Quantum Computing

I. Introduction and Quantum Cryptography

Frédéric Magniez

Introduction and Quantum algorithms
Monday afternoon: FM and Christoph Dürr
Tuesday morning: FM and Christoph Dürr

Quantum lower bounds
Thursday morning: Sophie Laplante (x2)

Quantum communication
Friday morning: Harry Buhrman (x2)
End of Moore’s Law?

"No exponential is forever. Your job is to delay forever.", Andrew Gordon Moore Feb. 2003.

The size of transistors is decreasing rapidly, around 2020 they will be of atomic size.

Quantum interferences around 2020...

- Today approach: avoid them
- Quantum computing: use them!
The superiority of quantum computing

Cryptography
- Key distribution protocol [Bennett-Brassard 1984]
  Implementation: ~100 km

Quantum information
- Teleportation [Bennett-Brassard-Crépeau-Jozsa-Peres-Wootters 1993]
  Realization: 1997 [Innsbruck]

Algorithms
- Period finding [Simon, Shor 1994] $\Rightarrow$ Factorization, discrete log...
- (unstructured) Database search [Grover 1996]

Size of quantum computers (in # of bits):
  1995: 2 [ENS], 1998: 3,
  2000: 5 [IBM] - 7 [Los Alamos]
  2001: 8 [IBM]
  2005: ~12 [IQC]
Quantum algorithms without quantum computers?

Background
- Turing machine, calculability, universality: [Turing 1936]
- Proposition: EDVAC (Electronic Discrete Variable Computer) [von Neumann 1945]
- First computer: Mark I [Robinson-Tootill-Williams 1949]

Quantum computing
- Idea: simulation of quantum systems [Feynman 1982]
- Models:
  - Turing machine: [Deutsch 1985, 1989], [Bernstein-Vazirani 1993]
  - Quantum circuits: [Yao 1993]
  - Cellular automata, finite automata...
- Technology:
  - First gate: 2 bits [ENS (Haroche) 1995]
  - First circuit: 5 bits [IBM (Chuang) 2000]
Deterministic bit

- State = element \( b \in \{0, 1\} \)
- Evolution = \( G : \{0, 1\} \rightarrow \{0, 1\} \)

\[ b \xrightarrow{[G]} b' = G(b) \]

Random bit

- State = Random distribution: \( d = \begin{pmatrix} p \\ q \end{pmatrix} \) \( p, q \in [0, 1] \) \( p + q = 1 \)
- Evolution = Stochastic matrix: \( G \in \mathbb{R}_{+}^{2 \times 2} \) \( \sum_j G_{ij} = 1 \)

\[ b \xrightarrow{[G]} b' \text{ with probability } G_{b'b} \]

\[ d \xrightarrow{[G]} d' = G d \]

- Examples
  
  Perfect coin: \( d = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \end{pmatrix} \)

  Identity: \( I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \)

  Negation: \( \text{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \)

  Coin flipping: \( \text{Flip} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \)
**Quantum bit (qubit)**

- **State** = quantum superposition: 2-dimensional l2-unit vector

  \[
  |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1
  \]

  \[
  |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \alpha = \langle 0|\psi \rangle \quad \beta = \langle 1|\psi \rangle
  \]

- **Measure** = randomized orthogonal projection

  \[
  \alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{Measure}} |\alpha|^2 |0\rangle + |\beta|^2 |1\rangle
  \]

- **Evolution** = unitary transformation \( G \in U(2) : G \in \mathbb{C}^{2 \times 2} \) \( G^*G = \text{Id} \)

  **Gate notation**

  \[
  |\psi\rangle \xrightarrow{G} |\psi'\rangle = G|\psi\rangle
  \]

  **Reversibility**

  \[
  |\psi'\rangle = G'|\psi\rangle \xrightarrow{G^*} |\psi\rangle
  \]
Examples of gates

Classical reversible gates
- Identity
  \[ |b\rangle \xrightarrow{I_2} |b\rangle \]
- Negation
  \[ |b\rangle \xrightarrow{\text{NOT}} |1 - b\rangle \]

Hadamard gate
- Definition:
  \[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \]
  \[ |b\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle) \]
- Properties: quantum coin flipping
  \[ |0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \]
  Measure
  \[ \frac{1}{2} |0\rangle \xrightarrow{\text{Measure}} \frac{1}{2} |1\rangle \]

\[ |b\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle) \]
  Measure
  \[ \frac{1}{2} |0\rangle \xrightarrow{\text{Measure}} \frac{1}{2} |1\rangle \]
Implementing qubits using photons
Implementing qubits using photons

**Characteristics**
- direction
- wavelength: color
- polarisation
Properties of the exiting light of a filter

- Light polarized as filter direction.
- Parallel light goes through the filter
- Orthogonal light cannot go through the filter

Diagonal polarization

- Randomized behavior
- Is it a random polarisation? NO
- This is a quantum superposition!
Properties of the exiting light of a filter

- Light polarized as filter direction.
- Parallel light goes through the filter
- Orthogonal light cannot go through the filter

Diagonal polarization

- Randomized behavior
- Is it a random polarisation? NO
- This is a quantum superposition!
Properties of the exiting light of a filter

- Light polarized as filter direction.
- Parallel light goes through the filter.
- Orthogonal light cannot go through the filter.

