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 is a well-established problem with numerous applications, including robotics, biology, and 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 inherently non-generic: they 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 an article published in 2011, Faugère, Safey El Din, and Spaenlehauer investigated such systems, providing a complexity analysis for Gröbner basis computation with F5 and introducing a criterion that removes all reductions to zero. 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 overdetermined bilinear systems and clarifies their algorithmic behavior. Collaboration with Sorina Ionica.

2 Comment

Je suis actuellement ingénieur d'étude en attente de confirmation du financement de thèse pour être en première année de thèse.