Quantum information and applications

Sophie Laplante – Frédéric Magniez

2021 – 2022

Contents

Part I
Sophie Laplante

1 Introduction

1.1 Qbits

- A classical bit is a variable $b \in \{0,1\}$.
- A random bit is a random variable $r \in [0,1]^2$ with $r_0 + r_1 = 1$, by L_1 normalization.
- A quantum bit, or qubit, is a complex pair $q \in \mathbb{C}^2$ with $|q_0|^2 + |q_1|^2 = 1$, by L_2 normalization.

Definition 1.1 Hilbert space

A Hilbert space $\mathcal{H}_N$ is a N-dimensional complex innerproduct space with a norm induced by innerproduct.

Where

Definition 1.2 Complex innerproduct

The complex innerproduct of u, v is $\langle u, v\rangle = u^\dagger v$, where $\dagger$ is the conjugate transpose operator.
The norm induced is $\|u\| := \sqrt{\langle u, u\rangle}$.

We use Dirac's notation "bra-ket" $\langle \dots \rangle$.
For the column vectors: $|\psi\rangle$
And for the row vectors: $\langle\, \phi \,| := |\phi\rangle^\dagger$.

One qubit is 2 complex normalized numbers. It is a 2 dimensional vector $u = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, with $\alpha, \beta \in \mathbb{C}$.

A computational basis is $B = \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\}$.

Example 1.1

If $u = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$, we have that $\|u\| = 1$, and in Dirac's notation, $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ so $u = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

- Two classical bits represents 4 configurations: $x \in \{0,1\}^2$.
- Two random bits reprensents 4 configurations, and each has some probability of occuring: $R \in [0,1]^4$ with $\sum_i R_i = 1$.
- For two qubits: $Q \in \mathbb{C}^4$ with $\sum_i |Q_i|^2 = 1$.

In Dirac's notation, a basis is $B = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. We also write in binary: $B = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, with $|x\rangle$ being a vector full of 0 except in the row x where there is a 1.

Example 1.2

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 1/\sqrt{2} \end{pmatrix}$$

1.2 Measurements

- In a classical system, measurements don't affect the description of the system.
- In a random system, with $r \in [0,1]^2$, observing the random bit makes it "collapse": it changes our knowledge of the state and therefore its description.
- In a quantum system, the measurement causes the system to "collapse".

  If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then the measurement in the standard basis will change the system. With probability $|\alpha|^2$ the outcome is 0 and the state changes to $|0\rangle$, and with probability $|\beta|^2$ the outcome is 1 and the state changes to $|1\rangle$.

Definition 1.3 Tensor product

The tensor product $A \otimes B$ is a product block by block.
For example with $A = \begin{pmatrix} u & v \\ w & x \end{pmatrix}$, $A \otimes B = \begin{pmatrix} uB & vB \\ wB & xB \end{pmatrix}$.

Here, for a n qubit $|\varphi\rangle \in \mathbb{C}^{2^n}$, a basis can be given by

$$\{|b_1\rangle \otimes ... \otimes |b_n\rangle \,|\, b_i \in \{0,1\}\}.$$

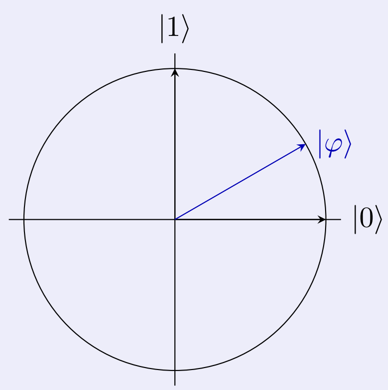
So we have a computational basis:

$$\{|b_0 b_1 ... b_{n-1}\rangle \,|\, b_i \in \{0,1\}\}.$$

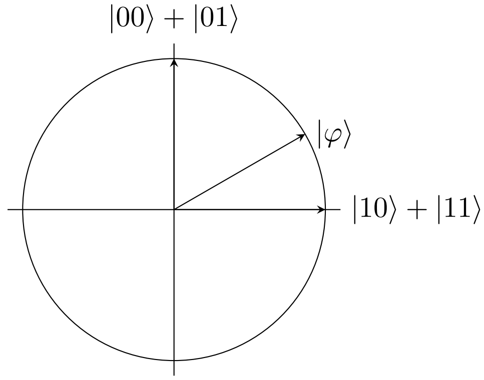
these are also written $|i\rangle$ with $0 \leqslant i \leqslant 2^n - 1$.

Definition 1.4 Measurement

If $|\varphi\rangle \in \mathcal{H}_N$, and we have a (orthonormal) basis $\mathcal{B} = \{|B_1\rangle, ..., |B_N\rangle\}$, then measuring $|\varphi\rangle$ in $\mathcal{B}$, the outcome will be i with probability $|\langle\varphi \,|\, B_i\rangle|^2$, and the state after measurement is $|B_i\rangle$.



It is also possible to perform partial measurements.
For a 2-qubit system, $|\varphi\rangle = \underbrace{a_{00}|00\rangle + a_{01}|01\rangle}_{\text{1st qubit is 0}} + \underbrace{a_{10}|10\rangle + a_{11}|11\rangle}_{\text{1st qubit is 1}}$



The measurement of the first qubit will project onto one of the two orthogonal subspaces: $\mathrm{span}\{|00\rangle, |01\rangle\}$ and $\mathrm{span}\{|10\rangle, |11\rangle\}$.

With a probability $|a_{00}|^2 + |a_{01}|^2$ it projects onto $\dfrac{|0\rangle \otimes (a_{00}|0\rangle + a_{01}|1\rangle)}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}$.

Example 1.3

Let $|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.
Measuring the first qubits gives with probability $(\frac{1}{\sqrt{2}})^2$ the outcome 0 and the state collapses to $\dfrac{1/\sqrt{2}|00\rangle}{1/\sqrt{2}} = |00\rangle$.

1.3 Bipartite systems

Consider a state $|\psi\rangle$ of $2n$ qubits shared by 2 players A and B.

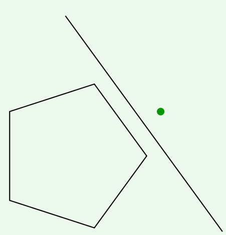
Definition 1.5 Separability

$|\psi\rangle$ is separable iff $\exists |\psi_A\rangle \in \mathcal{H}_{2^n}, |\psi_B\rangle \in \mathcal{H}_{2^n}, |\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$.
Otherwise, $|\psi\rangle$ is said to be entangled.

This is similar to a probability distribution having two random variables (X, Y) being independent.

Application 1.1 Entanglement $\neq$ correlation

The article from Einstein, Podelsky and Rosen of 1935 asks if quantum mechanics is complete.
In 1963, Bell, in order to demonstrate that nature is not just driven by probabilities, drove an experiment whose observations are a probability distribution, and showed that this probability distribution does not live in the space of distributions that have a classical explanation.



1.4 EPR paradox

Definition 1.6 "EPR paradox" (version of Bohm in 1951)

Two players share $|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$, and play the following game.
A gets a bit $x \in \{0, 1\}$ and measures the first qubit and gets an outcome $a \in \{0, 1\}$. Similarly, B gets $y \in \{0, 1\}$ and measures $b \in \{0, 1\}$.

If $x = y = 1$ they win if $a \neq b$. If x or $y = 0$ then they win if $a = b$.

NB

A strategy is a random source R and two deterministic functions $A(r_A, x) \mapsto 0$ or 1 and $B(r_B, y) \mapsto 0$ or 1.

The ressources allowed in a classical game are a shared random source of classical correlation: $r_A, r_B \sim R$, independent of the input x and y.

In the quantum settings they share some entangled bipartite state $|\psi_{AB}\rangle$.

Theorem 1.1

Any classical strategy wins with probability $\leqslant \frac{3}{4}$.
The best deterministic strategy (fixing r_A and r_B) is for A and B to always output 0. They win with probability $\leqslant \frac{3}{4}$.

So any general strategy is a mixture of deterministic strategies and cannot win with probability $> \frac{3}{4}$.

Theorem 1.2

There exists a quantum strategy that wins the game with probability $\approx 0.85 \gg \frac{3}{4}$.

Proof of theorem 1.2.

Suppose A and B share a state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. They win if $a \oplus b = x \wedge y$.
A will apply a rotation to her qubit:

$$R_{\theta_A} = \begin{pmatrix} \cos\theta_A & -\sin\theta_A \\ \sin\theta_A & \cos\theta_A \end{pmatrix}$$

Similarly, B applies a rotation R_{θ_B}.
Globally,

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \to \frac{1}{\sqrt{2}} R_{\theta_A} \otimes R_{\theta_B}(|00\rangle - |11\rangle)$$

$$\begin{aligned} |\psi_{00}\rangle &= (R_{\theta_A} \otimes R_{\theta_B})(|0\rangle \otimes |0\rangle) \\ &= R_{\theta_A}|0\rangle \otimes R_{\theta_B}|0\rangle \\ &= (\cos\theta_A|0\rangle + \sin\theta_A|1\rangle) \otimes (\cos\theta_B|0\rangle + \sin\theta_B|1\rangle) \end{aligned}$$

$$\begin{aligned} |\psi_{11}\rangle &= (R_{\theta_A} \otimes R_{\theta_B})|11\rangle \\ &= (-\sin\theta_A|0\rangle + \cos\theta_A|1\rangle) \otimes (-\sin\theta_B|0\rangle + \cos\theta_B|1\rangle) \end{aligned}$$

$$\begin{aligned} \frac{1}{\sqrt{2}}(|\psi_{00}\rangle - |\psi_{11}\rangle) &= \frac{1}{\sqrt{2}}\big[(\cos\theta_A\cos\theta_B - \sin\theta_A\sin\theta_B)|00\rangle \\ &\quad + (\sin\theta_A\sin\theta_B - \cos\theta_A\cos\theta_B)|11\rangle \\ &\quad + \ldots\big] \\ &= \frac{1}{\sqrt{2}}\big[\cos(\theta_A + \theta_B)|00\rangle - \cos(\theta_A + \theta_B)|11\rangle + \ldots\big] \\ &= \frac{1}{\sqrt{2}}\big(\cos(\theta_A + \theta_B)[|00\rangle - |11\rangle] \\ &\quad + \sin(\theta_A + \theta_B)[|01\rangle + |10\rangle]\big) \end{aligned}$$

Then they measure both qubits.

$$\mathbb{P}(\text{outcome is } 00) = \frac{1}{2}\cos^2(\theta_A + \theta_B)$$
$$\dots$$
$$\mathbb{P}(\text{outcome is } 01) = \frac{1}{2}\sin^2(\theta_A + \theta_B)$$

So $\mathbb{P}(a = b) = \cos^2(\theta_A + \theta_B)$.

