Alexandre Wallet
Chargé de Recherche Inria
Equipe-projet CAPSULE
Centre de l'Université de Rennes

Objet : Offre de post-doctorat
Intitulé : *Algorithmes de décision pour le problème des rotations du réseau cubique*

Description : Les problèmes d'isomorphismes entre structures combinatoires ou algébriques sont classiques en théorie de la complexité. Leur difficulté sert parfois de fondation pour des cryptosystèmes, typiquement lorsque la structure algébrique sous-jacente est celle d'un code correcteur d'erreurs ou d'une variété algébrique. Dans le cas des réseaux Euclidiens, autrement dit, des groupes abéliens discrets vivant dans des espaces vectoriels avec une notion de géométrie, le problème est étonnamment peu étudié. Sa version la plus naturelle consiste à décider si un réseau est une rotation du réseau cubique $\mathbb{Z}^n$. Un algorithme dû à Ducas [1] permet de détecter cette situation en temps $2^{n/2+\varepsilon}$, et de conclure ; c'est essentiellement le meilleur algorithme connu à ce jour. Informellement, l'algorithme découvre (ou non) des vecteurs unitaires orthogonaux en cherchant à construire une base bien réduite du réseau ambiant. L'intérêt de la méthode de Ducas est qu'il est suffisant de travailler dans la moitié de la dimension pour résoudre le problème — l'algorithme considère en effet des sous-réseaux et des routines exponentielles en leur dimension. Le critère utilisé pour détecter l'orthogonalité de vecteurs a le bon goût d'être simple à utiliser, mais est cependant peu raffiné et n'exploite pas une partie non négligeable de l'information obtenue après une étape de réduction. Nos expériences et analyses suggèrent en particulier qu'il est possible de réduire ce nombre d'étapes d'une part ; d'autre part qu'il doit être possible de travailler en dimension strictement plus petite que $\frac{n}{2}$, d'un facteur constant. Ce facteur a cependant un impact dans les analyses de sécurité de certains schémas de cryptographie théorique, où tout progrès non négligeable peut entraîner une réévaluation substantielle des paramètres.

L'objectif de ce post-doctorat est dans un premier temps de reprendre l'analyse de Ducas et d'exploiter justement les vecteurs supplémentaires pour raffiner le critère de détection. L'analyse pourra reposer sur des arguments ou hypothèses heuristiques sur le comportement de projections aléaotires et le nombre de vecteurs orthogonaux espérés à chaque étape. Si l'analyse conduit comme escompté à un gain constant dans l'exposant, idéalement une amélioration à $\frac{n}{3}+\varepsilon$, un article sera rédigé dans un second temps pour permette la diffusion du résultat. Nous espérons une soumission dans une conférence en lien avec la théorie de la complexité ou sur des thèmes généraux d'algorithmiques. Un prototype d'implémentation (en Python) de l'algorithme décrit sera espéré en complément des analyses proposées, mais n'est cependant pas un objectif primaire. On veillera à ce que les données expérimentales obtenues pour formuler les hypothèses heuristiques soient publiques et reproductibles. Le post-doctorat est prévu pour une durée de 6 mois et se déroulera dans l'équipe-projet Inria CAPSULE, au laboratoire IRISA du campus Beaulieu de l'Université de Rennes. Il sera supervisé par Alexandre Wallet, chargé de recherche Inria dans cette équipe. Un intérêt et des connaissances basiques en géométrie des nombres et théorie de réductions des réseaux Euclidiens sont un plus, mais ne sont pas strictement nécessaires.

Alexandre Wallet



1. *Provable Lattice Reduction of $\mathbb{Z}^n$ with Blocksize $n/2$*, Léo Ducas, 2023, https://eprint.iacr.org/2023/447