Diagonal polarization

- Randomized behavior
- Is it a random polarisation? NO
- This is a quantum superposition!
Properties of the exiting light of a filter

- Light polarized as filter direction.
- Parallel light goes through the filter
- Orthogonal light cannot go through the filter

Diagonal polarization

- Randomized behavior
- Is it a random polarisation? NO
- This is a quantum superposition!
Quantum superposition

Polarization state
- superposition: 2-dimensional vector
  \[ |\theta \rangle = \cos \theta |\rightarrow \rangle + \sin \theta |\uparrow \rangle \]
  \[ |0 \rangle = |\rightarrow \rangle \text{ and } |1 \rangle = |\uparrow \rangle \]

Filter
- measure: randomized orthogonal projection

Half-wave blade
- orthogonal symmetry with respect to his axis
- Hadamard gate: half-wave blade at \( \pi/8 \):
  \[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \]
- Two blades generate any orthogonal map \( G \in \mathcal{O}(2) \)
  \[ G \in \mathbb{R}^{2 \times 2} \text{ such that } tGG = \text{Id} \]
Problem

- Initially: no secret information between Alice and Bob
- End of protocol: a **private key** only known by Alice and Bob

**What is known classically**

- Impossible task, since all the information is on the channel
- What is **possible** using randomized protocols:
  - Amplify a secret by reducing the key
  - Identify a message using a key of same size

**Measure incertitude**

**No cloning**

- There is no way of cloning a quantum state
- Proof: later
Encryption using private key

One-time pad

Message: 0 1 1 0 0 1 0 1 1 1 0
Private key: 1 1 0 1 0 0 1 0 1 0 0

XOR mask: 1 0 1 1 0 1 1 1 0 1 0

- Theorem: perfect security if each bit of the key is used only once!
- For perfect security, one needs a key as long as the message...

DES

- More clever scheme using several time a same and smaller key
- No security proof
- In practice, quite sure if the key is not used too much...
- Usually, the private key is generated from RSA protocol or Diffie-Hellman protocol
Protocol: classical part

- **Reveal**: Alice and Bob reveal publicly their basis choices A&B only keep the bits with same basis choices (probability 1/2)

- **Privacy**: A&B checks few bits at random positions

- **Secret amplification + (identification) using few bits at random positions**

**Conclusion**

- **Private key generation without any prior secret (but no authentication)**

- **Small initial private key**

---

**Quantum protocol for key distribution** [Bennett-Brassard 84]

**Protocol: quantum part**

<table>
<thead>
<tr>
<th>Key</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photons:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basis:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photons:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Key: 1 1 0 0 1 1 0 1 0 1 0
Quantum protocol for key distribution [Bennett-Brassard 84]

Protocol: quantum part

<table>
<thead>
<tr>
<th>Key:</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Photons:|     |     |     |     |     |     |     |     |     |     |     |

| Basis:|   |   |   |   |   |   |   |   |   |   |   |

| Photons:|     |     |     |     |     |     |     |     |     |     |     |

| Key:   | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |

Protocol: classical part

- **Reveal**: Alice and Bob reveal publicly their basis choices
  
  A&B only keep the bits with same basis choices (probability 1/2)
  
  No observation of the communication $\rightarrow$ A&B have the same key!

- **Privacy**: A&B checks few bits at random positions

- Secret amplification + (identification) using few bits at random positions
Protocol: classical part
- **Reveal**: Alice and Bob reveal publicly their basis choices
  - A&B only keep the bits with same basis choices (probability 1/2)
  - No observation of the communication $\implies$ A&B have the same key!
- **Privacy**: A&B checks few bits at random positions
- **Secret amplification + (identification)** using few bits at random positions

Conclusion
- Private key generation without any prior secret (but no authentication)
- Small initial private key $\implies$ large private key with authentication

Quantum protocol for key distribution [Bennett-Brassard 84]

**Protocol: quantum part**

<table>
<thead>
<tr>
<th>Key</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basis:</td>
<td>[Diagram of basis choices]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photons:</td>
<td>[Diagram of photons]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basis:</td>
<td>[Diagram of basis choices]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photons:</td>
<td>[Diagram of photons]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key:</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Analysis of a first attack (for one photon)

Strategy I
- Eve observes the photon in some chosen basis
- Eve sends a new photon of same observed polarization

Analysis (assuming the bit is selected for the key)
- With prob. \( p = 50\% \), Eve guesses a wrong basis
- Then with prob. \( p \), Eve observes a wrong bit
- And with prob. \( p \), Bob observes the same bit than Eve

Conclusion
- Eve learns correctly the bit with prob \( p + p \times p = 75\% \)
- Eve is detected with probability \( p \times p = 25\% \)
Analysis of a second attack (for one photon)

**Strategy II**
- Same as Strategy I, but always with the same basis \((\pi/8, 5\pi/8)\)

**Analysis (assuming the bit is selected for the key)**
- With prob. \(p = \cos^2(\pi/8)\), Eve observes the same bit
- With prob. \(p\), Bob observes the same bit than Eve

