Introduction to Quantum Computing
Frédéric Magniez

INF554 - Lectures 8 & 9

The genesis

Copenhagen School (Bohr, Heisenberg, …)
- The state of a quantum particle is only fixed after a measurement
- Bennett, Brassard’84: perfectly secure quantum encryption… that can be used in practice!

Paradoxe of Einstein, Podolsky, Rosen’35
- Very distant particles remain linked!? 
- Aspect, Grangier, Roger, Dalibard’82: yes!
- Quantum encryption of Ekert’91 can be certifiable

Quantum boxes

Classical information is encoded using bit (0/1)
- The measure describes the state of the system
- A random bit is a ‘hidden’ bit

Quantum information is encoded using quantum-bit
- Several possible measures
- Outcome is determined during the measurement

Quantum key distribution

Problem
- Setting
  - No prior shared secret information between Alice and Bob
  - Authenticated classical channel
- Goal: Get a private key between Alice and Bob
- Application: One-time pad (Miller’1882-Shanon’1945)

Classical results
- Impossible: all the information is in the canal
- Possible (using randomized techniques):
  - Amplify the privacy of an imperfect private key
The protocol BB84 [Bennett-Brassard 84]

Protocol: classical part
- Reconciliation: Alice and Bob publicly announce their coding choices
  A&B only keep key bits with same choices
- Security: Intercepting and opening a box → errors
  A&B check few key bits at random positions
- Privacy amplification: Perfect key using with few other more key bits

Conclusion
- Secret key generation using an authenticated classical channel
  - Small initial private key → large private key, with no authenticated channel

Protocol: quantum part

Key:

Encoding:

Decoding:

Key:

Examples of transformations

Reversible classical transformation
- Identity
  \[ |b\rangle \rightarrow \text{Id} \rightarrow |b\rangle \]
- Negation
  \[ |b\rangle \rightarrow \text{NOT} \rightarrow |1 - b\rangle \]

Hadamard transformation
- Definition: half-wave blade at 22.5°
  \[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \]
- Properties: quantum coin flipping
  \[ |0\rangle \rightarrow H \rightarrow \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]
  \[ |1\rangle \rightarrow H \rightarrow \frac{1}{\sqrt{2}} (|1\rangle - |0\rangle) \]

Qubit

State
- 2-dimensional unit vector
  \[ |\psi\rangle = \cos \theta |0\rangle + \sin \theta |1\rangle \]
  general case (complex amplitudes):
  \[ |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1 \]

Measure
- Randomized orthogonal projection
  \[ \alpha |0\rangle + \beta |1\rangle \rightarrow \text{Measure} \]

Evolution
- Unitary transformation \( G \in U(2) \) (⇒ reversible)
  \[ G \in \mathbb{C}^{2 \times 2} \text{ s.t. } G^*G = \text{Id} \]
  \[ |\psi\rangle \rightarrow G |\psi\rangle = |\psi\rangle \]

Polarization of photons

State
- Polarization: 2-dimensional vector
  \[ |\theta\rangle = \cos \theta |0\rangle + \sin \theta |1\rangle \]

Measure
- Calcite crystal
  separates horizontal and vertical polarizations
  \[ \text{A measure modifies the system} \]

Transformation
- Well known transformation: half-wave blade
  orthogonal symmetry around its axis
- Any rotations (possibly with complex angles)
Exercice 1: Quantum key distribution

Implementation
- Explain how to realize the boxes of slide 3
- Implement the protocol of slide 4 using random bits, Hadamard transformations, and measurements

Analysis of a specific attack
- Assume a third party Eves intercepts a photon with probability 1/10, observes it, and forwards the projected photon to Bob
- Assume furthermore that Alice & Bob check each bit of their key with probability 1/10
- Compute
  - The probability Eve learns a bit of the secret key
  - The probability Eve is detected

Entanglement

Principle: 2 distant boxes which remain entangled
- Outcomes are random
  - but correlated if boxes are opened similarly
  - and uncorrelated otherwise

Bell’64 inequality
- Cooperative random game
  - Classical ≤ 75% of victory
  - Quantum > 85% of victory
- Experimental verification at Orsay in 1982
- Application: quantum certification

