complexity:
  - deterministic $1 + 2^{n-1}$
  - quantum 1
- $n = 1$: decide whether $f(0) = f(1)$ or not $\Rightarrow$ 2 queries ?

Quantum algorithm for $n = 1$

- Implementing f

$$|b\rangle \to \boxed{\mathbf{P}_f} \to (-1)^{f(b)}\,|b\rangle$$

- Hadamard gate

$$|b\rangle \to \boxed{\mathbf{H}} \to \frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^b\,|1\rangle\Big)$$

- Quantum circuit

$$|0\rangle \to \boxed{\mathbf{H}} \to \boxed{\mathbf{P}_f} \to \boxed{\mathbf{H}} \to \boxed{\text{meas.}} \to$$

Analysis

- Initialization: $|0\rangle$
- Parallelization: $\frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$
- Calling f : $\frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)$
- Interference: $\frac{1}{2}\Big\{(-1)^{f(0)}\left(|0\rangle + |1\rangle\right) + (-1)^{f(1)}\left(|0\rangle - |1\rangle\right)\Big\}$

Why does this work ?

$$\frac{1}{2}\left\{(-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)\right\}$$

$$=$$

$$\frac{1}{2}\left\{\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right\}$$

$$=$$

$$\begin{cases} \pm|0\rangle & f \text{ constant} \\ \pm|1\rangle & f \text{ balanced} \end{cases}$$

Register of n qubits

- a qubit $\psi \in \mathbb{C}^2$ with $\langle\psi|\psi\rangle = ||\,|\psi\rangle\,||^2 = 1$

$$|\psi\rangle = \sum_{x\in\{0,1\}} \alpha_x |x\rangle$$

- A register of n qubits $|\psi\rangle \in \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}}$

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \quad \text{with} \quad \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$$

- Notation:

$$|b_1 \cdots b_n\rangle \stackrel{\text{def}}{=} |b_1\rangle \otimes \cdots \otimes |b_n\rangle$$

- Example:

$$\begin{aligned} |00\rangle + |10\rangle &= (|0\rangle + |1\rangle) \otimes |0\rangle \\ \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &\neq |\psi_1\rangle \otimes |\psi_2\rangle \text{ for any qubit } \psi_i \end{aligned}$$

Unitary evolution

$$|\psi\rangle \to \mathbf{P}\,|\psi\rangle$$

where $\mathbf{P} \in \mathbb{C}^{2^n \times 2^n}$ is such that

$$\mathbf{P}^*\mathbf{P} = \mathbf{Id}_{2^n}$$

The bra-ket notation

- $$\langle\phi|\psi\rangle \stackrel{\text{def}}{=} \sum_{x\in\{0,1\}^n} \overline{\alpha_x}\beta_x$$
  where $|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$ and $|\psi\rangle = \sum_{x\in\{0,1\}^n} \beta_x |x\rangle$
- The $|\phi\rangle\langle\psi|$ operator

$$\begin{aligned} |\phi\rangle\langle\psi| : \mathbb{C}^2)^{\otimes n} &\rightarrow (\mathbb{C}^2)^{\otimes n} \\ |\psi'\rangle &\mapsto |\phi\rangle\langle\psi|\,|\psi'\rangle = \langle\psi|\psi'\rangle\,|\phi\rangle \end{aligned}$$

Exercise

1. What is the operator $\sum_{x\in\{0,1\}^n} |x\rangle\langle x|$?
2. Consider a matrix $\mathbf{P} = (P_{xy})_{\substack{x\in\{0,1\}^{2^n} \\ y\in\{0,1\}^{2^n}}} \in \mathbb{C}^{2^n\times 2^n}$. Express $\mathbf{P}$ in terms of the $|x\rangle\langle y|$.
3. Let $\mathbf{P}_0 \stackrel{\text{def}}{=} \sum_{x:x_i=0} |x\rangle\langle x|$ and $\mathbf{P}_1 \stackrel{\text{def}}{=} \sum_{x:x_i=1} |x\rangle\langle x|$. What can you say about P_0 and P_1 ?

