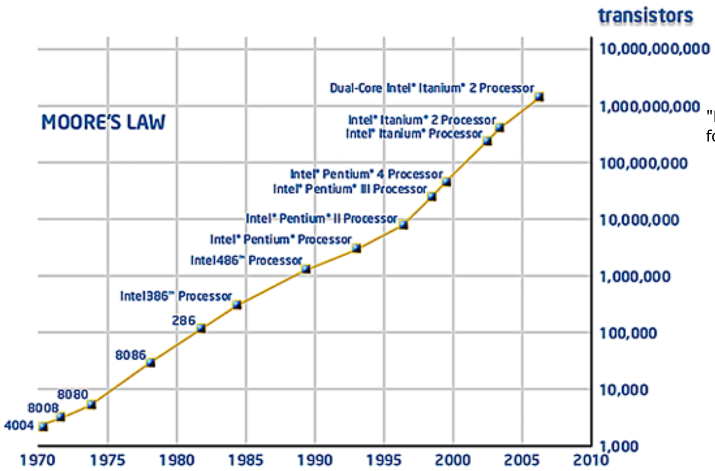
Supériorité de l'ordinateur Quantique

Frédéric Magniez

INF 561 - Cours 8 & 9

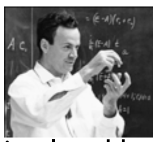
Toward nanotechnology

End of Moore's Law?



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

Quantum interferences around 2020...



- Current approach: avoid them
- Quantum computing: get benefit of them!

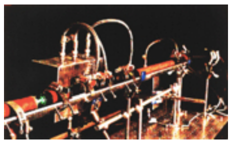
  Feynman'81: "Can quantum systems be probabilistically simulated by a clasical computer? [...] the answer is certainly, No!"

  Deutsch'85: Universal quantum Turing machine

The superiority of Quantum Computing

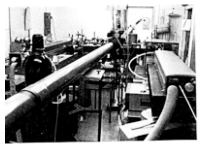
Cryptography



- Secrete Key Distribution Protocol [Bennett, Brassard'84]

  Implementation: ~100 km

Information Theory

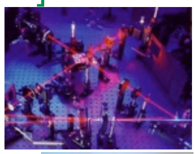


- EPR Paradox [Einstein, Podolsky, Rosen'35]

  Realization: 1982 [Orsay]

- Teleportation [Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters'93]

  Realization: 1997 [Innsbruck]



Algorithms

- Polynomial algorithm for Period Finding [Simon, Shor'94]

  ⇒ Factorization, Discrete Logarithm

- Quadratic speedup for Database Search [Grover'96]
- Quantum computer?

  1995: 2-qubit [ENS], 2000: 5-qubit [IBM], 2006: 12-qubit [Waterloo]

Quantum proofs for classical theorems

- http://arxiv.org/abs/0910.3376 [Drucker, de Wolf'09]

Computing?

Formal concepts

- Model of computation

  What is a machine, a program?

  Mathematical model of a computer?

- Hardness of a problem

  Calculable / Non-calculable

  Easy / Hard

- [Turing 1936]: Turing machine, calculability, universality

Church-Turing theses

- Weak version

  Any *reasonable* model of computation can be simulated on a Turing machine

  reasonable: physically realizable

  Turing machine ≈ today computer

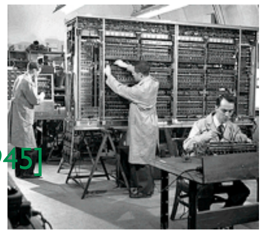
- Strong version

  Any reasonable model of computation can be *efficiently* simulated on a *probabilistic* Turing machine

  efficiently: using same amount of ressources (time and space)

Computers?

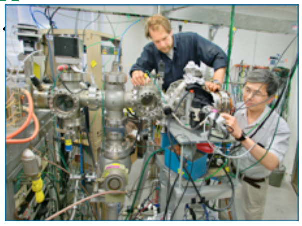
Classical computing



- 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]
- Turing machine, calculability, universality [Deutsch 1985,1989][Bernstein-Vazirani 1993], circuits [Yao 1993], cellular automata, finite automata...
- Technology: 2-qubit [1995], 5-qubit [2000], 12-qubit [2006]



Validity of Church-Turing theses

- Weak version is still valid
  - Calculability: quantum and classical computation have same power
- Strong version *could* be violated
  - Complexity: evidences that quantum computers can be exponentially faster than classical computers

