Lattices over Non-Archimedean Fields and Their Applications to Coding Theory

Michael Schaller
University of Zurich, Switzerland

30th Applications of Computer Algebra - ACA 2025

In this talk we will introduce lattices over non-archimedean fields following the work of Mahler [1] and Lenstra [2]. Welch and Scholtz [3] showed that the Berlekamp-Massey algorithm is closely related to continued fractions over the rational function field. It is well known for the real numbers that continued fractions are closely related to lattices. We will reinterpret the article of Welch and Scholtz in terms of lattice reduction over non-archimedean fields and then we will explore the work of Cohn and Heninger [4] on list decoding from the lattice point of view.

References

[1] K. Mahler. An analogue to Minkowski's geometry of numbers in a field of series. Annals of Mathematics, 42, 1941.

[2] A. K. Lenstra. Factoring multivariate polynomials over finite fields. Proceedings of the fifteenth annual ACM symposium on Theory of computing, 1983.

[3] L. Welch, and R. Scholtz. Continued fractions and Berlekamp's algorithm. IEEE Transactions on Information Theory, 1979

[4] H. Cohn, and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. Advances in Mathematics of Communications, 2015, `http://arxiv.org/abs/1008.1284`,