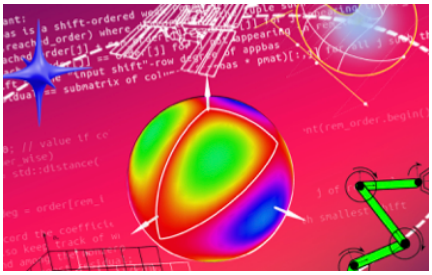

ID de Contribution: **28** Type: **Non spécifié**

Efficient algorithms for Riemann—Roch spaces by Grégoire Lecerf

mardi 26 septembre 2023 15:00 (1 heure)

Abstract. Riemann—Roch spaces are a cornerstone of modern applications of algebra to various areas of computer science: error correcting codes, secret sharing, multi-party computations, zero-knowledge proofs, resilience in distributed storage systems, interactive oracle proofs… Best performances are achieved for specific families of spaces known to be difficult to compute.
We will present a new probabilistic algorithm of Las Vegas type that computes Riemann—Roch spaces of plane projective curves in expected sub-quadratic time whenever the characteristic is zero or positive but sufficiently large. The method relies on the Brill—Noether theory (1874), bivariate polynomial elimination, Puiseux series expansions, and structured polynomial matrices. In case of curves with only ordinary singularities, we will present a faster variant that even supports any characteristic.
This is joint work with Simon Abelard (Thales SIX GTS, France), Elena Berardini (CNRS, University of Bordeaux, France), Alain Couvreur (Inria Saclay, France).