9.1 Marches aléatoires quantiques

Précédemment, nous avons vu que les gains obtenus lors de la recherche d'un élément par un algorithme randomisé pouvaient être encore amélioré par un passage au domaine du quantique, via l'algorithme de Grover. Dans la partie précédente, nous avons pu constater que les marches aléatoires apportent également dans le cadre classique des propriétés intéressantes. Il parait donc légitime de s'interroger sur l'existence d'une extension quantique pouvant éventuellement améliorer encore le gain. Un tel objet existe effectivement et nous allons tout d'abord le définir avant de développer quelques applications.

9.1.1 Réflexion quantique

Le phénomène de réflexion par rapport à un état quantique apparaissait déjà dans l'algorithme de Grover. Il se situe de plus à la base de la marche aléatoire quantique.

Définition 9.1. *La réflexion par rapport à un état quantique $|s\rangle$ consiste à se placer dans la base $(|s\rangle, |s\rangle^{\perp})$ et a prendre l'opposé des amplitudes sur les composantes dans $|s\rangle^{\perp}$.*

Calcul de la réflexion

Remarquons tout d'abord que l'on peut toujours se ramener à $|s\rangle = |0\rangle$. En effet, un changement de base est une transformation unitaire et il existe donc un opérateur quantique réalisant cette opération. Une fois ramené à une réflexion par rapport à $|0\rangle$, il suffit de prendre l'opposé de toutes les amplitudes sur les composantes différentes de $|0\rangle$. On obtient ainsi le calcul de la réflexion.

Reformulation de l'algorithme de Grover

Définition 9.2. *L'algorithme de Grover consiste à rechercher un élément $|x\rangle$ appartenant à un ensemble M d'états marqués. On note ϵ la fréquence des états marqués.*

Lemme 9.3. *L'algorithme de Grover peut s'exprimer grâce à des réflexions successives.*

Preuve: L'opérateur de Grover utilise deux états, $|s\rangle$ et $|t\rangle$. Le premier constitue l'état initial utilisé dans l'algorithme et le second est la superposition uniforme des états marqués. On rappelle que l'opérateur de Grover effectue une rotation d'angle $2 \times \Theta$ où $sin\Theta = \langle t|s\rangle$. Cela est équivalent à deux réflexion successives par rapport à $|t\rangle$ et $|s\rangle^{\perp}$ ou de manière équivalente par rapport à $|t\rangle^{\perp}$ et $|s\rangle$. □

Complexité de la recherche grâce à l'algorithme de Grover

Définition 9.4. *On appelle Setup l'opérateur construisant un état initial $|s\rangle$ à partir de l'état $|0\rangle$. Dans les calculs de complexité, on notera S son coût.*

Définition 9.5. *On appelle Checking l'opération consistant à vérifier l'appartenance d'un état $|x\rangle$ à un ensemble M. Dans les calculs de complexité, on notera C son coût.*

Lemme 9.6. *Si $|t\rangle$ est la projection de $|s\rangle$ sur un ensemble d'états marqués M alors la réflexion par rapport à $|t\rangle^{\perp}$ s'effectue en temps C.*

Preuve: Il suffit en effet d'employer l'opérateur *Checking* sur l'état $|s\rangle$ et de prendre l'opposé des amplitudes des éléments marqués. □

Théorème 9.7. *L'algorithme de Grover s'exécute avec une complexité $S + \frac{1}{\sqrt{\epsilon}} \times (C + 2 \times S)$.*

Preuve: L'algorithme de Grover s'initialise en temps S par un simple appel à *Setup* afin de construite l'état initial $|s\rangle$. On a montré dans le cours 6 que l'algorithme nécessitait ensuite $\frac{1}{\sqrt{\epsilon}}$ itérations. Chacune de ces itérations consiste à effectuer une réflexion par rapport à $|t\rangle^{\perp}$, projection de $|s\rangle$ sur M puis une réflexion par rapport à $|s\rangle$. D'après le lemme ci-dessus, la première étape nécessite un simple appel à *Checking* et s'effectue donc en temps C. La seconde partie nécessite de se ramener en $|0\rangle$ afin d'effectuer la réflexion. Il faut donc inverser *Setup* puis effectuer la réflexion par rapport $|0\rangle$ puis appliquer à nouveau *Setup* pour se replacer dans la bonne base. On a donc un coût par itération de $C + 2 \times S$, la réflexion par $|0\rangle$ étant négligeable par rapport à l'emploi de l'opérateur *Setup*. □

9.1.2 Construction des marches aléatoires quantiques

Cas général

La marche aléatoire classique permet de gagner en complexité en moyenne sur de nombreux problèmes. Il paraît donc intéressant de transposer cette technique dans le domaine quantique. Cependant, il apparaît vite que la transposition quantique des marches aléatoires nécessite de connaître le noeud d'où l'on provient. C'est pourquoi on la construit à partir de la marche aléatoire sur les arêtes.

