Introduction à la Théorie de Complexité Quantique

Tom Sarry

24 avril 2023

Université de Montréal

Table des Matières

Introduction

Le Problème

1. Machines de Turing (Programmes de Branchement, Circuits Booléens,...) sont basées sur la **physique classique**
2. On a de bonnes raisons de croire que le monde obéit à la **physique quantique**

Comment étudier la puissance du calcul quantique ?

Les Questions

1. Utiliser les outils existants ? (Modèles de Calcul, classes de complexité)
2. Situer la puissance de l'ordinateur quantique dans la hiérarchie connue
3. Résoudre des questions ouvertes ?

Les Questions

1. Utiliser les outils existants ? (Modèles de Calcul, classes de complexité)
2. Situer la puissance de l'ordinateur quantique dans la hiérarchie connue
3. Résoudre des questions ouvertes ? P $\neq$ NP

Modèles de Calcul Quantique

Différents Modèles

Extension logique : adapter les modèles existants pour supporter le calcul quantique :

- Turing Machines (TM) $\rightarrow$ QTM (Quantum TM)
- Finite Automata (FA) $\rightarrow$ QFA (Quantum FA)
- Boolean Circuits $\rightarrow$ Quantum Circuits : vu en classe !
- Branching Programs (BP) $\rightarrow$ QBP (Quantum BP)

Dates Importantes

- Turing 1936 : Machines de Turing
- Cook 1971 : Comment prouver $X \in \mathsf{NP}$
- Baianu 1971 : QFA
- Deutsch 1985 : QTM
- Bernstein, Verizani 1997 : Universal QTM (avec coût de simulation *raisonnable*)
- Nakanishi, 2000 : Programme de Branchement Quantique

LA classe de Compléxité Quantique : BQP

BQP par Circuits Quantiques

$L \in$ **BQP** :

- $\iff \exists$ un algo. quantique qui résolve le problème de décision avec haute probabilité en temps poly.
- $\iff \exists$ une famille uniforme de temps poly de circuits quantiques $\{Q_n : n \in \mathbb{N}\}$ tel que :
    1. $\forall n \in \mathbb{N}$, Q_n prend n qubits en entrée et produit un bit en sortie
    2. $\forall x \in L,\ Pr(Q_{|x|}(x) = 1) \geq 2/3$
    3. $\forall x \notin L,\ Pr(Q_{|x|}(x) = 0) \geq 2/3$

Rappel : Machines de Turing

1. Machines de Turing Déterministes : un chemin
2. Machines de Turing Non Déterministes : plusieurs chemins
3. Machines de Turing Probabilistes : plusieurs chemins, n'en suit qu'un
4. Machines de Turing Quantique :

Rappel : Machines de Turing

1. Machines de Turing Déterministes : un chemin
2. Machines de Turing Non Déterministes : plusieurs chemins
3. Machines de Turing Probabilistes : plusieurs chemins, n'en suit qu'un
4. Machines de Turing Quantique : suit plusieurs chemins en superposition

Rappel : BPP (Bounded-error Probabilistic Poly-time)

$L \in$ **BPP** : problèmes qui peuvent être efficacement résolus

- $\iff \exists$ un algo. qui résolve le problème de décision avec haute probabilité en temps poly.
- $\iff \exists$ une Machine de Turing Probabiliste M tel que :
    1. M fonctionne en temps poly
    2. $\forall x \in L,\ Pr(M \downarrow x = 1) \geq 2/3$
    3. $\forall x \notin L,\ Pr(M \downarrow x = 0) \geq 2/3$

Peut diminuer la probabilité d'erreur à 2^{-n^c} avec des votes majoritaires (Bornes de Chernoff)

BQP (Bounded-error Quantum Poly-time) par QTM

$L \in \mathsf{BQP}$:

- $\iff \exists$ un algo. quantique qui résolve le problème de décision avec haute probabilité en temps poly.
- $\iff \exists$ une Machine de Turing Quantique M tel que :
  1. M fonctionne en temps poly
  2. $\forall x \in L,\ Pr(M \downarrow x = 1) \geq {}^2/_3$
  3. $\forall x \notin L,\ Pr(M \downarrow x = 0) \geq {}^2/_3$