Bell-CHSH inequality as a classical game

Game
- Alice and Bob share random bits but cannot communicate
- Alice receives a random bit $a$, Bob $b$
- Alice returns a bit $a$, Bob $b$
- Goal: maximize $p = \sum_i P(x, y) (a \oplus b = x \land y)$
- CHSH inequality [1969]
  - The best probabilistic strategy achieves $p = 3/4$

Deterministic strategy
- Provide a deterministic strategy achieving $p = 3/4$
- Show that no deterministic strategy can achieve $p = 1$
- Conclude that $p \leq 3/4$ for every deterministic strategies

Randomized strategy
- We assume that both players have access to a shared source of randomness, called $\lambda$
  - Note: Physicists call $\lambda$ a hidden variable
  - Justify why this is the most powerful model of random resource
- Let $p_\lambda$ be the winning probability when $\lambda$ is fixed
  - Show that there must be some $\lambda$ such that $p_\lambda \geq p$
  - Conclude that the best probabilistic strategy achieves $p = 3/4$
\( n \)-qubit

**State**
- \(|\psi\rangle \in \mathbb{C}^{2^n}\) such that \(\|\psi\| = 1\)

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

- **Examples**
  - Separated 2-qubit: \(|00\rangle + |01\rangle = |0\rangle(|0\rangle + |1\rangle)\)
  - Entangled 2-qubit: \(|00\rangle + |11\rangle \neq |\psi_1\rangle|\psi_2\rangle \quad \text{EPR state}\)

**Measure**
- Randomized orthogonal projection

\[ \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \quad \text{Measure} \quad |\alpha_x|^2 |x\rangle \]

**Evolution**
- Unitary transformation \( G \in \mathcal{U}(2^n) \) \((G \in \mathbb{C}^{2^n \times 2^n} \text{ s.t. } G^*G = \text{Id})\)

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

---

**Transformation c-NOT**

**Definition**
- \(\text{c-NOT}(00) = |0b\rangle\)
- \(\text{c-NOT}(1b) = |1\rangle(1 - b)\)
- \(\text{c-NOT}(ab) = |a\rangle|a \oplus b\rangle\)

**Representation**
- Target bit
- Control bit

**Bell basis change**

\[ |x\rangle \xrightarrow{H} |\beta_x\rangle \quad |y\rangle \xrightarrow{\text{NOT}} |\beta_y\rangle \]

---

**Mathematical background: Tensor product**

**Vector spaces**
- \(V \otimes W\) vector spaces
- \(V \otimes W\) is the free vector space \(\text{Span} (v \otimes w : v \in V, w \in W)\)

With equivalence relations

- \((v + w) \otimes w = v \otimes w + w \otimes w\)
- \(v \otimes (w + w) = v \otimes w + v \otimes w\)
- \((c \cdot v) \otimes w = v \otimes (c \cdot w) = c \cdot (v \otimes w)\)

**Linear maps**
- \(\mathcal{L}: V \otimes X \rightarrow W \otimes Y\) : linear maps
- \(\mathcal{L} = T \otimes W \otimes Y\) is the linear map satisfying

\[ \mathcal{L}(v \otimes w) = S(v) \otimes T(w) \]

(and extended by linearity)

**Applications**
- Joint probability distributions on spaces \(V \otimes W\)

\[ \mathcal{D}(V \otimes W) = \mathcal{D}(V) \otimes \mathcal{D}(W) \neq \mathcal{D}(V) \otimes \mathcal{D}(W)\] (product distributions)

---

**Partial measure: 2-qubit case**

**Measure of first qubit**

- Projectors

\[ P_0 = |00\rangle\langle 00| + |01\rangle\langle 01| = |0\rangle \otimes I_2 \]

\[ P_1 = |10\rangle\langle 10| + |11\rangle\langle 11| = |1\rangle \otimes I_2 \]

\[ P_0 \perp P_1 = \text{Id} \]

