Coq and Gröbner basis

Laurent Théry
Marelle Project
INRIA Sophia-Antipolis
France

Motivations

1^{st} Calculemus Meeting

Roma 3 (Prof. Miola)

Challenge: Formalizing Buchberger's algorithm

Motivations

Proving + Computing

Benefits:

- formalizing mathematics
- theorems using computations
- certified implementation
- education
- ...

Book

Algorithms for computer algebra

Geddes and Czapor and Labahn

Coq

Coq

Calculus of Inductive Constructions

$$\lambda x_\alpha.\, B_\beta : \alpha \to \beta$$

$$F_{\alpha\to\beta}\, A_\alpha : \beta$$

$$((\lambda x.B)\ C) \qquad \rightsquigarrow \qquad B[x \leftarrow C]$$

Functional Programming

Functions:

$$\begin{aligned} fst &: \ \alpha * \beta \longrightarrow \alpha \\ snd &: \ \alpha * \beta \longrightarrow \beta \\ pair &: \ \alpha \longrightarrow \beta \longrightarrow \alpha * \beta \end{aligned}$$

New Function:

$$\lambda x\,.\,(pair\ \ (snd\ \ x)\ \ \ (fst\ \ x)) :\ \ \alpha * \beta \longrightarrow \beta * \alpha$$

Coq

Calculus of Inductive Constructions

```
Inductive ℕ:  Set:=
  O : ℕ
| S : ℕ→ℕ.

Fixpoint + (a, b:ℕ) :  ℕ :=
match a with
       O  => b
 | (S a') => (S (a' + b))
end
```

Natural Deduction

Rules:

$$\frac{A \wedge B}{A}\ \wedge elim_1 \qquad \frac{A \wedge B}{B}\ \wedge elim_2$$

$$\frac{A \qquad B}{A \wedge B}\ \wedge intro \qquad \frac{\begin{array}{c}A^i \\ \ldots \\ B\end{array}}{A \Rightarrow B}\ \Rightarrow intro[i]$$

Natural Deduction

Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{A \wedge B^{1}}{B}\wedge elim_2 \qquad \dfrac{A \wedge B^{1}}{A}\wedge elim_1}{B \wedge A}\wedge intro}{A \wedge B \Rightarrow B \wedge A}\Rightarrow intro[1]$$

Curry Howard

Rules:

$$\begin{aligned} \wedge elim_1 &: \quad A \wedge B \to A \\ \wedge elim_2 &: \quad A \wedge B \to B \\ \wedge intro &: \quad A \to B \to A \wedge B \end{aligned}$$

Proof:

$$\lambda x\,.\,(\wedge intro\ \ (\wedge elim_2\ \ x)\ \ (\wedge elim_1\ \ x)) :$$

$$A \wedge B \to B \wedge A$$

Coq

Calculus of Inductive Constructions

```
Inductive Even: ℕ -> Prop :=
  Even0  : (Even 0)
| EvenSS :
   ∀n, (Even n) -> (Even (S (S n))).

Theorem Even2: (Even (S (S 0))) :=
  (EvenSS 0 Even0).
```

Coq

```
Fixpoint nat_ind (
          P:  ℕ -> Prop,
          Hb:  (P 0),
          Hr:  ∀ n, (P n) -> (P (S n)),
          n:  ℕ          ) :  (P n) :=
      match n with
            0 => Hb
       | (S n') => Hr n' (nat_ind P Hb Hr n')
      end

nat_ind:
  ∀P, (P 0) -> (∀ P, (P n) -> (P (S n)) -> ∀n, (P n)
```

Intuitionistic Logic

$\exists x, y \in \mathbb{R} - \mathbb{Q}$ such that $x^y \in \mathbb{Q}$

Proof:

Let us consider $\sqrt{2}^{\sqrt{2}}$, there are two cases:

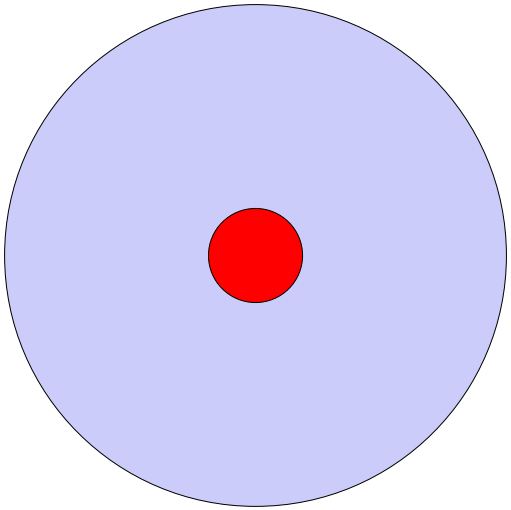
If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, we take $x = \sqrt{2}$ and $y = \sqrt{2}$