**Conclusion**
- Eve learn correctly the bit with prob. \(p = 85\%\)
- Eve is detected with prob. \(2 \times p(1 - p) = 25\%\)

**Theorem [2000]**
- The key distribution quantum protocol is unconditionally secure even on a noisy channel (provided the laws of Quantum Mechanic are correct)
Definition
- $|\psi\rangle \in \mathbb{C}^{\{0,1\}^n}$ such that $||\psi|| = 1$

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

where

$\sum_{x \in \{0,1\}^n} |\alpha_x|^2 = 1$

$\mathbb{C}^{\{0,1\}^2} = \mathbb{C}^{\{0,1\}} \otimes \mathbb{C}^{\{0,1\}} \neq \mathbb{C}^{\{0,1\}} \times \mathbb{C}^{\{0,1\}}$

Example:
- $|00\rangle + |01\rangle = |0\rangle \otimes (|0\rangle + |1\rangle)$
- $|00\rangle + |11\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$

Evolution: unitary transformation $G \in \mathcal{U}(2^n)$

$G \in \mathbb{C}^{2^n \times 2^n}$ s.t. $G^*G = \text{Id}$

Measure

$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \rightarrow $ Measure $|\alpha_x|^2 |x\rangle$
Definition
- Let $A$ (resp. $B$) be the set of $m_A$-bit strings (resp. $m_B$-bit strings).
- Let $H_A = \mathbb{C}^A$ and $H_B = \mathbb{C}^B$ be the corresponding Hilbert spaces.
- Then $H = H_A \otimes H_B = \mathbb{C}^{A \times B}$ is a bipartite system.

Notation

$|w_A w_B\rangle = |w_A\rangle \otimes |w_B\rangle = |w_A\rangle |w_B\rangle$ when $w_A \in A$, $w_B \in B$

Partial measurement over $A$ (resp. $B$)
- Define the partial inner product $\langle w_A | \psi \rangle = \sum_{w_B} \langle w_A w_B | \psi \rangle |w_B\rangle$
- Then the partial measurement over $A$ is

$$|\psi\rangle \xrightarrow{\text{Measure } A} \frac{\| \langle w_A | \psi \rangle \|^2}{\| \langle w_A | \psi \rangle \|} |w_A\rangle \langle w_A | \psi \rangle$$

Example

$\frac{1}{2} (|00\rangle + |01\rangle - |10\rangle + |11\rangle) \xrightarrow{\text{Measure } A}  \frac{1}{\sqrt{2}} |0\rangle (\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle))$

$= \frac{1}{\sqrt{2}} |1\rangle (\frac{1}{\sqrt{2}} (-|0\rangle + |1\rangle))$
Theorem
- Let $A$ and $B$ be the set of $n$-bit strings.
- Then there is no unitary transformation $U$ such that

$$\forall |\psi\rangle \in H_A, \quad U |\psi\rangle |0^n\rangle = |\psi\rangle |\psi\rangle$$

Proof for $n=1$
- Idea: compute $U \left( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\rangle \right)$ by 2 different ways
- By hypothesis

$$U \left( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\rangle \right) = \frac{1}{2} (|0\rangle + |1\rangle) (|0\rangle + |1\rangle) = \frac{1}{2} (|0\rangle |0\rangle + |0\rangle |1\rangle + |1\rangle |0\rangle + |1\rangle |1\rangle)$$

- By linearity of $U$

$$U \left( \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\rangle \right) = \frac{1}{\sqrt{2}} (U |0\rangle |0\rangle + U |1\rangle |0\rangle) = \frac{1}{\sqrt{2}} (|0\rangle |0\rangle + |1\rangle |1\rangle)$$

- Contradiction!
EPR paradox: Computer scientist approach

Game

- Alice and Bob may share some initial information but cannot communicate
- Alice, resp. Bob, gets a random bit $x$, resp. $y$
- Alice, resp. Bob, returns a bit $a$, resp. $b$
- **Goal**: maximize $p = \Pr_{x,y}(a \oplus b = x \land y)$

Classically

- Best deterministic strategy: $a = b = 0 \implies p = \frac{3}{4}$
- Proof
  4 cases for $(x,y)$, therefore $p > \frac{3}{4} \implies p = 1$
  Observe that $(x, y) \neq (1, 1) \iff x \land y = 0$
  $a \oplus b = 0 \iff a = b$

Therefore, A outputs the same bit than B for cases $(0,0), (1,0)$ and $(0,1)$
That is A and B always outputs the same bit $c$ for any cases!
Problem for case $(1,1)$ since $c \oplus c = 0 \neq 1 = 1 \land 1$
**EPR paradox: Computer scientist approach**

**Game**
- Alice and Bob may share some initial information but cannot communicate
- Alice, resp. Bob, gets a random bit $x$, resp. $y$  
- Alice, resp. Bob, returns a bit $a$, resp. $b$
- **Goal**: maximize $p = \Pr_{(x,y)}(a \oplus b = x \land y)$