- Measure of first qubit

\[ |\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \]

\[ |\psi\rangle = \frac{a}{\sqrt{a^2 + b^2 + c^2 + d^2}} |00\rangle + \frac{b}{\sqrt{a^2 + b^2 + c^2 + d^2}} |01\rangle + \frac{c}{\sqrt{a^2 + b^2 + c^2 + d^2}} |10\rangle + \frac{d}{\sqrt{a^2 + b^2 + c^2 + d^2}} |11\rangle \]

**Generalization**

- Partial measure project to a subspace compatible with the observation

\[ \text{Probability} = \text{square norm of the projection} \]

\[ \text{Outcome} = \text{renormalization of the projection} \]
Exercice 3

Partial vs complete measurement
- Consider any two-qubit state, and measure its first qubit and then its second qubit.
- Compute the probability distribution of the outcome.
- Conclude that observing the two qubits is equivalent to measuring each qubit individually in any order.
- Note: This can be generalized to any number of qubits.

Non-cloning
- Assume there is a unitary map U such that, for every qubit:
  \[ U(|i\rangle|0\rangle) = |i\rangle|\psi\rangle \]
- Compute \[ U(|i\rangle|0\rangle) \] for \[ |\psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \]
  using the definition of U.
  using the linearity of U and then again the definition of U.
- Get a contradiction and conclude.

Exercice 4: EPR state

Entangles boxes
- Implement the entangled boxes of slide 10 using EPR states.

Properties
- Show that applying a unitary U on the first qubit of an EPR state is equivalent to applying the transposed matrix of U on its second qubit.

Quantum game
- Prove the theorem of previous slide.

Bell-CHSH inequality as a quantum game

Reminder
- Goal: \[ \maximize \ p = \Pr(x \oplus y = x \land y) \]
Quantumly
- Alain and Bob share an EPR state:
  \[ x \]
  \[ y \]
- Bob performs a rotation of angle \[ \frac{\pi}{4} \]
- If \[ x = 1 \], Alice performs a rotation of angle \[ \frac{\pi}{4} \]
- If \[ y = 1 \], Bob performs a rotation of angle \[ -\frac{\pi}{4} \]
- Alice and Bob observe their qubit and send their respective outcomes.
- Theorem: \[ p = \cos^2 \left( \frac{\pi}{8} \right) \approx 0.85 \]
Realization: [Aspect-Grangier-Roger-Dalibard: Orsay'82]

Superdense coding [1992]

Problem
- Alice and Bob share an EPR state: \[ |\beta\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \]
- Alice wants to send two bits \( xy \) to Bob.
- But Alice can only send one qubit to Bob.
- Prove the theorem of previous slide.

Bell basis change
- Alice applies to its qubit \( \text{NOT} \) if \( y = 1 \), and \( \text{FLIP} \) if \( x = 1 \):
  \[ |\beta_{xy}\rangle \]
- Bob performs the inverse of the Bell basis change, and observes \( xy \).
Problem

- Alice wants to transmit a qubit $|\psi\rangle$ to Bob
- Bob: far and unknown position to Alice

Realization

The quantum communication does not reveal anything on $|\psi\rangle$!

Coin flipping

Problem

- Alice and Bob are far away
- They want to flip a coin in a fair way but they don’t trust each other

Classically

- Solutions based on harness assumptions of combinatorial problems
- No unconditionally secure solution

Quantumly

- There exists a protocol with maximal bias 0.25 [2001]
- There is no protocol with bias better than 0.207 [2002]
- There exists a protocol with maximal bias 0.207 [2009]

Weak version: election

- Alice wants head
- Bob wants tail
- There exists a protocol with arbitrarily small bias [2007]

EPR based coin flipping

Main idea

- Assume Alice & Bob share an EPR state

Fact

- $a$ with probability 1
- $a$ (resp. $b$) is a uniform random bit

Problems

- Who create the EPR state?
- If Alice does, Bob needs to check that is an EPR state:
  - For instance not $|00\rangle \rightarrow a=b=0$ with probability 1
- In order to check the EPR state, Bob needs the 2 qubits
  Then Alice needs to check that Bob gives back the correct qubit
The NSA is racing to build a computer that could break nearly every kind of encryption used to protect banking, medical, business and government records around the world.

