F4 ALGORITHM WITH THE F5'S CRITERIA

CECILIA TONELLI

ABSTRACT. Faugère in [2] gave an algorithm called F4 to compute more efficiently G-bases of ideals (of $K[x_1,\ldots,x_n]$) based on linear algebra, therefore inspired by Lazard (1983). Later in [3] Faugère published the algorithm F5 which has two strong criteria to detect S-polynomials whose reduction is zero, without explicitly calculating the reduction. However it took some years [4] to give a proof that F5 is correct (it returs a G-basis whenever it stops) and, as far as we know, it is only known that F5 stops under some modifications [1]. However F4 with FGLM, and F5 algorithms have been succesfully applied to solve overdetermined systems of equations coming from public cryptography (as HFE), and symmetric cryptography (streem cipher and block ciphers). In our exposition we explain these algorithms, according with Faugère recommendation [3] "...to translate F5 in F4- fashion" and show examples coming from HFE- like systems.

References

- [1] C. Eder, J. Gash, J. Perry, Modifying Faugères's F5 Algorithm to ensure termination.. arXiv: 1006.0318, (Dec. 2010).
- [2] J.C. Faugère, A new efficient algorithm for computing Gröbner bases (F₄) (1999), Journal of Pure and Applied Algebra 139, no. 1-3, pp.61-88.
- [3] J.C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F₅) (2002), ISSAC '02: Proceedings of the 2002 international symposium on Symbolic and algebraic computation (New York, NY, USA), ACM Press, pp. 75-83.
- [4] J.M.Gash, On efficient computation of Gröbner bases (2008), Ph.D. Thesis, University of Indiana.
- [5] D. Lazard, Gröbner-bases, gaussian elimination and resolution of systems of algebraic equations (1983),
 EUROCAL (J. A. van Hulzen, ed.), Lecture Notes in Computer Science, vol. 162, Springer, pp. 146-156.

Università di Pisa, Universidad Complutense de Madrid E-mail address: tonelli@mail.dm.unipi.it