Measurement of the i-th qubit

$$\begin{aligned}
V_0 &\stackrel{\text{def}}{=} < |x\rangle : x_i = 0 > \\
V_1 &\stackrel{\text{def}}{=} < |x\rangle : x_i = 1 > \\
\mathbf{P}_0 &\stackrel{\text{def}}{=} \sum_{x:x_i=0} |x\rangle \langle x| \\
&= \text{orthogonal projector onto } V_0 \\
\mathbf{P}_1 &\stackrel{\text{def}}{=} \sum_{x:x_i=1} |x\rangle \langle x| \\
&= \text{orthogonal projector onto } V_1
\end{aligned}$$

measuring the i-th qubit:

$$|\psi\rangle \rightarrow \boxed{\text{meas. qubit } i} \rightarrow \begin{cases} \frac{1}{||\mathbf{P}_0|\psi\rangle||}\mathbf{P}_0 |\psi\rangle & \text{with prob.}||\mathbf{P}_0 |\psi\rangle\, ||^2 \\ \frac{1}{||\mathbf{P}_1|\psi\rangle||}\mathbf{P}_1 |\psi\rangle & \text{with prob.}||\mathbf{P}_1 |\psi\rangle\, ||^2 \end{cases}$$

Measuring the first k qubits

Based on the projectors

$$P_a = \sum_{x \in \{0,1\}^n : x_1 \cdots x_k = a} |x\rangle \, |x\rangle$$

$$|\psi\rangle \rightarrow \boxed{\text{meas. the first } k \text{ qubit s}} \rightarrow \frac{1}{||\mathbf{P}_a \, |\psi\rangle \, ||} \mathbf{P}_a \, |\psi\rangle \text{ with prob.} ||\mathbf{P}_a \, |\psi\rangle \, ||^2$$

The c-NOT gate

$$
\begin{aligned}
\text{c-NOT}\,|0b\rangle &= |0b\rangle \\
\text{c-NOT}\,|1b\rangle &= \left|1\bar{b}\right\rangle \\
\text{c-NOT}\,|ab\rangle &= |a\rangle\,|a \oplus b\rangle \\
\text{c-NOT} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}
\end{aligned}
$$

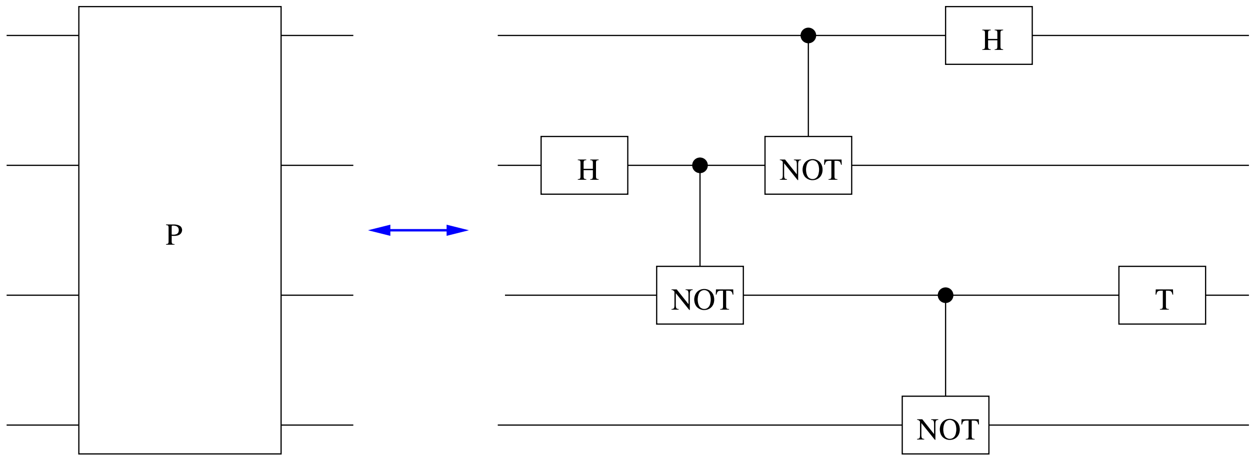
Generalization

$$
\begin{aligned}
\text{c-}\mathbf{P}\,|0b\rangle &= |0b\rangle \\
\text{c-}\mathbf{P}\,|1b\rangle &= |1\rangle\,\mathbf{P}\,|b\rangle
\end{aligned}
$$

