

Overdetermined Bilinear Polynomial Systems

Paul Mekhail

*Laboratoire MIS, Université de Picardie Jules Verne, Amiens,
France
paul.mekhail@u-picardie.fr*

1 Abstract

Solving multivariate polynomial systems over finite fields is a well-established problem with numerous applications in cryptology. A common approach relies on computing Gröbner bases using state-of-the-art algorithms such as F4 or F5. For generic systems—those that are regular or semi-regular—the F5 algorithm performs no reductions to zero during the computation. Although this genericity assumption is widespread, it does not always hold in practice. Bilinear systems, for example, are neither regular nor semi-regular, and thus require additional care to analyze and to compute their Gröbner bases while avoiding reductions to zero. In a 2011 article, Faugère, Safey El Din, and Spaenlehauer examined underdetermined bilinear systems, introducing a criterion that eliminates all reductions to zero, establishing their genericity in the Zariski topology, and providing a complexity analysis for computing their Gröbner bases. In this work, we extend their analysis to the overdetermined setting. This case is particularly relevant in cryptanalysis, where the results of Faugère et al. are sometimes applied beyond their intended scope. Our generalization formalizes Gröbner basis computations for such systems by introducing the notion of semi-biregularity. Collaboration with Sorina Ionica.

2 Comment

I am currently an ingénieur d'étude awaiting for PhD funding unlocking and would then be a first year PhD.