

Etats graphes et calcul quantique

Mehdi Mhalla, Simon Perdrix
Laboratoire Leibniz, Grenoble

14 janvier 2007

Résumé

Quelles sont les ressources minimales nécessaires à un calcul quantique universel? Cette simple question est l'une des plus fondamentales abordées pour la construction d'ordinateur quantique, et c'est l'une des questions les plus étudiées au sein de l'informatique quantique. En 2000, Raussendorf and Briegel [3] ont proposé un nouveau modèle de calcul quantique. Ils ont montré que si certains états quantiques initiaux, appelés états graphes, sont fournis, alors la simple capacité d'appliquer des mesures sur 1 qubit selon un observable dans le plan $X - Y$ ou selon Z , suffit au calcul quantique.

Les états graphes ont été largement étudiés ces cinq dernières années. L'étude récente [2] par Hein *et al.* donne une excellente introduction au domaine et inclut plus de 200 références. Ces travaux ont établi plusieurs résultats fondamentaux sur l'universalité du calcul quantique fondé sur des états graphes, les implémentations d'états graphes, l'intrication représentée par des états graphes, et ils ont prouvé des liens entre des concepts de base et la théorie des graphes.

En particulier, certaines mesures sur 1 qubit peuvent être interprétées comme une transformation sur le graphe.

Nous prouvons dans ce papier, que la capacité d'effectuer des mesures selon un observable dans le plan $X - Z$, sur une grille triangulaire, suffit au calcul quantique. Cette propriété implique que tout graphe est pivot mineur d'une grille triangulaire. De plus nous montrons que cette propriété n'est pas vérifiée par la grille standard, ou encore la grille hexagonale. Alors que les résultats de théorie des graphes ont permis de prouver des propriétés sur les états graphes (Bouchet [1] par exemple), nous présentons ici une implication inverse où les résultats quantiques permettent de déduire des propriétés sur les graphes.

1 Définitions

Un *état graphe* sur n bits quantiques (qubits) est un état quantique qui est une superposition de tous les états de base, i.e. un vecteur dans un \mathbb{C} espace vectoriel de dimension 2^n , dont une base est noté $\{|x\rangle, x \in \{0, 1\}^n\}$ ¹. Etant donné G , l'état graphe correspondant est noté $|G\rangle$:

$$|G\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{q_\Gamma(x)} |x\rangle, \quad (1)$$

où Γ est la matrice d'adjacence de $G = (V, E)$ sur $n = |V|$ sommets et $q_\Gamma(x) = \sum_{i < j: (i,j) \in E} x_i x_j$. La forme quadratique q_Γ vérifie $q_\Gamma(x) = x^T \Gamma^{\text{upper}} x$ où x est vu comme un vecteur colonne de $\{0, 1\}^n$, x^T est le vecteur transposé de x et Γ^{upper} est une matrice triangulaire supérieure obtenue à partir de Γ telle que $\forall i < j, \Gamma_{i,j}^{\text{sup}} = \Gamma_{i,j}$.

¹En informatique quantique, $|\phi\rangle$ est une notation pour le vecteur ϕ

2 Equivalence locale

L'intrication est un phénomène particulièrement important en informatique quantique. Elle est par exemple un ingrédient essentiel dans le protocole de téléportation quantique, mais également dans le calcul quantique à base d'états graphes proposé par Briegel et Raussendorf.

Non locale, l'intrication est un phénomène qui est invariant par application de transformations *unitaires* (i.e. réversibles) et *locales* (i.e. agissant sur un seul qubit). Des états graphes différents peuvent avoir la même intrication, par exemple tous les graphes connexes à 3 sommets représentent des états graphes ayant la même intrication.

Le problème consistant à savoir si deux graphes représentent des états graphes ayant la même intrication à été en partie résolu par Van den Nest [4] en utilisant la complémentation locale, une transformation sur les graphes étudiée par Bouchet [1] et qui consiste à complémenter le voisinage d'un sommet :

Définition 1 La complémentation locale de $G = (V, E)$ selon $u \in V$ est le graphe $G \star u = G \Delta K_{N_G(u)}$ où $K_{N_G(u)}$ est le graphe complet sur les voisins de u dans G et Δ la différence symétrique.

