

Sujet de thèse. Étude de codes LDPC quantiques

Gilles Zémor, Anthony Leverrier

La construction d'un ordinateur quantique, considérée comme un but réaliste par un nombre grandissant d'institutions, ne pourra voir le jour que grâce à l'utilisation de codes correcteurs quantiques efficaces afin de résister à la décohérence et préserver la continuité du calcul. Les codes dits «LDPC» (Low Density Parity Check), associés à des matrices de parité creuses, constituent la famille sur laquelle la recherche actuelle porte le plus d'efforts, et ceci pour plusieurs raisons. D'un point de vue pratique, les codes LDPC devraient être susceptibles d'admettre les algorithmes de décodage les plus rapides, comme c'est le cas pour les codes LDPC classiques. Cependant, la construction de bons codes se décodant efficacement se heurte à des problèmes théoriques importants. Les constructions de familles de codes LDPC quantiques pouvant corriger un nombre d'erreurs grandissant avec le nombre de qubits ne sont pas très nombreuses et sont délicates à obtenir. En outre, c'est une question très ouverte de savoir quel est le meilleur comportement de la plus petite configuration d'erreur non-correctible, en d'autres termes la plus grande distance minimale d'un code quantique en fonction du nombre n de qubits. Les meilleures constructions connues donnent un comportement de la distance en racine carrée de n , alors qu'on ne connaît aucune borne interdisant une distance linéaire en n , comme pour les codes quantiques généraux sans le caractère LDPC. Mentionnons également que les codes LDPC sont liés à des questions théoriques ouvertes, comme la détermination de la capacité du canal de dépolarisation pour laquelle on comprend que les codes qui l'atteindront devront être au moins partiellement LDPC. Enfin, alors que le décodage des codes LDPC classiques a été énormément étudié et est maintenant relativement bien maîtrisé, le cas quantique a été beaucoup moins investigué, en dehors du cas particulier du code torique de Kitaev.

Nous nous proposons d'aborder la question de la construction de codes quantiques de type LDPC. Nous chercherons à concilier des approches topologiques ou géométriques avec un point de vue combinatoire ou algébrique plus fréquent en théorie des codes classiques. Toutes les constructions de codes LDPC quantiques possèdent une connexion avec le code torique de Kitaev construit à partir d'un pavage simple d'un tore 2-dimensionnel, et il est important de ne pas perdre de vue cette vision géométrique qui a été très fertile. Nous prévoyons de commencer l'étude par l'examen d'une construction récente, due à Guth et Lubotzky [1] qui s'appuie sur des pavages de variétés de dimension 4. Cette construction est seulement la deuxième famille de codes LDPC quantiques de rendement constant

et de distance minimale se comportant comme une puissance de n , la première étant [3]. Une description plus algébrique de la construction de Guth et Lubotzky devrait permettre d'ouvrir la voie vers d'autres familles. Par ailleurs, un point de vue plus explicite et plus adapté aux codes qui nous permettrait d'être plus précis sur leurs paramètres. Enfin, ces codes possédant des propriétés d'expansion, gagneraient à être étudié du point de vue de leur décodage, à la lumière de nos travaux récents exploitant l'expansion pour le décodage [2].

Plus généralement, l'étude des complexes de dimension supérieure dans le but d'aboutir à des constructions de codes quantiques n'est jusqu'à présent qu'esquissée et mérite un regain d'attention. Il sera également opportun de s'intéresser à des bornes supérieures sur la distance minimale des codes quantiques de type LDPC.

Références

- [1] L. Guth and A. Lubotzky, Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds, *J. Math. Physics*, 55(8), 2014.
- [2] A. Leverrier, J-P. Tillich and G. Zémor, Quantum Expander Codes. *Foundations of Computer Science (FOCS) 2015*, pp. 810–824.
- [3] J-P. Tillich and G. Zémor, Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength, *IEEE Trans. Inf. Theory*, Vol. 60, No 2, pp. 1193–1202. 2014.

Talence, le 8 mars 2016

Gilles Zémor
Professeur,
Institut de Mathématiques ,
de Bordeaux, UMR 5251.

A handwritten signature in black ink, appearing to read 'G. Zémor', with a long horizontal flourish extending to the right.