Peut diminuer la probabilité d'erreur à 2^{-n^c} avec des votes majoritaires (Bornes de Chernoff)

Rappel : Machine de Turing Probabiliste

PTM : $M = (Q, \Sigma, \Gamma, \delta, q_0, F)$

- Q états
- Σ alphabet d'entrée
- Γ alphabet bande de calcul ($\Sigma \subseteq \Gamma, \# \in \Gamma$)
- δ fonction de transition
  $\delta : Q \times \Gamma \times Q \times \Gamma \times \{L, R\} \to [0, 1]$
- q_0 état initial
- $F \subseteq Q$ états acceptants

Rappel : Machine de Turing Probabiliste

Pas tous les δ donnent des PTM valides !

Pas tous les δ donnent des PTM valides !

$\sum_{q,\tau,d} \delta(p, \gamma, q, \tau, d) = 1, \quad \forall (p, \gamma) \in Q \times \Gamma$

Machine de Turing Quantique

QTM [BV97] : $M = (Q, \Sigma, \delta, q_0, F)$

- Q états
- Σ alphabet
- δ machine de contrôle quantique
  $\delta : Q \times \Sigma \times \Sigma \times Q \times \{L, R\} \to \mathbb{C}$
  $\delta(p, \sigma, \tau, q, d)$: amplitude
- q_0 état initial
- $F \subseteq Q$ états acceptants

Machine de Turing Quantique

- Pas tous les δ donnent des QTM valides !

Machine de Turing Quantique

- Pas tous les δ donnent des QTM valides !
- δ représente une **application linéaire** M_δ, nous désirons qu'elle soit unitaire

Machine de Turing Quantique

- Pas tous les δ donnent des QTM valides !
- δ représente une **application linéaire** M_δ, nous désirons qu'elle soit unitaire
- $M_\delta M_\delta^\dagger = \mathbb{I} \iff$ préserve la norme L_2 (M_δ finie)

Machine de Turing Quantique

- Pas tous les δ donnent des QTM valides !
- δ représente une **application linéaire** M_δ, nous désirons qu'elle soit unitaire
- $M_\delta M_\delta^\dagger = \mathbb{I} \iff$ préserve la norme L_2 (M_δ finie)
- Nombre infini de configurations (car bande de calcul) $\implies M_\delta$ infinie

Machine de Turing Quantique

Theorème (informel) [BV97] : δ est valide ssi M_δ satisfait :

1. Colonnes de longueur unitaire
2. Colonnes avec même position de la tête de lecture sont orthogonales
3. Colonnes avec une position de tête qui diffère de 2 cases sont orthogonales

Objectif : Deux configurations c_1, c_2 qui pourraient donner lieu a la même configuration c doivent être orthogonales.

Machine de Turing Quantique

Cas 1 : Têtes de lecture sur la même case

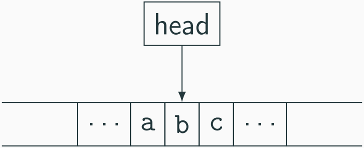

Figure 1: c_1

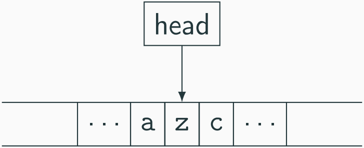

Figure 2: c_2

Machine de Turing Quantique

Cas 2 : Têtes de lecture diffèrent de 2 cases

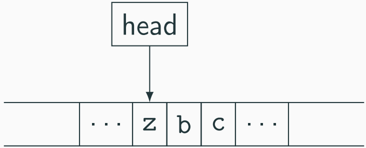

Figure 3: c_1

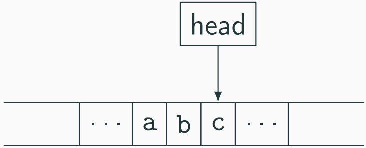

Figure 4: c_2

Cas 3 : Têtes de lecture diffèrent de 1 case ?

Machine de Turing Quantique

Cas 3 : Têtes de lecture diffèrent de 1 case ?

Non car obligation de bouger dans la direction $d \in \{L, R\}$!

