The block Wiedemann algorithm and systems of polynomial equations.

Éric Schost

Cheriton School of Computer Science, University of Waterloo, Canada

Coppersmith’s generalization of Wiedemann’s algorithm is a key ingredient in algorithms for integer factorization or discrete logarithms. I will describe how, in the recent years, it has also successfully been applied in contexts arising from algorithms for solving polynomial equations, such as Faugère and Mou’s sparse FGLM algorithm, or Villard’s recent breakthrough on bivariate resultants.