In this talk

1 qubit

- Definition
- Quantum key distribution

2 qubit

- Definition
- EPR Paradox and applications

Algorithms

- Toward factorization
  - Quantum Fourier transform
  - Applications
- Generalization

Conclusion

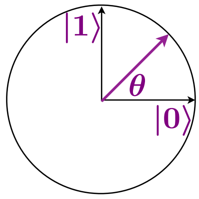
Logical bit

- Deterministic element: $b \in \{0,1\}$

Probabilistic bit

- Probabilistic distribution: $d = \begin{pmatrix} p \\ q \end{pmatrix}$ $\quad p, q \in [0,1]$, $p + q = 1$

Quantum bit (qubit)



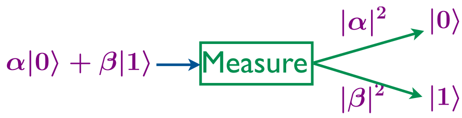
- State: 2-dimensional unit vector

$$|\psi\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

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



Logical bit

- Function: $f : \{0,1\} \to \{0,1\}, \quad b \mapsto f(b)$

Probabilistic bit

- Stochastic matrix:

$$P = \begin{pmatrix} p & p' \\ q & q' \end{pmatrix}, \quad d \mapsto d' = Pd$$

Quantum bit

- Evolution: unitary transformation $G \in \mathcal{U}(2)$ ($\Rightarrow$ reversible)

Definition: $G \in \mathbb{C}^{2\times 2}$ s.t. $G^* G = \mathrm{Id}$

$$|\psi\rangle \longrightarrow \boxed{G} \longrightarrow |\psi'\rangle = G|\psi\rangle$$

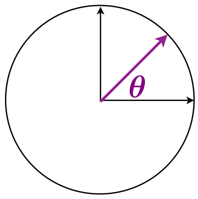
$$|\psi'\rangle = G|\psi\rangle \longrightarrow \boxed{G^*} \longrightarrow |\psi\rangle$$

Polarization of photons

State

- Polarization: 2-dimensional vector

  $$|\theta\rangle = \cos\theta|\rightarrow\rangle + \sin\theta|\uparrow\rangle$$

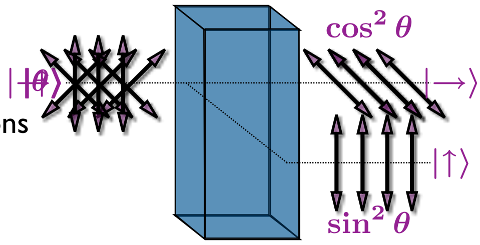


Measure

- Calcite crystal

  separates horizontal and vertical polarizations

  STOP A measure modifies the system

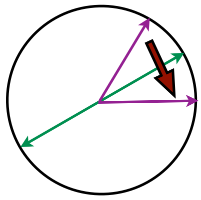


Transformation

- Well known transformation: half-wave blade

  orthogonal symmetry around its axis

- Any rotations (possibly with complex angles)



Examples of transformations

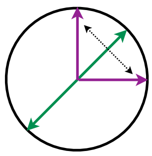
Reversible classical transformation

- Identity

  $|b\rangle$ ←- - - - - Id - - - - - → $|b\rangle$

- Negation

  $|b\rangle$ ←- - - - - *NOT* - - - - - → $|1-b\rangle$

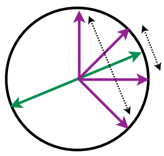


Hadamard transformation

- Definition: half-wave blade at 22,5°

  $$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

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



- Properties: quantum coin flipping

  $|0\rangle \rightarrow \boxed{H} \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \rightarrow$ Measure $\xrightarrow{\frac{1}{2}} |0\rangle$, $\xrightarrow{\frac{1}{2}} |1\rangle$

  $|b\rangle \rightarrow \boxed{H} \rightarrow \boxed{H} \rightarrow$ Measure $\rightarrow |b\rangle$

  STOP Measure does not commute!