	$y = 0$, $\theta_B = \frac{-\pi}{16}$	$y = 1$, $\theta_B = \frac{3\pi}{16}$
$x = 0$, $\theta_A = \frac{-\pi}{16}$	win if $a = b$, $\frac{-\pi}{8}$	win if $a = b$, $\frac{\pi}{8}$
$x = 1$, $\theta_A = \frac{3\pi}{16}$	win if $a = b$, $\frac{\pi}{8}$	win if $a \neq b$, $\frac{3\pi}{8}$

These values for θ_a and θ_B give the best probability to win.

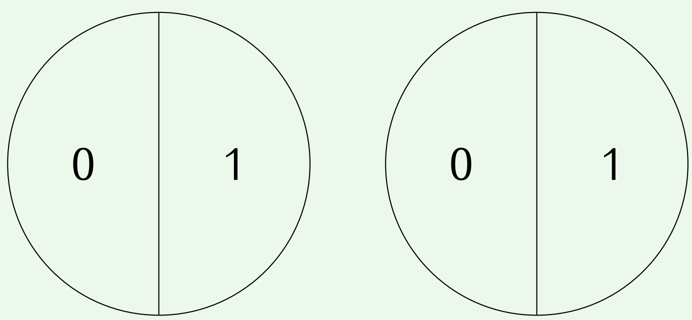
cskifo

Theorem 1.3 **(Tsirelson).**

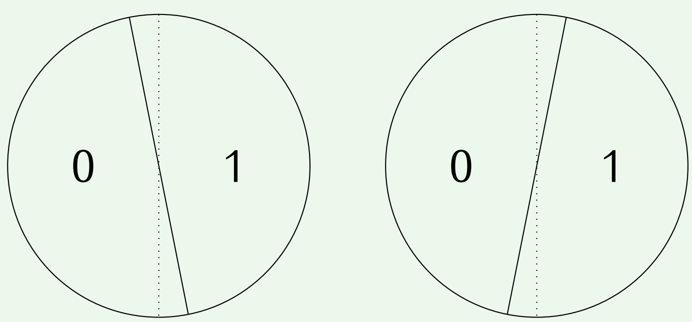
There is no better quantum strategy to win this game.

Illustration

Originally the qubits are the same.



But after the rotation



2 Evolution, circuits, superdense coding, teleportation

2.1 Evolution

- In the classical randomised case, the operations are applied on probabilistic vectors and maintain the L_1 norm. These are stochastic matrices.

- In the quantum case, we use unitary matrices.

Definition 2.1 **Unitary matrices**

U is unitary iff $U^tU = I$, or equivalently $\forall x, \|Ux\|_2 = \|x\|_2$.

If we restrict to real number, these are orthogonal matrices.

Example 2.1 **Hadamard matrix**

The Hadamard matrix is defined by $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.
Then $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Exercise 2.1

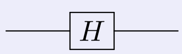
1. Compute $H \otimes H$.
2. Generalize to $H^{\otimes n} = \underbrace{H \otimes ... \otimes H}_{n \text{ times}}$.
3. Compute $H^{\otimes n}|0...0\rangle$ and $H^{\otimes n}|x_1...x_n\rangle$.

2.2 Circuits

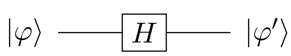
It is not easy to use quantum Turing machine because we could be in a superposition of terminal and non terminal states. Therefore we work more on circuits. However circuits can solve undecidable problems, so a constraint on them will be that a Turing machine must be able to generate it.

Definition 2.2 **Hadamard gate**

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



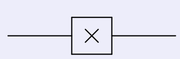
The circuit



computes $|\varphi'\rangle = H|\varphi\rangle$.

Definition 2.3 **Not gate**

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



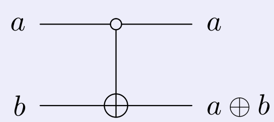
Definition 2.4 Phase flip

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

Definition 2.5 Cnot gate

$$|a, b\rangle \mapsto |a, b \oplus a\rangle$$

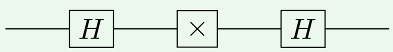


Exercise 2.2

Write out the corresponding unitary matrix.

Exercise 2.3

Compute the output of



2.3 Superdense coding (Bennet & Wiesner (1992))

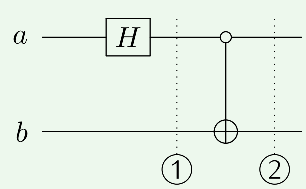
Superdense coding is a protocol in which A conveys two classical bits to B by sending one qubit to B.

They share a bipartite state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ before the protocol begins.

Theorem 2.1 Holevo's theorem (1973)

You cannot encode more than n classical bits on n qubits.

Example 2.2



For the first step:

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

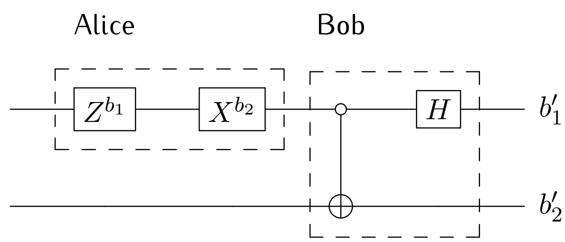
$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Definition 2.6 **Bell states**

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

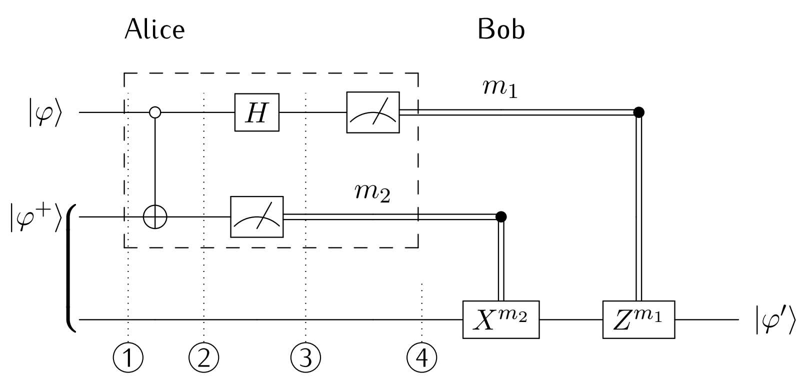
A wants to send the bits b_1 and b_2 to B.
With $Z^b = Z$ if $b = 1$ and I otherwise, the protocol is the following.



We have that $b_1 = b'_1$ and $b_2 = b'_2$.

2.4 Teleportation (Bennet, Brassard, Crépeau, Jozsa, Peres, Wooters (1993))

A has a qubit $|\varphi\rangle$. She wants to transmit it to B using two classical bits and one ebit (B shares an entagled pair prior to the protocol).



Result 2.2

$|\varphi'\rangle = |\varphi\rangle$

Proof of result 2.2.

1. $|\varphi\rangle \otimes |\varphi^+\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle)$
2. $= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$
3. $= \frac{1}{2}(\alpha|000\rangle + \beta|001\rangle + \alpha|100\rangle + \beta|101\rangle + \alpha|011\rangle + \beta|010\rangle + \alpha|111\rangle + \beta|110\rangle)$

Voilà !

2.5 (Simplified) Holevo's theorem

Definition 2.7 Shannon entropy

Let X be a random variable with distribution over outcomes $\{p_1, ..., p_n\}$.
The Shannon entropy $H(X)$ is defined by

$$H(x) = \sum_{i=1}^{n} -p_i \log_2(p_i).$$

Definition 2.8 Mutual information

Let X and Y be random variables.
The mutual information $I(X:Y)$ is defined by

$$I(X:Y) = H(X) - H(X \mid Y).$$

It measures how correlated the variables are.

Property 2.3

$I(X:Y) = I(Y:X)$

Definition 2.9 Density matrix

For a source of quantum states $\xi = \{(|\varphi_i\rangle, p_i)\}$, the mathematical representation of such a state is a density matrix

$$\rho = \sum p_i |\varphi_i\rangle\langle\varphi_i|.$$

ρ here is a "mixed" quantum state.

Example 2.3

If the $|\varphi_i\rangle$ are basis elements then the corresponding density matrix is diagonal with trace 1.

Definition 2.10 Von Neumann entropy

The von Neumann entropy $S(\rho)$ of a density matrix is defined as

$$S(\rho) = -\mathrm{Tr}(\rho \ln(\rho))$$

This can be defined since the density matrices are positive semi-definite and have trace 1, so $\mathrm{Tr}(\rho \ln(\rho))$ means that we take the spectrum $\lambda_1, ..., \lambda_n$,

$$S(\rho) = -\sum_{i=1}^{n} \lambda_i \ln(\lambda_i).$$

Definition 2.11 (Holevo) Accessible information

For any ensemble[a] $\xi = \{(|\varphi_i\rangle, p_i)\}$, the accessible information $\chi(\xi)$ is defined by

$$\chi(\xi) = S(\rho) - \sum_i p_i S(|\varphi_i\rangle\langle\varphi_i|).$$

[a] It is a probability distribution.