According to documents provided by former NSA contractor Edward Snowden, the effort to build "a cryptologically useful quantum computer" — a machine exponentially faster than classical computers — is part of a $79.7 million research program titled "Penetrating Hard Targets." Much of the work is housed under classified contracts at a laboratory in College Park, Md.

Physicists and computer scientists have long speculated about whether the NSA's efforts to develop quantum computing technology, which exploits the peculiar properties of matter at the atomic scale, might one day let the agency break the encryption used in most commercial transactions or safeguard government secrets.

"It seems improbable that the NSA could be engaging in a technology push in an area that is known to be of no value to them," said Simon Simon, a senior fellow at the Brookings Institution, a policy research organization in Washington. "For a government that has access to a wide array of sources of information, the cost of a quantum computer is likely to be a fraction of the cost of alternative access to the information."
Quantum parallelism

**n-qubit**
- Superposition of all possible values
- \(2^n\) possible values

**Parallel computation**
- In one step, \(2^n\) computations
- But only one outcome can be (randomly) observed!

**Strategy**
- Combine cleverly those values before measuring them...

---

Logical computing

**Gates**
- A gate \(C\) is a function on at most 3 qubits
  - Example: AND, OR, NOT,...

**Circuit**
- A circuit is a sequence of gates \(C = C_L \ldots C_2 C_1\)
  - The size of \(C\) is its number \(L\) of gates
  - \(C\) computes a function \(f\) if for all input \(x\): \(C(x, 0^k) = (f(x), z)\)

**Theorem**
- Any function can be computed by a circuit using only NOT, OR, AND gates

---

Quantum gates and circuits

**Gates** \(U \in U(2^k), \ k = 1, 2, 3\)
- A quantum gate is a unitary map that acts upon at most 3 qubits

**Tensor product of gates**
- \((G_1 \otimes G_2)\left|\psi_1\right\rangle\left|\psi_2\right\rangle = (G_1\left|\psi_1\right\rangle)(G_2\left|\psi_2\right\rangle)\)

**Circuit**
- A quantum circuit is a sequence of gates (extended by \(\otimes\) \(\text{Id}\))

**Theorem**
- Any unitary can be realized exactly by a circuit
  and approximated using only gates \(c\text{-NOT}\) and \(\sqrt{H}\)

---

Reversible computing

**Reversible circuit**
- A logical circuit is reversible if each gate is reversible
- A reversible circuit is also a quantum circuit
  (since it permutes logical states)

**Embedding**
- \(f : \{0, 1\}^n \rightarrow \{0, 1\}^m\)
- \(f_B : \{0, 1\}^{n+m} \rightarrow \{0, 1\}^{n+m}\)
- \(f_B(x, y) = (x, y \oplus f(x))\)
  where: \(0 \oplus 1 = 1 \oplus 0 = 1\)
  \(0 \oplus 0 = 1 \oplus 1 = 0\)
  \(u \oplus v = (u_1 \oplus v_1, u_2 \oplus v_2, \ldots)\)

**Theorem**
- If a function \(f\) can be computed by a logical circuit of size \(L\), then \(f_B\) can also be computed by a reversible circuit of size \(O(L)\)

**Universality**
- The Toffoli gate \((c\text{-NOT})\) is universal for reversible computing
  \(T(a, b, c) = (a, b, c \oplus (a \land b))\)
Quantum implementation of classical functions

Normal form
- Function: $f : \{0, 1\}^n \rightarrow \{0, 1\}$
- Circuit: $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$
  $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$

Alternative form $S_f$
- Boolean function: $f : \{0, 1\}^n \rightarrow \{0, 1\}$
- Circuit:

$$|x\rangle \xrightarrow{U_f} |x\rangle$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{S_f} \frac{1}{\sqrt{2}}((f(x)) - |1 \oplus f(x)\rangle)$$

Conclusion:

$$U_f(|x\rangle \otimes |\psi\rangle) = S_f(|x\rangle) \otimes |\psi\rangle$$

Deutsch-Jozsa problem
- Oracle input: $f : \{0, 1\}^n \rightarrow \{0, 1\}$ a black-box function such that $f$ is either constant or balanced
- Output: 0 iff $f$ is constant

Query complexity
- Deterministic: $2^{n+1} + 1$
- Quantum: 1

Special case $n=1$
- No restriction on $f$
- Deterministic vs quantum: 2 queries vs 1 query

Quantum solution ($n=1$)

Nonreversible! $x \mapsto f(x)$ can be nonreversible!