Otherwise $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, we have

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\sqrt{2})} = \sqrt{2}^2 = 2$$

we take $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

Trust



Small trusted computing base

Gröbner Basis

Polynomials

Coefficient (a): $[parameter\, A]$

$1, -2, 0$

Monomial (m): $[(list_n\ \mathbb{N})]$

$x, x^2, y^3, x^2z^4, \mathbf{1}$

Polynomials in Coq

```
Inductive list:  Set -> Prop :=
  nil  :  ∀ A, (list A)
| cons :
   ∀A, A -> (list A) -> (list A).

(cons ℕ 0 (cons ℕ (S 0) (nil ℕ))):  (list ℕ)
```

Polynomials in Coq

```
Inductive list_n:  Set -> ℕ -> Prop :=
  nil_n  :  ∀ A, (list_n A 0)
| cons_n :
   ∀A,∀p, A -> (list_n A p) -> (list_n A (S p)).

(cons_n ℕ 0 (S 0) (nil_n ℕ)):  (list_n (S 0) ℕ)
```

Polynomials

Term (t): $[(A * Monomial)]$

$$2x, 4x^2, 5x^2z^4, 4$$

Polynomial (p): $[\{p : (list\ term) \mid (canonical\ p)\}]$

$$2x + 4x^2 + 5x^2z^4 + 4$$

Operations on Polynomials

An admissible monomial ordering: [*parameter* <]

$$5x^2z^4 + 4x^2 + 2x + 4$$

$$x^2z^4 > x^2 > 2x > 4$$

We write

$$5x^2z^4 \overset{>}{+} 4x^2 \overset{>}{+} 2x \overset{>}{+} 4$$

Operations on Polynomials

Adding 2 polynomials:

$$\begin{array}{rrcrcr} & 2x^2y & & & \overset{>}{+} & 4 \\ + & x^2y & \overset{>}{+} & 4x^2 & \overset{>}{+} & -2 \\ \hline & 3x^2y & \overset{>}{+} & 4x^2 & \overset{>}{+} & 2 \end{array}$$

Operations on Polynomials

Multiplying by a term:

$$\begin{array}{rccccc} & x^2y & \overset{>}{+} & 2x^2 & \overset{>}{+} & 2 \\ . & & & & & 2z \\ \hline & 2x^2yz & \overset{>}{+} & 4x^2z & \overset{>}{+} & 4z \end{array}$$

Induction on Polynomials

Structural Induction:

$$(P\,0) \wedge (\forall a.\, \forall p.\, (P\,p) \Rightarrow (P\,(a \stackrel{>}{+} p))) \Rightarrow \forall p.\, (P\,p)$$

Induction on Polynomials

Lexical ordering over polynomials $<_p$:

- $0 <_p t \overset{>}{+} p$
- $m_1 < m_2 \Rightarrow a_1 m_1 \overset{>}{+} p <_p a_2 m_2 \overset{>}{+} q$
- $p <_p q \Rightarrow a_1 m \overset{>}{+} p <_p a_2 m \overset{>}{+} q$

Induction using the ordering:

$$(\forall p.\, (\forall q.\, q <_p p \Rightarrow (P\, q)) \Rightarrow (P\, p)) \Rightarrow \forall p.\, (P\, p)$$

Polynomial Ideals

A set of polynomials I is an $ideal$ iff:

$$\forall p, q \in I,\ p + q \in I$$

$$\forall p \in I, \forall t \in T,\ t.p \in I$$

Polynomial Ideals

The set S generates an ideal $<S>$:

$$p \in <S>$$

$$\Longleftrightarrow$$

$$\exists k \in \mathbb{N}, p = \sum_{i<k} t_i.p_i \ (\forall i < k.\, t_i \in T \text{ and } p_i \in S.)$$

S is a $basis$ for the ideal I iff $<S>= I$

Polynomial Ideals

Buchberger's algorithm:

$$\forall p.\ p \in <S> \ \vee \ p \notin <S>$$

Reduction

Cancelling terms of p by polynomials of S.

