

Meeting: 1001, Evanston, Illinois, SS 9A, Special Session on Solving Polynomial Systems

1001-12-401 **Marc Moreno Maza*** (moreno@csd.uwo.ca), Computer Science Department, Middlesex College Building, London, Ontario N6A 5B7, Canada, and **Boulier** and **Oancea**. *On Polynomial Gcds over Direct Products of Fields Given by Towers of Simple Extensions.*

Let K be a field of multivariate rational functions over an infinite field. Let L be a direct product of fields extending K by a tower of algebraic extensions. We present a modular algorithm for computing polynomial gcds over L based on a Hensel lifting strategy.

The rational reconstruction is avoided by guessing the denominator of the gcd before the lifting step. The algorithm may not stop but does terminate with probability one. Our implementation shows a significant improvement with respect to other methods. (Received August 31, 2004)