Reversible implementation of $f$

$\alpha|0\rangle + \beta|1\rangle \rightarrow S_f \rightarrow (-1)^{f(0)}|b\rangle|0\rangle + (-1)^{f(1)}|\beta\rangle|1\rangle$

Hadamard gate: half-wave blade at 22.5°

$|b\rangle \rightarrow H \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{f(1)}|1\rangle)$

Quantum circuit

$$|0\rangle \rightarrow H \rightarrow S_f \rightarrow H \rightarrow \text{Measure}$$
General solution for Deutsh-Jozsa

Reversible implementation of $f$

$$\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \rightarrow |S_f \rangle \rightarrow \sum_{x \in \{0,1\}^n} f(x) |f(x)\alpha_x |x\rangle$$

Quantum Fourier transform

$$QFT_n |0\rangle = \sum_{y} (-1)^{x \cdot y} |y\rangle$$

Quantum circuit

$$|0\rangle \rightarrow |QFT\rangle \rightarrow |S_f \rangle \rightarrow |QFT\rangle \rightarrow \text{Measure} \rightarrow ?$$

Bernstein-Vazirani

Problem
- Oracle input: $f : \{0,1\}^n \rightarrow \{0,1\}$ a black-box function such that $f(x) = \alpha \cdot x$ for some fixed $\alpha \in \{0,1\}^n$
- Output: $\alpha$

Query complexity
- Randomized: $n$
  - Query $f^{(i+1)}|0^n\rangle = \alpha_i$ for $i=1,2,\ldots,n$
- Quantum: $1$

Quantum circuit

$$|0\rangle \rightarrow |QFT\rangle \rightarrow |S_f \rangle \rightarrow |QFT\rangle \rightarrow \text{Measure} \rightarrow |\alpha\rangle$$

Analysis

$$|0\rangle \rightarrow |QFT\rangle \rightarrow |S_f \rangle \rightarrow |QFT\rangle \rightarrow \text{Measure} \rightarrow f \text{ constant?} |00\ldots0\rangle$$

Initialization: $|00\ldots0\rangle$

Parallelization: $\frac{1}{2^n} \sum_{x \in \{0,1\}^n} |x\rangle$

Query to $f$: $\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle$

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

Final state: $\left(\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |00\ldots0\rangle + \sum_{y \notin 00\ldots0} \alpha_y |y\rangle\right)$

Exercise: Analysis

$$|0\rangle \rightarrow |QFT\rangle \rightarrow |S_f \rangle \rightarrow |QFT\rangle \rightarrow \text{Measure} \rightarrow |\alpha\rangle$$

Initialization:

Parallelization:

Query to $f$:

Interferences:

Final state:
On the difficulty of factorization

**RSA Challenges**
- [http://www.rsasecurity.com/rsalabs](http://www.rsasecurity.com/rsalabs)
- RSA-640 (193 digits):

  \[
  3107418240490043721350750035888567930037346022842727545720161948823206440518081504556346829671723867824379162738303341547107310850191954852900733724822783525742386454014691736602477652346609 = \ \begin{array}{c}
  1634733645809253848443133883865008684178367033303213211188588333301004908512121186751579 \\
  1900871281664822113126851573935413975471686785865154908686853908027103021448857191261465571
  \end{array}
  \]

- RSA-100, $1,000, 1991
- RSA-640, $20,000, 2005

**RSA Algorithm (allows private communication)**
- security based on the difficulty of factorizing

Asymmetric encryption

**One-way functions**
- Example: multiplication / factorization
- Bases of modern encryption (Rivest, Shamir, Adleman’77)