Example: $p = 3x^2y^2 \overset{>}{+} 2z^3$ and $S = \{xy \overset{>}{+} 1, z \overset{>}{+} 2\}$

We have

$$\begin{array}{rcccl} & 3x^2y^2 & & \overset{>}{+} & 2z^3 \\ - & 3x^2y^2 & \overset{>}{+} \quad 3xy & & \\ \hline & & -3xy & \overset{>}{+} & 2z^3 \end{array}$$

So $p \rightarrow_S -3xy \overset{>}{+} 2z^3$

Reduction

Cancelling terms of p by polynomials of S.

Example: $p = 3x^2y^2 \overset{>}{+} 2z^3$ and $S = \{xy \overset{>}{+} 1, z \overset{>}{+} 2\}$

We have

$$\begin{array}{rcccc} & 3x^2y^2 & \overset{>}{+} & 2z^3 & \\ - & & & 2z^3 & \overset{>}{+} \quad 4z^2 \\ \hline & 3x^2y^2 & & & \overset{>}{+} \quad -4z^2 \end{array}$$

So $p \rightarrow_S 3x^2y^2 \overset{>}{+} -4z^2$

Reduction

$$p \rightarrow_S^+ q \iff p \rightarrow_S p_1 \ldots \rightarrow_S \ldots \rightarrow_S p_n \rightarrow_S q$$

$$p \rightarrow_S^* q \iff p \rightarrow_S^+ q \wedge \forall r. \neg(q \rightarrow_S r)$$

Reduction

Properties:

$$\forall p\, q,\ p \rightarrow_S q \Rightarrow q < p$$

$$\forall p\, q,\ p \rightarrow_S q \Rightarrow (p \in <S> \iff q \in <S>)$$

It follows

$$\forall p,\ \exists q.\, p \rightarrow_S^* q$$

if $p \rightarrow_S^* 0$ then $p \in <S>$

Reduction

Key Properties:

$$\forall p\, q,\ p - q \rightarrow_S^* 0 \Rightarrow \exists r.\, (p \rightarrow_S^+ r \wedge q \rightarrow_S^+ r)$$

$$\forall p, q, r.\, p \rightarrow_S q \Rightarrow \exists s.\, p - r \rightarrow_S^+ s \wedge q - r \rightarrow_S^+ s$$

Gröbner Basis

Definition

S is a Gröbner basis $\iff \forall p \in <S> . p \rightarrow^*_S 0$

Buchberger's algorithm:

Completion algorithm à la KB

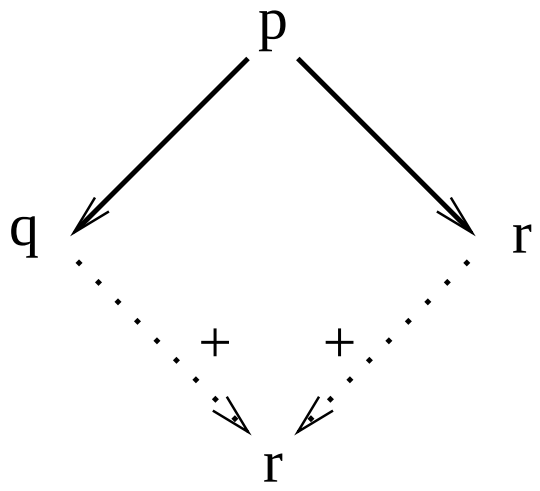
$S \longrightarrow S'$ such that $<S>=<S'>$ and S' is a Gröbner basis.

$p \in <S> \iff p \rightarrow^*_{S'} 0$

Gröbner Basis

Theorem:

if $\rightarrow_S$ confluent then S is a Gröbner basis.



Gröbner Basis

We take an arbitrary $p = \sum_{i<k} t_i.p_i$ with $p_i \in S$.

We want to prove that $p \rightarrow_S^* 0$

This is done by induction on k.

If $k = 0$, we have $p = 0$, so $p \rightarrow_S^* 0$.

Gröbner Basis

If $k \neq 0$, we take $q = \sum_{i<k-1} t_i.p_i$.

We have $q \rightarrow_S^* 0$ by induction.

We have $p - q = t_k p_k$ so $p - q \rightarrow_S^+ 0$.