Les transitions d'une marche aléatoire classique était définies par une matrice stochastique représentant les évolutions possibles à partir d'un noeud. L'analogue quantique remplace ces matrices stochastiques par des opérateurs unitaires. Ces opérateurs sont notés F^x pour tout x sommet du graphe G.

De cette manière, on a définit une amplitude de transition permettant de passer de $|x\rangle$ à $|y\rangle$. Cette amplitude n'est définie que sur les $|y\rangle$ qui sont voisins de $|x\rangle$. C'est pourquoi on parle d'analogie avec la marche sur les arêtes plutôt que sur les sommets.

Une étape de la marche qui consiste à passer de $|x\rangle$ à $|y\rangle$. On utilise un double registre considérant l'origine et la destination de l'arête. On le note $|x\rangle\,|y\rangle$. L'étape se calcule alors en appliquant la transformation unitaire F^x au registre $|y\rangle$ ce qui correspond au parcours des arêtes. Ensuite, on intervertit les deux registres à l'aide d'un opérateur *Swap*. La destination devient ainsi l'origine de la prochaine itération et la précédente origine est prête à recevoir le prochain calcul.

Définition 9.8. *On définit ainsi l'opérateur W tel que :*

$$W = Swap \times (\sum_x |x\rangle\,\langle x| \otimes F^x)$$

Cas particulier utilisé pour l'algorithme de recherche

Dans le cadre de la recherche par marche aléatoire quantique, on cherche à avoir certaines propriétés supplémentaires. Celles-ci concernent principalement l'écart de phase et les états stationnaires. A cette fin, on choisit des opérateurs F^x particuliers tout comme on le faisait dans le cas classique. On introduit l'état $|p_x\rangle = \sum_y \sqrt{p_{xy}}\,|y\rangle$ traduisant les probabilités classique dans le domaine quantique. On définit ensuite les transitions par l'opérateur définit pour chaque x : $F^x = 2\,|p_x\rangle\,\langle p_x| - 1$.

Lemme 9.9. *Soit π une distribution stationnaire de la marche aléatoire alors l'état $|s\rangle = \sum \sqrt{\pi_x}\,|x\rangle\,|p_x\rangle$ est stationnaire.*

Preuve: Appliquons l'opérateur W à l'état $|s\rangle$. La distribution π étant stationnaire, on sait que $\sum_{x\in\pi} \sqrt{\pi_x}\,|p_x\rangle = \sum x \in \pi\sqrt{\pi_x}\,|x\rangle$. On en déduit donc que l'application de l'opérateur W à l'état $|s\rangle$ donne :

$$Swap \times \sum_x (|x\rangle\,\langle x|) \otimes (F^s)$$

$$Swap \times \sum_x (|p_x\rangle)(\sqrt{\pi_x}\,|x\rangle)$$

d'où

$$W\,|s\rangle = \sum_x \sqrt{\pi_x}\,|x\rangle\,|p_x\rangle = |s\rangle$$

□

De plus, un tel opérateur F^x nous assure que la différence de phase vérifie :

$$\Delta(W(P)) = \sqrt{\delta(P)}$$

9.1.3 Recherche par marche aléatoire quantique

Approximation de la réflexion quantique

Dans l'algorithme de Grover vu plus haut, on remarque l'utilisation de *Setup* deux fois afin de calculer la réflexion par rapport à l'état $|s\rangle$. Ces appels pourraient être évités si on pouvait calculer directement la réflexion par rapport à cet état. Prenons une transformation unitaire ayant pour unique vecteur propre $|s\rangle$. Il suffit alors d'effectuer une approximation de phase et d'en déduire le résultat souhaité.