**Classically**
- Best deterministic strategy: $a = b = 0 \implies p = \frac{3}{4}$
- Proof
  - 4 cases for $(x,y)$, therefore $p > \frac{3}{4} \implies p = 1$
  - Observe that $(x, y) \neq (1, 1) \iff x \land y = 0$
    - $a \oplus b = 0 \iff a = b$
  - Therefore, A outputs the same bit than B for cases $(0,0), (1,0)$ and $(0,1)$
  - That is A and B always outputs the same bit $c$ for any cases!
  - Problem for case $(1,1)$ since $c \oplus c = 0 \neq 1 = 1 \land 1$
- **Theorem**: The best random strategy is not better than the best deterministic strategy
  - Proof: a random strategy is nothing else than a random choice followed by a deterministic strategy!
**Game**
- Alice and Bob may share some initial information but cannot communicate
- Alice, resp. Bob, gets a random bit \( x \), resp. \( y \)
- Alice, resp. Bob, returns a bit \( a \), resp. \( b \)
- **Goal**: maximize \( p = \Pr_{x,y}(a \oplus b = x \land y) \)

**Quantumly**
- Alice and Bob shares an EPR pair \( \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \)
- If \( x = 1 \), Alice rotates its qubit by \( \pi/8 \)
- If \( y = 1 \), Bob rotates its qubit by \( -\pi/8 \)
- Alice and Bob observe their qubit and send their outcome
- **Theorem** \( p = \frac{5+\sqrt{2}}{8} \approx 0.8 \)
- **Proof:**
**EPR paradox: Computer scientist approach**

**Game**
- Alice and Bob may share some initial information but cannot communicate
- Alice, resp. Bob, gets a random bit \( x \), resp. \( y \)
- Alice, resp. Bob, returns a bit \( a \), resp. \( b \)
- **Goal**: maximize \( p = \Pr_{x,y}(a \oplus b = x \land y) \)

**Quantumly**
- Alice and Bob shares an EPR pair \( \frac{1}{\sqrt{2}}(|00⟩ + |11⟩) \)
- If \( x = 1 \), Alice rotates its qubit by \( \pi/8 \)
- If \( y = 1 \), Bob rotates its qubit by \( -\pi/8 \)
- Alice and Bob observe their qubit and send their outcome
- **Theorem** \( p = \frac{5+\sqrt{2}}{8} \approx 0.8 \)
- **Proof**: \( x = y = 0 \)
  Alice observes 0 with prob. \( 1/2 \), then Bob always observes the same bit!

\[
\frac{1}{\sqrt{2}}(|00⟩ + |11⟩) \quad \text{Measure A} \quad \frac{1}{2} |0⟩|0⟩
\]
\[
\frac{1}{2} |1⟩|1⟩
\]

\( p_{00} = 1 \)
Game
- Alice and Bob may share some initial information but cannot communicate
- Alice, resp. Bob, gets a random bit \( x \), resp. \( y \)
- Alice, resp. Bob, returns a bit \( a \), resp. \( b \)
- Goal: maximize \( p = \Pr(x \oplus y = x \land y) \)

Quantumly
- Alice and Bob shares an EPR pair \( \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \)
- If \( x = 1 \), Alice rotates its qubit by \( \pi/8 \)
- If \( y = 1 \), Bob rotates its qubit by \(-\pi/8 \)
- Alice and Bob observe their qubit and send their outcome
- Theorem: \( p = \frac{5+\sqrt{2}}{8} \approx 0.8 \)
- Proof: \( x = 0, y = 1 \)

If Alice observes 0, then Bob gets 0 with prob. \( \cos^2(\pi/8) = 0.85 \)
If Alice observes 1, then Bob gets 1 with prob. \( \cos^2(\pi/8) = 0.85 \)
\[ p_{01} = 0.85 (= p_{10}) \]
**Game**
- Alice and Bob may share some initial information but cannot communicate
- Alice, resp. Bob, gets a random bit $x$, resp. $y$
- Alice, resp. Bob, returns a bit $a$, resp. $b$
- **Goal**: maximize $p = \Pr(a \oplus b = x \land y)$

**Quantumly**
- Alice and Bob shares an EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- If $x = 1$, Alice rotates its qubit by $\pi/8$
- If $y = 1$, Bob rotates its qubit by $-\pi/8$
- Alice and Bob observe their qubit and send their outcome
- **Theorem** $p = \frac{5 + \sqrt{2}}{8} \approx 0.8$
- **Proof**: $x = y = 1$ The state before the measure is now:

$$\frac{1}{\sqrt{2}}((c|0\rangle + s|1\rangle)(c|0\rangle - s|1\rangle) + (-s|0\rangle + c|1\rangle)(s|0\rangle + c|1\rangle))$$

$$= \frac{1}{\sqrt{2}}(-2cs|01\rangle + 2cs|10\rangle + \ldots)$$

$$p_{11} = 4(cs)^2 = 0.5$$

EPR paradox: Computer scientist approach
Game
- Alice and Bob may share some initial information but cannot communicate
- Alice, resp. Bob, gets a random bit $x$, resp. $y$
- Alice, resp. Bob, returns a bit $a$, resp. $b$
- Goal: maximize $p = \Pr_x(a \oplus b = x \land y)$