Exercise 2.4

Prove that for any pure quantum state φ, $S(|\varphi\rangle\langle\varphi|) = 0$.

It means that for these simple ensembles consisting of distributions over pures states, the accessible information is just $S(\rho)$. In this simplified case, $\chi(\xi)$ is just $S(\rho)$.

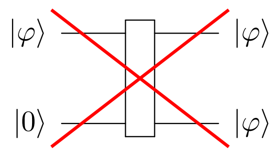
Theorem 2.4 Simplified Holevo's theorem

If $X \sim (p_1, ..., p_n)$ (representing a source of symbols $1, ..., n$), and i is encoded as a pure quantum state $|\varphi_i\rangle$ so that $\rho = \sum_i p_i |\varphi_i \times \varphi_i|$ is the mixed state corresponding to sending $|\varphi_i\rangle$ with probability p_i.
The receiver gets ρ and wants to recover i by making a measurement. Let Y be the outcome of the measurement.
Then $I(X : Y) \leqslant \chi(\xi) = O(\log(\text{dimension of the space}))$.

2.6 No cloning theorem

Theorem 2.5

There is no unitary u that can copy qubits: $\forall|\varphi\rangle, u(|\varphi\rangle_n \otimes |0\rangle_n) = |\varphi\rangle \otimes |\varphi\rangle$.



Proof of theorem 2.5.

Assume such a u exists. Then $u|0\rangle|0\rangle = |0\rangle|0\rangle$ and $u|1\rangle|0\rangle = |1\rangle|1\rangle$, therefore

$$\begin{aligned} u(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle) &= \frac{1}{\sqrt{2}}u(|00\rangle) + \frac{1}{\sqrt{2}}u|10\rangle \\ &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &\neq \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \end{aligned}$$

C'est ce que je voulais !

3 Quantum complexity classes

Definition 3.1 Circuit definition of $\mathbf{P}$

$L \in \mathbf{P}$ iff there exists a uniform[a] family of polynomial-sized circuits $\mathcal{C} = \{C_n\}_{n \geqslant 0}$, where n is the input length, such that $\forall n, \forall x \in \Sigma^n, x \in L \iff C_{|x|}(x) = 1$.

[a] There exists a polynomial-time Turing machine taking n in unary and producing the circuit.

Definition 3.2 Circuit definition of $\mathbf{BPP}$

$L \in \mathbf{BPP}$ iff there exists a uniform polynomial-size circuit family $\mathcal{C} = \{C_n\}_{n \geqslant 0}$ with C_n having 2 inputs, x of length n and r of length $n^{O(1)}$, and such that

- $x \in L \implies \mathbb{P}_r(C_{|x|}(x, r) = 1) \geqslant \frac{2}{3}$
- $x \notin L \implies \mathbb{P}_r(C_{|x|}(x, r) = 1) \leqslant \frac{1}{3}$

Definition 3.3 $\mathbf{BQP}$

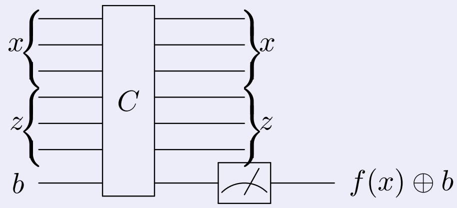
$L \in \mathbf{BQP}$ iff there exists a uniform polynomial-size circuit $\mathcal{Q} = \{C_n\}_{n \geqslant 0}$ such that

- $\forall x \in L, \mathbb{P}(C_n \underbrace{|x\rangle}_{\text{input}} \underbrace{|0\rangle}_{\text{ancilla}} = 1) \geqslant \frac{2}{3}$

- $\forall x \notin L, \mathbb{P}(C_n \underbrace{|x\rangle}_{\text{input}} \underbrace{|0\rangle}_{\text{ancilla}} = 1) \leqslant \frac{1}{3}$

Definition 3.4 **Quantum circuit**

A quantum circuit C computes a (boolean) function f if it is in the following form:

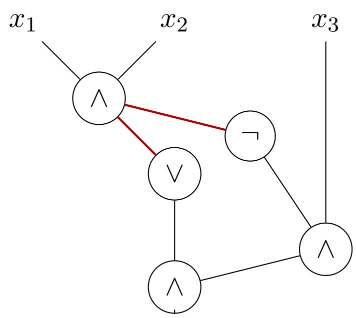


Theorem 3.1 **Bernstein-Vazirani**

$\mathbf{BPP} \subseteq \mathbf{BQP}$

Proof of theorem 3.1.

There are many problems to overcome when converting classical circuit to quantum ones, in partical how to deal with inputs and gate results needing to be used multiple times.



Also, the circuit is not reversible (not computing a unitary) and not in normal form as required.
The solution is to use reversible Turing machines or reversible computation, which was introduced via thermodynamics of computation.

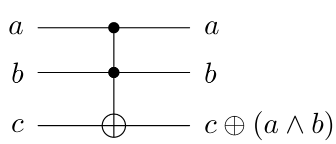
Result 3.2 **Bennet 1989**

Any Turing machine computing in time T and space S can be implemented by a "reversible Turing machine" in time $T^{1+\varepsilon}$ and space $S \log T$.

Result 3.3 **Fredkin and Toffoli, 1982**

Ane circuit of depth d and width w can be simulated by a reversible circuit of depth $d^{1+\varepsilon}$ and width $w \log d$.

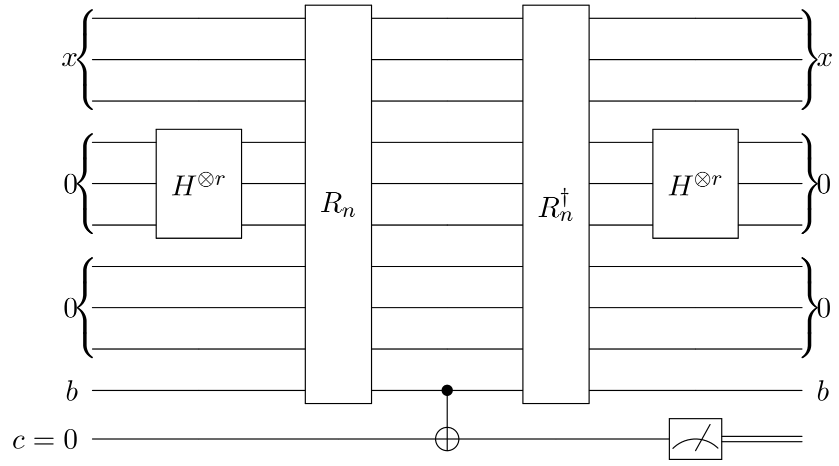
This is done by using the Toffoli gate:



The idea is, with $L \in \mathbf{BPP}$ and $\mathcal{C}$ a circuit family for L,

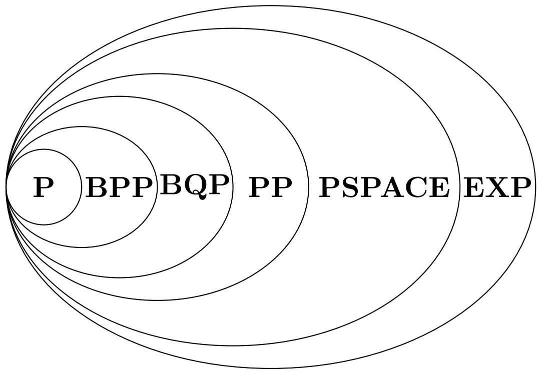
1. Transform C_n into R_n a reversible circuit that computes $R_n(\underbrace{x, r}_{\text{input}}, z, b) = x, r, z, b \oplus C_n(x, r)$

2. Produce "randomness"



It remains to show that the probability that the outcome is correct is greater than $\frac{2}{3}$ for all inputs.

Voilà !



4 Quantum algorithms

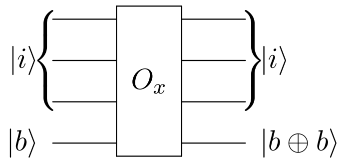
We will study query complexity. The complexity measure is the number of accesses that are made to the input in order to solve a problem.

In the classical query model we consider an input $x_1 ... x_n$.

- Deterministically, we count 1 each time some variable x_i is fetched.
- In randomized algorithm, we count the expected number of times that the special operation $i \mapsto x_i$ is executed. It acts like an oracle.

Definition 4.1 Quantum query model

We are given a unitary O_x.
$O_x|i\rangle|b\rangle = |i\rangle|x_i \oplus b\rangle$



Quantum circuits use an oracle model. The measure of complexity is the number of O_x gates that are used in a circuit.

4.1 Deutsch-Jozra Algorithm

Consider the problem

Problem

Input: $x \in \{0,1\}^N$ with $N = 2^n$.
Promise: one of the 2 cases occurs, with w_H the Hamming weight:

1. $w_H(x) \in \{0, N\}$
2. $w_H(x) = \frac{N}{2}$

i.e., x is either constant or balanced.
Output: which case was given as input.

Result 4.1 **Lower bounds**

- Any deterministic algorithm must query at least $\frac{N}{2} + 1$ bits of the input.
- For randomized algorithms, if k queries are made, then the error is at least 2^{-k}.
- There is a quantum algorithm that makes no error and uses two quantum queries.