Définition 9.10. *On appellera cette approximation de phase Update et sa complexité sera notée U. Cette opération utilise une différence de phase Δ.*

Lemme 9.11. *La complexité de chaque itération de l'algorithme de Grover vaut maintenant $C + 2 \times U \times N$ où N est le nombre d'appels nécessaire sur l'opérateur unitaire afin d'obtenir la phase associé à l'état actuel.*

Preuve: Le calcul de la réflexion s'effectue maintenant en trois temps. Tout d'abord on calcule la phase de l'état actuel avec une précision Δ par l'intermédiaire de l'opérateur *Update*. Ce calcul nécessite donc un nombre N d'appels à l'opérateur réflexion associé à la phase que l'on calcul. Il suffit ensuite de vérifier si la phase est nulle. Si ce n'est le cas, on prend l'opposé de l'amplitude. Cette partie s'effectue donc à l'aide de l'opérateur *Checking*. Enfin, afin de pouvoir reprendre le calcul pour la suite, il faut inverser les opérations utilisées dans le calcul de la phase et donc effectuer N appels à *Update* à nouveau. La complexité totale est donc en $C + 2 \times N \times U$. □

Nous avons maintenant besoin d'un opérateur unitaire tel que la grandeur $N \times U$ soit négligeable devant S. L'opérateur W de la marche aléatoire quantique remplit bien cet office et permet donc un gain de complexité sur le calcul de la réflexion.

Utilisation de la marche aléatoire quantique

L'algorithme de recherche de Grover est maintenant simplement modifié afin de prendre en compte la nouvelle manière de calculer la réflexion.

Théorème 9.12. *La recherche par marche quantique s'effectue en temps $S + \frac{1}{\sqrt{\epsilon}} \times (\frac{1}{\sqrt{\delta}} \times U + C)$.*

Preuve: La construction de l'état initial superposé n'est pas modifié est continu d'être effectué par l'opérateur *Setup*. Cependant, les $\frac{1}{\sqrt{\epsilon}}$ itérations utilisent les résultats obtenus précédemment. Il suffit donc de prendre les opposés des états marqués par l'opérateur *Checkin* puis d'effectuer la recherche de phase. Cette recherche doit être effectué avec une précision $\sqrt{\delta}$ car on souhaite obtenir une différence de phase d'au-moins Δ. Il est donc nécessaire d'effectuer $\frac{1}{\sqrt{\delta}}$ appels à l'opérateur *Update*. Il ne reste finalement plus qu'à effectuer la mesure et renvoyer le résultat en temps constant. On obtient ainsi bien la complexité recherchée en $S + \frac{1}{\sqrt{\epsilon}} \times (\frac{1}{\sqrt{\delta}} \times U + C)$. □

Remarquons ainsi que, alors que le passage au quantique permettait de gagner un facteur $\sqrt{\epsilon}$ sur le nombre d'appels nécessaires à une recherche, l'utilisation de la marche aléatoire quantique permet de gagne un facteur $\sqrt{\delta}$ sur le nombre d'appels lors de l'approximation de la réflexion.

9.1.4 Applications

Nous allons maintenant étudier deux exemples d'application de cette recherche par marche quantique. Tout d'abord dans la vérification qu'un ensemble de nombres sont deux à deux distincts puis dans la recherche de triangles dans un graphe.

Eléments deux à deux distincts

On possède une liste de n nombres entiers et on cherche à savoir s'ils sont tous deux à deux distincts. De manière classique, il est évident de trouver un algorithme effectuant cette vérification en temps linéaire puisque l'on peut simplement parcourir la liste en cochant les cases d'un tableau témoin contenant tous les entiers. Ces derniers sont en effet bornés en informatique et de toute façon, l'utilisation d'un tableau dynamique ferait l'affaire sinon, à condition de supposer que la mémoire disponible n'est pas un caractère limitant. Il est également trivial de vérifier que cette complexité linéaire est optimale car il serait impossible de donner une réponse positive sans lire la totalité de l'entrée, ce qui s'effectue en temps linéaire.

En 2002, Scott Aaronson et Yaojun Shi ont démontré le théorème suivant. La démonstration admise ici peut être trouvé dans le journal de l'ACM de juillet 2004.

Théorème 9.13. *La borne minimale de complexité quantique du problème de distinction des éléments est $n^{2/3}$.*

Andris Ambainis a par la suite trouvé un algorithme utilisant la marche quantique sur le graphe de Johnson permettant d'atteindre la borne inférieure. Nous allons donc décrire et étudier la complexité de cet algorithme.