Quantum key distribution

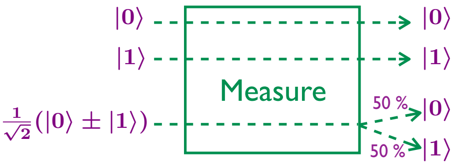
Problem

- Setting
  - No prior shared secret information between Alice and Bob
  - Authenticated classical channel
- Goal: Get a private key between Alice and Bob

Classical results

- **Impossible**, since all the information is in the canal
- However, one **can** (using randomized techniques):
  - **Amplify** the privacy of an imperfect private key by shortening it

Incertitude in the measure



Impossibility of cloning

- Impossibility of duplicating an unknown state
- Proof based on the linearity of quantum transformations

Main idea of quantum key distribution

Primitive

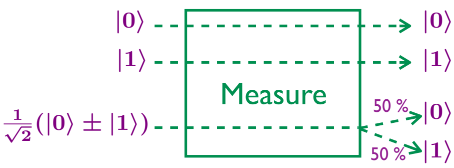
- Alice choses 2 random bits *a,c*
- Alice creates and sends to Bob qubit $H^c|a\rangle$

- Bob gets qubit from $|\psi\rangle$ Alice
- Bob choses 1 random bit *d*
- Bob measures $H^d|\psi\rangle$ and gets bit *b*

H^2=Id

Facts

- c=d → b=a with **probability 1**
- c≠d → b=a with **probability 1/2**



Reconciliation

- Alice & Bob exchange their value *c,d*

Remarks

- If *c=d*, Alice & Bob know *a=b without revealing a,b*
- "*without revealing*" can be formalized...

The protocol BB84 [Bennett-Brassard 84]

Protocol: quantum part

Key:	0	1	1	0	0	1	0	1	1	1	0
Encoding:		H			H			H	H		H
Qubit:	↔	⤡	↕	↔	⤢	↕	↔	⤡	⤡	↕	⤢

Decoding:	H		H			H		H			H
Qubit:	⤢	⤡	⤡	↔	⤢	⤡	↔	↕	⤡	↕	↔
Key:	1	1	0	0	1	1	0	1	0	1	0

Protocol: classical part

- Reconciliation: Alice and Bob publicly announce their coding choices
  A&B only keep key bits with same choices (prob. 1/2)
  If no third party observes communication, then A&B get same key
- Security: A&B check few key bits at random positions
- Secret amplification using with few other more key bits

Conclusion

- Key generation without any prior shared secret information but using an authenticated classical channel
- Small initial private key → large (and authentified) private key

Preliminaries: Tensor product

Vector spaces

- V, W: vector spaces
- $V\otimes W$ is the free vector space Span ($v\otimes w : v\in V, w\in W$)
  with equivalence relations
  $(v_1+v_2)\otimes w = v_1\otimes w + v_2\otimes w$
  $v\otimes (w_1+w_2) = v\otimes w_1 + v\otimes w_2$
  $(c\cdot v)\otimes w = v\otimes(c\cdot w) = c\cdot(v\otimes w)$

Linear maps

- $S: V\to X,\quad T: W\to Y$: linear maps
- $S\otimes T :\ V\otimes W\to X\otimes Y$ is the linear map satisfying
  $S\otimes T\ (v\otimes w) = S(v)\otimes T(w)$
  (and extended by linearity)

Applications

- Joint probability distributions on spaces V, W
  $\mathcal{D}(V\times W) = \mathcal{D}(V)\otimes\mathcal{D}(W) \neq \mathcal{D}(V)\times\mathcal{D}(W)$ (: product distributions)

n-qubit

Definition

- $|\psi\rangle \in \mathbb{C}^{\{0,1\}^n}$ such that $\||\psi\rangle\| = 1$

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

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

Examples: $\frac{|00\rangle+|01\rangle}{\sqrt{2}} = |0\rangle \otimes \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

$\frac{|00\rangle+|11\rangle}{\sqrt{2}} \neq |\psi_1\rangle \otimes |\psi_2\rangle$

Unitary transformations: $G \in \mathcal{U}(2^n)$

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

$$|\psi\rangle \dashrightarrow \boxed{G} \dashrightarrow |\psi'\rangle = G|\psi\rangle$$

Measure

$$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \dashrightarrow \boxed{\text{Measure}} \xrightarrow{|\alpha_x|^2} |x\rangle$$

