Cylindrical Algebraic Decomposition in Coq

MAP 2010 - Logroño 13-16 November 2010

Assia Mahboubi

INRIA Microsoft Research Joint Centre (France)
INRIA Saclay – Île-de-France
École Polytechnique, Palaiseau

November 9th 2010

This work has been partially funded by the FORMATH project, nr. 243847, of the FET program within the 7th Framework program of the European Commission.

Yesterday

- We have defined the language of first order (discrete) ordered fields.

Yesterday

- We have defined the language of first order (discrete) ordered fields.
- We have defined the theory of (discrete) real closed fields.

Yesterday

- We have defined the language of first order (discrete) ordered fields.
- We have defined the theory of (discrete) real closed fields.
- We are interested in intuitionistic the theory of discrete real closed fields (we will see it is the same as the classical).

Yesterday

- We have defined the language of first order (discrete) ordered fields.
- We have defined the theory of (discrete) real closed fields.
- We are interested in intuitionistic the theory of discrete real closed fields (we will see it is the same as the classical).
- We have stated the theorem of quantifier elimination for the theory of discrete real closed fields.

Yesterday

- We have defined the language of first order (discrete) ordered fields.
- We have defined the theory of (discrete) real closed fields.
- We are interested in intuitionistic the theory of discrete real closed fields (we will see it is the same as the classical).
- We have stated the theorem of quantifier elimination for the theory of discrete real closed fields.
- We want to formalize a (constructive) proof of this theorem in the Coq system, meaning we want a quantifier elimination program.

Formal definition of the field signature

Terms on the language of fields.

```
Inductive term : Type :=
| Var of nat
| C0 : term
| C1 : term
| Add of term & term
| Opp of term
| Mul of term & term
| Inv of term.
```

Formal definition of a first order theory

For an arbitrary type `term` of terms, formulas are:

```
Inductive formula (term : Type) : Type :=
| Equal of term & term
| Leq of term & term
| Not of formula
| And of formula & formula
| Or of formula & formula
| Implies of formula & formula
| Exists of nat & formula
| Forall of nat & formula.
```

Theory of real closed fields

We use a record type to define a type which is simultaneously equipped with a field signature and a theory of real closed fields.

```
Record rcf := RealClosedField{
  carrier : Type;
  Req : carrier -> carrier -> bool;
  Rleq : carrier -> carrier -> bool;
  zero : carrier;
  one : carrier
  opp : carrier -> carrier;
  add : carrier -> carrier -> carrier;
  mul : carrier -> carrier -> carrier;
  inv : carrier -> carrier;
  _ : associative add;
  _ : commutative add;
  _ : left_id zero add;
  _ : left_inverse zero opp add;
  ...}.
```

Instances of the theory of real closed fields

An instance of this theory is constructed when:

- We have formed a concrete type
  for instance the type `Ralg` of real algebraic numbers
- We have defined field constants and implemented field operations
  Zero, one, addition, ...
- We have proved the theorems specifying these operations
  Addition is commutative, ...
- We have gathered all this in an element of the record type

```
Definition Ralg_rcf :=
     RealClosedField Ralg Ralg0 Ralg1 Ralg_opp ...
```

What do we formalize?

- A signature Σ (of rings)

  The type `term`
- The terms on Σ

  The elements `t : term`
- The first order statements $\mathcal{F}(\Sigma, \mathbb{N})$

  The elements `f : formula`
- The definition of Σ-structure

  The type `rcf` (which contains specifications).
- The Σ-structures themselves

  The elements `MyRcf : rcf`

What do we formalize?

- An interpretation function $[t(\mathbf{x})]_{R,e}$ from terms in $\mathcal{L}(\Sigma, \mathbb{N}))$ in a Σ-structure

  `eval: (seq (carrier R))-> term -> (carrier R)`

- An interpretation function $[f(\mathbf{x})]_{R,e}$ from formulas in $\mathcal{F}(\Sigma, \mathbb{N}))$ in Coq statements

  `holds: (seq (carrier R))-> formula -> Prop`

- $R, e \models f$

  A proof of the Coq statement `(holds e f)`

- R is a model of the theory of (discrete) real closed fields

  $R : rcf$

Semantic quantifier elimination

A theory T on a language Σ with a set of variables $\mathcal{V}$ admits semantic quantifier elimination if

- for every $\phi \in \mathcal{F}(\Sigma, \mathcal{V})$,
- there exists a quantifier free formula $\psi \in \mathcal{F}(\Sigma, \mathcal{V})$
- such that for any model M of T, and for any list e of values,

$$M, e \models \phi \text{ iff } M, e \models \psi$$

This is the (a priori weaker) quantifier elimination result we formalize.