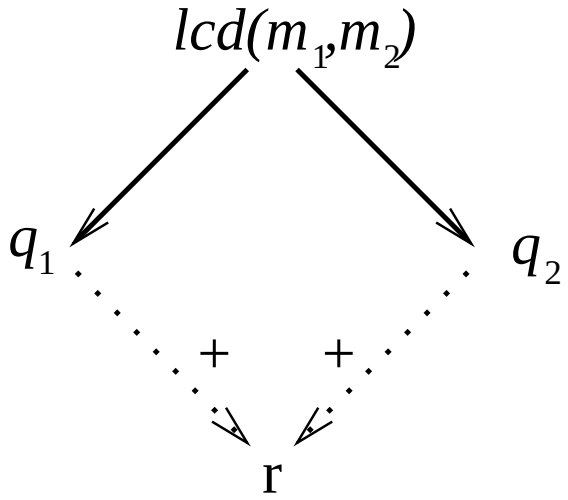
It implies that there exists r such that $p \rightarrow_S^+ r$ and $q \rightarrow_S^+ r$. Key Property 1

$q \rightarrow_S^* 0$ and $q \rightarrow_S^+ r$, by the main hypothesis we have $r \rightarrow_S^* 0$.

$p \rightarrow_S^* r$ and $r \rightarrow_S^* 0$, so $p \rightarrow_S^* 0$.

Spolynomials

$$p_1 = a_1 m_1 \stackrel{>}{+} p'_1 \quad \in S$$
$$p_2 = a_2 m_2 \stackrel{>}{+} p'_2 \quad \in S$$



$$Spoly(p_1, p_2) = q_2 - q_1$$

Spolynomials

Theorem:

if for all $p_1, p_2 \in S.\, Spoly(p_1, p_2) \rightarrow_S^* 0$

then for all $p \in <S>$, $p \rightarrow_S^* 0$

Spolynomials

We prove that to get

$$\forall p \text{ if } p \rightarrow_S^* q \text{ and } p \rightarrow_S^* r \text{ then } q = r.$$

it is sufficient to prove that

$$\forall p\ q \in S, Spoly(p, q) \rightarrow_S^* 0$$

Spolynomials

We take an arbitrary p and proceed by induction using $<$.

We suppose that if $q < p$ and $q \rightarrow_S^* r$ and $q \rightarrow_S^* s$ then $r = s$.

If p is irreducible, we have $r = p = s$.

Spolynomials

If p is reducible, we have p_1 et p_2 such that

$$p \rightarrow_S p_1 \rightarrow_S^* r \text{ et } p \rightarrow_S p_2 \rightarrow_S^* s.$$

Since $p_1 < p$ and $p_2 < p$,

it is sufficient to find a p_3 such that

$$p_1 \rightarrow_S^* p_3 \text{ and } p_2 \rightarrow_S^* p_3$$

to get $r = p_3 = s$ by the induction hypothesis.

Spolynomials

There are 4 possible cases for the reductions to p_1 and p_2.

Case 1: $p = t \stackrel{>}{+} q \rightarrow_S t \stackrel{>}{+} q_1 = p_1$ and

$$p = t \stackrel{>}{+} q \rightarrow_S t \stackrel{>}{+} q_2 = p_2.$$

We have $q < p$, $q \rightarrow_S q_1$ et $q \rightarrow_S q_2$.

If we take q_3 such that $q_1 \rightarrow_S^* q_3$ we have $q_2 \rightarrow_S^* q_3$ by induction.

If we take p_3 such that $t \stackrel{>}{+} q_3 \rightarrow_S^* p_3$ then $p_1 \rightarrow_S^* p_3$ and $p_2 \rightarrow_S^* p_3$.

Spolynomials

Case 2: $p = t \overset{>}{+} q \rightarrow_S q - q_3 = p_1$ and

$$p = t \overset{>}{+} q \rightarrow_S t \overset{>}{+} q_2 = p_2.$$

We have $q \rightarrow_S q_2$,

so we get that there exists q_4 such that

$q_1 - q_3 \rightarrow_S^+ q_4$ and $q_2 - q_3 \rightarrow_S^+ q_4$. Key Property 2

As we have $t \overset{>}{+} q_2 \rightarrow_S q_2 - q_3$, we get $p_2 \rightarrow_S^+ q_4$.