Définition 9.14. *Le graphe de Johnson de paramètres (n, r) est le graphe ayant pour sommets l'ensemble des sous-ensembles de r éléments parmi un ensemble de taille n. Deux sommets sont voisins si et seulement si ils ne diffèrent que d'un élément.*

L'algorithme consiste à tirer un sommet du graphe au hasard puis à effectuer une marche aléatoire à partir de ce sommet. A chaque étape, on vérifie si l'élément nouveau est bien distinct des trois autres éléments du noeud dans lequel on arrive.

Théorème 9.15. *Cet algorithme a une complexité de l'ordre de $n^{2/3}$.*

Preuve: Remarquons tout d'abord que l'écart spectral entre les noeuds du graphe et nécessaire à l'approximation de la réflexion par l'approximation de phase est δ et est de l'ordre de $1/r$. D'autre part, la probabilité de succès ϵ de trouver une collision parmi un noeud aléatoire est équivalent à $(r/n)^2$. En effet, on sélectionne r éléments au hasard sur n au total et on a besoin de deux éléments identiques. La sélection est de l'ordre de r/n pour chaque élément donc la collision a une probabilité de l'ordre de $(r/n)^2$.
On peut donc en déduire que le temps d'exécution de l'algorithme est :

$$S + (n/r)^{2/2}(\sqrt{r} \times U + C)$$

L'opération *Setup* consiste uniquement à choisir r éléments parmi n et est donc effectuée en un temps de l'ordre de r. Les opérations d'*Update* et de *Checking* sont en fait effectuées en temps constant. On arrive donc à la conclusion que la complexité T de l'algorithme vaut :

$$r + \frac{n}{\sqrt{r}}$$

On remarque que, en prenant $r = n^{2/3}$ on obtient bien la complexité recherchée de $n^{2/3}$. □

Corollaire 9.16. *L'algorithme de marche quantique sur le graphe de Johnson est optimal pour le problème de distinction des éléments.*

Recherche de triangle dans un graphe

Ce second problème est plus géométrique. Etant donné un graphe à n noeuds, on cherche à savoir s'il existe un triangle, c'est-à-dire un cycle de longueur trois. De manière classique, ce problème nécessite un parcours sur l'ensemble des arêtes ce qui, sur un graphe quelconque est de l'ordre de n^2. L'utilisation directe de l'algorithme de recherche de Grover permet de réduire cette complexité en $n^{3/2}$. Une borne minimale quantique existe et nous l'admettrons ici, bien qu'elle ne soit par particulièrement précise.

Théorème 9.17. *Une borne minimale pour le problème de recherche de triangle est n.*

L'algorithme développé par Frédéric Magniez, Miklos Santha et Mario Szegedy permet d'améliorer la complexité de ce problème dans des proportions intéressantes. L'idée de base de l'algorithme est d'utiliser deux marches quantiques récursives sur un graphe de Johnson.

Théorème 9.18. *Un tel algorithme a une complexité en $n^{1.3}$.*

Preuve: L'algorithme se développe comme suit. On commence par sélectionner un sous-ensemble A des sommets du graphe G contenant r sommet ainsi que un sommet quelconque$u$ n'appartenant pas à A. Il faut alors construire la restriction du graphe G au sous-ensemble A ce qui se fait en temps r^2. Immédiatement, on vérifie si u forme un triangle avec cette restriction par une recherche quantique en temps $r^{2/3}$.
On entre alors dans la deuxième partie de l'algorithme. On recherche un sommet u formant un triangle avec le sous-graphe $G|_A$ puis on trouve l'arête du triangle contenue dans ce sous-graphe.

Remarquons que trouver une arête appartenant à un triangle revient à trouver un triangle en ajoutant une recherche en $\sqrt{n}$ pour trouver le dernier sommet. La recherche d'un triangle nécessite donc seulement de répéter les deux premières étapes au sein d'une recherche par l'algorithme de Grover sur l'ensemble des sous-graphes de r éléments. On retrouve ainsi une marche de Johnson et la complexité devient $r^2 + (n/r)(\sqrt{r} \times r + \sqrt{n} \times r^{2/3}$.
On remarque qu'en choisissant $r = n^{3/5}$, on obtient bien une complexité en $n^{1.3}$. □