Semantic quantifier elimination

The formalization of the theorem in our framework is:

- Program a quantifier elimination procedure:

```
Fixpoint quantifier_elim :
  formula term -> formula term := ...
```

- Prove :

```
Lemma quantifier_elim_correct : forall (R_rcf : rcf),
  forall (f : formula term)(ctx : seq (R R_rcf)),
  (holds ctx f) <-> (holds ctx (quantifier_elim f)).
```

Decidability

There is a boolean test which given a context an a first-order formula, determines whether the formula holds or not:

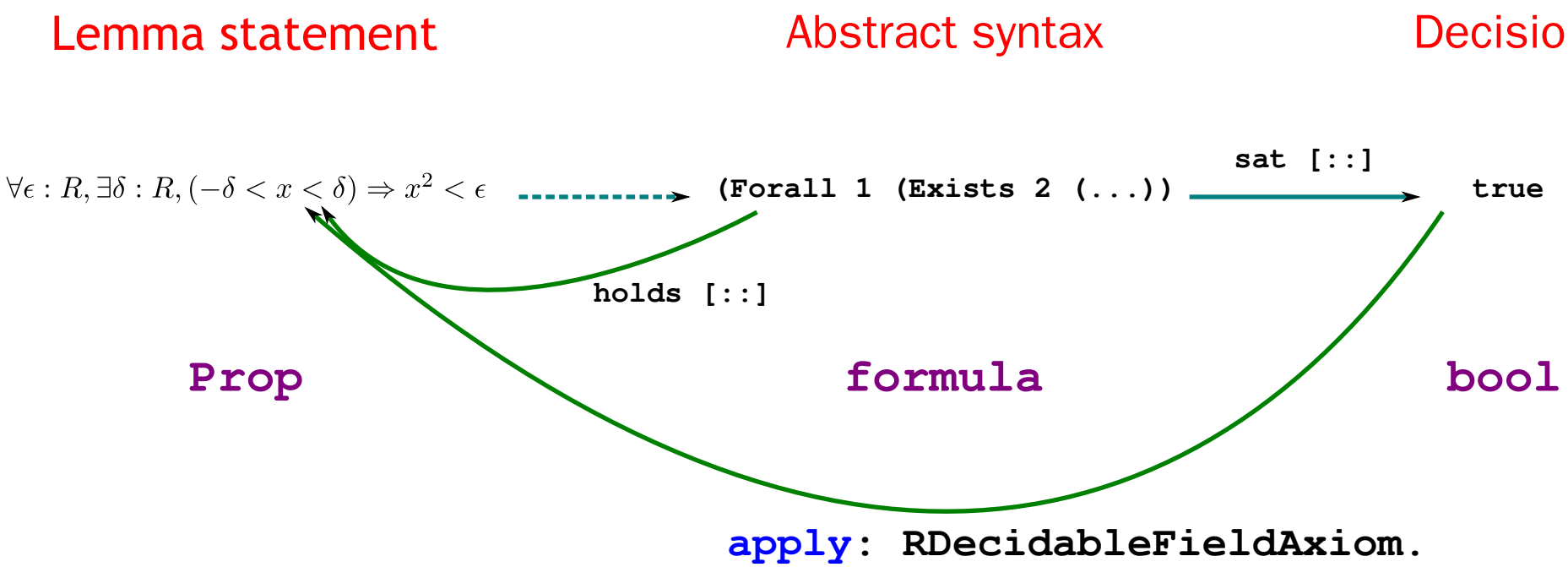
```
Definition DecidableField.axiom R
   (sat : seq (carrier R) -> formula -> bool) :=
   forall ctx f, (holds ctx f) <-> (sat ctx f = true).
```

If the semantic quantifier elimination is proved, program `sat` by:

- Eliminating quantifiers
- Deciding the obtained quantifier-free formula instanciated with parameters of the desired context

From proofs to proof-producing procedure

The (so-called) reflexion scheme:



Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.
  - Consider $\exists x, F$ where F is quantifier free

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.
  - Consider $\exists x, F$ where F is quantifier free
  - F is equivalent to its disjunctive normal form: $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} L_{i,j}$

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.
  - Consider $\exists x, F$ where F is quantifier free
  - F is equivalent to its disjunctive normal form: $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} L_{i,j}$
  - The existential quantifier distributes over the disjunctions.

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.
  - Consider $\exists x, F$ where F is quantifier free
  - F is equivalent to its disjunctive normal form: $\bigvee_{i=1}^{n} \bigwedge_{j=1}^{m} L_{i,j}$
  - The existential quantifier distributes over the disjunctions.
  - The hypothesis is applied to every conjunction $\bigwedge_{j=1}^{m} L_{i,j}$

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.