If we take p_3 such that $q_4 \rightarrow_S^* p_3$ we have

$p_1 \rightarrow_S^* p_3$ and $p_2 \rightarrow_S^* p_3$.

Spolynomials

Case 3: $p = t \overset{>}{+} q \longrightarrow_S t \overset{>}{+} q_2 = p_1$ and

$$p = t \overset{>}{+} q \longrightarrow_S q - q_3 = p_2.$$

symmetric to case 2.

Spolynomials

Case 4: $p = t \overset{>}{+} q \rightarrow_S q - q_2 = p_1$ and

$$p = t \overset{>}{+} q \rightarrow_S q - q_3 = p_2.$$

We have $p_1 - p_2 = q_2 - q_3 = aSpoly(r_1, r_2)$.

By the induction hypothesis $Spoly(r_1, r_2) \rightarrow_S^* 0$.

We have $p_1 - p_2 \rightarrow_S^* 0$.

So there exists p_4 such that $p_1 \rightarrow_S^+ p_4$ et $p_2 \rightarrow_S^+ p_4$.

Key Property 1

If we take p_3 such that $p_4 \rightarrow_S^* p_3$,

We have $p_1 \rightarrow_S^* p_3$ and $p_2 \rightarrow_S^* p_3$.

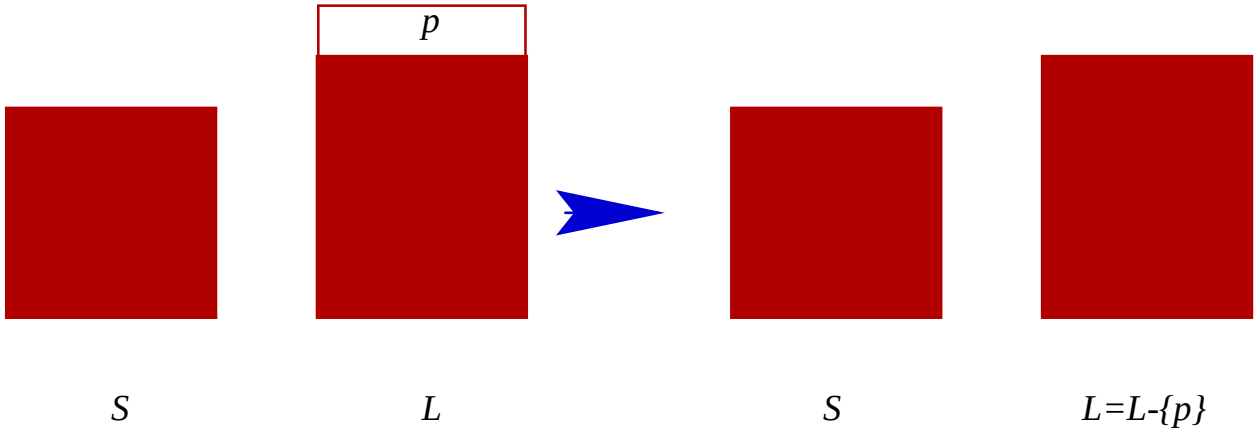
Algorithm

Init:

