Algorithmes quantiques pour l’algèbre linéaire

Informations pratiques. Le stage se déroulera au centre Inria de Nancy, dans l’équipe [CARAMBA](#). Il sera encadré par Xavier Bonnetain et Pierre-Jean Spaenlehauer.

Contact. xavier.bonnetain@inria.fr, pierre-jean.spaenlehauer@inria.fr

1 Contexte

Algèbre linéaire. Depuis les travaux fondateurs de Strassen [Str69], de nombreux algorithmes pour l’algèbre linéaire ont été proposés, améliorant tant les exposants asymptotiques que la complexité pratique. Il est possible de décomposer ces algorithmes en opérations arithmétiques élémentaires (telles que $(x, y) \mapsto x + y$ et $(x, y) \mapsto xy$) et ainsi obtenir des circuits, dont on peut comparer le nombre d’opérations, la profondeur ou le nombre de bits nécessaires, cf. par exemple [Sto00].

Informatique quantique. En parallèle, un formalisme alternatif de calcul a été développé [Deu85], celui de l’informatique quantique, qui capture ce qu’il est théoriquement possible de faire avec un ordinateur quantique. Ce formalisme travaille sur des *qubits*, qui contiennent des *superpositions* de données, ce qui permet de résoudre certains problèmes plus efficacement. Cette souplesse supplémentaire vient avec une contrainte, qui est que les opérations en informatique quantique doivent être réversibles. On peut toujours décomposer un algorithme en circuit, mais avec des règles légèrement différentes : il n’est pas possible de copier un qubit, et les opérations élémentaires doivent être réversibles (par exemple, $(x, y) \mapsto (x, x + y)$ et $(x, y, z) \mapsto (x, y, z + xy)$).

S’il est toujours possible de transformer un circuit non réversible en circuit réversible, la méthode générale [Ben89] est coûteuse en temps ou en mémoire, et il est possible de faire mieux avec des algorithmes spécialisés.

2 Objectifs

L’objectif du stage est d’étudier des versions réversibles d’algorithmes de calcul formel pour l’algèbre linéaire sur les corps finis — par exemple la résolution de systèmes linéaires ou la multiplication de matrices — qui prendront en entrée une superposition d’états. Le but sera de concevoir des algorithmes quantiques plus efficaces que ceux obtenus par les méthodes génériques de transformation des circuits non réversibles.

References

- [Ben89] Charles H. Bennett. Time/space trade-offs for reversible computation. *SIAM J. Comput.*, 18(4):766–776, 1989.
- [Deu85] David Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400(1818):97–117, 1985.
- [Sto00] Arne Storjohann. *Algorithms for matrix canonical forms*. PhD thesis, ETH Zurich, 2000.
- [Str69] Volke Strassen. Gaussian elimination is not optimal. *Numer. Math.*, 13:354–356, 1969.