- Now by induction on the structure of an arbitrary formula:

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.

- Now by induction on the structure of an arbitrary formula:
  - All cases are trivial except for quantified formulas.

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.

- Now by induction on the structure of an arbitrary formula:
  - All cases are trivial except for quantified formulas.
  - Existential case:

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.

- Now by induction on the structure of an arbitrary formula:
  - All cases are trivial except for quantified formulas.
  - Existential case:
    - ★ $\exists x, F$ where F can be considered qf (by induction).

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.

- Now by induction on the structure of an arbitrary formula:
  - All cases are trivial except for quantified formulas.
  - Existential case:
    - $\exists x, F$ where F can be considered qf (by induction).
    - The first lemma applies.

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.

- Now by induction on the structure of an arbitrary formula:
  - All cases are trivial except for quantified formulas.
  - Existential case: Ok

Sufficient condition (for discrete structures)

Suppose it is possible to eliminate the $\exists$ in $\exists x, \bigwedge_{i=1}^{n} L_i$.

- Then it is possible to eliminate a single prenex $\exists$.

- Now by induction on the structure of an arbitrary formula:
  - All cases are trivial except for quantified formulas.
  - Existential case: Ok

  - Universal case: $\forall x, F$ where F can be considered qf (by induction).
    - ★ Since $(F \vee \neg F)$ holds, $\forall x, F$ is equivalent to $\neg \exists x, \neg F$.
    - ★ $\neg F$ is quantifier free: the lemma applies to $\exists \neg F$.
    - ★ The outermost negation does not introduce quantifiers.

Sufficient condition (semantic version)

What we need to prove is that for any candidate theory R:

- There is a projection operator:

```
Parameter proj : nat -> formula -> formula.
```

- Such that:

```
Definition wf_proj_axiom proj := forall n f,
    literal_conjunction f -> qf_form (proj n f).

Definition holds_proj_axiom R proj :=
  forall n f ctx, literal_conjunction f ->
  (holds ctx (Exists n f)) <-> holds ctx (proj n f).
```

From language of fields to language of rings

Remark:

- Any first order sentence in this theory has an equivalent in the language of discrete ordered rings (possibly with more quantifiers, and we can allow rational constants).
- Hence:
  - For any first order sentence in the language of ordered rings
  - We want to construct a quantifier free formula in the language of rings which is equivalent to the former, in the theory of real closed fields.
  - We restrict our study to polynomial atoms.

Sufficient condition (geometric version)

Some vocabulary:

- Algebraic set: The set of roots of a finite number of polynomials.
  Realizations of an equality atom.
- Semi-algebraic set: The set of points satisfying a (disjunction of) finite number of polynomial inequalities (and equalities).
  Realization of quantifier-free formulas.
- Basic semi-algebraic set:

$$\{x \in R^k \mid P(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

Semi-algebraic sets are finite unions of basic semi-algebraic sets.

Sufficient condition (geometric version)

Theorem (Projection of semi-algebraic sets)

For any discrete real closed field R, for any S basic semi-algebraic set of R^{k+1} defined by polynomials with rational coefficients, the projection of S on R^k is a semi-algebraic set.

We only prove the theorem for basic semi-algebraic sets.

Emptiness of a one dimensional basic semi-algebraic set

Quantifier elimination amounts to deciding whether a basic semi-algebraic:

$$\{x \in R \mid P(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

is empty or not, for $P \in R[X]$ and $\mathcal{Q} \subset R[X]$ (finite).

The Tarski Query "oracle"

Definition (Tarski Query)

Let R be a real closed fields and $P, Q \in R[X]$ with $P \neq 0$. The Tarski Query of P and Q is defined as:

$$TQuery(P, Q) := \sum_{x \in R, P(x)=0} sign\ Q(x)$$

By sign we mean:

$$\begin{aligned} TQuery(P, Q) \quad := \quad & 1 \quad \times \sharp\{x \mid P(x) = 0 \wedge Q(x) > 0\} \\ + \quad & 0 \quad \times \sharp\{x \mid P(x) = 0 \wedge Q(x) = 0\} \\ + \quad & -1 \quad \times \sharp\{x \mid P(x) = 0 \wedge Q(x) < 0\} \end{aligned}$$

The Tarski Query "oracle"

Definition (Tarski Query)