Transformation $\mathrm{c\!-\!NOT}$

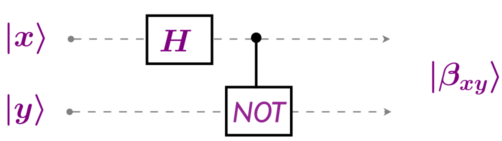
Definition

$$\mathrm{c\!-\!NOT}|0b\rangle = |0b\rangle$$
$$\mathrm{c\!-\!NOT}|1b\rangle = |1\rangle|(1-b)\rangle$$
$$\mathrm{c\!-\!NOT}|ab\rangle = |a\rangle|a\oplus b\rangle$$

$$\mathrm{c\!-\!NOT} = \begin{pmatrix} 1000 \\ 0100 \\ 0001 \\ 0010 \end{pmatrix}$$

Representation

Bell basis change



$$|\beta_{00}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\beta_{01}\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\beta_{11}\rangle = \tfrac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Partial measure: 2-qubit case

Measure of first qubit

- Projectors $P_0 = |00\rangle\langle 00| + |01\rangle\langle 01| = |0\rangle\langle 0| \otimes \mathbf{I_2}$
  $P_1 = |10\rangle\langle 10| + |11\rangle\langle 11| = |1\rangle\langle 1| \otimes \mathbf{I_2}$

$$P_0 \overset{\perp}{\oplus} P_1 = Id$$

- Measure of first qubit

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \dashrightarrow \boxed{\text{Measure 1}}$$

$$\xrightarrow{||P_0|\psi\rangle||^2 = a^2+b^2} \frac{1}{||P_0|\psi\rangle||} P_0|\psi\rangle = |0\rangle \frac{a|0\rangle + b|1\rangle}{\sqrt{a^2+b^2}}$$

$$\xrightarrow{||P_1|\psi\rangle||^2 = c^2+d^2} \frac{1}{||P_1|\psi\rangle||} P_1|\psi\rangle = |1\rangle \frac{c|0\rangle + d|1\rangle}{\sqrt{c^2+d^2}}$$

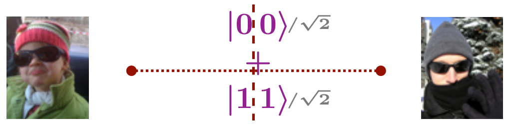
Interpretation

- Partial measure project to a subspace compatible with the observation
  Probability = square norm of the projection
  Outcome = renormalization of the projection

EPR paradox

Protocol

- Assume Alice & Bob shares an EPR state: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  Alice has the first qubit, and Bob the second one



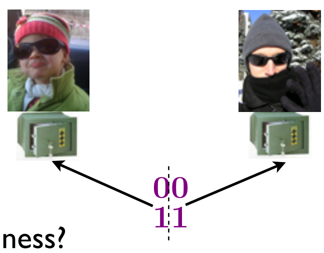
- Alice & Bob observe their qubit and respectively get bit *a,b*

Fact

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

Classical analogue?

- Shared randomness model:
  Alice and Bob has access to shared random bits
  → Non product distribution:
  00 with prob. 1/2 and 11 with prob. 1/2



- Can we simulate quantum physic using shared randomness?

Bell-CHSH inequality as a classical game

Game

- Alain and Bob share some initial information but cannot communicate
- Alain receives a random bit *x*, Bob *y*
- Alain returns a bit *a*, Bob *b*

- Goal: maximize $p = \Pr_{x,y}(a \oplus b = x \wedge y)$

$\wedge$	0	1
0	0	0
1	0	1

$\oplus$	0	1
0	0	1
1	1	0

Classically: CHSH inequality [1969]

- Best deterministic strategy: $a = b = 0 \implies p = \frac{3}{4}$
- Theorem: the best probabilistic strategy is not better than the best deterministic strategy

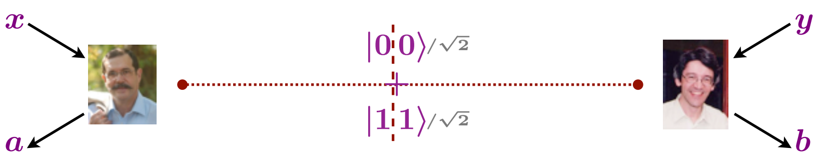
Bell-CHSH inequality as a quantum game

Reminder

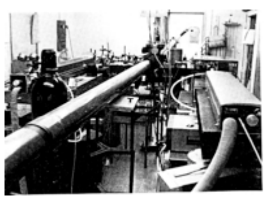
- Goal: maximize $p = \Pr_{x,y}(a \oplus b = x \wedge y)$