On dit que deux graphes G et G' sont localement équivalents ssi il existe une suite de complémentations locales transformant G en G' .

Théorème 2 (Van den Nest) Si deux graphes G et G' sont localement équivalents alors $|G\rangle$ et $|G'\rangle$ ont la même intrication.

De plus, la caractérisation de l'intrication par la complémentation locale est une conjecture :

Conjecture 3 G et G' sont localement équivalents ssi $|G\rangle$ et $|G'\rangle$ ont la même intrication.

Etant donné un graphe $G = (V, E)$, un *pivot* selon l'arête $uv \in E$ transforme le graphe G en $G \wedge uv = G \star u \star v \star u$ (voir figure 1). On vérifie facilement que $G \star u \star v \star u = G \star v \star u \star v$ pour tout $uv \in E$. Un pivot correspond à une complémentation du sous graphe tripartite A, B, C .

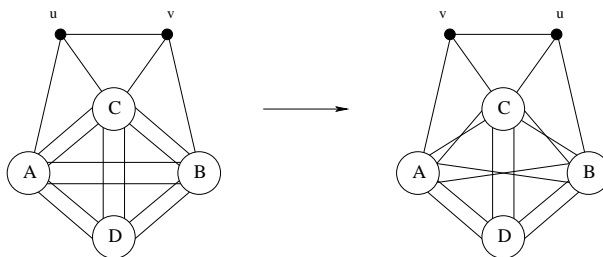


FIG. 1 – Pivot selon uv

Un graphe G est *pivot mineur* d'un graphe G' s'il peut être obtenu à partir de G' par des effacements de sommets et des pivots.

3 Action d'une mesure sur un état graphe

Parmi les évolutions possibles d'un système quantique, il y a des évolutions réversibles : les *transformations unitaires* ; mais également des transformations irréversibles : les *mesures projectives*. Une mesure projective est une opération probabiliste entièrement décrite par un *observable*. Un observable est une matrice M hermitienne ($M^\dagger = M$)². Une telle matrice admet une décomposition spectrale $M = \sum_i \lambda_i P_i$, où les P_i sont des projecteurs ($P_i^2 = P_i$). Une mesure selon un observable $M = \sum_i \lambda_i P_i$ d'un état quantique $|\phi\rangle$ produit avec probabilité $p_i = (|\phi\rangle)^\dagger \cdot P_i |\phi\rangle$ le résultat classique λ_i . L'état quantique du système devient alors $\frac{P_i |\phi\rangle}{\sqrt{p_i}}$.

Des exemples d'observables sont les matrices de Pauli X, Y et Z :

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

On appelle mesure selon un observable dans le plan $X - Y$, une mesure selon un observable de la forme $\cos(\alpha)X + \sin(\alpha)Y$.

Contrairement aux opérations unitaires locales, les mesures projectives modifient l'intrication d'un état graphe. Plus précisément, après la mesure d'un qubit d'un état graphe, le qubit mesuré n'est plus intriqué avec les autres qubits, on considère que ce qubit est consommé par la mesure. Ainsi la mesure d'un qubit d'un état graphe à n qubits, produit un état quantique à $n - 1$ qubits. Pour certains observables, l'état produit par la mesure est un état graphe :

- Pour tout $G = (V, E)$ et pour tout qubit $v \in V$, la mesure de v selon Z transforme $|G\rangle$ en $|G \setminus v\rangle$. Une mesure selon Z peut donc être interprétée comme une suppression de sommet.
- Pour tout $G = (V, E)$ et pour toute paire de qubits $(u, v) \in E$, les mesures de u et v selon X transforment $|G\rangle$ en $|(G \wedge uv) \setminus u \setminus v\rangle$ (voir figure 2).

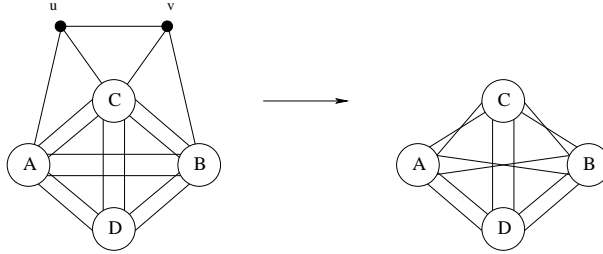


FIG. 2 – Mesures de u et v selon X

Un résultat fondateur sur l'utilisation des états graphes en informatique quantique a été prouvé par Briegel et Raussendorf [3] : toute transformation unitaire sur un ou plusieurs qubits peut être simulée en appliquant sur un état graphe $|G\rangle$, où G est une grille, des mesures selon l'observable Z ou selon un observable dans le plan $X - Y$.

