Cryptology ePrint Archive: Report 2011/164

On the relation between the MXL family of algorithms and Gröbner basis algorithms

Martin Albrecht and Carlos Cid and Jean-Charles Faugère and Ludovic Perret

Abstract: The computation of Gröbner bases remains one of the most powerful methods for tackling the Polynomial System Solving (PoSSo) problem. The most efficient known algorithms reduce the Gröbner basis computation to Gaussian eliminations on several matrices. However, several degrees of freedom are available to generate these matrices. It is well known that the particular strategies used can drastically affect the efficiency of the computations. In this work we investigate a recently-proposed strategy, the so-called "Mutant strategy", on which a new family of algorithms is based (MXL, MXL2 and MXL3). By studying and describing the algorithms based on Gröbner basis concepts, we demonstrate that the Mutant strategy can be understood to be equivalent to the classical Normal Selection strategy currently used in Gröbner basis algorithms. Furthermore, we show that the "partial enlargement" technique can be understood as a strategy for restricting the number of S-polynomials considered in an iteration of the F4 Gröbner basis algorithm, while the new termination criterion used in MXL3 does not lead to termination at a lower degree than the classical Gebauer-Möller installation of Buchberger's criteria. We claim that our results map all novel concepts from the MXL family of algorithms to their well-known Gröbner basis equivalents. Using previous results that had shown the relation between the original XL algorithm and F4, we conclude that the MXL family of algorithms can be fundamentally reduced to redundant variants of F4.

Category / Keywords: foundations /

Publication Info: in submission

Date: received 1 Apr 2011, last revised 18 Jan 2012

Contact author: martinralbrecht at googlemail com