Let R be a real closed fields and $P, Q \in R[X]$ with $P \neq 0$. The Tarski Query of P and Q is defined as:

$$TQuery(P, Q) := \sum_{x \in R, P(x)=0} sign\ Q(x)$$

By sign we mean:

$$\begin{aligned} TQuery(P, Q) \quad := \quad & 1 \quad \times \sharp\{P = 0, Q > 0\} \\ + \quad & 0 \quad \times \sharp\{P = 0, Q = 0\} \\ + \quad & -1 \quad \times \sharp\{P = 0, Q < 0\} \end{aligned}$$

The Tarski Query "oracle"

Properties:

- $TQuery(P, Q) = \sharp\{P = 0, Q > 0\} - \sharp\{P = 0, Q < 0\}$

The Tarski Query "oracle"

Properties:

- $TQuery(P, Q) = \sharp\{P = 0, Q > 0\} - \sharp\{P = 0, Q < 0\}$
- $TQuery(P, Q^2) = \sharp\{P = 0, Q > 0\} + \sharp\{P = 0, Q < 0\}$

The Tarski Query "oracle"

Properties:

- $TQuery(P, Q) = \sharp\{P = 0, Q > 0\} - \sharp\{P = 0, Q < 0\}$
- $TQuery(P, Q^2) = \sharp\{P = 0, Q > 0\} + \sharp\{P = 0, Q < 0\}$
- $TQuery(P, 1) = \sharp\{P = 0\}$

The Tarski Query "oracle"

Properties:

- $TQuery(P, Q) = \sharp\{P = 0, Q > 0\} - \sharp\{P = 0, Q < 0\}$
- $TQuery(P, Q^2) = \sharp\{P = 0, Q > 0\} + \sharp\{P = 0, Q < 0\}$
- $TQuery(P, 1) = \sharp\{P = 0\}$
- $TQuery(P, 1) =$
$$\sharp\{P = 0, Q = 0\} + \sharp\{P = 0, Q > 0\} + \sharp\{P = 0, Q < 0\}$$

The Tarski Query "oracle"

In other words:

$$\begin{bmatrix} TQuery(P,1) \\ TQuery(P,Q) \\ TQuery(P,Q^2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} \sharp\{P=0, Q=0\} \\ \sharp\{P=0, Q>0\} \\ \sharp\{P=0, Q<0\} \end{bmatrix}$$

The Tarski Query "oracle"

In other words:

$$\begin{bmatrix} TQuery(P,1) \\ TQuery(P,Q) \\ TQuery(P,Q^2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} \sharp\{P=0, Q=0\} \\ \sharp\{P=0, Q>0\} \\ \sharp\{P=0, Q<0\} \end{bmatrix}$$

Fortunately, $M := \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix}$ is invertible.

The Tarski Query "oracle"

In other words:

$$\begin{bmatrix} TQuery(P,1) \\ TQuery(P,Q) \\ TQuery(P,Q^2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} \sharp\{P=0, Q=0\} \\ \sharp\{P=0, Q>0\} \\ \sharp\{P=0, Q<0\} \end{bmatrix}$$

Fortunately, $M := \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix}$ is invertible.

$$\begin{bmatrix} \sharp\{P=0, Q=0\} \\ \sharp\{P=0, Q>0\} \\ \sharp\{P=0, Q<0\} \end{bmatrix} = M^{-1} \begin{bmatrix} TQuery(P,1) \\ TQuery(P,Q) \\ TQuery(P,Q^2) \end{bmatrix}$$

Tarski Queries and emptiness test

- The one dimensional basic semi-algebraic set

$$\{x \in R \mid P(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

is non empty iff $\sharp\{P = 0, Q > 0\} > 0$

Tarski Queries and emptiness test

- The one dimensional basic semi-algebraic set

$$\{x \in R \mid P(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

  is non empty iff $\sharp\{P = 0, Q > 0\} > 0$
- Tarski Queries provide an emptiness test for one sign condition.

Tarski Queries and emptiness test

- The one dimensional basic semi-algebraic set

$$\{x \in R \mid P(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

  is non empty iff $\sharp\{P = 0, Q > 0\} > 0$
- Tarski Queries provide an emptiness test for one sign condition.
- What about a basic semi-algebraic set with more sign conditions?

Multi Tarski Queries

Let $\mathcal{Q} := \{Q_1, \ldots, Q_n\} \subset R[X]$:

- A sign assignment for $\mathcal{Q}$ is:

$$\sigma : Q_i \mapsto \epsilon_i \in \{0, -1, 1\}$$

Multi Tarski Queries

Let $\mathcal{Q} := \{Q_1, \ldots, Q_n\} \subset R[X]$:

- A sign assignment for $\mathcal{Q}$ is:

$$\sigma : Q_i \mapsto \epsilon_i \in \{0, -1, 1\}$$

- Let $\Sigma := \{0, -1, 1\}^{\mathcal{Q}}$ be the set of all possible sign assignments for $\mathcal{Q}$.