Tensor product

$$
\begin{aligned}
\mathbf{P}_1 : (\mathbb{C}^2)^{\otimes m} &\quad\rightarrow\quad (\mathbb{C}^2)^{\otimes m} \\
\mathbf{P}_2 : (\mathbb{C}^2)^{\otimes n} &\quad\rightarrow\quad (\mathbb{C}^2)^{\otimes n} \\
\mathbf{P}_1 \otimes \mathbf{P}_2 : (\mathbb{C}^2)^{\otimes (m+n)} &\quad\rightarrow\quad (\mathbb{C}^2)^{\otimes (m+n)} \\
|\psi_1\rangle \otimes |\psi_2\rangle &\quad\mapsto\quad \mathbf{P}_1 |\psi_1\rangle \otimes \mathbf{P}_2 |\psi_2\rangle
\end{aligned}
$$

Quantum circuit



Theorem 2. *There exists a finite universal set of* 1 *and* $2-$*qubit gates*

Exercise : no cloning

Is there a quantum circuit $\mathbf{C}$ on 2 qubits such that

$$\mathbf{G}\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$$

for every $\psi \in \mathbb{C}^2$?

Exercise : circuit for producing Bell states

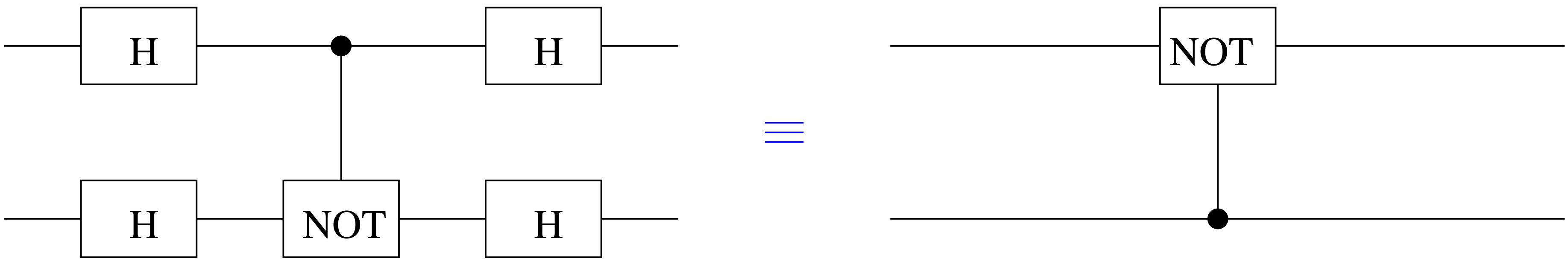
Consider the following Bell states

$$\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\
|\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)
\end{aligned}$$

1. What can you say about these states ?
2. Give a quantum circuit that maps $|ab\rangle$ to $|\beta_{ab}\rangle$ for $a, b \in \{0, 1\}$.