Quantumly
- Alice and Bob shares an EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- If $x = 1$, Alice rotates its qubit by $\frac{\pi}{8}$
- If $y = 1$, Bob rotates its qubit by $-\frac{\pi}{8}$
- Alice and Bob observe their qubit and send their outcome
- Theorem $p = \frac{5+\sqrt{2}}{8} \approx 0.8$
- Proof:

Conclusion: $p = \frac{1}{4}(1 + 0.85 + 0.85 + 0.5) = 0.8$
The gate \( c\text{-NOT} \)

**Definition**

\[
\begin{align*}
c\text{-NOT}|0b\rangle &= |0b\rangle \\
c\text{-NOT}|1b\rangle &= |1\rangle|(1 - b)\rangle \\
c\text{-NOT}|ab\rangle &= |a\rangle|a \oplus b\rangle
\end{align*}
\]

\[
c\text{-NOT} = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix}
\]

**Representation**

- **control bit**
- **action bit**

**Generalization**

\[
\begin{align*}
c\text{-}G|0b\rangle &= |0b\rangle \\
c\text{-}G|1b\rangle &= |1\rangle G|b\rangle
\end{align*}
\]
Application of Bell states

Bell states construction

\[ |x\rangle \xrightarrow{H} |\beta_{xy}\rangle \]
\[ |y\rangle \xrightarrow{\text{NOT}} |\beta_{xy}\rangle \]

\[ |\beta_{00}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \]
\[ |\beta_{01}\rangle = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \]
\[ |\beta_{10}\rangle = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \]
\[ |\beta_{11}\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle) \]

Superdense coding

- Alice and Bob share an EPR state \( |\beta_{00}\rangle \)
- Alice wants to send \( x, y \) to Bob
- Alice performs on its qubit the transformation \( \text{NOT}^y \times \text{FLIP}^x \)
- Alice sends its qubit to Bob
- Bob performs a Bell measurement and reads \( x, y \)
- \textbf{Conclusion} \,: 1-qubit = 2 bits!
Problem
- Alice wants to send a qubit $|\psi\rangle$ to Bob
- Bob is in faraway and unknown position
- One-way classical communication (radio) is possible: Alice $\rightarrow$ Bob

Quantum teleportation

Teleportation

The classical communication reveals no information about $|\psi\rangle$!
Implementation of teleportation

Circuit

\[ |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \]

\[ |0\rangle \rightarrow H \rightarrow \text{NOT} \rightarrow |x\rangle \]

\[ |0\rangle \rightarrow \text{NOT} \rightarrow |y\rangle \]

Analyze

\[ |\psi\rangle|0\rangle|0\rangle \rightarrow \frac{1}{\sqrt{2}} (\alpha|0\rangle + \beta|1\rangle)(|0\rangle|0\rangle + |1\rangle|1\rangle) \]

\[ = \frac{1}{2} |\beta_{00}\rangle (\alpha|0\rangle + \beta|1\rangle) \]

\[ + \frac{1}{2} |\beta_{01}\rangle (\alpha|1\rangle + \beta|0\rangle) \]

\[ + \frac{1}{2} |\beta_{10}\rangle (\alpha|0\rangle - \beta|1\rangle) \]

\[ + \frac{1}{2} |\beta_{11}\rangle (\alpha|1\rangle - \beta|0\rangle) \]

End of protocol

- Bob “correct” its qubit depending of received bits \( x, y \)
Quantum Computing
2. Quantum Fourier Transform

Frédéric Magniez
**Deutsch-Jozsa Problem**

- Input: $f : \{0, 1\}^n \rightarrow \{0, 1\}$ 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
Quantum solution \( n = 1 \)

STOP \( x \mapsto f(x) \) is not necessarily reversible!

Implementation of \( f \)

\[
|b\rangle \xrightarrow{S_f} (-1)^{f(b)}|b\rangle
\]

Hadamard gate

\[
|b\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)
\]

Quantum circuit

\[
|0\rangle \xrightarrow{H} S_f \xrightarrow{H} \text{Measure} \xrightarrow{?}
\]
Analyse ($n = 1$)

$|0\rangle \xrightarrow{H} |H_i\rangle \xrightarrow{S_f} |S_f\rangle \xrightarrow{H} |H\rangle \xrightarrow{\text{Measure}} ?$
Analyse ($n = 1$)

Initialization: $|0\rangle$

$|0\rangle \xrightarrow{H} |S_f\rangle \xrightarrow{H} \text{Measure} \xrightarrow{?}$
Analyse ($n = 1$)

Initialization: $|0\rangle$

Parallelization: $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
Analysing \( n = 1 \)

**Initialization:** \(|0\rangle\)

**Parallelization:** \(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\)

**Query the function:** \(\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)\)
Analyse ($n = 1$)

\[ |0\rangle \xrightarrow{} H \xrightarrow{} S_f \xrightarrow{} H \xrightarrow{} \text{Measure} \xrightarrow{} ? \]

**Initialization:** $|0\rangle$

**Parallelization:** $\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$

**Query the function:** $\frac{1}{\sqrt{2}} ((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)$

**Interferences:** $\frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle))$
Analyse \( n = 1 \)

![Circuit Diagram]

Initialization: \( |0\rangle \)

Parallelization: \( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \)

Query the function: \( \frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \)