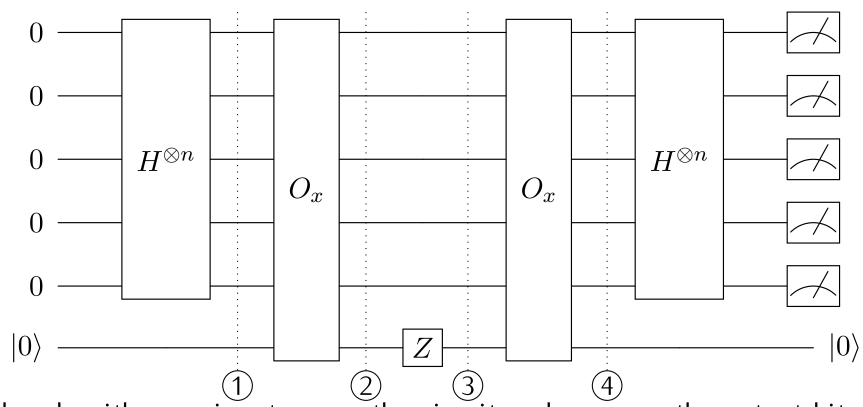
Proof of result 4.1.

Proposition 4.2

$$H^{\otimes n}|0...0\rangle = \frac{\frac{1}{\sqrt{2}}}{\sum_{x \in \{0,1\}^n}} |x\rangle$$

$$H^{\otimes n}|x_1...x_n\rangle = \frac{\frac{1}{\sqrt{2}}}{\sum_{x \in \{0,1\}^n}} (-1)^{x \cdot z}|x\rangle$$

where $x \cdot z = \sum_{i=1}^{n} (x_i \cdot z_i) \mod z$.



To complete the algorithm, on input x, run the circuit and measure the output bits. If the output is 0^n return "constant" and else return "balanced".

1. $\left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle\right) \otimes |0\rangle$

2. $\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|x_i\rangle$

3. $\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{x_i}|i\rangle|x_i\rangle$

4. $\left(\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{x_i}|i\rangle\right) \otimes |0\rangle$

Case 1. x is constant.

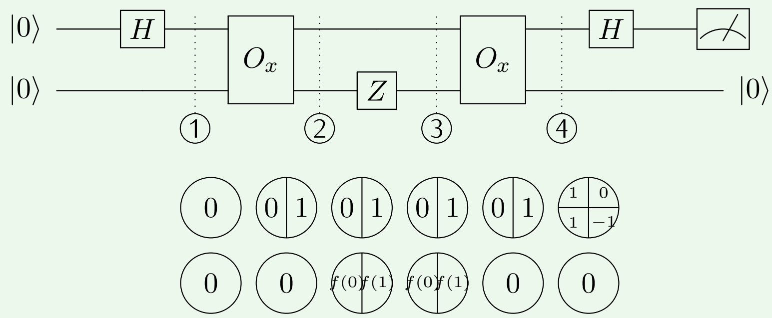
Then 4. is either $|\psi\rangle \otimes 0$ or $-|\psi\rangle \otimes |0\rangle$, with $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum |i\rangle$.
$H^{\otimes n}|\psi\rangle = |0\rangle$ so at the end we measure 0^n.

Case 2. x is balanced.
We claim that 4 $\perp|\psi\rangle$, therefore $H4 \perp H|\psi\rangle$, which means that the probability of measuring 0^n is 0.

$$\begin{aligned}\langle 4 \,|\, \psi\rangle &= \left(\frac{1}{\sqrt{2^n}} \sum_i (-1)^{x_i} |i\rangle\right) \left(\frac{1}{\sqrt{2^n}} \sum_j |j\rangle\right) \\ &= \frac{1}{2^n} \sum_i (-1)^{x_i}\end{aligned}$$

Youpi !

Example 4.1 2 bits string as input



4.2 Bernstein Vazirani

Definition 4.2 Walsh-Hadamard code

$$\begin{array}{rcl}\{0,1\}^n & \longrightarrow & \{0,1\}^{2^n} \\ a & \longmapsto & (a \cdot 0^n, a \cdot 0^{n-1}1, ..., a \cdot 1^n)\end{array}$$

Problem

Input: $x \in \{0,1\}^N$ with $N = 2^n$
Promise: x is a codeword in Walsh-Hadamard code, and $\exists a \in \{0,1\}^n$ such that $x_i = i \cdot a \mod 2$ (with bitwise boolean inner product)
Output: a

Classically, n queries suffice (the numbers of one bit), and n steps are necessary since this is a system of linear equations.

Quantumly, the same circuit as for DJ solves BV.

At the end of the circuit we have 5$= \frac{1}{\sqrt{N}} \sum_{B \in \{0,1\}^n} \left(\sum_i (-1)^{x_i} (-1)^{i \cdot B}\right) |B\rangle|0\rangle$.

Consider the coeff of $|a\rangle$ in 5, $\sum_i (-1)^{x_i} (-1)^{i \cdot a} = 2^n = N$. So all others are 0, and $|a\rangle$ =5.

4.3 Simon's problem and algorithm

Problem

Input: $X = [N]^N$ (a N-tuple of integers in $\{0, ..., N-1\}$) with $N = 2^n$. Think instead of X as a function $f(x) \in \{0,1\}^n$ with $x \in \{0,1\}^n$.

Promise: $\exists a \in \{0,1\}^n$

1. $\forall x, f(x) = f(x \oplus a)$ (with the bitwise XOR)
2. $\forall x \neq y \oplus a, f(x) \neq f(y)$

Example

$f(000) = f(110) = 101$, $x = 000$, $a = 110$, $x \oplus a = 110$, $f(x) = f(x \oplus a) = 101$.
$f(111) = f(001) = 001 \neq 101$.

f matches pairs to the same value, and the pairs depend on a.

Output: a

Theorem 4.3

1. The randomized query complexity is $\Theta(\sqrt{N})$.
2. The quantum query complexity is $\Theta(1)$ for a constant error probability.

Proof sketch for 1.

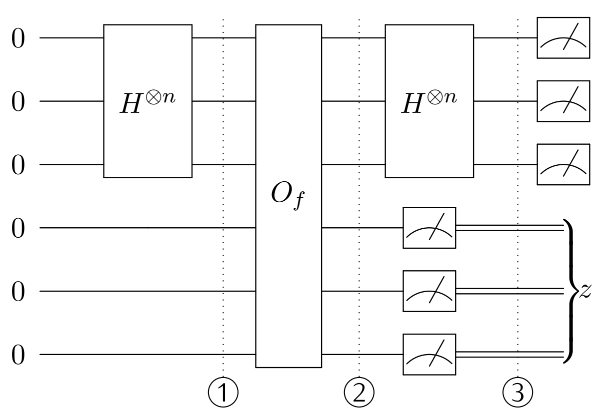
The idea is that the problem cannot be solved unless the algorithm makes two queries to x and y such that $f(x) = f(y)$, so that $a = x \oplus y$.
If the algorithm has made queries $x_1, \ldots, x_k$ such that $f(x_1), \ldots, f(x_k)$ are all distinct, how many possibilities for a are still viable? How many are roled out? $\binom{k}{2}$

$$\begin{aligned}
\mathbb{P}(\text{success in } \leqslant m \text{ queries}) &\leqslant \sum_{k=0}^{m-1} \mathbb{P}(\text{the first } k \text{ queries are distinct and the } k+1 \text{ is a collision}) \\
&\leqslant \sum_{k=0}^{m-1} \frac{k \longleftarrow k \text{ ways to get a collision with } k \text{ prior queries}}{2^n - \binom{k}{2} \longleftarrow \text{number of choices for } a \text{ among the } N - \binom{k}{2} \text{ remaining}} \\
&\leqslant \frac{m^2}{2^n - m^2}
\end{aligned}$$

This implies $m \geqslant \sqrt{2^n}$.

cskifo

Proof (Simon 93-94).



1. $\displaystyle \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle|0\rangle$
2. $\displaystyle \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle$

In Simon's algorithm we have a hidden mask a of unknown $a_1, \ldots, a_n$, and the first iteration has an outcome y such that $a \cdot y \equiv 0 \mod 2$ (with the bitwise inner product). Therefore $n-1$ linearly independent equations suffice to recover a.

At each step, the problem of getting $y^{(k)} \in \mathrm{span}\{y^{(1)}, ..., y^{(k-1)}\}$ increases. After k iterations where all the equations were linearly independent, the probability that the next iteration will not be in the span of the previous ones is $\frac{2^n - 2^k}{2^n} \geqslant \frac{1}{2}$.
Therefore by running this t times the expectancy of number of successful runs is greater than $\frac{t}{2}$. By running it $4k$ times, by Markov inequality, the probability of success is greater than $\frac{3}{4}$.
In fact, a more precise calculation shows that the probability that $k-1$ successive runs all give a linearly independent y is greater than $\frac{1}{4}$. So to get a success probability greater than $\frac{1}{2}$ we run the algorithm 3 times (so a total of $4(k-1)$ runs) and the probability of failing twice is $\left(\frac{3}{4}\right)^3 = \frac{27}{64} < \frac{1}{2}$.

Voilà !

4.4 Grover's search algorithm

Problem

Input: $f : \{0,1\}^n \to \{0,1\}$ (think of it as some $X = \{0,1\}^N$ for $N = 2^n$)
Output: $x \in \{0,1\}^n$ such that $f(x) = 1$ or else, $\perp$

The difficulty of finding 1 depends on the number of solutions.
This problem is often called unstructure search.

Let $M = \#\{x \mid f(x) = 1\}$ be the number of solutions.

- Classicaly, $\Theta(N)$ queries are required.
- Quantumly, $O(\sqrt{N})$ queries suffice to solve with probability $\geqslant \frac{2}{3}$.