Exercise

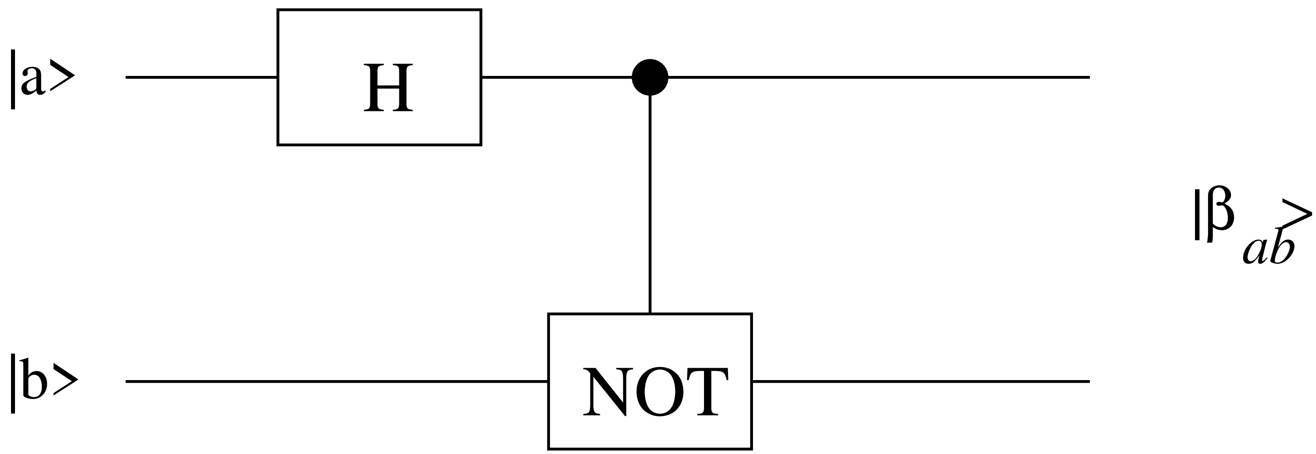
1. Show that



2. Propose a swap-gate that is based on c-NOT gates

Superdense Coding

- Transmitting 2 classical bits by sending only one qubit when Alice and Bob share an EPR pair $|\beta_{00}\rangle$
- Bell change of basis

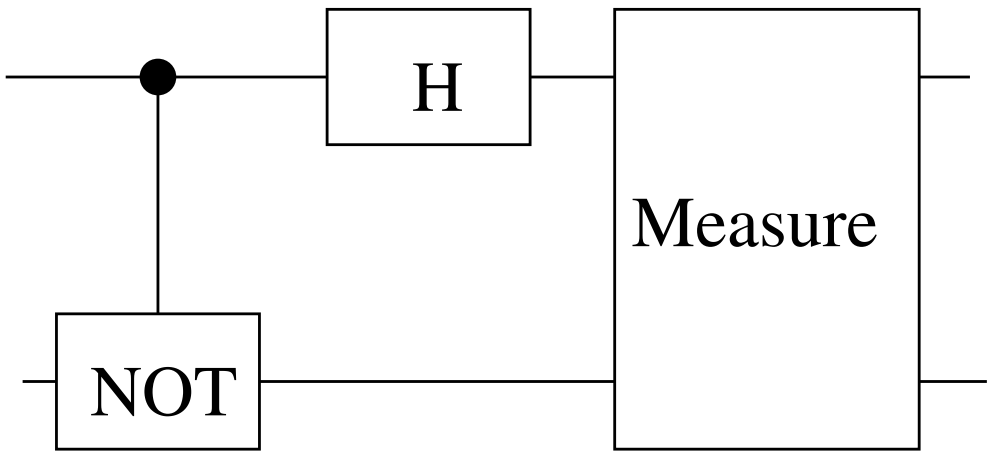


$$|\beta_{00}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\beta_{01}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$|\beta_{10}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\beta_{11}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Exercise : Bell measurement

1. What is c-NOT* ?
2. What is $\mathbf{H}^*$?
3. What is the effect of the following circuit on the Bell state $|\beta_{ab}\rangle$?