- RSA-100, $1,000, 1991
- RSA-640, $20,000, 2005

Quantum algorithm for factorization

**Classical reduction**
- Factorization can be reduced to period finding (of some arithmetic function)

**Quantum tool: Fourier Transform**
- FT reveals the period of a signal
- FT is (very) fast on a quantum superposition

From period finding to factorization

**Theorem** [Simon-Shor’94]
- Finding the period of any function on an abelian group can be done in quantum time \(\text{poly (log } |G|\) \)

**Order finding**
- Input: integers \(n\) and \(a\) such that \(\gcd(a,n)=1\)
- Output: the smallest integer \(q \neq 0\) such that \(a^q \equiv 1 \mod n\)
- Reduction: to period finding the period of \(x \mapsto a^x \mod n\) is \(q\)

**Factorization**
- Input: integer \(n\)
- Output: a nontrivial divisor of \(n\)

**Reduction**: Factorization \(\leq\) Order finding
- Check that \(\gcd(a,n)=1\)
- Compute the order \(q\) of \(a \mod n\)
- Restart if \(q\) is odd or \(a^{q/2} \equiv -1 \mod n\)
- Otherwise \((a^{q/2} - 1)(a^{q/2} + 1) = 0 \mod n\)
- Return \(\gcd(a^{q/2} \pm 1, n)\)
Simon’s problem

Finding the period

Oracle input: \( f : \{0,1\}^n \rightarrow \{0,1\}^n \) a black-box function

\[
\begin{array}{c|c|c}
|x\rangle & U_f & |x\rangle \\
|0\rangle & U_f & |f(x)\rangle \\
\end{array}
\]

such that \( 3a \neq 0^n : \forall x \neq y, f(x) = f(y) \iff y = x \oplus a \)

Output: the period \( s \)

Complexity

- Randomly: \( 2^{O(n)} \) queries
- Quantumly: \( O(n) \) queries and time \( O(n^2) \)

Realization of \( QFT \) using Hadamard gates:

\[
|b\rangle = \frac{1}{\sqrt{2^n}} \sum y \in \mathbb{Z}_2^n |y\rangle
\]

Quantum solution

\[
\begin{array}{c}
|0^n\rangle \xrightarrow{QFT} |y\rangle \\
|0^n\rangle \xrightarrow{U_f} |f(x)\rangle \xrightarrow{QFT} |y\rangle \\
|0^n\rangle \xrightarrow{Measure} |y : y \in \mathbb{Z}_2^n\rangle
\end{array}
\]

Initialization: \( |0^n\rangle|0^n\rangle \)

Parallelization: \( \frac{1}{\sqrt{n}} \sum x |x\rangle|0^n\rangle \)

Query to \( f \): \( \frac{1}{\sqrt{n}} \sum x |x\rangle|f(x)\rangle \)

Filter: \( \frac{1}{\sqrt{n}} (|x\rangle + |x \oplus v\rangle)|f(x)\rangle \)

Interferences:

\[
\frac{1}{\sqrt{n}} \sum y |y\rangle|f(x)\rangle
\]

Probability = square norm of the projection

Outcome = renormalization of the projection

More difficult...

Finding the period

Construction of a linear system

- After \( n + k \) iterations: \( y_1, y_2, \ldots, y_{n+k} \in \mathbb{Z}_2 \)
- \( y = 0^n \) is solution of the linear system in \( \mathbb{Z}_2 \):

\[
\begin{align}
\begin{cases}
y_1 \cdot t &= 0 \\
y_2 \cdot t &= 0 \\
\vdots \\
y_{n+k} \cdot t &= 0
\end{cases}
\Leftrightarrow
\begin{cases}
y_1^2 + y_1^2 t_1 + \cdots + y_1^2 t_n &= 0 \\
y_2^2 + y_2^2 t_1 + \cdots + y_2^2 t_n &= 0 \\
\vdots \\
y_{n+k}^2 + y_{n+k}^2 t_1 + \cdots + y_{n+k}^2 t_n &= 0
\end{cases}
\end{align}
\]