Quantumly

- Alain and Bob share an EPR state



- Bob performs a rotation of angle $\frac{\pi}{8}$
- If $x = 1$, Alain performs a rotation of angle $\frac{\pi}{4}$
- If $y = 1$, Bob performs a rotation of angle $-\frac{\pi}{4}$
- Alain et Bob observe their qubit and send their respective outcomes
- Theorem: $p = \cos^2(\frac{\pi}{8}) \approx 0.85$

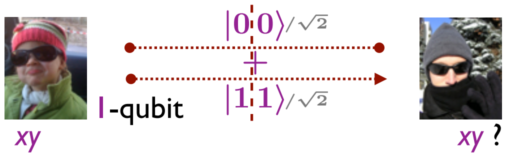


Realization: [Aspect-Grangier-Roger-Dalibard: Orsay'82]

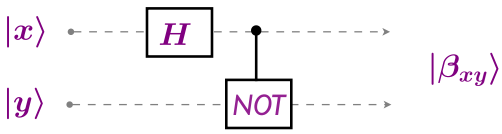
Superdense coding [1992]

Problem

- Alice & Bob share an EPR state: $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Alice wants to send two bits xy to Bob
- But Alice can only send one qubit to Bob



Bell basis change



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

Protocol

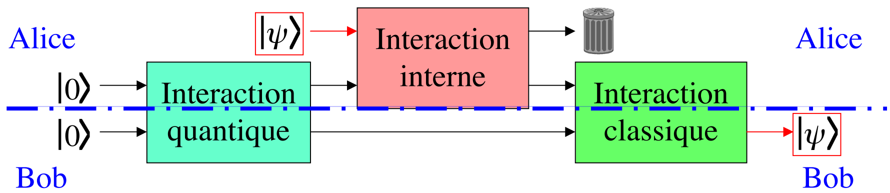
- Alice applies to its qubit *NOT*, if y=1; and *FLIP*, if x=1 $\quad FLIP = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
- Alice sends its qubit to Bob
- Bob performs the inverse of the Bell basis change, and observes xy

Quantum teleportation

Problem

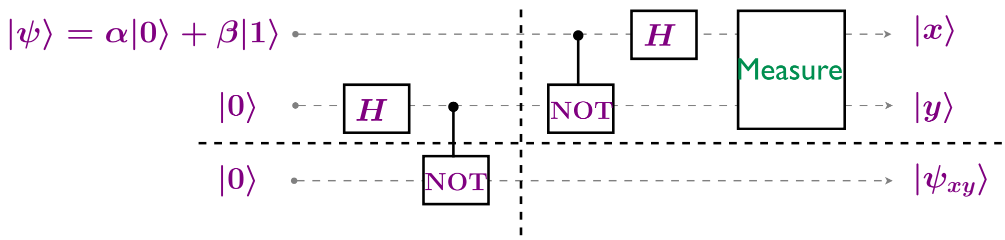
- Alice wants to transmet a qubit $|\psi\rangle$ to Bob
- Bob: far and unknown position to Alice

Realization



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

Circuit



Exercise

- Compute the state of the system before the measure
- Write the qubit state $|\psi_{xy}\rangle$ as a function of observed values *x,y*
- Explain the end of the protocol

Realizations

- 1 photon [Zeilinger et al : Innsbruck'97]
- 1 photon, 6 km [Gisin et al : Genève'02]
- 1 atome [Blatt et al : Innsbruck'04]
- Today: over 100km

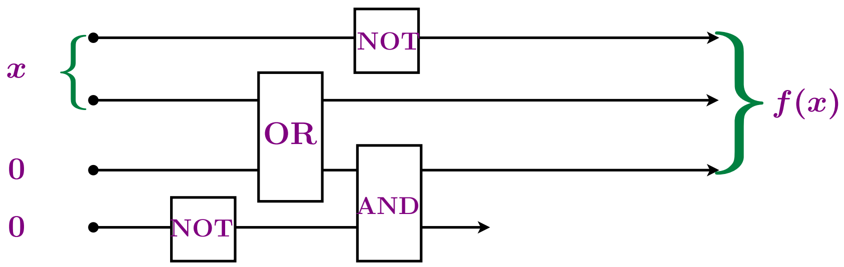
Gates

- A gate *C* is a function on at most **3** qubits

  Example: AND, OR, NOT, ...

