Computing Riemann–Roch spaces for algebraic geometry codes

Elena Berardini
Eindhoven University of Technology

Reed–Solomon codes are a well–known technique to represent data in the form of vectors, such that the data can be recovered even if some vector coordinates are corrupted. These codes have many properties. They allow reconstructability of coordinates which have been erased. They ensure the privacy of the data against an adversary learning many coordinates. They are compatible with the addition and the multiplication of data. Nevertheless, they suffer from some limitations. For instance, the storage size of vector coordinates grows logarithmically with the number of coordinates. So–called algebraic geometry (AG) codes are a generalization of Reed–Solomon codes that enjoys the same properties, while being free of these limitations. Therefore, the use of AG codes provides complexity gains, and turns out to be useful in several applications such as distributed storage [2], distributed computation on secrets [4], and zero-knowledge proofs [3]. Algebraic geometry codes are constructed by evaluating spaces of functions, called Riemann–Roch spaces, at the rational points on a curve. It follows that the computation of these spaces is crucial for the implementation of AG codes. In this talk, I will present a recent work joint with S. Abelard, A. Couvreur and G. Lecerf [1] on the effective computation of bases of Riemann–Roch spaces of curves. I will discuss the ideas behind our algorithm, including in particular Brill–Noether theory.

The curves used in the construction of AG codes were for the most part limited to those for which the Riemann–Roch bases were already known. This new work and the ones that will follow will allow the construction of AG codes from more general curves.

References

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

[2] 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. Assoc. Women Math. Ser. Springer, Cham, 2017, pp. 95–127.

[3] S. Bordage, M. Lhotel, J. Nardi, and H. Randriam. *Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes*. Preprint. 2022.

[4] 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.