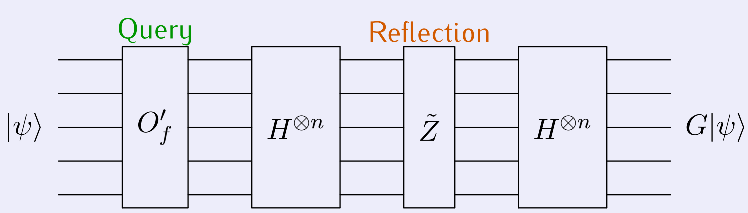
Definition 4.3 **Variant of query unitary**

We used to use $O_f|x\rangle|b\rangle \longmapsto |x\rangle|f(x) \oplus b\rangle$.
Now we use instead $O'_f|x\rangle \longmapsto (-1)^{f(x)}|x\rangle$.

Exercise 4.1

Show that two applications of O_f suffice to implement O'_f.
Hint: look at previous circuits.

Definition 4.4 **First iteration of Grover's algorithm**



where

Definition 4.5 **Gate $\tilde{Z}$**

$\tilde{Z} = 2|0^n\rangle\langle 0^n| - I$ is a conditional phase flip

$$\tilde{Z} : |x\rangle \longmapsto \begin{cases} -|x\rangle & \text{if } x \neq 0^n \\ |x\rangle & \text{if } x = 0^n \end{cases}$$

Definition 4.6

$$|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle = H^{\otimes n}|0^n\rangle$$

Proposition 4.4

$$H^{\otimes} \tilde{Z} H^{\otimes n} = 2|\Psi\rangle\langle\Psi| - I$$

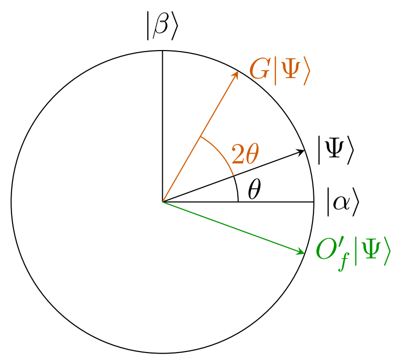
This is a reflection about $|\Psi\rangle$.

Consider

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{\tilde{x}, f(\tilde{x})=0} |\tilde{x}\rangle \quad \text{and} \quad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_{x, f(x)=1} |x\rangle.$$

$|\alpha\rangle$ and $|\beta\rangle$ are orthogonal and $|\Psi\rangle$ is a linear combination of $|\alpha\rangle$ and $|\beta\rangle$:

$$|\Psi\rangle = \frac{1}{\sqrt{N}}^{\sqrt{N-M}} |\alpha\rangle + \frac{1}{\sqrt{N}}^{\sqrt{M}} |\beta\rangle.$$



$$\begin{aligned} O'_f|\Psi\rangle &= O'_f \frac{1}{\sqrt{N}} \sum_x |x\rangle \\ &= \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle \end{aligned}$$

Let's compute θ which is the angle between $|\Psi\rangle$ and $|\alpha\rangle$.

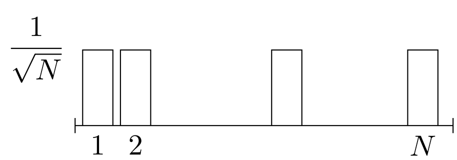
$$\begin{aligned} |\Psi\rangle &= \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle \\ &= \frac{\sqrt{N-M}}{\sqrt{N}}|\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}|\beta\rangle \end{aligned}$$

$\sin\frac{\theta}{2} = \frac{\sqrt{M}}{\sqrt{N}}$ and $\theta = 2\arcsin(\frac{\sqrt{M}}{\sqrt{N}}$, so, roughly, when M is small, $\frac{\theta}{2} \approx \frac{\sqrt{M}}{\sqrt{N}}$.

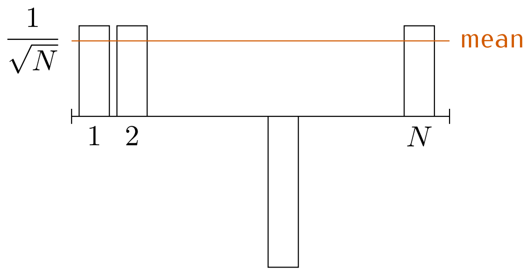
Lemma 4.5

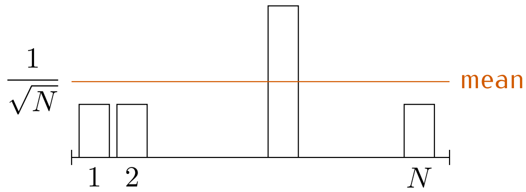
1. $G|\Psi\rangle = \cos 3\theta 2|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$
2. $G^k|\Psi\rangle = \cos\frac{(2k+1)\theta}{2}|\alpha\rangle + \sin\frac{(2k+1)\theta}{2}|\beta\rangle$

Now we have to find k such that $(2k+1)\frac{\theta}{2} \approx \frac{\pi}{2}$. We find $k \approx \left(\frac{\pi}{2}\frac{\sqrt{N}}{\sqrt{M}} - 1\right)\frac{1}{2}$, which is $O(\sqrt{N})$.



Make one query:





Exercise 4.2

Given some function f, write a circuit that implements O_f or O'_f using Toffoli gates.

$$f : \bigvee_{x, f(x)=1} \left(\bigwedge_{x_i=1} x_i \right) \wedge \left(\bigwedge_{x_i=0} \overline{x_i} \right).$$

Part II
Frédéric Magniez

5 Extensions of GS

5.1 Unknown number of solutions

Suppose that there is an unknown number of solutions m.
Let $f : \{0,1\}^n \to \{0,1\}$ and $N = 2^n$.

Theorem 5.1

There exists a quantum algorithm that gives x such that $f(x) = 1$ with expected number of queries $O\left(\sqrt{\frac{N}{m}}\right)$.

Theorem 5.2

Assume $m = 0$ or $m \geqslant m_0$.

Then there exists a quantum algorithm with number of queries $O\left(\sqrt{\frac{N}{m_0}}\right)$ and high probability of success ($\geqslant \frac{9}{10}$).

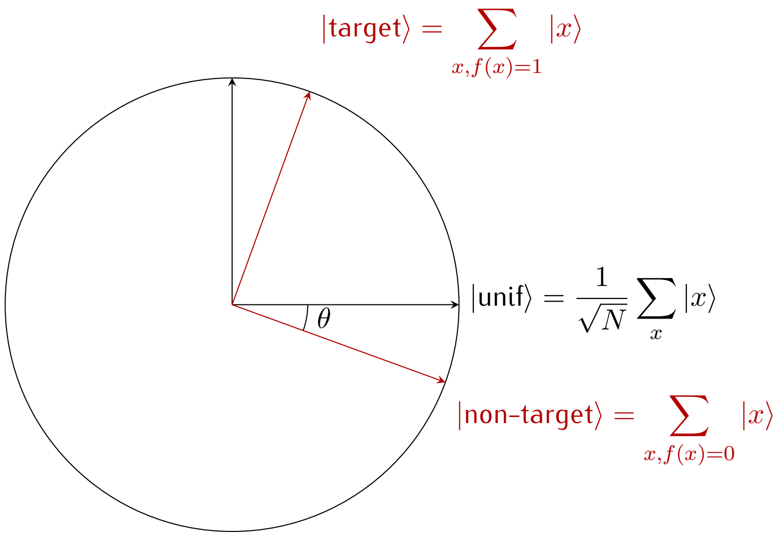
Proof of theorem 5.2.

Algorithm

If $m_0 \geqslant \frac{N}{4}$, do random search with 5 queries.
Compute k_0 the number of iteration in GS with $m = m_0$.
Let $k \in [\![0, 100k_0]\!]$ be a random number.
Run GS with k iterations.

Claim 5.3

If $m \geqslant m_0$ the success probability is almost greater than $\frac{1}{2}$.



Proof of claim 5.3.

$|\text{unif}\rangle = \sin\theta |\text{target}\rangle + \cos\theta |\text{non-target}\rangle$
$G^t |\text{unif}\rangle = (\sin(2t+1)\theta) |\text{target}\rangle + (\cos(2t+1)\theta) |\text{non-target}\rangle$
$\langle \text{target} \,|\, G^t \,|\, \text{unif} \rangle = \sin(2t+1)\theta$
So the success probability after t steps in $(\sin(2t+1)\theta)^2$.
Therefore the success probability is

$$\mathbb{E}_{k \in [\![0, 100k_0]\!]} (\sin(2k+1)\theta)^2 \sim \int_0^{\gg \pi} \sin^2 x \, dx \sim \frac{1}{2}.$$

C'est ce que je voulais !

Voilà !

Theorem 5.4

Given two parameters $\varepsilon > 0$ and $\delta > 0$, there exists a quantum algorithm that computes $\tilde{m}$ such that $|m - \tilde{m}| \leqslant \varepsilon m$, with a number of queries $O\left(\sqrt{\frac{N}{m}}\frac{1}{\varepsilon} \log \frac{1}{\delta}\right)$ and with a probability of success $\geqslant 1 - \delta$.

5.2 Applications

Definition 5.1 Quantum time

The measure of time in a quantum algorithm is the number of gates in it.

Example 5.1 SAT

Let $\varphi = c_1 \wedge \ldots \wedge c_m$, over n variables. We search for $x \in \{0,1\}^n$ such that $\varphi(x) = 1$.
A classical algorithm computes in time $O(2^n)$.
By using GS with $f = \varphi$, the quantum time is $O((n+m)\sqrt{2^n})$ and the number of qubits is $O(n+m)$.