Interferences: \( \frac{1}{2}((-1)^{f(0)}(|0\rangle + |1\rangle) + (-1)^{f(1)}(|0\rangle - |1\rangle)) \)

Final state: \( \frac{1}{2}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle) \)
Analyse \((n = 1)\)

\[ |0\rangle \quad \text{H} \quad S_f \quad \text{H} \quad \text{Measure} \]

**Initialization:** \(|0\rangle\)

**Parallelization:** \(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\)

**Query the function:** \(\frac{1}{\sqrt{2}}((-1)^f(0)|0\rangle + (-1)^f(1)|1\rangle)\)

**Interferences:** \(\frac{1}{2}((-1)^f(0)(|0\rangle + |1\rangle) + (-1)^f(1)(|0\rangle - |1\rangle))\)

**Final state:** \(\frac{1}{2}((-1)^f(0) + (-1)^f(1))|0\rangle + ((-1)^f(0) - (-1)^f(1))|1\rangle)\)
Quantum Fourier transform

$QFT_n |x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$

where $x \cdot y = \sum_i x_i y_i \mod 2$
Deutsch-Josza algorithm

\[ |0^n\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \left( -1 \right)^{f(x)} |x\rangle \rightarrow |0^n\rangle \] iff \( f \) is constant

**Initialization:** \( |00\ldots0\rangle = |0^n\rangle \)

**Parallelization:** \( \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \)

**Query the function:** \( \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} \left( -1 \right)^{f(x)} |x\rangle \)

**Interferences:** \( \frac{1}{2^n} \sum_{x,y \in \{0,1\}^n} \left( -1 \right)^{f(x)+x \cdot y} |y\rangle \)

**Amplitude of \( |0^n\rangle \):** \( \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \left( -1 \right)^{f(x)} \)
Simon problem

Problem
- Input: \( f : \{0, 1\}^n \rightarrow \{0, 1\}^n \) such that que
  \[
  \exists s \in \{0, 1\}^n : \forall x \neq y, \quad f(x) = f(y) \quad \iff \quad y = x \oplus s
  \]
- Output: \( s \)
- Constraint: \( f \) is a black-box

\[
\begin{align*}
|x\rangle & \quad \xrightarrow{U_f} \quad |x\rangle \quad \xleftarrow{U_f} \quad |x\rangle \\
|0\rangle & \quad \xrightarrow{U_f} \quad |f(x)\rangle \quad \xleftarrow{U_f} \quad |w \oplus f(x)\rangle
\end{align*}
\]

Complexity
- Randomly: \( 2^{\Omega(n)} \) queries
- Quantumly: \( O(n) \) queries and \( O(n^3) \) 2-qubit gates

Idea
Use \( QFT \) for finding the periode \( s \).
Quantum solution

\[ |0^n\rangle \xrightarrow{\text{QFT}_n} U_f \xrightarrow{\text{QFT}_n} \text{Measure} \xrightarrow{} |y\rangle : y \in s^\perp \]

\[ |0^n\rangle \xrightarrow{\text{Measure}} |f(x)\rangle \]
Quantum solution

Initialization: $|0^n⟩|0^n⟩$

Diagram:

\[
|0^n⟩ \xrightarrow{QFT_n} U_f \xrightarrow{QFT_n} |y⟩ : y ∈ s^⊥\]

Measure

\[
|0^n⟩ \xrightarrow{Measure} |f(x)⟩\]
Quantum solution

\[ |0^n\rangle \xrightarrow{QFT_n} U_f \xrightarrow{QFT_n} \text{Measure} \xrightarrow{} |y\rangle : y \in s^\perp \]

\[ |0^n\rangle \xrightarrow{\text{Measure}} |f(x)\rangle \]

Initialization: \[ |0^n\rangle |0^n\rangle \]

Parallelization: \[ \frac{1}{2^{n/2}} \sum_{x} |x\rangle |0^n\rangle \]
Quantum solution

\[ |0^n\rangle \xrightarrow{\text{QFT}_n} U_f \xrightarrow{\text{QFT}_n} \text{Measure} \rightarrow |y\rangle : y \in s^\perp \]
\[ |0^n\rangle \xrightarrow{\text{Measure}} |f(x)\rangle \]

Initialization: \[ |0^n\rangle|0^n\rangle \]

Parallelization: \[ \frac{1}{2^{n/2}} \sum_x |x\rangle|0^n\rangle \]

Query \( f \): \[ \frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle \]
Quantum solution

\[ |0^n\rangle \xrightarrow{QFT_n} U_f \xrightarrow{QFT_n} |y\rangle : y \in s^\perp \]

\[ |0^n\rangle \xrightarrow{\text{Measure}} |f(x)\rangle \]

**Initialization:** \[ |0^n\rangle|0^n\rangle \]

**Parallelization:** \[ \frac{1}{2^{n/2}} \sum_x |x\rangle|0^n\rangle \]

**Query \( f \):** \[ \frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle \]

**Filter:** \[ \frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)|f(x)\rangle \]
Quantum solution

\[ |0^n\rangle \rightarrow U_f \rightarrow QFT_n \rightarrow \text{Measure} \rightarrow |y\rangle : y \in s^\perp \]

\[ |0^n\rangle \rightarrow \text{Measure} \rightarrow |f(x)\rangle \]