- The \( y \) are of rank \( n - 1 \) with proba \( \geq 1 - 1/2^{n+1} \)
- System solutions: \( 0^n \) and \( s \)

Complexity

- Constructing the system: \( O(n) \) queries, time \( O(n^2) \)
- Solving the system: no query, time \( O(n^2) \)

Period Finding

- Oracle input: function \( f \) on \( G \) such that

\[
f \text{ is strictly periodic for some unknown } H \subseteq G.
\]

\[
f(x) = f(y) \iff y \in xH
\]

- Output: generator set for \( H \)

Examples

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

Quantum polynomial time algorithms (in \( \log|G| \))

- Abelian groups \( G \): \( QFT \)-based algorithm [1995]
- Normal period groups \( H : QFT \)-based algorithm [2000]
- Solvable groups \( G \) of constant exponent and constant length [2003]
Hard instances

**Shift problem**
- Dihedral group $\mathbb{Z}_N \times \mathbb{Z}_2$: sub-exponential time $2^{O(\sqrt{\log N})}$ [2003]
- $f(-, 0) = [2, 5, 12, 3, 9, 7, 6, 10, 15, 4]$ 
- $f(-, 1) = [3, 5, 7, 6, 10, 15, 4, 2, 5, 12]$ 

**Graph Isomorphism**
- Instance of Period Finding on the symmetric group where we just know how to implement QFT... [1997]

**General case**
- Polynomial number of queries to $f$, but exponential post-processing time [1999]

Preliminary remarks

**Implementation of $f$**
\[ \sum_x \alpha_x |x\rangle \xrightarrow{S_f} \sum_x (-1)^{f(x)} \alpha_x |x\rangle = \sum_x \alpha_x |x\rangle - 2\alpha_{x_0} |x_0\rangle \]

**Double Hadamard gate**
\[ |x_1\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{f(x)} |1\rangle) \]
\[ |x_2\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{f(x)} |1\rangle) \]

\[ |x\rangle = |x_1 x_2\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} \sum_y (-1)^{x \cdot y} |y\rangle \]

with $x \cdot y = x_1 y_1 + x_2 y_2 \mod 2$

Grover search algorithm

**Grover problem**
- Oracle input: $f: \{0, 1\}^n \rightarrow \{0, 1\}$ such that $\exists x_0 : f(x_0) = 1$
- Output: $x_0$
- Constraint: $f$ is a black-box

**Query complexity**
- Randomized: $\Theta(2^n)$
- Quantum: $\Theta(\sqrt{2^n})$

\[ n = 2 \Rightarrow 1 \text{ query} \]

Quantum solution ($n = 2$)

\[ |0\rangle \xrightarrow{H} |0\rangle \xrightarrow{S_f} \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{f(x_0)} |1\rangle) \xrightarrow{H} \frac{1}{\sqrt{2}} \sum_x |x\rangle - |x_0\rangle \]

**Initialization:** $|00\rangle$

**Parallelization:** $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

**Query to $f$:** $\frac{1}{2} \sum_x |x\rangle - |x_0\rangle$

**Interferences:** $|00\rangle - \frac{1}{2} \sum_y (-1)^{x \cdot y} |y\rangle$

**Query to $\delta_0$:** $-|00\rangle - \frac{1}{2} \sum_y (-1)^{x \cdot y} |y\rangle - 2|00\rangle = -H \otimes H |x_0\rangle$

**Final state:** $-|x_0\rangle$
Geometrical analysis

**Grover operator**

\[ \begin{array}{c}
\text{Vect}_\theta(|x_0\rangle, |\text{unif}\rangle) \\
S_f = -S_{|0\rangle} = S_{|1\rangle} \\
H^{\otimes 2} S_{|00\rangle} H^{\otimes 2} = S_{|\text{unif}\rangle} \\
G = S_{|\text{unif}\rangle} S_{|x_0\rangle} = R_{2\theta} \\
\text{with } \sin \theta = \langle \text{unif}|x_0\rangle = \frac{1}{2}
\end{array} \]

After 1 iteration

\[ |\text{unif}\rangle \mapsto -G|\text{unif}\rangle = -|x_0\rangle \]