Sachant que tout algorithme quantique peut être décrit par une transformation unitaire, le modèle de calcul consistant à mesurer les qubits d'un état graphe constitue un modèle universel de calcul quantique.

Une conséquence de l'universalité du modèle de Briegel et Raussendorf est le résultat suivant :

² M^\dagger est l'adjoint de M , i.e. la transposée conjuguée de M

Lemme 4 *Pour tout graphe $H = (V, E)$, il existe une grille $G = (V', E')$ telle que des mesures selon X, Y ou Z transforment l'état graphe $|G\rangle$ en $|H\rangle$.*

La question de l'obtention d'un état graphe particulier à partir d'une grille est une question importante au niveau de l'implémentation physique. En effet, un état graphe "régulier" comme une grille peut être relativement facilement produit physiquement, alors qu'un état graphe quelconque est actuellement impossible à obtenir directement. La démarche consiste donc à produire un état graphe régulier comme une grille, puis à mesurer une partie des qubits pour transformer la grille en le graphe désiré.

Le lemme 4 montre que la capacité à mesurer des qubits selon X, Y ou Z suffit à la production de tout état graphe à partir d'une grille. Nous étudions dans la suite la possibilité de produire tout état graphe en n'utilisant que des mesures selon X et Z . Nous donnons également une interprétation en théorie des graphes des résultats.

4 Pivot mineur

Nous allons ensuite prouver une propriété de théorie des graphes en nous fondant sur des résultats quantiques.

Théorème 5 *Tout graphe est pivot mineur d'une grille triangulaire.*

Preuve Pour prouver ce théorème on va réduire le problème à un problème quantique et ce en deux étapes.

- Tout état graphe peut être obtenu à partir d'une série de mesures selon X et Z à partir d'un état graphe correspondant à une grille triangulaire. Pour cela on va d'abord se placer dans le modèle des circuits quantiques (circuits composés de portes correspondant à des transformations unitaires sur un ou deux qubits et analogue du modèle des circuits logiques classiques). On va alors prouver qu'il existe un circuit planaire composé uniquement de 2 types de portes H et ΛZ pour préparer tout état graphe (lemme 7). On prouvera ensuite que les portes $H, \Lambda Z$ et l'identité peuvent être simulées en n'utilisant que des mesure selon X et Z sur la grille triangulaire.
- On prouvera enfin que toute séquence de mesure selon X et Z peut être interprétée graphiquement comme effacements de sommet et pivots. (lemme 6)

□

Lemme 6 *Toute préparation d'état graphe utilisant des mesures selon X et Z peut être faite en utilisant des mesures selon Z , et selon X uniquement sur des paires de sommets voisins.*

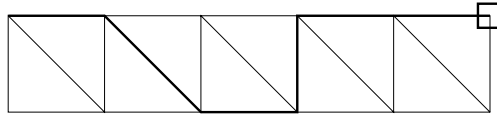
Preuve Considérons une mesure selon X , par commutativité on peut considérer que c'est la première mesure. Le nouvel état après la mesure est point fixe d'un opérateur de Pauli ne contenant que des Z . Or aucun état graphe ne vérifie cette propriété qui ne peut être changée que par une mesure selon X d'un voisin. □

Lemme 7 *Pour tout graphe G , il existe un circuit planaire C_G composé de ΛZ et de H uniquement, pour préparer $|G\rangle$.*

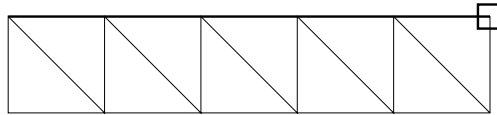
Preuve La porte ΛZ suffit pour engendrer les états graphes [2], il existe alors un circuit planaire composé de ΛZ et de $SWAP$ pour préparer tout état graphe. Il suffit ensuite de remarquer que la porte $SWAP$ se décompose en ΛZ et H . \square

La simulation par mesure selon X et Z de tout circuit utilisant les portes ΛZ et H peut se visualiser par les figures suivantes (les sommets sur les traits épais sont mesurés selon X et les autres selon Z (à noter qu'il est important de pouvoir simuler l'identité dans ce genre de modèle pour des raisons de synchronisme pour la composabilité). L'état des qubits de sortie (représentés par un carré) correspond à l'application de la transformation unitaire à simuler aux qubits d'entrée (qubits en gras sur la première colonne).