Superdense Coding (II)

- Alice and Bob share an EPR pair $|\beta_{00}\rangle$
- Alice wants to send to Bob two bits a and b
- Alice performs on her qubit the transformation $\mathbf{Z}^a\mathsf{NOT}^b$ where

$$\mathbf{Z}\,|b\rangle = (-1)^b\,|b\rangle$$

- Alice sends her qubit to Bob
- Bob performs a Bell measurement and recovers a and b

$$1 \text{ qubit } = 2 \text{ bits}$$

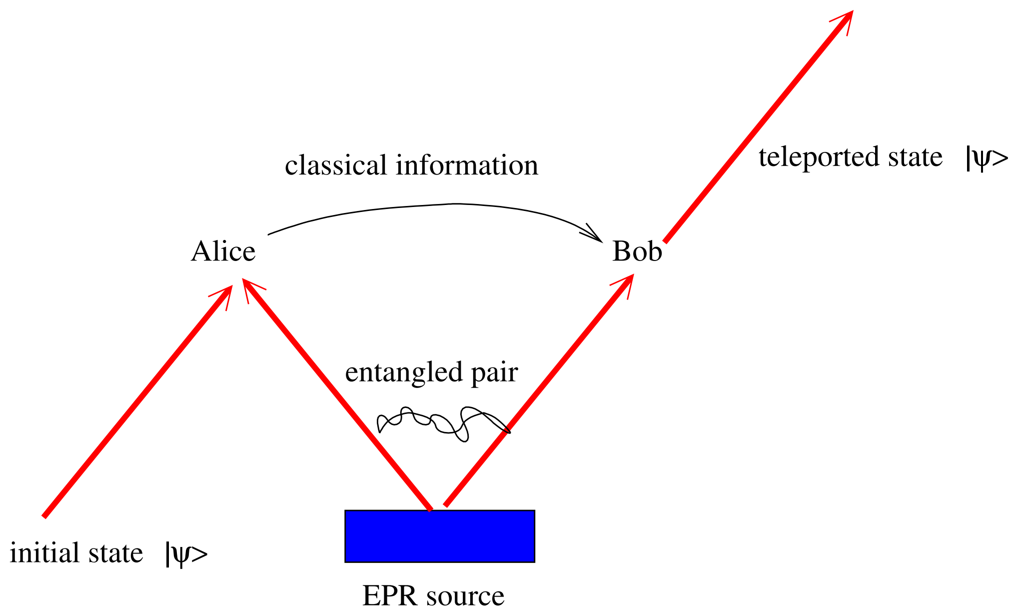
Why it works

$$
\begin{aligned}
|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad & \xrightarrow{00} \quad |\beta_{00}\rangle \\
& \xrightarrow{01} \quad \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\beta_{01}\rangle \\
& \xrightarrow{10} \quad \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\beta_{10}\rangle \\
& \xrightarrow{11} \quad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\beta_{11}\rangle
\end{aligned}
$$