**Initialization:** \[ |0^n\rangle |0^n\rangle \]

**Parallelization:** \[ \frac{1}{2^{n/2}} \sum_x |x\rangle |0^n\rangle \]

**Query \( f \):** \[ \frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle \]

**Filter:** \[ \frac{1}{\sqrt{2}} (|x\rangle + |x \oplus s\rangle) |f(x)\rangle \]

**Interferences:** \[ \frac{1}{2^{(n+1)/2}} \sum_y ((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}) |y\rangle |f(x)\rangle \]
Quantum solution

\[ |0^n\rangle \xrightarrow{\text{QFT}_n} U_f \xrightarrow{\text{QFT}_n} |y\rangle : y \in s^\perp \]

Initialization: \[ |0^n\rangle |0^n\rangle \]

Parallelization: \[ \frac{1}{2^{n/2}} \sum_x |x\rangle |0^n\rangle \]

Query \( f \): \[ \frac{1}{2^{n/2}} \sum_x |x\rangle |f(x)\rangle \]

Filter: \[ \frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)|f(x)\rangle \]

Interferences:
\[ \frac{1}{2^{(n+1)/2}} \sum_y \left( (-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y} \right) |y\rangle |f(x)\rangle \]
\[ \frac{1}{2^{(n+1)/2}} \sum_y (-1)^{x \cdot y} (1 + (-1)^{s \cdot y}) |y\rangle |f(x)\rangle \]
Quantum solution

Initialization: $|0^n\rangle|0^n\rangle$

Parallelization: $\frac{1}{2^{n/2}} \sum_x |x\rangle|0^n\rangle$

Query $f$: $\frac{1}{2^{n/2}} \sum_x |x\rangle|f(x)\rangle$

Filter: $\frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)|f(x)\rangle$

Interferences:

$\frac{1}{2^{(n+1)/2}} \sum_y ((-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y})|y\rangle|f(x)\rangle$

$\frac{1}{2^{(n+1)/2}} \sum_y (-1)^{x \cdot y}(1 + (-1)^{s \cdot y})|y\rangle|f(x)\rangle$

$\frac{1}{2^{(n-1)/2}} \sum_{y: s \cdot y = 0} (-1)^{x \cdot y}|y\rangle|f(x)\rangle$
Find the period $s$

**Linear system**

- After $n + k$ iterations: $y^{(1)}, y^{(2)}, \ldots, y^{(n+k)} \in s^\perp$

- If $s = 0^n$ the $y$'s have full rank ($n$) with prob. $\geq 1 - \frac{1}{2^k}$

- If $s \neq 0^n$ the $y$'s have rank $n - 1$ with prob. $\geq 1 - \frac{1}{2^{k+1}}$

- Linear system where $t$ denotes the unknown vector:

$$
\begin{align*}
    y^{(1)} \cdot t &= 0 = y^{(1)}_1 t_1 + y^{(1)}_2 t_2 + \ldots + y^{(1)}_n t_n \\
    y^{(2)} \cdot t &= 0 = y^{(2)}_1 t_1 + y^{(2)}_2 t_2 + \ldots + y^{(1)}_n t_n \\
    &\vdots \\
    y^{(n+k)} \cdot t &= 0 = y^{(n+k)}_1 t_1 + y^{(n+k)}_2 t_2 + \ldots + y^{(n+k)}_n t_n
\end{align*}
$$

**System solutions:** $0^n$ and $s$
Any abelian group

- Find the period of any function over an abelian group $G$ can be done in $\text{poly}(\log |G|)$ quantum time.

Generalization
Any abelian group

- Find the period of \textit{any} function over an abelian group $G$ can be done in $\text{poly}(\log |G|)$ quantum time
- \textbf{Order Finding} can be solved in quantum polynomial time
  
  \begin{itemize}
  \item Input: $n, a \in \mathbb{N}$ such that $\text{pgcd}(a, n) = 1$
  \item Output: the smallest integer $r \neq 0$ such that $a^r = 1 \mod n$
  \item Reduction: the period of $x \mapsto a^x \mod n$ is $r$
  \end{itemize}
Any abelian group

- Find the period of any function over an abelian group $G$ can be done in $\text{poly}(\log|G|)$ quantum time
- Order Finding can be solved in quantum polynomial time
  
  Input: $n, a \in \mathbb{N}$ such that $\text{pgcd}(a, n) = 1$
  
  Output: the smallest integer $r \neq 0$ such that $a^r = 1 \mod n$
  
  Reduction: the period of $x \mapsto a^x \mod n$ is $r$

Factorization

- Input: $n \in \mathbb{N}$
- Output: a nontrivial divisor of $n$
Any abelian group

- Find the period of any function over an abelian group $G$ can be done in $\text{poly}(\log|G|)$ quantum time
- Order Finding can be solved in quantum polynomial time
  