Circuit

- A circuit is a sequence of gates $C = C_L \dots C_2 C_1$
- 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

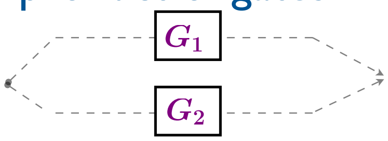
- Any function can be computed by a circuit using only NOT, OR, AND gates

Gates $\quad U \in \mathcal{U}(2^k), \quad k = 1, 2, 3$

- A quantum gate is a unitary map that acts upon at most **3** qubits

Tensor product of gates

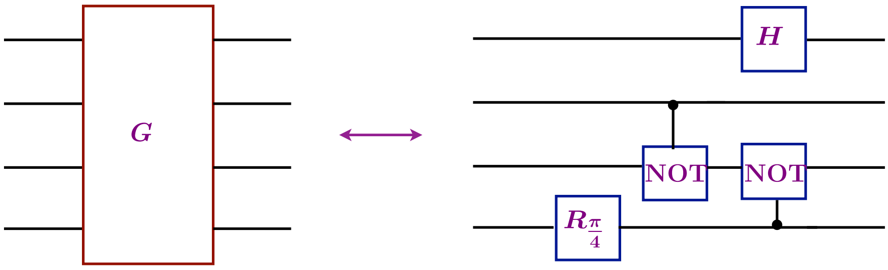
$|\psi_1\rangle|\psi_2\rangle$



$(G_1 \otimes G_2)|\psi_1\rangle|\psi_2\rangle = (G_1|\psi_1\rangle)(G_2|\psi_2\rangle)$

Circuit

- A quantum circuit is a sequence of gates (extended by $\otimes$ Id)



Theorem

- Any unitary can be realized exactly by a circuit
  and approximated using only gates c-NOT and $\sqrt{}$H

Normal form

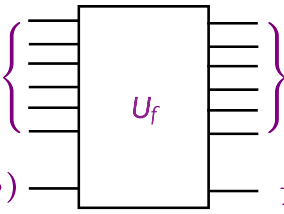
- Function: $f : \{0,1\}^n \to \{0,1\}^m$
- Circuit: $U_f : |x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$
  $|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$

Circuit for S_f

- Boolean function: $f : \{0,1\}^n \to \{0,1\}$
- Ancilla: $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Circuit:

$|x\rangle$

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



$|x\rangle$

$\frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle)$

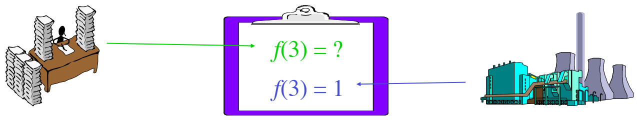
$= \frac{(-1)^{f(x)}}{\sqrt{2}}(|0\rangle - |1\rangle)$

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

A first quantum algorithm [1992]

Deutsch-Jozsa problem

- Oracle input: $f : \{0, 1\}^n \to \{0, 1\}$ 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 ($n=1$)

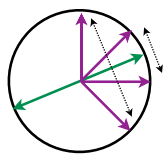
 $x \mapsto f(x)$ can be nonreversible!

Reversible implementation of f

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

Hadamard gate: half-wave blade at 22,5°

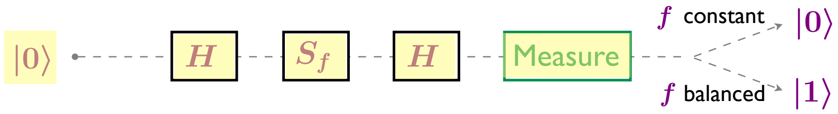
$$|b\rangle \dashrightarrow \boxed{H} \dashrightarrow \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$



Quantum circuit

$$|0\rangle \dashrightarrow \boxed{H} - \boxed{S_f} - \boxed{H} - \boxed{\text{Measure}} \dashrightarrow ?$$

Analysis (n=1)



