Efficient algorithms for Riemann—Roch spaces

Grégoire Lecerf
CNRS & École polytechnique, France
gregoire.lecerf@lix.polytechnique.fr

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 and recent fast algorithms for Puiseux series and structured polynomial matrices. In case of curves with only ordinary singularities, we will present a faster variant that even supports any characteristic.