

Titre du travail de thèse :

Etude théorique et expérimentale de l'intrication à grande dimension dans les algorithmes et les protocoles de communication quantiques.

Directeur et encadrant :

Directeur : J.-M. Merolla, CR1, HDR de l'Université de Franche-Comté

Co-encadrant (50%) : F. Holweck, Maître de Conférences, UTBM

Description:

Depuis la publication des articles de Shor [1] et Grover [2] nous savons qu'il existe des algorithmes quantiques qui surclassent leurs homologues classiques. En particulier l'algorithme de Shor factorise en temps polynomial les grands nombres, ce qui a pour conséquence de casser le cryptosystème RSA sur lequel s'appuient beaucoup de système de sécurité informatique. Le phénomène quantique d'intrication, i.e. la possibilité que des parties (particules) distinctes d'un système soient corrélées au-delà des capacités classiques, est reconnue comme une des ressources centrales responsable des performances des algorithmes quantiques. Mais le rôle et la nature de cette intrication au cœur des algorithmes ou plus généralement au niveau des communications quantiques, sont encore mal compris. Récemment des études numériques ont été conduites [3,4] sur des algorithmes particuliers mais cette approche ne fournit pas d'explication des phénomènes observés.

On propose d'étudier dans cette thèse l'intrication présente dans les algorithmes quantiques à l'aide d'une modélisation géométrique de l'intrication dans les systèmes multipartites purs à quelques composants [5,6,7,8].

Ce travail devrait permettre de :

1) mieux comprendre, qualitativement, la nature des états intriqués présents dans les algorithmes quantiques connus (Shor, Grover) mais aussi dans des protocoles de communications quantiques (codes-correcteur d'erreur) dans l'esprit de [9].

2) Construire des outils pour comprendre l'intrication dans des grands systèmes et préparer ainsi une déclinaison expérimentale de ce travail. C'est dans ce cadre que le candidat sera amené à proposer une architecture dans le domaine fréquentiel permettant la création et la manipulation de qubits dans un espace à grande dimension.

3) Au-delà de la manipulation de qubits et de la description de leur intrication, ce travail s'attachera à explorer la généralisation des outils mathématiques aux qudits, c'est-à-dire des objets de dimension supérieures à deux. Une démonstration expérimentale sera alors envisagée en utilisant le banc photonique développé.

[1] Shor, P. W. (1999). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2), 303-332.

[2] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* (pp. 212-219). ACM.

[3] Rossi, M., Bruß, D., & Macchiavello, C. (2013). Scale invariance of entanglement dynamics in Grover's quantum search algorithm. *Physical Review A*, 87(2), 022331.

Dossier à envoyer à Arnaud Marchant : arnaud.marchant@utbm.fr – Tel : 03.84.58.35.44

Tous les dossiers incomplets seront refusés.

- [4] Batle, J., Ooi, C. R., Farouk, A., Alkhambashi, M. S., & Abdalla, S. (2016). Global versus local quantum correlations in the Grover search algorithm. *Quantum Information Processing*, 15(2), 833-849.
- [5] Holweck, F., Luque, J. G., & Thibon, J. Y. (2012). Geometric descriptions of entangled states by auxiliary varieties. *Journal of Mathematical Physics*, 53(10), 102203.
- [6] Holweck, F., Luque, J. G., & Thibon, J. Y. (2014). Entanglement of four qubit systems: A geometric atlas with polynomial compass I (the finite world). *Journal of Mathematical Physics*, 55(1), 012202.
- [7] Holweck, F., Luque, J. G., & Planat, M. (2014). Singularity of type D4 arising from four-qubit systems. *Journal of Physics A: Mathematical and Theoretical*, 47(13), 135301.
- [8] Lévy, P., & Holweck, F. (2015). Embedding qubits into fermionic Fock space: Peculiarities of the four-qubit case. *Physical Review D*, 91(12), 125029.
- [9] Holweck F., Jaffali H., & Nounouh Ismael (2016). Grover's algorithm and the Secant varieties. A paraître dans *Quantum Information Processing*