

Une approche graphique pour la simulation et la vérification en informatique quantique

Sujet thèse 2018

Encadrement : Simon Perdrix (simon.perdrix@loria.fr), Emmanuel Jeandel (emmanuel.jeandel@loria.fr)

Lieu : Loria (équipe Mocqua), Nancy

Date début : Automne 2018.

Contexte

L'informatique quantique est un sujet de recherche en plein essor. Un traitement quantique de l'information permet en théorie de résoudre certains problèmes informatiques hors de portée des ordinateurs classiques. Les annonces de Google¹, le flagship européen sur les technologies quantique, les programmes britannique (NQIT²) et néerlandais (QuTech³) ainsi que la commercialisation de nouvelles machines quantiques par la société D-Wave⁴, démontrent que l'informatique quantique est en train d'entrer dans une nouvelle ère. L'émergence de machines quantiques est très prometteuse, mais ouvre aussi des nouvelles problématiques concrètes comme la programmation et la vérification quantique de ces machines. En effet, les machines quantiques commercialisées aujourd'hui sont-elles véritablement quantiques ? Peut-on les simuler efficacement avec un ordinateur classique ? L'émergence de l'ordinateur quantique doit aussi être accompagnée de langages de programmation adaptés. Le développement d'outils et de méthodes formelles

¹<https://www.aps.org/publications/apsnews/201705/quantum.cfm>

²Networked Quantum Information Technologies, <http://nqit.ox.ac.uk>

³Quantum Technology, <http://qutech.nl>

⁴<http://www.dwavesys.com>

permettant la vérification et l'utilisation de machines quantiques est donc essentiel dans le développement de l'ordinateur quantique.

Le ZX-calculus [4] est un puissant langage graphique pour l'informatique quantique. Le ZX-calculus a de multiples applications en théorie de l'information quantique [5] : codes correcteurs d'erreurs quantiques [2, 3, 8, 9], calcul par mesures [6, 10, 11], mais aussi questions fondamentales de mécanique quantique [1, 7].

Objectifs

Le ZX-calculus est un langage de diagrammes, muni d'une puissante théorie équationnelle [12] qui permet de décider si deux diagrammes représentent la même évolution quantique. Cependant décider si deux diagrammes sont équivalents peut nécessiter un grand nombre d'étapes de calcul.

- Le premier objectif sera de développer des techniques permettant de donner des conditions nécessaires à l'équivalence de diagrammes, basées par exemples sur des invariants, ou des évaluations aléatoires des diagrammes.
- Le deuxième objectif sera de développer des algorithmes permettant d'évaluer et de simuler efficacement des diagrammes du ZX-calculus et aussi d'identifier des familles de diagrammes pour lesquels le calcul de la sémantique peut être efficace, par exemple en utilisant des propriétés structurelles comme la largeur arborescente.
- Enfin, les points précédents seront également abordés dans le cas où les diagrammes sont paramétrés par des variables: à quelle condition peut-on peut-on réduire le problème au cas sans variables ?

Les résultats théoriques de ces trois points seront implémentés et intégrés à l'outil Quantomatic [13, 14], un assistant de preuve diagrammatique.

References

- [1] Miriam Backens & Ali Nabi Duman (2014): *A complete graphical calculus for Spekkens' toy bit theory*. *Foundations of Physics*, pp. 1–34, doi:10.1007/s10701-015-9957-7.

- [2] Niel de Beaudrap & Dominic Horsman (2017): *The ZX calculus is a language for surface code lattice surgery*. In: *QPL 2017*. Available at <https://arxiv.org/abs/1704.08670>.
- [3] Nicholas Chancellor, Aleks Kissinger, Joschka Roffe, Stefan Zohren & Dominic Horsman (2016): *Graphical Structures for Design and Verification of Quantum Error Correction*. Available at <https://arxiv.org/abs/1611.08012>.
- [4] Bob Coecke & Ross Duncan (2011): *Interacting quantum observables: categorical algebra and diagrammatics*. *New Journal of Physics* 13(4), p. 043016. Available at <http://stacks.iop.org/1367-2630/13/i=4/a=043016>.
- [5] Bob Coecke & Aleks Kissinger (2017): *Picturing Quantum Processes: A First Course in Quantum Theory and Diagrammatic Reasoning*. Cambridge University Press, doi:10.1017/9781316219317.
- [6] Ross Duncan (2013): *A graphical approach to measurement-based quantum computing*. doi:10.1093/acprof:oso/9780199646296.003.0003.
- [7] Ross Duncan & Kevin Dunne (2016): *Interacting Frobenius Algebras Are Hopf*. In: *Proceedings of the 31st Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2016*, ACM, New York, NY, USA, pp. 535–544, doi:10.1145/2933575.2934550. Available at <http://doi.acm.org/10.1145/2933575.2934550>.
- [8] Ross Duncan & Liam Garvie (2017): *Verifying the Smallest Interesting Colour Code with Quantomatic*. Available at <https://arxiv.org/abs/1706.02717>.
- [9] Ross Duncan & Maxime Lucas (2014): *Verifying the Steane code with Quantomatic*. *Electronic Proceedings in Theoretical Computer Science* 171, pp. 33–49, doi:10.4204/EPTCS.171.4.
- [10] Ross Duncan & Simon Perdrix (2010): *Rewriting measurement-based quantum computations with generalised flow*. *Lecture Notes in Computer Science* 6199, pp. 285–296, doi:10.1007/978-3-642-14162-1_24. Available at <http://personal.strath.ac.uk/ross.duncan/papers/gflow.pdf>.

- [11] Clare Horsman (2011): *Quantum picturalism for topological cluster-state computing*. *New Journal of Physics* 13(9), p. 095011. Available at <http://stacks.iop.org/1367-2630/13/i=9/a=095011>.
- [12] Emmanuel Jeandel, Simon Perdrix & Renaud Vilmart (2017): *A Complete Axiomatisation of the ZX-Calculus for Clifford+T Quantum Mechanics*. LICS'18. Available at <https://hal.archives-ouvertes.fr/hal-01529623>. ArXiv:1705.11151.
- [13] A. Kissinger, L. Dixon, R. Duncan, B. Frot, A. Merry, D. Quick, M. Soloviev & V. Zamdzhiev (2011): *Quantomatic*. Available at <https://sites.google.com/site/quantomatic/>.
- [14] Aleks Kissinger & Vladimir Zamdzhiev (2015): *Quantomatic: A Proof Assistant for Diagrammatic Reasoning*. In Amy P. Felty & Aart Middeldorp, editors: *Automated Deduction - CADE-25*, Springer International Publishing, Cham, pp. 326–336, doi:10.1007/978-3-319-21401-6_22.