Initialization: $|0\rangle$

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

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

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

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

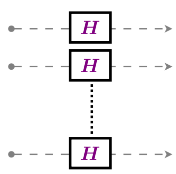
General solution for Deutsh-Jozsa

Reversible implementation of f

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

Quantum Fourier transform

$QFT_n \equiv$

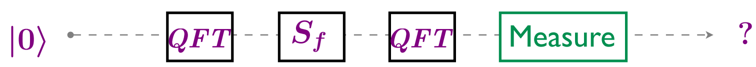


$$|b\rangle \;\text{---}\; \boxed{H} \;\text{---}\!\!\rightarrow \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$$

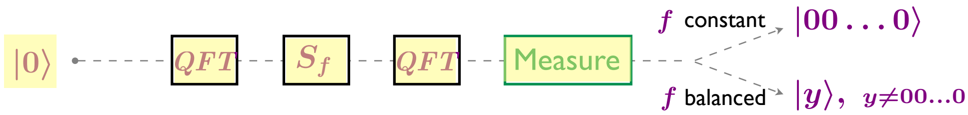
$$QFT_n|x\rangle = \frac{1}{2^{n/2}}\sum_y (-1)^{x\cdot y}|y\rangle$$

where $x \cdot y = \sum_i x_i y_i \mod 2$

Quantum circuit



Analysis



Initialization: $|00\ldots0\rangle$

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

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

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

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

Bernstein-Vazirani

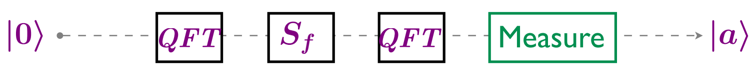
Problem

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

Query complexity

- Randomized: n
  Query $f(0^{i-1}10^{n-i})=a_i$, for $i=1,2,\ldots,n$
- Quantum: 1

Quatum circuit



Analysis

$$|0\rangle \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{S_f} \dashrightarrow \boxed{QFT} \dashrightarrow \boxed{\text{Measure}} \dashrightarrow |a\rangle$$

Initialization: $|00\ldots0\rangle$

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

Query to *f*: $\frac{1}{2^{n/2}} \sum_{x\in\{0,1\}^n} (-1)^{a\cdot x}|x\rangle = QFT|a\rangle$

Interferences: $QFT^2|a\rangle$

Final state: $|a\rangle$

On the difficulty of fatorizing

RSA Challenges

- http://www.rsasecurity.com/rsalabs

Challenge Number	Prize ($US)	Status	Submission Date	Submitter(s)
RSA-576	$10,000	Factored	December 3, 2003	J. Franke et al.
RSA-640	$20,000	Factored	November 2, 2005	F. Bahr et al.
RSA-704	$30,000	Not Factored		
RSA-768	$50,000	Not Factored		
RSA-896	$75,000	Not Factored		
RSA-1024	$100,000	Not Factored		
RSA-1536	$150,000	Not Factored		
RSA-2048	$200,000	Not Factored		

- RSA-640 (193 digits) :

  31074182404900437213507500358885679300373460228427275457201619488232064405180815045563468296717232867824379162728380334154710731085019195485290073377248227835257423864540146917366024776523466 09

  =

  16347336458092538484431338838650908598417836700330923121811108523893331001045081512121181675115 79

  x

  1900871281664822113126851573935413975471896789968515493666638539088027103802104498957191261465571

- RSA Algorithm (allows private communication)

  security based on the difficulty of factorizing

Theorem [Simon-Shor'94]

- Finding the period of *any* function on an abelian group can be done in quantum time 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 $a^q = 1 \mod n$
- Reduction to period finding: the period of $x \to a^x \mod n$ is q

Factorization

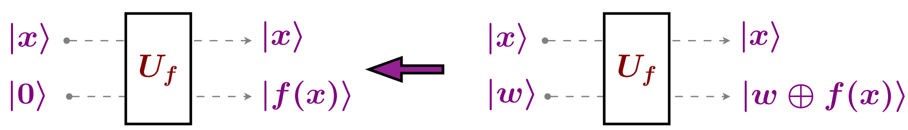
- Input: integer n
- Output: a nontrivial divisor of n

Reduction : Factorization $\leq_R$ Order finding

- Check that gcd(a,n)=1
- Compute the order q of $a \mod n$
- Restart if q is odd or $a^{q/2} \neq -1 \mod n$
- Otherwise $(a^{q/2} - 1)(a^{q/2} + 1) = 0 \mod n$
- Return gcd($a^{q/2} \pm 1, n$)

Problem

- Oracle input: $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ a black-box function



such that $\exists s \in \{0,1\}^n : \forall x \neq y,\ f(x) = f(y) \iff y = x \oplus s$

