ZX-Calculs pour l'informatique quantique, et leur complétude

Renaud Vilmart [1]

Renaud Vilmart a soutenu sa thèse [2] opérée au sein du LORIA sous la direction de Emmanuel Jeandel et Simon Perdrix le 19 septembre 2019 à l'université de Lorraine.

Mes travaux de thèse ont porté sur des problèmes de complétude pour un langage graphique dédié au calcul quantique nommé ZX-Calcul.

Approche graphique de l'informatique quantique

En calcul quantique, la brique élémentaire de l'information est un bit quantique, ou *qubit*. Un qubit est simplement une combinaison linéaire complexe des deux bits classiques 0 et 1. On peut ainsi voir un qubit comme un élément de $\mathbb{C}^2$.

La juxtaposition de deux systèmes quantiques s'obtient mathématiquement en effectuant leur produit tensoriel. Ainsi, un état sur n qubits est représenté par un vecteur de $\mathbb{C}^{2^n}$, et un opérateur quantique, opérant sur un état de n qubits pour obtenir un état de m qubits est représenté par une application linéaire de $\mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$. Du fait de la taille des espaces considérés, l'approche matricielle n'est pas idéale pour représenter opérateurs et états quantiques.

Pour résoudre ce problème, une inspiration peut être prise du côté « classique » du calcul, où les fonctions booléennes peuvent être représentées par des circuits booléens (cf. figure 1(a)). Dans ces derniers, l'information (bit) transite à travers des

1. vilmart@lsv.fr.

2. https://tel.archives-ouvertes.fr/tel-02395443.

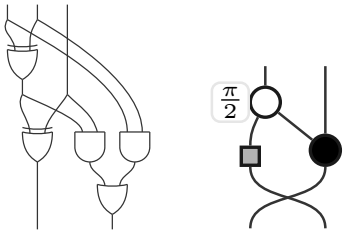


FIGURE 1. Un circuit booléen (a) et un diagramme ZX (b).

fils, auxquels sont appliquées des portes logiques. Les entrées et les sorties d'un programme sont visualisées par les fils du haut et du bas respectivement. Des programmes peuvent ensuite être composés et joignant les fils de sortie du premier circuit aux fils d'entrée du deuxième. Cette représentation a comme intérêt, entre autres, d'être proche d'une implémentation physique du calcul (les portes logiques sont réalisées sur nos ordinateurs par des transistors).

Différentes représentations graphiques des systèmes quantiques ont donc été introduites, parmi lesquelles les circuits quantiques (le modèle le plus fréquemment utilisé à l'heure actuelle), et le ZX-Calcul, qui a été au centre de ma thèse.

Le ZX-Calcul a été introduit en 2008 par Bob Coecke et Ross Duncan [1], et est issu de l'application de la théorie des catégories à l'informatique quantique. Les objets manipulés dans ce langage sont appelés des diagrammes (cf. figure 1(b)), et sont composés des portes élémentaires [3] α , α , . Les deux premières sont duales l'une de l'autre, elles ont un nombre arbitraire d'entrées et de sorties, et sont paramétrées par un angle $\alpha \in \mathbb{R}$. Par convention, cet angle est choisi comme étant 0 s'il n'est pas spécifié.

Ces portes élémentaires peuvent ensuite être connectées par des fils, en utilisant , , et , et le résultat de ces compositions représente une application linéaire. Étant donné un diagramme D, on note $[\![D]\!]$ cette application linéaire. En particulier, $[\![\,|\,]\!]$ est l'identité sur $\mathbb{C}^2$, tandis que $[\![\,\cap\,]\!]$ est un état intriqué (non séparable) particulier sur deux qubits.

Ces diagrammes obtenus par compositions des portes élémentaires permettent de représenter toutes les applications linéaires de dimension une puissance de 2. En d'autres termes, n'importe quel opérateur quantique $\mathbb{C}^{2^n} \to \mathbb{C}^{2^m}$ peut être représenté

3. Les portes élémentaires sont en réalité verte, rouge, et jaune respectivement. Elles ont été adaptées en nuance de gris pour un tirage en noir et blanc.

par un diagramme ZX avec n fils d'entrée et m fils de sortie. On dit que le langage est *universel*.

