Maxime Dénès
INRIA
"Verifying computer algebra algorithms: refinements and automation to the rescue"

Abstract:

Proof assistants like Coq provide a unified framework to describe the implementation of algorithms and their proofs of correctness. Using such a tool to formalize computer algebra algorithms seems a natural idea, but can be thorny in practice, because of the tension between rich proof-oriented datastructures and efficient computation-oriented implementations. We will describe how refinements can help to separate these concerns, while automation can ease correctness proofs. These techniques have been applied to Karatsuba's polynomial multiplication or Strassen's matrix product, and could help in the proof of the basic perturbation lemma in homological algebra.