- Output: the period s

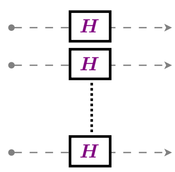
Complexity

- Randomized: $2^{\Omega(n)}$ queries
- Quantum: O(n) queries and time O(n^3)

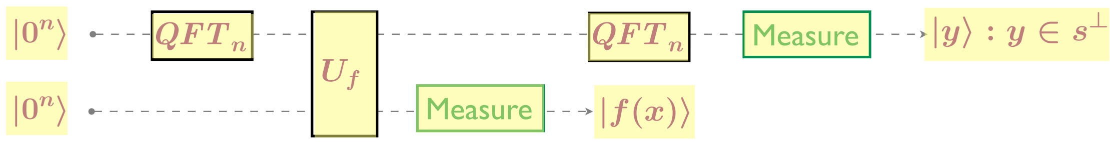
Idea

- Use a Fourier transformation: $QFT_n|x\rangle = \frac{1}{2^{n/2}} \sum_y (-1)^{x \cdot y} |y\rangle$
  where $x \cdot y = \sum_i x_i y_i \mod 2$
- Realization of QFT_n using Hadamard gates:

$$|b\rangle \xrightarrow{\boxed{H}} \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle) \qquad QFT_n \equiv$$



Quantum solution



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

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

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

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

Partial measure: project to a subspace compatible with the observation

Probability = square norm of the projection

Outcome = renormalization of the projection

Interferences:

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

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

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

Finding the period

Construction of a linear system

- After $n+k$ iterations: $y^1, y^2, \ldots, y^{n+k} \in s^\perp$
- s is solution of the linear system in t:

$$\left\{\begin{array}{r} y^1 \cdot t = 0 \\ y^2 \cdot t = 0 \\ \vdots \\ y^{n+k} \cdot t = 0 \end{array}\right. \quad \leftrightarrow \quad \left\{\begin{array}{r} y_1^1 t_1 + y_2^1 t_2 + \ldots + y_n^1 t_n = 0 \\ y_1^2 t_1 + y_2^2 t_2 + \ldots + y_n^2 t_n = 0 \\ \vdots \\ y_1^{n+k} t_1 + y_2^{n+k} t_2 + \ldots + y_n^{n+k} t_n = 0 \end{array}\right.$$

- If $s=0^n$ the y^i are of rank n with proba $\geq 1-1/2^k$
- If $s\neq 0^n$ the y^i are of rank $n-1$ with proba $\geq 1-1/2^{k+1}$
- System solutions: 0^n and s

Complexity

- Constructing the system: $O(n)$ queries, time $O(n)$
- Solving the system: no query, time $O(n^3)$

More difficult…

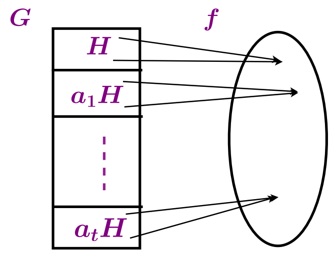
Period Finding(G)

- Oracle input: function f on G such that

  f is *strictly* periodic for some unknown $H \leq G$:

$$f(x) = f(y) \iff y \in xH$$

- 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: $G = \mathbb{Z}^2,\ H = \{(rx, x) : x \in \mathbb{Z}\}$
- Pell's equations: $G = \mathbb{R}$
- Graph Isomorphism: $G = \mathcal{S}_n$

Quantum polynomial time algorithms (in log|G|)

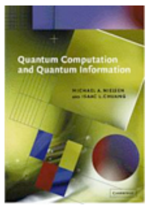
- Abelian groups G: *QFT*-based algorithm [1995]
- Normal period groups H: *QFT*-based algorithm [2000]
- Solvable groups G of constant exponent and constant length [2003]
- …

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

- Authors: A. Yu. Kitaev, A. H. Shen, M. N. Vyalyi
- Editor: American Mathematical Society
- Collection: Graduate Studies in Mathematics

Lecture Notes for Quantum Computation

- Author: John Preskill
- Website: http://www.theory.caltech.edu/~preskill/ph229/

Quantum proofs for classical theorems

- Author: Andrew Drucker, Ronald de Wolf
- Website: http://arxiv.org/abs/0910.3376