Example 5.2 Collision finding

Definition 5.2 Collision finding

Input: $H : [N] \to [N]$ a 2-to-1 function $(\forall x \exists! y \neq x, H(x) = H(y))$
Output: $x \neq y$ such that $H(x) = H(y)$

A first attempt could be to consider $f : x \longmapsto \begin{cases} 1 & \text{if } H(x) = H(0) \text{ and } x \neq 0 \\ 0 & \text{otherwise} \end{cases}$
The problem is that it uses $O(\sqrt{N})$ queries to H.
But there exists a random algorithm with same complexity.

Algorithm

Take at random $x_1, \ldots, x_k$
Query $H(x_1), \ldots, H(x_k)$
Output a collision in $x_1, \ldots, x_k$ if any

It can still be improved by using a classical space polynomial in $\log N$ by a quantum algorithm:

Algorithm

$S = [\![0, k-1]\!]$
Query H on S (If there is already a collision in S, stop)
GS $x \in [N] \setminus S = [\![k, N-1]\!]$ such that $H(x) \in H(S)$. That is $f : x \longmapsto \begin{cases} 1 & \text{if } H(x) \in S \text{ and } x \notin S \\ 0 & \text{otherwise} \end{cases}$ with $m = k$.

The total number of queries to H is $k + O(\sqrt{\frac{N}{k}})$ and the time complexity is $O(\sqrt[3]{N}\mathrm{poly}(N))$.

Example 5.3 Exact traveling salesman

Consider a graph with n vertices.
The random time complexity is $O(2^n \mathrm{poly}(n))$.
The quantum time complexity is $O((1,728)^n \mathrm{poly}(n))$.

5.3 Amplitude amplification

Theorem 5.5

Given a random or quantum algorithm A finding x such that $f(x) = 1$ with success probability $\geqslant \varepsilon$ (if there is any).
Then there is a quantum algorithm B such that

- B is made of
  - $O(\frac{1}{\sqrt{\varepsilon}} \log \frac{1}{\delta})$ blocks of quantum version of A and its inverse
  - $O(\frac{1}{\sqrt{\varepsilon}} \log \frac{1}{\delta})$ queries to f
  - $O(\frac{1}{\sqrt{\varepsilon}} \log \frac{1}{\delta} \times \text{input size})$ qubits and gates.
- B outputs x such that $f(x) = 1$ with probability $1 - \delta$ (if there is any).

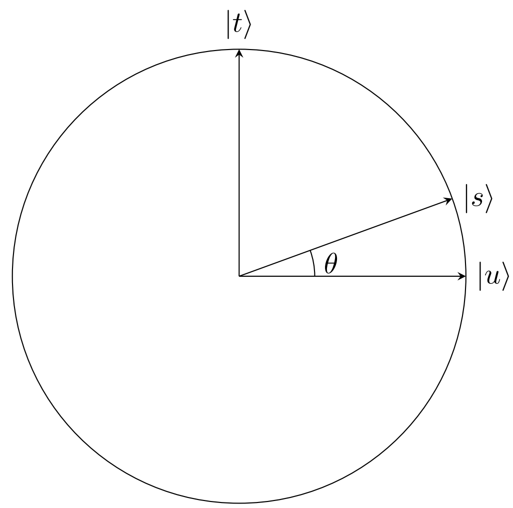
Proof of theorem 5.5.

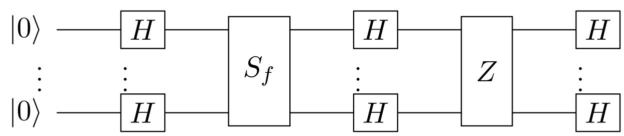
The quantum version of A is $A|0...0\rangle = \sum_x \alpha_x|x\rangle|\psi_x\rangle$ such that $\sum_{x,f(x)=1} |\alpha_x|^2 \geqslant \varepsilon$.

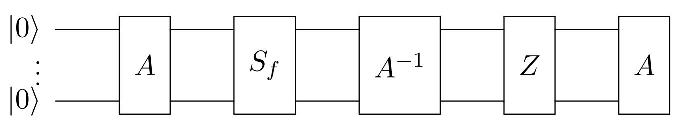
$$|t\rangle = \frac{1}{\sqrt{\mu}} \sum_{x,f(x)=1} \alpha_x|x\rangle|\psi_x\rangle$$

$$|u\rangle = \frac{1}{\sqrt{1-\mu}} \sum_{x,f(x)=0} \alpha_x|x\rangle|\psi_x\rangle$$

$$\sin\theta = \sqrt{u} \geqslant \sqrt{\varepsilon}$$







Youpi !

5.4 Application

Example 5.4 3SAT

Let $\varphi = c_1 \wedge ... \wedge c_m$ with c_i composed of 3 variables.
GS finds a solution in time $O((\sqrt{2})^n \mathrm{poly}(n,m))$.
There exists a random algorithm in time $O((\frac{4}{3})^n \mathrm{poly}(n,m))$.

It is the Schoning algorithm:

Schoning algorithm

Take a random $a \in \{0,1\}^n$.
Start a random local search of $3n$ steps. Stop if $\varphi(a) = 1$.

Theorem 5.6

The probability that this algorithm find a solutino with $3n$ steps is $\geqslant (\frac{3}{4})^n$.

Corollary 5.7

Amplitude amplification applied like this gives a quantum algorithm with time $(\sqrt{\frac{4}{3}})^n \mathrm{poly}(n, m)$.

Example 5.5 Element distinction

Consider $H : [N] \to [N]$. We want to find $i \neq j$ such that $H(i) = H(j)$ if there are any.

Algorithm

GS: $\sqrt{\frac{N^2}{1}} = N$ queries
Quantum algorithm:

- Take S composed of k elements in $[N]$ at random.
- Query H on S (and stop if there is a collision) $\longrightarrow k$ queries
- GS for a colision in $[N] \setminus S$ with $S \longrightarrow \sqrt{N}$ queries

The probability of success is $\varepsilon = \mathbb{P}_S(\exists i \in S, \exists j \in [N] \setminus S, H(i) = H(j)) \sim \frac{2k}{N}$.
By using amplitude amplification on this algorithm uses $(k + \sqrt{N})\sqrt{\frac{N}{k}}$ queries. With $k = \sqrt{N}$ it makes $N^{3/4}$ queries.

Example 5.6 Quantum optimization

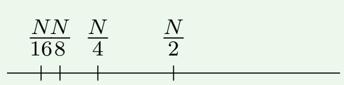
Problem

Let $f : [N] \to [R]$ with $R = \mathrm{poly}(N)$.
Find x such that $f(x)$ it minimum.

Algorithm

Take $x \in [N]$ at random.
Use GS to find y such that $f(y) < f(x)$ (with success probability $\geqslant 1 - 1/N$).
If none was found output x and stop.
Else start again with $x \leftarrow y$.

The worst case uses N iterations.
The average case consider f is injective. It uses $\sqrt{2} + \sqrt{4} + \sqrt{8} + ... + \sqrt{N}$ iterations.



Theorem 5.8

The expected number of queries is $O(\sqrt{N})$, with a success probability $1 - \sqrt{1}\sqrt{N}$.

Example 5.7 Fourier transform

Definition 5.3 Simon's problem (recap)

$f : \{0, 1\} \to \mathbb{R}$
$\exists! s, f(x) = f(y) \Leftrightarrow x = y \oplus s$ or $x = y$
where $x \oplus y = (x_i \oplus y_i)_i = (x_i + y_i \mod 2)_i$
$((\mathbb{Z}_2)^n, \oplus)$ is a group

Case 1. $(\mathbb{Z}_2)^n$
$H^{\otimes n}$ is a (quantum) Fourier transform over $(\mathbb{Z}_2)^n$:

$$\sum_{x\in\{0,1\}^n} \alpha_x|x\rangle \longmapsto \sum_{y\in\{0,1\}^n} \widehat{\alpha}_y|y\rangle$$

where $\widehat{\alpha}_y = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot y}\alpha_x$, and $x\cdot y = \sum x_i y_i \mod 2$.

Case 2. $\mathbb{Z}_N$

Definition 5.4 Quantum Fourier Transform (QFT)

Define QFT_N by $\sum_{x=0}^{N-1}\alpha_x|x\rangle \longmapsto \sum_{y=0}^{N-1}\widehat{\alpha}_y|y\rangle$, where $\widehat{\alpha}_y = \frac{1}{\sqrt{N}}\sum_x \omega_N^{x\cdot y}\alpha_x$ and $\omega_N = e^{\frac{2i\pi}{N}}$.

Remark 5.1

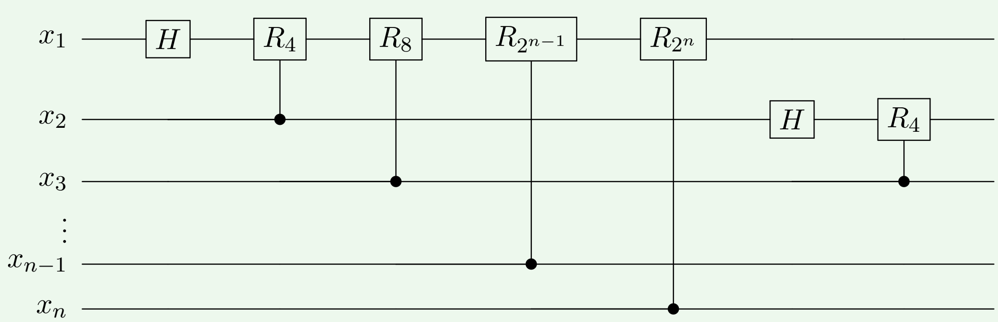
For $N=2^n$, $\mathrm{QFT}_N|0\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle = H^{\otimes n}|0\rangle$.

When $N=2^n$, $\mathrm{QFT}_N|x\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}\omega_N^{x\cdot y}|y\rangle = \frac{1}{\sqrt{N}}\sum_{(y_1,\dots,y_n)\in\{0,1\}^n} w_N^{x(y_1 2^{n-1}+y_2 2^{n-2}+\dots+y_n)}|y_1\dots y_n\rangle$.