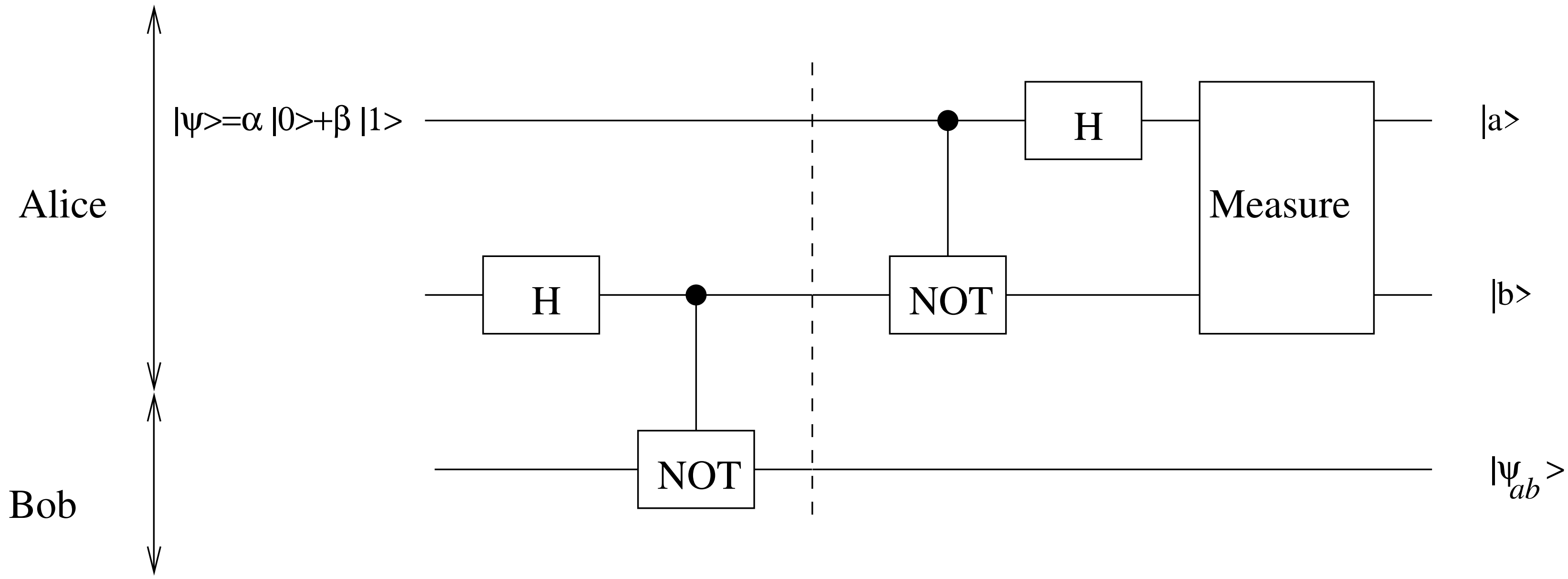
Quantum teleportation

Problem:

- Alice wants to send a qubit $|\psi\rangle$ to Bob
- Bob far away from Alice
- classical communication is possible
- they share the Bell state $|\phi^+\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, Alice holds the first qubit whereas Bob holds the second qubit.



The circuit



Exercise

Explain how this works

Analysis

$$
\begin{aligned}
|\psi\rangle\,|0\rangle\,|0\rangle \quad &\rightarrow \quad \frac{1}{\sqrt{2}}\left(\alpha\,|0\rangle + \beta\,|1\rangle\right)\left(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle\right) \\
&= \quad \frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|100\rangle + \beta\,|111\rangle\right) \\
&\rightarrow \quad \frac{1}{\sqrt{2}}\left(\alpha\,|000\rangle + \alpha\,|011\rangle + \beta\,|110\rangle + \beta\,|101\rangle\right) \\
&\rightarrow \quad \frac{1}{2}\left(\alpha\,|000\rangle + \alpha\,|100\rangle + \alpha\,|011\rangle + \alpha\,|111\rangle\right. \\
&\qquad \left. +\beta\,|010\rangle - \beta\,|110\rangle + \beta\,|001\rangle - \beta\,|101\rangle\right) \\
&= \quad \frac{1}{2}\,|00\rangle\left(\alpha\,|0\rangle + \beta\,|1\rangle\right) + \frac{1}{2}\,|01\rangle\left(\alpha\,|1\rangle + \beta\,|0\rangle\right) + \\
&\qquad \frac{1}{2}\,|10\rangle\left(\alpha\,|0\rangle - \beta\,|1\rangle\right) + \frac{1}{2}\,|11\rangle\left(\alpha\,|1\rangle - \beta\,|0\rangle\right)
\end{aligned}
$$

Another explanation

$$
\begin{aligned}
\frac{1}{\sqrt{2}} (\alpha |0\rangle + \beta |1\rangle) (|0\rangle |0\rangle + |1\rangle |1\rangle) \quad = \quad & \frac{1}{2} |\beta_{00}\rangle (\alpha |0\rangle + \beta |1\rangle) \\
& + \frac{1}{2} |\beta_{01}\rangle (\alpha |1\rangle + \beta |0\rangle) \\
& + \frac{1}{2} |\beta_{10}\rangle (\alpha |0\rangle - \beta |1\rangle) \\
& + \frac{1}{2} |\beta_{11}\rangle (\alpha |1\rangle - \beta |0\rangle)
\end{aligned}
$$

