RÉDUCTION QUANTIQUE DE LA RECHERCHE DE MOTS DE CODE COURTS AU PROBLÈME DE DÉCODAGE

THOMAS DEBRIS–ALAZARD, MAXIME REMAUD, AND JEAN-PIERRE TILLICH

Nous donnons une réduction quantique du problème de recherche de mots de petit poids dans un code linéaire aléatoire au problème de décodage en métrique de Hamming. C'est la première fois qu'une telle réduction (classique ou quantique) est obtenue. Celle-ci adapte aux codes linéaires la ré-interprétation due à Stehlé, Steinfield, Tanaka and Xagawa de la réduction quantique de Regev de la recherche de vecteurs courts au problème de la recherche de vecteur proche en réseaux. La métrique de Hamming est bien plus grossière que la métrique euclidienne et cette adaptation a nécessité plusieurs nouveaux ingrédients pour qu'elle fonctionne. Par exemple,

- dans le but d'avoir une réduction significative il est nécessaire en métrique de Hamming de choisir un rayon de décodage suffisamment large et cela nécessite dans beaucoup de cas d'aller au-delà du rayon sous lequel le problème décodage a une solution unique;
- une étape cruciale pour l'analyse de notre réduction est le choix de la distribution d'erreurs qui est donnée à l'algorithme de décodage. Pour les réseaux, les erreurs sont généralement tirées selon une distribution gaussienne. Cependant, il s'avère que la distribution de Bernoulli (l'analogue en codes de la distribution gaussienne) est trop étalée et ne peut donc pas être utilisée pour la réduction en codes. A la place, nous choisissons une distribution uniforme sur les erreurs d'un poids fixé. Ceci rend l'analyse de l'algorithme beaucoup plus délicate qu'avec une distribution de Bernoulli et cela a notamment nécessité des développements asymptotiques précis des polynômes de Krawtchouk;
- enfin, l'ajout d'une étape d'amplification d'amplitude est nécessaire afin d'obtenir le résultat annoncé.

Inria, Saclay
Email address: thomas.debris@inria.fr

Atos Quantum Lab, Les Clayes-sous-Bois and Inria de Paris, Paris 75012
Email address: maxime.remaud@atos.net

Inria de Paris, Paris 75012
Email address: jean-pierre.tillich@inria.fr