Fact 5.9

$$\begin{aligned}\mathrm{QFT}_{2^n}|x\rangle &= \frac{1}{\sqrt{2^n}}(|0\rangle+\omega_{2^n}^{2^{n-1}x}|1\rangle)\otimes(|0\rangle+\omega_{2^n}^{2^{n-2}x}|1\rangle)\otimes\dots\otimes(|0\rangle+\omega_{2^n}^{x}|1\rangle)\\ &= \frac{1}{\sqrt{2^n}}(|0\rangle+\omega_{2}^{x}|1\rangle)\otimes(|0\rangle+\omega_{2^2}^{x}|1\rangle)\otimes\dots\otimes(|0\rangle+\omega_{2^n}^{x}|1\rangle)\\ &= \frac{1}{\sqrt{2^n}}(|0\rangle+\omega_{2}^{x_n}|1\rangle)\otimes(|0\rangle+\omega_{2^2}^{2x_{n-1}+x_n})\otimes\dots\otimes(|0\rangle+\omega_{2^n}^{x}|1\rangle)\end{aligned}$$

where $x = x_1 2^{n-1} + x_2 2^{n-2} + \dots + x_n$.



The number of gates is $\sim \frac{n^2}{2}$ and the depth is n.
With error $\varepsilon > 0$ there exists a circuit with $O(n\log(\frac{n}{\varepsilon})$ gates and a depth of $O(\log n + \log\log\frac{1}{\varepsilon})$.
In the general case, with $n=\log N$, we have the exact value with $O(n^2)$ gates and a depth of $O(n)$ and with error $\varepsilon>0$, with $O(n\log\frac{n}{\varepsilon}+\log^2\frac{1}{\varepsilon})$ gates and a depth of $O(\log n + \log\log\frac{1}{\varepsilon})$.

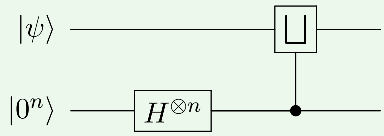
Example 5.8 Phase optimisation

Input:

- quantum state $|\psi\rangle$ on n qubits
- acces to unitary $\bigsqcup$

Promises: $\bigsqcup|\psi\rangle = e^{i\alpha}|\psi\rangle$
Goal: Find α

Case 1. $\alpha = \frac{2i\pi x}{2^n}$ with $x \in \{0, 1, ..., 2^n - 1\}$.



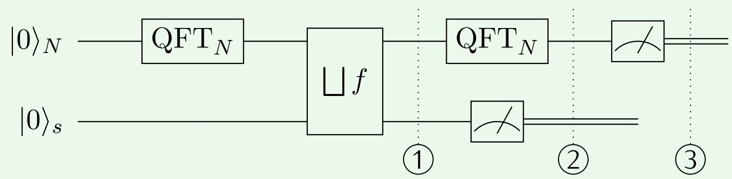
The output is

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^{n-1}} (\bigsqcup |\psi\rangle)|y\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^{n-1}} \omega_{2^n}^{x \cdot y} |\psi\rangle \otimes |y\rangle$$
$$= |\psi\rangle \otimes \mathrm{QFT}_{2^n} |x\rangle$$

So we just apply $\mathrm{QFT}_{2^n}^{-1}$ to get $|x\rangle$.

Example 5.9 Period finding

Input: $f : \mathbb{Z}_N \longrightarrow S$ where S is of size polynomial in N
Promise: $\exists! r \in \mathbb{Z}_N$ such that $\forall x, y \in \mathbb{Z}_N, f(x) = f(y) \Leftrightarrow r \mid (x - y) \Leftrightarrow y - x \in r\mathbb{Z}$
Goal: Find r



1. $\displaystyle \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle$

2. We measure "Z". Fix $a \in [\![0, r-1]\!]$ such that $f(a) = Z$.

$$\sum_{x, f(x) = f(a)} |x\rangle |f(a)\rangle = \sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |a + kr\rangle |f(a)\rangle$$

3.

$$\frac{\sqrt{r}}{N} \sum_{y=0}^{N-1} \left(\sum_{k=0}^{\frac{N}{r}-1} \omega_N^{y(a+kr)} \right) |y\rangle = \frac{\sqrt{r}}{N} \sum_{y=0}^{N-1} \omega_N^{ya} \cdot \left(\sum_{k=0}^{\frac{N}{r}-1} \omega_N^{ykr} \right) |y\rangle$$
$$= \frac{1}{\sqrt{r}} \sum_{t=0}^{r-1} \omega_N^{\frac{tNa}{r}} |\frac{tN}{r}\rangle$$

6 Lower bounds on query complexity

Given $F : \{0,1\}^N \longrightarrow \{0,1\}$ a total function (defined everywhere), we want to solve the problem
Input: $x \in \{0,1\}^N$ with query access only
Output: $F(x)$

We define the deterministic complexity of F as follows

$$D(F) := \min_{\substack{\text{deterministic} \\ \text{algo computing } F}} \max_{x \in \{0,1\}^N} \#\mathrm{Queries}(A, x)$$

its random complexity as follows

$$R_\varepsilon(F) := \min_{\substack{\text{random algo} \\ \text{computing } F \\ \text{with error } \leqslant \varepsilon}} \max_{x \in \{0,1\}^N} \#\mathrm{Queries}(A, x)$$

and its quantum complexity as follows

$$Q_\varepsilon(F) := \min_{\substack{\text{quantum algo}\\ \text{computing } F\\ \text{with error } \leqslant\varepsilon}} \max_{x\in\{0,1\}^N} \#\text{Queries}(A,x)$$

Fact 6.1

$N \geqslant D(F) \geqslant R_\varepsilon(F) \geqslant Q_\varepsilon(F)$

Usually, $\varepsilon = \frac{1}{3}$ and we don't write it.

Theorem 6.2

For any total function $F : \{0,1\}^N \longrightarrow \{0,1\}$, $D(F) \leqslant R^3(F)$ and $D(F) \leqslant Q^4(F)$.

Corollary 6.3

In order to get exponential separation, one needs to consider partial functions $F : D \longrightarrow \{0,1\}$ with $D \subsetneq \{0,1\}^N$, like in the algorithms we saw.

6.1 Polynomial method

Theorem 6.4 Main theorem

Let A be a T-query quantum algorithm for F with error $\leqslant \varepsilon$.
Then there is a N-variable (real) polynomial P of degree $\leqslant 2T$ such that $\forall x \in \{0,1\}^N, |P(x) - F(x)| \leqslant \varepsilon$.

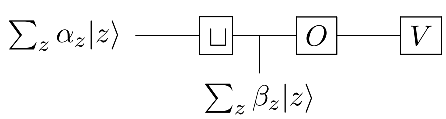
Proof of theorem 6.4.

Lemma 6.5

Let A be a T-query quantum algorithm for F with error $\leqslant \varepsilon$.
Then its final state can be written as $|\psi^x\rangle - \sum_z \alpha_z(x)|z\rangle$ where α_z is an N-variable (complex) polynomial of degree $\leqslant T$.

Proof of lemma 6.5.

The proof is by induction of the step of the algorithm.



$\beta_z = \sum_{z'} U_{zz'}\alpha_{z'}$ so U and V do linear combination of coefficients, so the degree does not increase.
For O, $|i,b,w\rangle \longmapsto |i, b\oplus x_i, w\rangle$, so

$$|i,0,w\rangle \longmapsto (1-x_i)|i,0,W\rangle + x_i|i,1,w\rangle$$
$$|i,1,w\rangle \longmapsto x_i|i,0,W\rangle + (1-x_i)|i,1,w\rangle$$

So $\sum_{i,b,w} \alpha_{i,b,w}|i,b,w\rangle \longrightarrow \sum_{i,b,w} \beta_{i,b,w}|i,b,w\rangle$ where $\begin{cases} \beta_{i,0,w} = (1-x_i)\alpha_{i,0,w} + x_i\alpha_{i,1,w} \\ \beta_{i,1,w} = x_i\alpha_{i,0,w} + (1-x_i)\alpha_{i,1,w} \end{cases}$
If α are degree t polynomials, the β are degree $t+1$ polynomials.

Voilà !

Assume the output is the first bit. Let $|\psi\rangle = \sum \alpha_z|z\rangle$ b the final state.

$$P(x) = \mathbb{P}(A \text{ outputs } 1) = \sum_{z \text{ starts with } 1} \alpha_z^* \alpha_z$$

but all α_z and α_z^* are degree T polynomials. So $P(x)$ is a $2T$-degree polynomial, and $\forall x, |P(x) - F(x)| \leqslant \varepsilon$.

Voilà !

Definition 6.1

Let $\deg_\varepsilon(F)$ be the minimum degree of N-variable (real) polynomial P such that $\forall x \in \{0,1\}^N, |P(x) - F(x)| \leqslant \varepsilon$.

Corollary 6.6

$Q_\varepsilon(F) \geqslant \frac{1}{2}\deg_\varepsilon(F)$ and $R_\varepsilon(F) \geqslant \deg_\varepsilon(F)$.

6.2 Case of symmetric functions

Definition 6.2 Symmetric function

F is symmetric if $\forall \sigma \in \mathfrak{S}_N, \forall x \in \{0,1\}^N, F(x) = F(x_{\sigma(1)}, ..., x_{\sigma(N)}) =: F(\sigma(x))$.

Fact 6.7

If F is symmetric, there exists $G : [\![1, N]\!] \longrightarrow \{0,1\}$ such that $\forall x \in \{0,1\}^N, F(x) = G(|x|)$.