The Deutsch-Josza problem

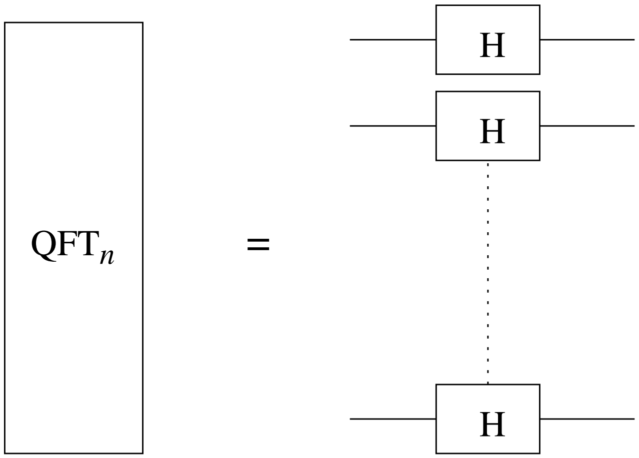
- Input: $f : \{0,1\}^n \to \{0,1\}$ either constant or balanced
- Output: 0 iff f is constant
- Constraint: f is a black-box
- Query complexity:
  - deterministic $1 + 2^{n-1}$
  - quantum 1

The Deutsch-Josza algorithm

Implementing f quantumly

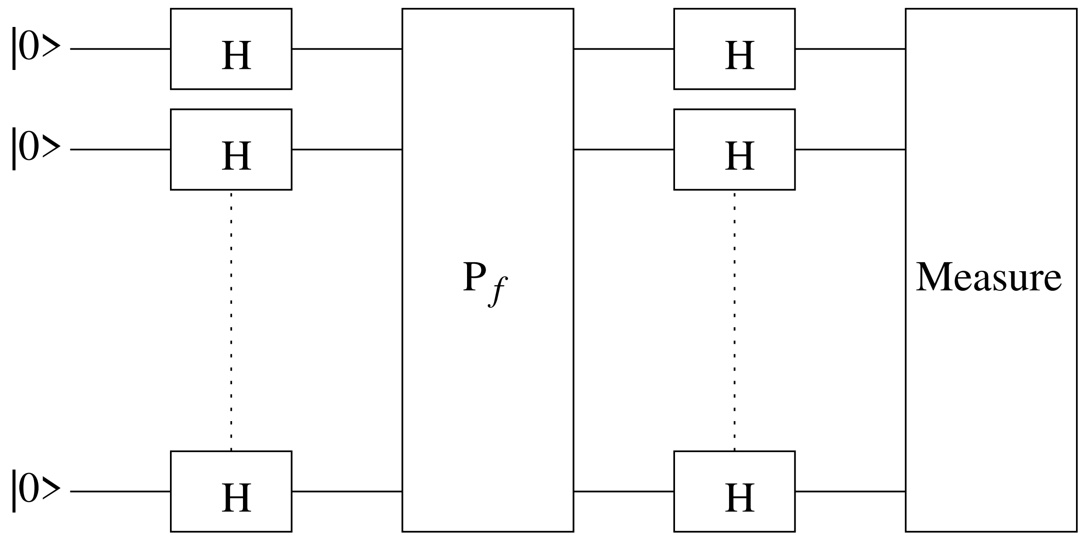
$$|x\rangle \xrightarrow{\mathbf{P}_f} (-1)^{f(x)}\,|x\rangle$$

Quantum Fourier Transform



Exercise

1. Give a formula for $\mathsf{QFT}_n \left| x \right\rangle$
2. Show that the following circuit answers the problem



The Bernstein-Vazirani problem

- Input: $f : \{0,1\}^n \to \{0,1\}$ where $f(x) = a \cdot x$ for some $a \in \{0,1\}^n$
- Output: a

Exercise

1. Give a quantum circuit that solves this problem by querying f only once
2. Give the classical query complexity for this problem

The reason of the quantum advantage

- Intrication but classical intrication (correlation) is also possible. However quantum intrication is much stronger (EPR paradox, violation of Bell inequalities)
- complex amplitudes ? No, because we can replace a qubit by two qubits with real amplitudes
- interference (negative numbers)