

Involutive Bases

Gareth Evans

University of Wales, Bangor

`gevans@informatics.bangor.ac.uk`

April 20, 2004

Abstract

In this seminar we will start by recalling some Gröbner Bases theory before introducing the notion of an Involutive Basis. We will then define some involutive divisions before looking at the involutive basis completion algorithm.

Gröbner Bases

Recap:

Gröbner Bases

Recap:

- Gröbner Bases involve polynomials over a ring

Gröbner Bases

Recap:

- Gröbner Bases involve polynomials over a ring
- We want to solve the Ideal Membership Problem

Gröbner Bases

Recap:

- Gröbner Bases involve polynomials over a ring
- We want to solve the Ideal Membership Problem
- We add 'S-polynomials' to the system to ensure completion

Gröbner Bases

Recap:

- Gröbner Bases involve polynomials over a ring
- We want to solve the Ideal Membership Problem
- We add 'S-polynomials' to the system to ensure completion
- We are left with unique reductions and a set of irreducible monomials

Involutive Bases: Motivation

Here are some reasons why we might want to study involutive bases:

- An involutive basis is a Gröbner Basis

Involutive Bases: Motivation

Here are some reasons why we might want to study involutive bases:

- An involutive basis is a Gröbner Basis
- There is no 'redundancy' in an involutive basis

Involutive Bases: Motivation

Here are some reasons why we might want to study involutive bases:

- An involutive basis is a Gröbner Basis
- There is no 'redundancy' in an involutive basis
- An involutive basis has extra combinatorial structure

Involutive Bases: Motivation

Here are some reasons why we might want to study involutive bases:

- An involutive basis is a Gröbner Basis
- There is no 'redundancy' in an involutive basis
- An involutive basis has extra combinatorial structure
- Early indications show that the computation of involutive bases is more efficient (e.g. less steps during reduction, ...)

Basic Properties of Involutive Bases

- We impose a restriction on the divisibility of monomials

Basic Properties of Involutive Bases

- We impose a restriction on the divisibility of monomials
- The span of an involutive basis is a disjoint sum of the span of the Gröbner basis (picture)

Basic Properties of Involutive Bases

- We impose a restriction on the divisibility of monomials
- The span of an involutive basis is a disjoint sum of the span of the Gröbner basis (picture)
- For a finite input ideal, an involutive basis may not be finite (unlike a Gröbner Basis which is always finite)

Definitions

- Let us represent monomials as multidegrees or as elements of the Abelian monoid $(\mathbb{N}^n, +)$

Definitions

- Let us represent monomials as multidegrees or as elements of the Abelian monoid $(\mathbb{N}^n, +)$
- An involutive division is defined on $(\mathbb{N}^n, +)$ if a subset of multiplicative variables is associated to each n -tuple or monomial v in a finite subset $\mathcal{N} \subset \mathbb{N}^n$ and two technical conditions on the involutive cones are satisfied.

Definitions

- Let us represent monomials as multidegrees or as elements of the Abelian monoid $(\mathbb{N}^n, +)$
- An involutive division is defined on $(\mathbb{N}^n, +)$ if a subset of multiplicative variables is associated to each n -tuple or monomial v in a finite subset $\mathcal{N} \subset \mathbb{N}^n$ and two technical conditions on the involutive cones are satisfied.
- An involutive division is globally defined if the assignment of the multiplicative indices is independent of the set \mathcal{N} . Otherwise it is locally defined.

Definitions

- Let us represent monomials as multidegrees or as elements of the Abelian monoid $(\mathbb{N}^n, +)$
- An involutive division is defined on $(\mathbb{N}^n, +)$ if a subset of multiplicative variables is associated to each n -tuple or monomial v in a finite subset $\mathcal{N} \subset \mathbb{N}^n$ and two technical conditions on the involutive cones are satisfied.
- An involutive division is globally defined if the assignment of the multiplicative indices is independent of the set \mathcal{N} . Otherwise it is locally defined.
- A monomial division $\frac{m}{n} = p$ is allowed if all the variables in p are multiplicative for n .

Involutive Divisions

One classical example of a globally defined involutive division is the *Pommaret* division P . It assigns the multiplicative variables according to the following simple rule: if $k \in \{1, \dots, n\}$ is the smallest index such that $\mu_k > 0$, then $N_P(\mu) = \{1, \dots, k\}$.

Involutive Divisions

One classical example of a globally defined involutive division is the *Pommaret* division P . It assigns the multiplicative variables according to the following simple rule: if $k \in \{1, \dots, n\}$ is the smallest index such that $\mu_k > 0$, then $N_P(\mu) = \{1, \dots, k\}$.