  **Input:** $n, a \in \mathbb{N}$ such that $\gcd(a, n) = 1$
  
  **Output:** the smallest integer $r \neq 0$ such that $a^r = 1 \mod n$
  
  **Reduction:** the period of $x \mapsto a^x \mod n$ is $r$

**Factorization**

- **Input:** $n \in \mathbb{N}$
- **Output:** a nontrivial divisor of $n$

**Reduction:** Factorization $\leq_R$ Order Finding

- Take a random $a$ and check that $\gcd(a, n) = 1$
- Compute the order $r$ of $a \mod n$
- Start again if either $r$ is odd or $a^{r/2} = -1 \mod n$
- Otherwise $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \mod n$
- Return $\gcd(a^{r/2} \pm 1, n)$
Quantum Fourier transform over a cyclic group

Classically
- The best known classical algorithm for Fourier transform over $\mathbb{Z}_N$ requires a circuit of size $O(N \log N)$

Theorem
- There is quantum circuit of size $O((\log N)^3)$ that implements $QFT_{\mathbb{Z}_N}$

Theorem
- There is a quantum circuit of size $O(\log N \log((\log N)/\varepsilon) + \log^2(1/\varepsilon))$ that implements $QFT_{\mathbb{Z}_N}$ with error $\varepsilon > 0$
Summarize of Shor algorithm

- With uniform probability we observe $y : ry = 0 \mod M$
  $$ry = kM \Rightarrow y/M = k/r$$
- A decomposition in irreducible fraction of $y/M$ gives $t/z$ such that $z|r$

Theorem

$$\Pr_{k,k'=0,...,r-1} [\text{ppcm}(z,z') = r] \geq 0.4$$

Conclusion

- A few runs of Shor algorithm solves Order Finding with probability $\Omega(1)$

Remark

- One can easily check if the order is correct since
  $$(r'|r \text{ et } a^{r'} = 1) \implies r' = r$$
Hidden Subgroup Problem

- Input: a group $G$ and a function $f$ over $G$ such that, for some unknown subgroup $H \leq G$,

$$f(x) = f(y) \iff x^{-1}y \in H$$

- Output: a generating set of $H$

Examples

- Simon Problem: $G = (\mathbb{Z}_2)^n$, $H = \{0, s\}$
- Factorization: $G = \mathbb{Z}$, $H = r\mathbb{Z}$
- Discrete logarithm: $G = \mathbb{Z}^2$, $H = \{(rx, x) : x \in \mathbb{Z}\}$
- Pell’s equations: $G = \mathbb{R}$
- Graph Isomorphism: $G = S_n$

Theorem: For every finitely generated abelian group, the Hidden Subgroup Problem can be solved in time $\text{poly}(\log|G|)$
More difficult...

**Non-abelian groups**
- General case: polynomial number of queries but exponential time
- If $H$ is normal, $QFT$ finds $H$ in polynomial time
- if $G$ is smoothly solvable, polynomial time
- Symmetric group, we know how to do... $QFT$  
- Dihedral group $\mathbb{Z}_N \rtimes \mathbb{Z}_2$ sub-exponential time $2^{O(\sqrt{\log N})}$

\[
\begin{array}{cccccccc}
 f(\cdot, 0) & 2 & 5 & 12 & 3 & 9 & 7 & 6 & 10 & 15 & 4 \\
 f(\cdot, 1) & 3 & 9 & 7 & 6 & 10 & 15 & 4 & 2 & 5 & 12 \\
\end{array}
\]

**Collision Problem:**
- $f$ is 2-to-1 but non-périodic: find a collision
  - randomized complexity $\Theta(\sqrt{N})$
  - quantum complexity $\Theta(N^{1/3})$
- Decides if $f$ is injective
  - randomized complexity $\Theta(N)$
  - quantum complexity $\Theta(N^{2/3})$
  - (the algorithm uses a quantum Markov chain!)
Non-abelian groups

- General case: polynomial number of queries but exponential time
- If $H$ is normal, $QFT$ finds $H$ in polynomial time
- if $G$ is smoothly solvable, polynomial time
- Symmetric group, we know how to do... $QFT$
- Dihedral group $\mathbb{Z}_N \rtimes \mathbb{Z}_2$ sub-exponential time $2^{O(\sqrt{\log N})}$

Collision Problem:

- $f$ is 2-to-1 but non-periodic: find a collision
  - randomized complexity $\Theta(\sqrt{N})$
  - quantum complexity $\Theta(N^{1/3})$
- Decides if $f$ is injective
  - randomized complexity $\Theta(N)$
  - quantum complexity $\Theta(N^{2/3})$
  (the algorithm uses a quantum Markov chain!)
How many quantum algorithms?

**Unstructured problems**
- Grover algorithm 1996

**Algebraically structured problems**
- Shor algorithm 1994

**Very structured problems** (dichotomy search, sorting, ...)
- Classical algorithms are optimal 2000

**Problem with few structure**
- Ambainis algorithm 2003
  A quantum walks (analogy to random walks) can improve the implementation of Grover operator
- Examples
  - Element Distinctness: $(\text{Grover})^2 \rightarrow O(N^{3/4}), \text{Ambainis} \rightarrow \Theta(N^{2/3})$ 2003
  - Triangle finding: $(\text{Grover})^2 \rightarrow O(N^{3/2}), (\text{Ambainis})^2 \rightarrow O(N^{1.3})$ 2005