Théorie équationnelle et complétude

Un problème soulevé par cette approche graphique, est que la représentation d'un opérateur quantique n'est pas unique. De la même façon que deux circuits booléens différents peuvent représenter la même fonction booléenne, deux diagrammes ZX peuvent représenter le même opérateur (il existe deux diagrammes différents D_1 et D_2 tels que $[\![D_1]\!] = [\![D_2]\!]$).

Une démarche possible pour remédier à ce problème est l'introduction d'une *théorie équationnelle*, c'est-à-dire un ensemble d'équivalences de diagrammes (ou axiomes) qui permettent de déterminer s'ils représentent le même opérateur. Un tel ensemble d'axiomes est donné en figure 2. Dans l'axiome (EU), les angles β_i sont obtenus à partir des angles α_i de façon non-triviale, et qu'on ne spécifiera pas ici.

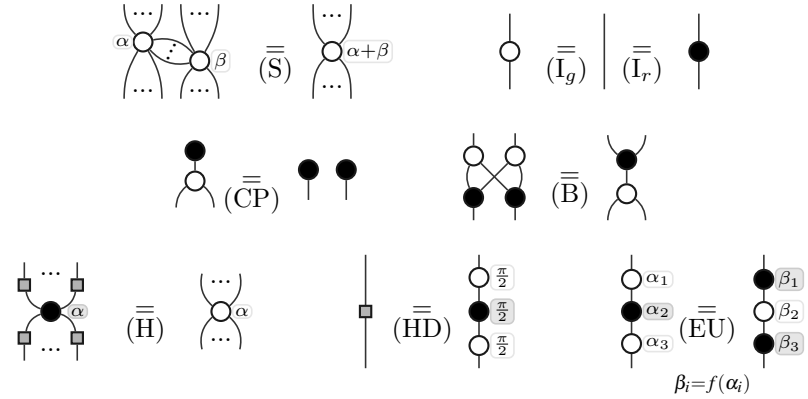
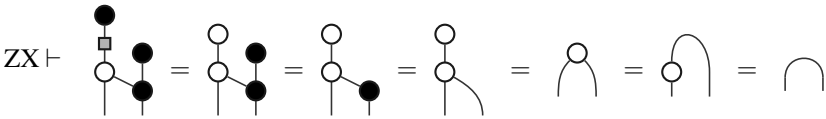


FIGURE 2. Une axiomatisation possible pour le ZX-Calcul.

À ces axiomes viennent s'en ajouter d'autres, plus élémentaires, qui peuvent être regroupés dans le résultat suivant : toute déformation de diagramme est une transformation valide. On peut alors démontrer, par exemple :



où « ZX $\vdash$ » signifie qu'on utilise les axiomes ci-dessus pour faire cette dérivation.

On peut alors se demander si l'on dispose de *suffisamment* d'axiomes. C'est le problème de complétude. Le langage est dit *complet* s'il possède la propriété suivante :

$$\forall D_1, D_2,\ \ [\![D_1]\!] = [\![D_2]\!] \iff \mathrm{ZX} \vdash D_1 = D_2$$

En d'autres termes, le langage est complet s'il possède suffisamment d'axiomes pour transformer un diagramme en un autre lorsqu'ils représentent tous deux le même opérateur.

Ce problème n'est pas aisé à résoudre, et a d'abord été traité pour des restrictions du langage (appelées *fragments*). Un fragment n'est en général plus universel, mais il peut être *approximativement universel*, c'est-à-dire que l'on peut approcher avec la précision voulue n'importe quel opérateur quantique avec des diagrammes du fragment. C'est le cas par exemple du fragment $\frac{\pi}{4}$, obtenu en restreignant les angles dans  et  à des multiples de $\frac{\pi}{4}$.

