Codes géométriques sur les courbes et les surfaces

Elena Berardini
Coding Theory and Cryptology Group, TU/e

Les codes de Reed–Solomon sont largement utilisés pour représenter des données sous forme de vecteurs. 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 les preuves zero-knowledge [5] et le stockage distribué [4].

Les codes géométriques sont construits en évaluant des familles de fonctions, appelées espaces de Riemann–Roch, en les points rationnels d'une variété. Il s'ensuit que le calcul de ces espaces est crucial pour la mise en œuvre des codes géométriques. Dans la première partie de 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. Au contraire, les algorithmes de calcul des espaces de Riemann–Roch des surfaces ont été très peu étudiés. Cependant, des outils de la géométrie algébrique permettent d'étudier les espaces de Riemann–Roch d'une surface et de déduire des bornes pour les paramètres des codes construits à partir de ceux-ci. Dans la deuxième partie de l'exposé, je présenterai ces outils et les informations qu'on peut en tirer sur les codes. Je discuterai ensuite l'intérêt de certaines familles de surfaces par rapport à d'autres, dans le domaine des codes. Ces résultats font partie de deux travaux avec Y. Aubry, F. Herbaut et M. Perret [2, 3].

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] Y. Aubry, E. Berardini, F. Herbaut, and M. Perret, *Bounds on the minimum distance of algebraic geometry codes defined over some families of surfaces*, 2019. To appear in Contemporary Mathematics of the AMS.

[3] ——, *Algebraic geometry codes over abelian surfaces containing no absolutely irreducible curves of low genus*, Finite Fields and Their Applications, 70 (2021), p. 101791.

[4] A. Barg, K. Haymaker, E. W. Howe, G. L. Matthews, and A. Várilly-Alvarado, *Locally recoverable codes from algebraic curves and surfaces*, in Algebraic geometry for coding theory and cryptography, vol. 9 of Assoc. Women Math. Ser., Springer, Cham, 2017, pp. 95–127.

[5] S. Bordage and J. Nardi, *Interactive oracle proofs of proximity to algebraic geometry codes*, arXiv preprint arXiv:2011.04295, (2020).