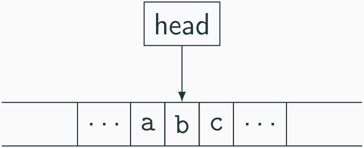

Figure 5: c_1

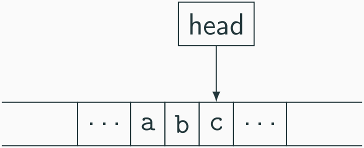

Figure 6: c_2

Analyse de BQP

BQP

- **But :**

BQP

- **But :** situer la classe, prouver inclusions
- **Comment :**

BQP

- **But :** situer la classe, prouver inclusions
- **Comment :** trouver un problème X **BQP**-complet

BQP

- **But :** situer la classe, prouver inclusions
- **Comment :** trouver un problème X **BQP**-complet
- **Problème :** on n'en connait pas !

Exemple

- **Entrée :** 1 qubit $|x\rangle$
- **Problème :** $|x\rangle = |1\rangle$?

Exemple

- **Entrée :** 1 qubit $|x\rangle$
- **Problème :** $|x\rangle = |1\rangle$?
- **Promesse :** $|x\rangle = |1\rangle \vee |x\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$

~~BQP~~ Promise-BQP

APPROX-QCIRCUIT-PROB (AQP) :

- **Entrée :** Circuit Quantique C sur n qubits, $\alpha, \beta \in [0, 1]$

~~BQP~~ Promise-BQP

APPROX-QCIRCUIT-PROB (AQP) :

- **Entrée :** Circuit Quantique C sur n qubits, $\alpha, \beta \in [0, 1]$
- **Problème :** Mesure du premier qubit de $C|0^n\rangle$ donne 1 avec probabilité $\geq \alpha$, ou $\leq \beta$?

~~BQP~~ Promise-BQP

APPROX-QCIRCUIT-PROB (AQP) :

- **Entrée :** Circuit Quantique C sur n qubits, $\alpha, \beta \in [0, 1]$
- **Problème :** Mesure du premier qubit de $C\,|0^n\rangle$ donne 1 avec probabilité $\geq \alpha$, ou $\leq \beta$?
- **Promesse :** $\alpha > \beta$

~~BQP~~ Promise-BQP

AQP est **BQP**-hardu

Preuve (ébauche) : $\forall L \in$ **BQP**, utiliser **AQP** comme oracle avec $\alpha = {}^2\!/_3, \beta = {}^1\!/_3$

1. Fixer x, Q_n
2. Construire C_x tel que $C_x \left|0^n\right\rangle = \left|x\right\rangle$
3. Joindre C_x et Q_n en un circuit C'
4. Demander à l'oracle $(C', {}^2\!/_3, {}^1\!/_3)$

Résultat 1 : BQP faible pour elle même

$$\mathsf{BQP}^{\mathsf{BQP}} = \mathsf{BQP}$$

Résultat 2 : Inclusions (basiques)

$$\mathrm{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathrm{PP} \subseteq \mathrm{PSPACE} \subseteq \mathrm{EXP}$$

Supposition : Hiérarchie Polynomiale

$$\mathsf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP}$$

- **Rappel :**
  $\mathsf{P} = \Sigma_0^p = \Pi_0^p \subseteq \mathsf{NP} = \Sigma_1^p \subseteq \cup_k \Delta_k^p = \mathsf{PH} \subseteq \mathsf{PSPACE}$

Supposition : Hiérarchie Polynomiale

$$\mathsf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathsf{PP} \subseteq \mathsf{PSPACE} \subseteq \mathsf{EXP}$$

- **Rappel :**
  $\mathsf{P} = \Sigma_0^p = \Pi_0^p \subseteq \mathsf{NP} = \Sigma_1^p \subseteq \cup_k \Delta_k^p = \mathsf{PH} \subseteq \mathsf{PSPACE}$
- Fourier Sampling $\in$ **BQP**, $\notin$ PH?

Conclusion

Conclusion

- Modèles de Calcul Quantiques
- QTM
- **BQP** (QMA, EQP, AWPP, ...)

Sources

- Bernstein, Verizani 1997, *Quantum Complexity Theory*
- Deutsch 1985, *Quatum Theory, the Church-Turing Principle and the Universal Quantum Computer*
- Fortnow 2003, *One Complexity Theorist's View of Quantum Computing*
- `https://complexityzoo.net/`