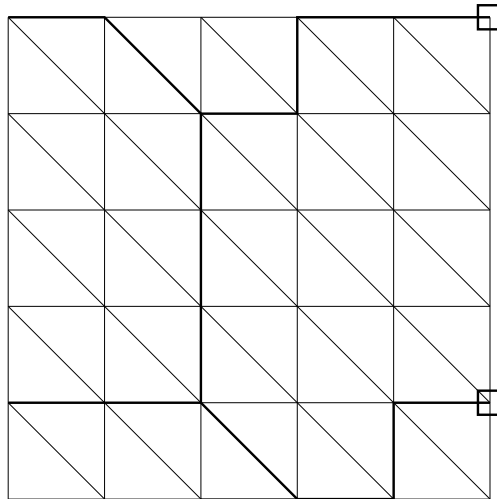
– Simulation de Id :



– Simulation de H :



– Simulation de ΛZ :



Nous allons ensuite prouver que la grille standard (modèle utilisé pour le calcul par mesure) ne permet pas de générer par pivot mineur tous les graphes.

Théorème 8 Pour tout graphe G et toute arête uv de G si G n'a pas de cycle impair alors $G \wedge uv$ n'a pas de cycle impair.

Preuve

Si G n'a pas de cycles impair alors pour tout arête uv :

1. Le voisinage commun C de u et v est vide,
2. Les voisinages A et B sont des stables.
3. Tout chemin $u_1 \dots u_n$ entre deux sommets de B (de A), n a un nombre pair d'arêtes.
4. Tout chemin $u_1 \dots u_n$ entre un sommet de A et un sommet de B a un nombre impair d'arêtes.

Par l'absurde, supposons qu'après le pivot sur l'arête uv on ait créé un cycle impair alors on a créé un chemin avec un nombre pair d'arêtes entre A et B (en effet le pivot ne fait que créer et retirer des arêtes entre A et B).

Considérons un plus court chemin w, P, w' dans $G' = G \wedge uv$ qui viole 3 ou 4. P doit intersecter $A \cup B$ sinon le chemin contredirait 3 ou 4 pour G . Il est donc de la forme $wP_1w''P_2w'$ et la minimalité amène donc à une contradiction. □

Corollaire 9 :

- Il existe un graphe qui n'est pas pivot mineur de la grille.
- Il existe un graphe qui n'est pas pivot mineur de la grille hexagonale.

On voit alors que la grille triangulaire offre un avantage par rapport a la grille standard : elle permet de se contenter de mesures dans un seul plan.

Théorème 10 toute transformation unitaire sur un ou plusieurs qubits peut être simulée en appliquant sur un état graphe $|G\rangle$, où G est une grille triangulaire, des mesures selon un observable dans le plan $X - Z$.

Références

- [1] André Bouchet. Connectivity of isotropic systems. In *Combinatorial Mathematics : Proceedings of the Third International Conference, 1995*, volume 555 of *Ann. New York Acad. Sci.*, pages 81–93. New York Acad. Sci., 1989.
- [2] Marc Hein, Wolfgang Dür, Jens Eisert, Robert Raussendorf, Maarten Van den Nest, and Hans Jürgen Briegel. Entanglement in graph states and its applications. In *Proceedings of the International School of Physics "Enrico Fermi" on "Quantum Computers, Algorithms and Chaos"*, Quantum Computers, Algorithms and Chaos, July 2005.
- [3] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86 :5188–5191, May 2001.
- [4] Maarten Van den Nest. *Local equivalence of stabilizer states and codes*. PhD thesis, Faculty of Engineering, K. U. Leuven, Belgium, May 2005.