Calcul d'espaces de Riemann–Roch pour les codes géométriques

Elena Berardini
Coding Theory and Cryptology Group
Technical University Eindhoven

Les codes de Reed–Solomon sont largement utilisés pour représenter des données sous forme de vecteurs, de sorte que les données peuvent être récupérées même si certaines coordonnées des vecteurs sont corrompues. Ces codes ont de nombreuses propriétés. Leurs paramètres sont optimaux. Ils permettent de reconstruire des coordonnées qui ont été effacées. Ils sont compatibles avec l'addition et la multiplication de données. Néanmoins, ils souffrent de certaines limitations. Notamment, la taille de stockage des coordonnées des vecteurs augmente de manière logarithmique avec le nombre de coordonnées. Les codes dits géométriques généralisent les codes de Reed–Solomon en bénéficiant des mêmes propriétés, tout en étant libres de ces limitations. Par conséquent, l'utilisation de codes géométriques apporte des gains de complexité, et s'avère utile dans plusieurs applications telles que le calcul distribué sur les secrets [3] et les preuves zero-knowledge [2].

Les codes géométriques sont construits en évaluant des familles de fonctions, appelées espaces de Riemann–Roch, en les points rationnels d'une courbe. Il s'ensuit que le calcul de ces espaces est crucial pour la mise en œuvre des codes géométriques. Dans cet exposé, je présenterai un travail récent en collaboration avec S. Abelard, A. Couvreur et G. Lecerf [1] sur le calcul effectif des bases des espaces de Riemann–Roch de courbes. Après avoir révisé l'état de l'art sur le sujet, je discuterai des idées à la base de notre algorithme, en particulier la théorie de Brill–Noether et l'utilisation des expansions de Puiseux. Les courbes utilisées dans la construction des codes géométriques sont pour la plupart limitées à celles pour lesquelles les bases de Riemann–Roch sont déjà connues. Ce nouveau travail et ceux qui suivront, permettront la construction de codes géométriques à partir de courbes plus générales.

References

[1] S. Abelard, E. Berardini, A. Couvreur, and G. Lecerf. "Computing Riemann-Roch spaces via Puiseux expansions". `https://hal.inria.fr/hal-03281757/file/rrgeneral.pdf`. 2021.

[2] S. Bordage and J. Nardi. "Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes". In: *arXiv preprint arXiv:2011.04295* (2020).

[3] R. Cramer, M. Rambaud, and C. Xing. "Asymptotically-Good Arithmetic Secret Sharing over $Z/p^\ell Z$ with Strong Multiplication and Its Applications to Efficient MPC". In: Springer-Verlag, 2021.