

Título: BASES DE GÖBNER: DESARROLLO FORMAL EN COQ

Nombre: Pérez Vega, Gilberto

Universidad: Universidad de A Coruña

Departamento: INTELIGENCIA ARTIFICIAL Y COMPUTACION

Fecha de lectura: 21/01/2005

Programa de doctorado: COMPUTACIÓN

Dirección:

> **Director:** Barja Pérez José M^a

Tribunal:

> **presidente:** FREIRE NISTAL JOSE LUIS

> **secretario:** MANUEL LADRA GONZÁLEZ

> **vocal:** INMACULADA PEREZ DE GUZMAN MOLINA

> **vocal:** FELIPE GAGO COUSO

> **vocal:** MANUEL OJEDA ACIEGO

Descriptor:

> LOGICA

> LOGICA DEDUCTIVA

> TEORIA DE LA DEMOSTRACION

> TEORIA DE LENGUAJES FORMALES

> POLINOMIOS

> INTUICION

> MATEMATICAS

> ALGEBRA

> LOGICA INDUCTIVA

El fichero de tesis no ha sido incorporado al sistema.

Localización: Biblioteca Xeral - Rectorado - A Maestranza

Resumen: En primer lugar, se aborda, de forma ajustada a lo que se va a necesitar, las nociones más prácticas del sistema Coq que son necesarias para comprender la formalización de la teoría matemática de los polinomios, su reducción y bases de Gröbner.

El trabajo específico comienza con la formalización de los términos de

"n" variables, así como las operaciones más usuales de polinomios en el sistema Coq. Se implementa el orden lexicográfico profundizado en la prueba de que dicho orden es bien fundado.

Para formalizar el anillo de polinomios en varias variables, se describen las pruebas de la estructura de cuerpo abstracto.

Se implementan los polinomios y los polinomios canónicos, formalizando una igualdad explícita de polinomios original, describiendo también sus operaciones. Se implementa el orden de polinomios demostrando que es noetheriano. Asimismo, se implementa el concepto de ideal.

Se generaliza, en el sistema de Coq, el algoritmo de la división de polinomios en varias variables. Una vez implementada dicha división, llamada reducción; se estudia la relación entre congruencia y reducción, obteniéndose la forma normal módulo un conjunto de polinomios.

Finalmente, se introduce el concepto de base de Gröbner, estudiando y probando su equivalencia con otras caracterizaciones alternativas. Para resolver estas equivalencias se da una versión del Lema de Newman, implementando un esquema de recursión sobre polinomios canónicos, así como propiedades de la confluencia de la reducción.