



## 1. DATOS BÁSICOS DEL TFG:

**Título:** Los algoritmos F4 y F5 de Faugère.

**Descripción general** (resumen y metodología):

Las bases de Gröbner son sistemas de ecuaciones que definen las variedades algebraicas y que permiten estudiarlas de manera computacional. En la actualidad son objeto de estudio en la asignatura Álgebra Conmutativa Computacional. En dicha asignatura se explica el primer algoritmo desarrollado para su cálculo, el algoritmo de Buchberger. El cálculo de la complejidad algorítmica del mismo no es sencillo, pero en cualquier caso hay instancias para las que se requiere un número de cálculo muy grande. Hay varias alternativas que buscan mejorar la eficiencia del cálculo de bases de Gröbner. Dos de ellas se deben al matemático francés Faugère, que en los años 1999 y 2002 presentó dos alternativas denominadas F4 y F5. De hecho, la corrección de este último no fue demostrada hasta el año 2012.

En lo que concierne al algoritmo F4, la idea principal consiste en no calcular un resto de S-polinomios en cada iteración, sino en utilizar técnicas de álgebra lineal para calcular varios de estos restos a la vez.

Con respecto al F5, la principal idea consiste en eliminar cálculos innecesarios de S-polinomios explotando la relación con los generadores iniciales. Utiliza la conocida como aproximación basada en firmas.

Este Trabajo de Fin de Grado pretende estudiar ambos algoritmos, demostrando la corrección de los mismos.

**Tipología:** Estudio de casos, teóricos o prácticos, relacionados con la temática del Grado.

**Objetivos planteados:**

1. Estudiar la relación entre el cálculo de bases de Gröbner y el álgebra lineal.
2. Homogenización y deshomogenización de bases de Gröbner.
3. Descripción del algoritmo F4.
4. Uso del criterio de Buchberger para demostrar la corrección de F4.
5. Aproximación basada en firmas.
6. Descripción del algoritmo F5.

**Bibliografía básica:**

- David A. Cox, John Little, Donal O'Shea, Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Undergraduate Texts in Mathematics, Springer Cham, ISSN 0172-6056, <https://doi.org/10.1007/978-3-319-16721-3>. (<https://link.springer.com/book/10.1007/978-3-319-16721-3>)
- Christian Eder, Jean-Charles Faugère, A survey on signature-based algorithms for computing Gröbner bases, Journal of Symbolic Computation, Volume 80, Part 3, 2017, Pages 719-784, ISSN 0747-7171, <https://doi.org/10.1016/j.jsc.2016.07.031>. (<https://www.sciencedirect.com/science/article/pii/S0747717116300785>)
- Jean-Charles Faugère, A new efficient algorithm for computing Gröbner bases (F4), Journal of Pure and Applied Algebra, Volume 139, Issues 1-3, 1999, Pages 61-88, ISSN 0022-4049, [https://doi.org/10.1016/S0022-4049\(99\)00005-5](https://doi.org/10.1016/S0022-4049(99)00005-5).

(<https://www.sciencedirect.com/science/article/pii/S0022404999000055>)

**Recomendaciones y orientaciones para el estudiante:**

**Plazas:** 1

**2. DATOS DEL TUTOR/A:**

**Nombre y apellidos:** FRANCISCO JAVIER LOBILLO BORRERO

**Ámbito de conocimiento/Departamento:** ÁLGEBRA

**Correo electrónico:** jlobillo@ugr.es

**3. COTUTOR/A DE LA UGR (en su caso):**

**Nombre y apellidos:**

**Ámbito de conocimiento/Departamento:**

**Correo electrónico:**

**4. COTUTOR/A EXTERNO/A (en su caso):**

**Nombre y apellidos:**

**Correo electrónico:**

**Nombre de la empresa o institución:**

**Dirección postal:**

**Puesto del tutor en la empresa o institución:**

**Centro de convenio Externo:**

**5. DATOS DEL ESTUDIANTE:**

**Nombre y apellidos:** JORGE RABADAN BEJARANO

**Correo electrónico:** jrabbj@correo.ugr.es