Cours 5 — 08 février

Enseignant : Frédéric Magniez *Rédacteur : Boris Arnoux*

5.1 Complexité

5.1.1 Classes de complexité

Pour rendre plus aisée l'étude de la complexité intrinsèque des problèmes que l'on est amené à étudier, on utilise les classes de complexité.

Définition 5.1. *Une classe de complexité est un ensemble de problèmes qui, sous certains aspects, sont comparables.*

Par exemple, on trouve la classe P des prolèmes que l'on peut résoudre en temps polynomial sur une machine déterministe classique.

5.1.2 Problèmes décisionnels

On exprime généralement les problèmes sous forme de problème de décision. Par exemple :

"Décomoser N en deux facteurs non triviaux"

$\Leftrightarrow$ "Poser log(N) fois la question : N a-t-il un facteur plus petit que P"

Ce qui revient à faire une recherche dichotomique.

Quelques problèmes de décision de référence :
- "3-SAT" : Satisfiabilité de formules logiques.
- "3-COLORABLE" : Les sommets d'un graphe peuvent ils être coloriés sans que deux sommets adjacents soient de la même couleur ?
- Primalité : Donné un entier, décider si celui-ci est premier ou non.

5.1.3 Les classes de complexité usuelles

P

Définition 5.2. *Les problèmes de la classe P sont solubles en temps polynomial sur une machine déterministe classique.*

Par exemple, le tri est un problème de classe P. La résolution en temps polynomial des problèmes concernés se fait sans utilisation d'aléatoire (machine de Turing non probabiliste).

NP

Définition 5.3. *Les problèmes de la classe NP sont ceux dont on peut vérifier la solution en temps polynomial.*

La classe NP contient la classe P, et les problèmes NP complets. Un problème NP complet est un problème de NP qui est plus dur que tout problème de NP. C'est à dire qu'à partir d'un solveur problème NP complet, on peut résoudre n'importe quel problème de NP. Lorsqu'un problème est plus difficile qu'un problème NP complet, mais non prouvé comme étant NP, on dit qu'il est NP difficile.

BPP

Définition 5.4. *La classe BPP contient tous les problèmes pour lesquels il existe un algorithme aléatoire classique en temps maximal probabiliste, qui accepte toute solution vraie avec une probabilité $\frac{2}{3}$ et rejette toute solution fausse avec une probabilité $\frac{2}{3}$.*

Il est important de noter que le choix de $\frac{2}{3}$ est totalement arbitraire, on peut remplacer par toute valeur strictement supérieure à $\frac{1}{2}$.

BQP

Définition 5.5. *La classe BQP contient tous les problèmes pour lesquels il existe un algorithme aléatoire quantique en temps maximal probabiliste, qui accepte toute solution vraie avec une probabilité $\frac{2}{3}$ et rejette toute solution fausse avec une probabilité $\frac{2}{3}$.*

De la même façon, $\frac{2}{3}$ est ici un choix arbitraire.

PSPACE

Définition 5.6. *La classe $PSPACE$ contient tous les problèmes qui peuvent être résolus dans un espace mémoire polynomial.*

On peut remarquer que cette classe de problèmes est la plus générale.

5.1.4 Relations entre les classes de complexité

On a les inclusions suivantes :

$$P \subseteq NP \subseteq PSPACE$$

$$P \subseteq BPP \subseteq BQP \subseteq PSPACE$$

On considère généralement que $P \neq NP$,$NP \neq NPSPACE$ et $BQP \neq BPP$. Cependant, il n'y a aucune preuve que $P \neq PSPACE$. Ainsi, toutes ces classes pourraient être égales.

Un des problèmes de la théorie de la complexité en informatique quantique, consiste à trouver des problèmes dans BQP qui ne sont pas dans BPP. On s'attend à ce que des problèmes tels que la factorisation, ou le logarithme discret sur courbes elliptiques soient dans ce cas.

5.2 Portes et circuits quantiques

5.2.1 Portes quantiques

Définition

Les portes quantiques sont les éléments de base de l'ordinateur quantique.

Définition 5.7. *Une porte est une transformation unitaire qui agit sur au plus trois qbits.*

Bien que les portes quantiques soient agencées en circuits, il faut noter que dans un ordinateur quantique "réel" les portes seraient plutôt comme des instructions assembleur pour un ordinateur classique. Elles sont successivement appliquées à des registres de qbits, sans que le circuit qu'elles constituent ne soit réellement gravé.

Produit tensoriel de portes

Le produit tensoriel de deux portes quantiques est simplement l'application en parallèle de deux portes quantiques.

$$(G_1 \otimes G_2) \left|\Phi_1\right\rangle \left|\Phi_2\right\rangle = (G_1 \left|\Phi_1\right\rangle)(G_2 \left|\Phi_2\right\rangle)$$

On peut étentdre une porte à plus de trois entrées en faisant son produit tensoriel avec l'identité.