Another important example is the *Janet* division J . In order to define it, we must introduce certain subsets of the given set $\mathcal{N} \subset \mathbb{N}^n$:

$$(d_k, \dots, d_n) = \{\mu \in \mathcal{N} \mid \mu_i = d_i, k \leq i \leq n\}$$

Involutive Divisions

One classical example of a globally defined involutive division is the *Pommaret* division P . It assigns the multiplicative variables according to the following simple rule: if $k \in \{1, \dots, n\}$ is the smallest index such that $\mu_k > 0$, then $N_P(\mu) = \{1, \dots, k\}$.

Another important example is the *Janet* division J . In order to define it, we must introduce certain subsets of the given set $\mathcal{N} \subset \mathbb{N}^n$:

$$(d_k, \dots, d_n) = \{\mu \in \mathcal{N} \mid \mu_i = d_i, k \leq i \leq n\}$$

Now the index n is multiplicative for a $\mu \in \mathcal{N}$ if $\mu_n = \max_{\nu \in \mathcal{N}} \{\nu_n\}$. The index $k < n$ is multiplicative for an n -tuple $\mu \in (d_{k+1}, \dots, d_n)$, if $\mu_k = \max_{\nu \in (d_{k+1}, \dots, d_n)} \{\nu_k\}$. Obviously, the assignment of multiplicative variables depends here on the set \mathcal{N} .

Determining Janet Multiplicative Variables

Here is an algorithm to determine the Janet multiplicative variables for a set of monomials.

Inputs: A finite list $\mathcal{N} = \{v^{(1)}, \dots, v^{(k)}\}$ of pairwise different monomials from \mathbb{N}^n

Output: A list $N = \{N_{J,\mathcal{N}}(v^{(1)}), \dots, N_{J,\mathcal{N}}(v^{(k)})\}$ of lists of multiplicative variables

BEGIN

$\mathcal{N} = \text{sort}(\mathcal{N}, <_{\text{invlex}})$; $v = \mathcal{N}[1]$;

$p_1 = n$; $I = \{1, \dots, n\}$; $N[1] = I$;

FOR j **from** 2 **to** $|\mathcal{N}|$ **DO**

$p_2 = \max\{i \mid (v - \mathcal{N}[j])_i \neq 0\}$; $I = I \setminus \{p_2\}$;

IF $p_1 < p_2$ **THEN**

$I = I \cup \{p_1, \dots, p_2 - 1\}$;

END_IF

$N[j] = I$; $v = \mathcal{N}[j]$; $p_1 = p_2$;

END_FOR

RETURN N

END

Theorems

Let L be a continuous and constructive division. In the case of termination, the involutive completion algorithm terminates for any finite generating set F of an ideal I with an involutive basis.

Theorems

Let L be a continuous and constructive division. In the case of termination, the involutive completion algorithm terminates for any finite generating set F of an ideal I with an involutive basis.

Both the Pommaret and Janet involutive divisions are continuous and constructive.

Theorems

Let L be a continuous and constructive division. In the case of termination, the involutive completion algorithm terminates for any finite generating set F of an ideal I with an involutive basis.

Both the Pommaret and Janet involutive divisions are continuous and constructive.

Let L be a Noetherian division. Then every ideal I possesses a finite involutive basis with respect to the division L (A bit of a fudge!)

Theorems

Let L be a continuous and constructive division. In the case of termination, the involutive completion algorithm terminates for any finite generating set F of an ideal I with an involutive basis.

Both the Pommaret and Janet involutive divisions are continuous and constructive.

Let L be a Noetherian division. Then every ideal I possesses a finite involutive basis with respect to the division L (A bit of a fudge!)

The Janet division is Noetherian but the Pommaret division is not (the non-termination for the Pommaret division is due to the use of 'bad' coordinates and is the so-called problem of δ -regularity). However for certain ω -type term orders the Gröbner Basis is found after a finite number of steps of computing the Pommaret basis.

The Involutive Completion Algorithm

Here is a simple algorithm to compute an involutive basis.

Inputs: Finite basis F of the ideal I , term order $<$, involutive division L .

Output (in the case of termination): Involutive Basis G of I w.r.t. $<$.

BEGIN

$G = \phi;$

WHILE $F \neq \phi$ **DO**

$G = \text{Autoreduce}(G \cup F);$

$F = \phi;$

FOR EACH $g \in G$ **DO**

FOR EACH X_i **WHICH IS NOT MULTIPLICATIVE FOR** $LM(g)$ **DO**

$f = \text{Normal_Form}(gX_i, G);$

IF $f \neq 0$ **THEN** $F = F \cup \{f\};$

END_FOR

END_FOR

END_WHILE

RETURN G

END