---

**Geometrical analysis, general case**

\[ \begin{array}{c}
\text{Vect}_\theta(|x_0\rangle, |\text{unif}\rangle) \\
S_f = -S_{|0\rangle} = S_{|1\rangle} \\
H^{\otimes 2} S_{|00\rangle} H^{\otimes 2} = S_{|\text{unif}\rangle} \\
G = S_{|\text{unif}\rangle} S_{|x_0\rangle} = R_{2\theta} \\
\text{with } \sin \theta = \langle \text{unif}|x_0\rangle = \frac{1}{2}
\end{array} \]

After \( T = 2 / \pi \cdot \sqrt{2^n} \) iterations

\[ |\text{unif}\rangle \mapsto -G^T |\text{unif}\rangle \approx -|x_0\rangle \]

---

**How many quantum algorithms exist?**

- **Unstructured problems**
  - Grover algorithm [1996]

- **Algebraic problems**
  - Simon-Shor algorithm [1994]

- **Well structured problems**
  - Classical algorithms are optimal!

- **Problems with few structures**
  - Quantum walk based algorithms [2003]
    - quantum analogy of random walks
  - Examples
    - Element Distinctness, Commutativity: \( \mathbb{N}^{\otimes 3} \)
    - Triangle Finding: \( \mathbb{N}^{\otimes 7} \) (lower bound \( \mathbb{N} \))
    - Square Finding: \( \mathbb{N}^{\otimes 21} \) (lower bound \( \mathbb{N} \))
    - Matrix Multiplication: \( \mathbb{N}^{\otimes 3} \) (lower bound \( \mathbb{N}^{\otimes 3} \))
    - AND-OR Tree evaluation: \( \mathbb{N} \)

---

**To continue...**

- **An Introduction to Quantum Computing**
  - Authors: Phillip Kaye, Raymond Laflamme, Michele Mosca
  - Editor: Oxford University Press

- **Quantum Computation and Quantum Information**
  - Authors: Michael A. Nielsen, Isaac L. Chuang
  - Editor: Cambridge University Press

- **Classical and Quantum Computation**
  - Editor: American Mathematical Society

- **Lecture Notes for Quantum Computation**
  - Author: John Preskill
  - Website: [http://www.theory.caltech.edu/~preskill/ph229/](http://www.theory.caltech.edu/~preskill/ph229/)

- **Quantum proofs for classical theorems**
  - Author: Andrew Drucker, Ronald de Wolf
Where does the quantum superiority come from?

Entanglement?
- “Classical entanglement” exists: shared randomness
- But quantum entanglement is “stronger”
  Bell-CHSH inequality and applications

Complex amplitudes?
- No: they can be simulated using only real amplitude

Negative amplitudes?
- Yes: they can induce destructive interferences

Hardness of amplitudes?
- No: amplitudes must be easily computable for being physically realizable

Applications
- Unfalsifiable money, artificial intelligence, …

Quantum computing
- For a better understanding of quantum phenomenon
- New mathematical tool for proving results in classical computing!

Technology
- Computer, intermediate models: boson sampling
- Certification: encryption, random generator, computation

Some quantum centers in the world

www.pcqc.fr

Welcome
The Paris Centre for Quantum Computing (PCQC) in Paris, France, brings together computer scientists, theoretical and experimental physicists and mathematicians that work in and around Paris. Our goal is to develop most quantum information and communication technologies and lead the way from a Personal Computer (PC) to a Quantum Computer (QC).

Future

Openings
PCQC is welcoming applications for a number of PhD and postdoc positions.

In addition, every year, the different ENSIT institution (INRIA, IMAG, LIRMM, LIRMM) have permanent job openings in Computer Science and in Physics, including quantum information. The application deadline is usually in early January. We recommend interested parties to contact a PCQC member at least two months before the deadline to discuss the possibilities and the different application processes.

Events
The PCQC members are organizing regularly seminars, workshops, schools or conferences.

You can find more information about upcoming and past events here. You can also join our mailing list.

Join our Mailing List
Name *
First Last
Email *

Submit