Portes intriquantes

Certaines portes de plus de une entrée sont intriquantes, c'est une des propriété qui rend le calcul quantique fondementalement différent du calcul classique.

Définition 5.8. *On dit qu'une porte est intriquante si elle associe un état intriqué en sortie à un état pur en entrée.*

En particulier, la porte C-NOT est intriquante.

Preuve:

$$\text{C-NOT}\frac{(\left|0\right\rangle + \left|1\right\rangle)\left|1\right\rangle}{\sqrt{2}} = \frac{(\left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|0\right\rangle)}{\sqrt{2}}$$

□

Circuit

Calcul logique Un circuit est une composition de portes en produit tensoriel avec l'identité.

Définition 5.9. *On dit qu'un circuit $C = C_L...C_2C_1$ calcule logiquement une fonction F si : $C(x, 0^k) = (F(x), z)$ La taille d'un circuit est le nombre de portes qu'il faut pour le réaliser, et la complexité de la fonction F est la taille minimale d'un circuit capable de la calculer. Cette complexité ne dépend pas du choix de portes effectué.*

Calcul quantique *On dit, de la même façon, qu'un circuit quantique $U = U_L...U_2U_1$ calcule une fonction F avec une erreur ϵ si pour toute entrée x :*

$$\sum_z |\langle F(x), z| U |x, 0^k\rangle|^2 \geq 1 - \epsilon$$

5.3 Familles universelles de portes

Les portes quantiques opèrent sur un nombre réduit d'entrées, mais un aglorithme quantique peut nécessiter beaucoup plus d'entrées. On essaye donc comme en informatique classique, de déterminer avec quels ensembles minimaux de portes on peut construire tout algorithme quantique. En pratique, on essaye d'approcher une transformation unitaire par une suite de portes d'une famille donnée, avec une qualité d'approximation donnée.

Définition 5.10. *Soient U et V deux transformations unitaires. Dans le cadre de l'approximation de U par V, on appelle qualité d'approximation la quantité suivante :*

$$E(U, V) = \max_{|\Phi\rangle} \|(U - V)|\Phi\rangle\|$$

Cette mesure d'approximation permet de définir une famille universelle de portes quantiques.

Définition 5.11. *Une famille de portes est dite universelle si tout opérateur unitaire de n-qbit peut être approché à une précision arbitrairement grande par un circuit composé de portes de cette famille.*

Du fait que l'on doit par exemple être capable de simuler la porte C-NOT, il existe des contraintes sur de telles familles universelles. En particulier, comme C-NOT est intriquante toute famille universelle doit contenir au moins une porte intriquante.

On peut trouver un résultat plus fort :

Théorème 5.12. *Une famille contenant une porte intriquante à 2 qbits, et toutes les portes à 1 qbit, est universelle.*

Ce résultat permet de trouver des familles universelles de portes quantiques en recherchant des familles de portes capables de faire une approximation de précision arbitrairement grande sur les portes à 1 qbit seulement. Ceci est facilité par le théorème suivant.

Théorème 5.13. *Une famille de deux portes à 1 qbit (rotations) est universelle si les deux conditions suivantes sont vérifiées :*

1. *leurs axes ne sont des axes non parallèles sur la sphère de Bloch.*
2. *Si α β sont leurs angles de rotation, $\frac{\alpha}{\pi}$ et $\frac{\beta}{\pi}$ ne sont pas rationels.*

Des exemples de familles de portes universelles sont :
- C-NOT, H (hadamard), et Toffoli.
- NOT, $\sqrt{H}$ et C-NOT.
- la porte C-NOT et toutes les portes sur 1 qbit.

5.4 Efficacité des approximations

Les familles de portes universelles peuvent simuler n'importe quelle transformation unitaire, mais à quel prix ? On voudrait savoir, si il est possible de faire une approximation polynomiale.

Définition 5.14. *On dit qu'on peut faire l'approximation d'une transformation unitaire U de façon polynomiale avec un ensemble de portes E, si on peut l'approcher à une précision ϵ avec un nombre de portes de E polynomial en $\frac{1}{\epsilon}$ et polynomial en le nombre de qbits.*

Par des arguments de dénombrement, on peut montrer que la plupart des transformations unitaires ne peuvent faire l'objet d'une approximation polynomiale. Il existe en effet beaucoup plus de transformations que de circuits pour les calculer. Cependant, comme le montre le théorème de Solovay Kitaev, cette difficulté ne provient pas de la simulation des portes à 1 qbit.

Théorème 5.15. *(Solovay-Kitaev) Soit G un ensemble de portes de 1 qbit dont :*
- *Les axes ne sont pas parallèles dans la sphère de Bloch*
- *Les angles ne sont pas exprimables par multiplication de π par un rationel.*
- *Les inverses peuvent être implémentés par un nombre fini de portes de G.*

Alors, toute porte de 1 qbuit peut faire l'objet d'une approxiation à la précision ϵ en utilisant $O(log^e(\frac{1}{\epsilon}))$ portes de G, où e est une constante positive.