S=S *L=Spoly(S*S)*

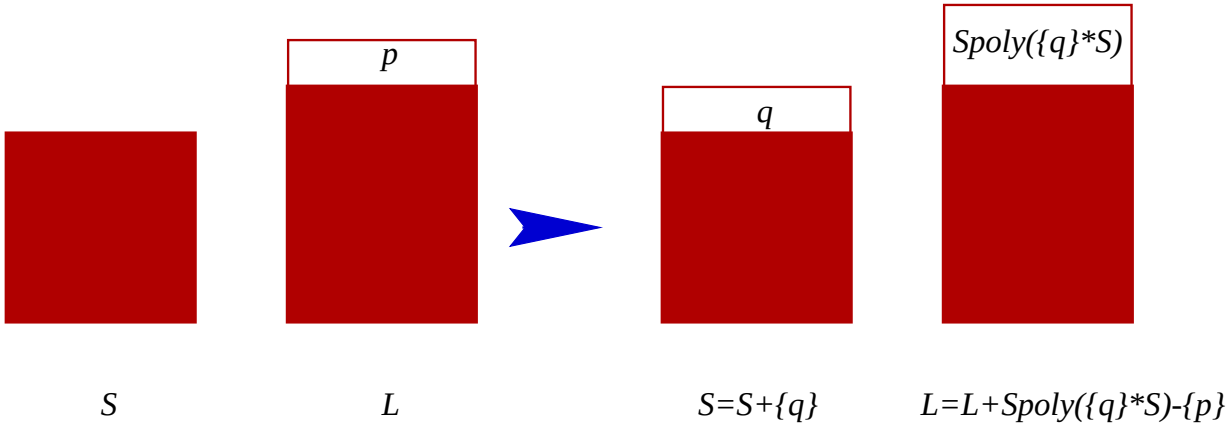
Algorithm

Case: $p \rightarrow_S^* 0$



Algorithm

Case: $p \rightarrow_S^* q$ $(q \neq 0)$

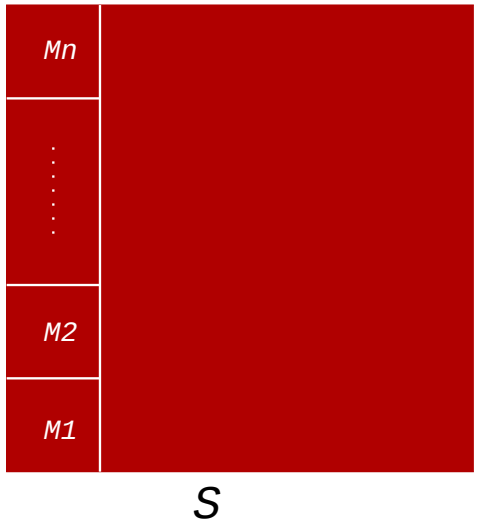


Correctness

$$p \in <S> \Rightarrow q \in <S> \Rightarrow Spoly(p,q) \in <S>$$

$$S \subset S' \Rightarrow p \rightarrow_S^* 0 \Rightarrow p \rightarrow_{S'}^* 0$$

Termination



Dickson's lemma

The algorithm

```
let rec SpolyL p l1 l2 = match l2 with
| [] -> l1
| (q::l2) ->(spoly p q)::(SpolyL p l1 l2)

let rec SpolyProp l = match l with
| [] -> []
| (p::l) -> (SpolyL p (SpolyProp l) l)
```

The algorithm

```
let rec buchf l1 l2 = match l2 with
| [] -> l1
| (p::l2) ->
    let r = (reducef l1 p) in
    if (zeroP r)
    then (buchf l1 l2)
    else
        (buchf (r::  l1) (SpolyL r l2 l1))
    end

let buch l1 = buchf l1 (SpolyProd l1)
```

Lessons Learned

Choosing a 'right' proof path

Never underestimate the foundation work

Prove once, use everywhere

Wikipedia effect

What more?

Dickson Lemma

Constructive Proof:

Henrik Persson: Open Induction

Using Gröbner Basis

Proof Procedure:

Jérôme Creci, Loïc Pottier: Gb tactic

Using Gröbner Basis

Ring Tactic: $\forall x\ y \in \mathbb{R}, (x+y)z = zx + yz$

Gb Tactic:

$$\forall x\ y \in \mathbb{C}, x^2 + y^2 = 0 \rightarrow xy = 0 \rightarrow x + y = 0$$

Using Gröbner Basis

$$P_1 = 0, \ldots P_r = 0 \rightarrow P = 0$$

$$\Longleftrightarrow$$

$$\exists n, P^n \in <P_1, \ldots, P_r>$$

Using Gröbner Basis

If

$$\mathcal{F} = \{t(1 - zP) - e_0, tP_1 - e_1, \ldots, tP_r - e_r\} \cup$$

$$\{e_i e_j | 0 \leq i < j \leq r\} \cup \{te_i | 0 \leq i \leq r\}$$

then

$$\exists n, P^n \in <P_1, \ldots, P_r>$$

$$\Longleftrightarrow$$

$$kt - Re_0 - Re_1 \ldots R_r e_r \in \mathrm{Gb}(\mathcal{F})$$

for $t > x_1 > \cdots > x_m > z > e_0 > \cdots > e_r$

More Polynomials

Subresultants and PRS 98%

Cylindrical Algebraic Decomposition 60%

Assia Mahboubi Phd

More Polynomials

Finding a 'right' proof path

Polynomial representation:

$$A[x, y] \text{ as } (A[x])[y]$$

Horner: $a_0 + X^{n_0}(a_1 + X^{n_1}(\ \ldots\ ))$