Theorem 6.8 Main theorem bis

Suppose F is symmetric.
Let A be a T-query quantum algorithm for F with error $\leqslant \varepsilon$.
Then there exists a 1-variable polynomial q of degree $\leqslant 2T$ such that $\forall i \in [\![1, N]\!], |q(i) - G(i)| \leqslant \varepsilon$.

Definition 6.3 Symmetrisation

$$\tilde{P}(x) := \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} P(\sigma(x))$$

$\tilde{P}$ is symmetric and a polynomial of degree $\leqslant 2T$, and $\forall x, |\tilde{P}(x) - F(x)| \leqslant \varepsilon$.

Fact 6.9

There exists a 1-variable polynomial q of degree $\leqslant 2T$ such that $\forall x, P(x) = q(|x|)$.

Example 6.1 Application to PARITY

$$\mathrm{PARITY}(x) = \bigoplus x_i = \begin{cases} 1 & \text{if } \#\{i \,|\, x_i = 1\} \text{ is even} \\ 0 & \text{otherwise} \end{cases}$$

With $\varepsilon = \frac{1}{3}$, if $|q(|x|) - \mathrm{PARITY}(x)| \leqslant \frac{1}{3}$, then $q(0) \geqslant \frac{2}{3}$, $q(1) \leqslant \frac{1}{3}$, $q(2) \geqslant \frac{2}{3}$,... then $(q - \frac{1}{2})(0) > 0$, $(q - \frac{1}{2})(1) < 0$,..., so $q - \frac{1}{2}$ has N distinct roots, so $\deg(q - \frac{1}{2}) \geqslant N$.
So $Q_{\frac{1}{3}}(\mathrm{PARITY}) \geqslant \frac{N}{2}$.

Definition 6.4

$\Gamma(F) = \min\{|2k - N + 1| \,|\, G(k) \neq G(k+1)\}$

Theorem 6.10 **Paturi's theorem (1992)**

Let F be symmetric non constant.
Then $\deg_{\frac{1}{3}}(F) = \Theta(\sqrt{N(N-\Gamma(F))})$.

Corollary 6.11

$Q_{\frac{1}{3}}(F) = \Omega(\sqrt{N(N-\Gamma(F))})$

There is even a stronger result.

Theorem 6.12

Let F be symmetric non constant.
Then $Q_{\frac{1}{3}}(F) = \Theta(\sqrt{N(N-\Gamma(F))})$.

Corollary 6.13

$R_{\frac{1}{3}}(F) \leqslant Q^2_{\frac{1}{3}}(F)$

Using the same tools one can prove that $Q_\varepsilon(\text{CollisionFinding}) = \Omega(N^{\frac{1}{3}})$.

6.3 Adversary method

6.3.1 Measure of progress

Fix a quantum algorithm with T queries, computing F with error ε.
Define $|\psi_t^x\rangle$ the state of the algorithm before the $(t+1)^{\text{th}}$ query. $|\psi_T^x\rangle$ is the final state.
Fix $R \subseteq \{0,1\}^n \times \{0,1\}^n$ or ($D \times D$ if F is partial) such that $(x,y) \in R$ implies $F(x) \neq F(y)$.
Define $W_t = \sum_{(x,y)\in R} \langle \psi_t^x \,|\, \psi_t^y \rangle$.

1. $W_0 = |R|$ ($|\psi_0^x\rangle = |\psi_0^y\rangle = \sqcup_0|0\ldots0\rangle$)
2. $F(x) \neq F(y)$ also has error $\leqslant \varepsilon$ implies $|\langle \psi_T^x \,|\, \psi_T^y\rangle| \leqslant 2\sqrt{\varepsilon(1-\varepsilon)}$ ($|\psi_T^x\rangle$ is almost $\perp$ to $|\psi_t^y\rangle$), so $W_T \leqslant 2\sqrt{\varepsilon(1-\varepsilon)}|R|$.

   So if $\forall t, W_t - W_{t+1} \leqslant \Delta$ then $T \geqslant (1 - 2\sqrt{\varepsilon(1-\varepsilon)})\frac{|R|}{\Delta}$.

6.3.2 Bound Δ

$$
\begin{aligned}
W_t - W_{t+1} &= \sum_{(x,y)\in R} |\langle \psi_t^x \,|\, \psi_t^y\rangle| - |\langle \psi_{t+1}^x \,|\, \psi_{t+1}^y\rangle| \\
&\leqslant \sum_{(x,y)\in R} \left|\langle \psi_t^x \,|\, \psi_t^y\rangle - \langle \psi_{t+1}^x \,|\, \psi_{t+1}^y\rangle\right|
\end{aligned}
$$

Fix $(x,y) \in R$. $F(x) \neq F(y)$ so $x \neq y$.

$$
|\psi_t\rangle^x \;\text{———}\; \boxed{O^x} \;\text{———}\; \boxed{\sqcup_{t+1}} \;\text{———}\; |\psi_{t+1}^x\rangle
$$

$$
\begin{aligned}
\langle \psi_{t+1}^x \,|\, \psi_{t+1}^y\rangle &= \langle \psi_t^x O^x \sqcup_{t+1} \mid \sqcup_{t+1} O^y \psi_{t+1}^y\rangle \\
&= \langle \psi_t^x O^x \,|\, O^y \psi_{t+1}^y\rangle \\
&= \langle \psi_t^x \,|\, O^x O^y \,|\, \psi_{t+1}^y\rangle
\end{aligned}
$$

So

$$|\langle\psi_t^x\,|\,\psi_t^y\rangle - \langle\psi_{t+1}^x\,|\,\psi_{t+1}^y\rangle| = |\langle\psi_t^x\,|\,(\mathrm{Id} - O^xO^y)\,|\,\psi_t^x\rangle$$

There is a special case when $(x, y) \in R$ implies $\exists! i, x_i \neq y_i$. When $j \neq i$, $O^xO^y|j, b, w\rangle = \mathrm{Id}(j, b, w)$, and when $j = i$, $O^xO^y|i, b, w\rangle = (i, 1 \uplus b, w)$.

$$|\langle\psi_t^x\,|\,\mathrm{Id} - O^xO^y\,|\,\psi_t^y\rangle| = |\langle\psi_t^x\,|\,\mathrm{Id} - O^{(i)}\,|\,\psi_t^y\rangle$$

$|\psi_t^x\rangle = \sum_j \alpha_{t,j}^x|j, z\rangle$ and $|\psi_t^y\rangle = \sum_j \alpha_{t,j}^y|j, z\rangle$
So for $j \neq i$, $(\mathrm{Id} - O^{(i)}|j\rangle|\psi_j\rangle = 0$

$$\begin{aligned}|\langle\psi_t^x\,|\,\mathrm{Id} - O^{(i)}\,|\,\psi_t^y\rangle &= |\langle\psi_t^x\,|\,(\mathrm{Id} - O^{(i)})\,|\,\alpha_{t,i}^y|i\rangle|\psi_i^y\rangle| \\ &= \overline{alpha_{t,i}}^y\langle i|\langle\psi_i^x\,|\,(\mathrm{Id} - O^{(i)})\alpha_{t,i}^y|i\rangle|\varphi_i^y\rangle| \qquad =\leqslant 2|\alpha_{t,i}^x\alpha_{t,i}^y|\end{aligned}$$

So in this special case, $W_t - W_{t+1} \leqslant 2\sum_{i=1}^N \sum_{(x,y)\in R, x_i\neq y_i} |\alpha_{t,i}^x\alpha_{t,i}^y|$.

Corollary 6.14

$$T \geqslant (\frac{1}{2} - \sqrt{\varepsilon(1-\varepsilon)}\frac{|R|}{\max_t \sum_i \sum_{(x,y)\in R, x_i\neq y_i}}|\alpha_{t,i}^x\alpha_{t,i}^y|$$

Example 6.2 **Application to OR**

$R = \{(0, ..., 0)\} \times \{(1, 0, ..., 0), (0, 1, 0, .., 0), ..., (0, ..., 0, 1)\}$ so $|R| = N$.
Fix t.

$$\begin{aligned}\sum_{i=1}^N |\alpha_{t,i}^{O^N}\alpha_{t,i}^{(i)}| &\leqslant \sum_{i=1}^N |\alpha_{t,i}^{O^N}| \times 1 \\ &\leqslant \sqrt{\sum_{i=1}^N |\alpha_{t,i}^{O^N}|^2} \times \sqrt{\sum_{i=1}^N 1} \\ &\leqslant \sqrt{N}\end{aligned}$$

So $T \geqslant (\frac{1}{2} - \sqrt{\varepsilon(1-\varepsilon)})\sqrt{N}$.

6.4 Simulation of a quantum circuit

Consider the following problem.
Input: n classical bits $x \in \{0, 1\}^n$, quantum circuit on n qubits wih T 3-qubits gates
Output: n random bits distributed y distributed as the measure $j\ c|x\rangle$.

We consider a simplification, with only gates NOT, C-NOT, Toffoli and Hadamard.

Algorithm **Schrödinger approach**

Compute step by step the amplitute of state after each gate.

Its time complexity is $O(T + 2^n)$ and its space complexity is the amplitude of type $\frac{a}{2^{k/2}}$ where k is the number of Hadamard gates and $a \in [\![-2^{k/2}, 2^{k/2}]\!]$, so $O(k2^n) = O(T2^n)$.

Corollary 6.15

BQP $\subseteq$ EXPTIME

We can also apply the same method to random algorithms by replacing the Hadamard gate by CF$\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$.
But there is a stronger result.

Proposition 6.16

$\mathbf{BQP} \subseteq \mathbf{PSPACE} = \mathbf{QSPACE}$

And furthermore

Proposition 6.17

$\mathbf{BQP} \subseteq \mathbf{PP}$

Index of definitions

Index of results