Contributions

Au début de ma thèse, il n'existait pas de résultat de complétude pour un fragment approximativement universel du ZX-Calcul. Cette question de complétude dans un fragment approximativement universel peut d'ailleurs être également posée pour les circuits quantiques mais, à nouveau, sans réponse positive.

Une percée a été obtenue lorsque mes directeurs de thèse et moi avons donné un ensemble d'axiomes spécifique au fragment $\frac{\pi}{4}$ et démontré sa complétude [4]. Notre méthode de preuve a ensuite été réutilisée par une équipe oxfordienne pour obtenir un résultat similaire dans le langage entier [3], au prix de l'introduction de nouveaux générateurs et d'un nombre conséquent d'axiomes. Nous avons ensuite nous-mêmes fourni un ensemble d'axiomes plus concis pour le langage sans restriction [5], puis affiné ce résultat via l'utilisation de formes normales [6]. Enfin, j'ai réduit l'ensemble d'axiomes à celui donné en Figure 2 en montrant que l'on préservait la complétude [8].

Ce dernier résultat est particulièrement intéressant, car on peut donner une interprétation très naturelle à chacun de ces axiomes, qui ont par ailleurs été démontrés comme étant (presque) minimaux (c'est-à-dire qu'aucun des axiomes ne peut être déduit des autres, à l'exception de (B) pour lequel il n'existe pas encore de preuve).

Applications

Le ZX-Calcul possède deux propriétés très importantes, qui lui procurent une utilité particulière :

> (1) sa souplesse : en effet, il s'abstrait de contraintes physiques qui ont dicté la conception d'autres modèles comme les circuits quantiques ou le calcul par mesure. Cette souplesse lui permet entre autres d'unifier les différents modèles cités à l'instant. Le langage est d'ailleurs en train de gagner du terrain comme le langage par défaut pour décrire des systèmes quantiques ;

(2) sa théorie équationnelle, qui de plus est très intuitive. Celle-ci peut d'une part être utilisée pour prouver formellement qu'un processus quantique vérifie sa spécification, e.g. [2]. Elle peut, d'autre part, être utilisée pour optimiser l'implémentation de processus quantiques [7]. Cela fait du ZX-Calcul le candidat parfait pour un compilateur à l'interface d'un langage de programmation quantique haut-niveau et du matériel physique sur lequel les programmes vont être implémentés.

Références

[1] Bob Coecke and Ross Duncan. Interacting quantum observables : Categorical algebra and diagrammatics. *New Journal of Physics*, 13(4) :043016, Apr 2011.

[2] Ross Duncan and Maxime Lucas. Verifying the Steane code with Quantomatic. In Bob Coecke and Matty Hoban, editors, *Proceedings of the 10th International Workshop on Quantum Physics and Logic, Castelldefels (Barcelona), Spain, 17th to 19th July 2013*, volume 171 of *Electronic Proceedings in Theoretical Computer Science*, pages 33–49. Open Publishing Association, 2014.

[3] Amar Hadzihasanovic, Kang Feng Ng, and Quanlong Wang. Two complete axiomatisations of pure-state qubit quantum computing. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 502–511, New York, NY, USA, 2018. ACM.

[4] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A complete axiomatisation of the ZX-calculus for Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 559–568, New York, NY, USA, 2018. ACM.

[5] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. Diagrammatic reasoning beyond Clifford+T quantum mechanics. In *Proceedings of the 33rd Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '18, pages 569–578, New York, NY, USA, 2018. ACM.

[6] Emmanuel Jeandel, Simon Perdrix, and Renaud Vilmart. A generic normal form for zx-diagrams and application to the rational angle completeness. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–10, June 2019.

[7] Aleks Kissinger and John van de Wetering. Reducing the number of non-clifford gates in quantum circuits. *Phys. Rev. A*, 102 :022406, Aug 2020.

[8] Renaud Vilmart. A near-minimal axiomatisation of zx-calculus for pure qubit quantum mechanics. In *2019 34th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS)*, pages 1–10, June 2019.