Multi Tarski Queries

Let $\mathcal{Q} := \{Q_1, \ldots, Q_n\} \subset R[X]$:

- A sign assignment for $\mathcal{Q}$ is:

$$\sigma : Q_i \mapsto \epsilon_i \in \{0, -1, 1\}$$

- Let $\Sigma := \{0, -1, 1\}^{\mathcal{Q}}$ be the set of all possible sign assignments for $\mathcal{Q}$.
- Let $A := \{0, 1, 2\}^{\mathcal{Q}}$. For every $\alpha \in A$, let $\mathcal{Q}^{\alpha} := \prod Q_i^{\alpha(Q_i)}$

Multi Tarski Queries

Now define:

- $TQuery(P, \mathcal{Q}^A) := [TQuery(P, \mathcal{Q}^{\alpha_1}), \ldots, TQuery(P, \mathcal{Q}^{\alpha_{3^n}})]$ where the elements $\alpha_1, \ldots, \alpha_{3^N}$ of A are in lexicographic order.

Multi Tarski Queries

Now define:

- $TQuery(P, \mathcal{Q}^A) := [TQuery(P, \mathcal{Q}^{\alpha_1}), \ldots, TQuery(P, \mathcal{Q}^{\alpha_{3^n}})]$
  where the elements $\alpha_1, \ldots, \alpha_{3^N}$ of A are in lexicographic order.
- $v(P = 0, \Sigma) := [\sharp\{P = 0, \sigma_1\}, \ldots, \sharp\{P = 0, \sigma_{3^n}\}]$
  where the elements $\sigma_1, \ldots, \sigma_{3^N}$ of Σ are in lexicographic order.

Multi Tarski Queries

Now define:

- $TQuery(P, \mathcal{Q}^A) := [TQuery(P, \mathcal{Q}^{\alpha_1}), \ldots, TQuery(P, \mathcal{Q}^{\alpha_{3^n}})]$
  where the elements $\alpha_1, \ldots, \alpha_{3^N}$ of A are in lexicographic order.
- $v(P = 0, \Sigma) := [\sharp\{P = 0, \sigma_1\}, \ldots, \sharp\{P = 0, \sigma_{3^n}\}]$
  where the elements $\sigma_1, \ldots, \sigma_{3^N}$ of Σ are in lexicographic order.
- $(M_n)_{n \in \mathbb{N}}$ by $M_1 := M$ and $M_{k+1} := M_k \otimes M$

Multi Tarski Queries

Now define:

- $TQuery(P, \mathcal{Q}^A) := [TQuery(P, \mathcal{Q}^{\alpha_1}), \ldots, TQuery(P, \mathcal{Q}^{\alpha_{3^n}})]$
  where the elements $\alpha_1, \ldots, \alpha_{3^N}$ of A are in lexicographic order.
- $v(P = 0, \Sigma) := [\sharp\{P = 0, \sigma_1\}, \ldots, \sharp\{P = 0, \sigma_{3^n}\}]$
  where the elements $\sigma_1, \ldots, \sigma_{3^N}$ of Σ are in lexicographic order.
- $(M_n)_{n \in \mathbb{N}}$ by $M_1 := M$ and $M_{k+1} := M_k \otimes M$

Theorem

$$TQuery(P, \mathcal{Q}^A) = M_n.v(P = 0, \Sigma)$$

(and M_n is invertible)

Computing Tarski Queries

Theorem

For any two polynomials $P, Q \in R[X]$ with $P \neq 0$, the value of $TQuery(P, Q)$ only depends on the sign of the leading coefficients of polynomials occurring in the chain of remainders of P and $P'Q$ and on the degree of these remainders.

It is obtained as a the number of sign changes in the signed remainder chain.

Consequence on the emptiness test

- The emptiness of a basic semi-algebraic set

$$\{x \in R \mid P(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

  is determined by the degrees and signs of the leading coefficients of the polynomials occurring in the remainder chains of P and the $P'\mathcal{Q}^{\alpha}$.

- The emptiness of a basic semi-algebraic set

$$\{x \in R \mid \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

  is determined by the degrees and signs of the leading coefficients of the polynomials occurring in the remainder chains of C and C' and C and the $C''\mathcal{Q}^{\alpha}$, where $C = \prod_{i=1}^{n} Q_i$.

Back to quantifier elimination

Given a basic semi-algebraic set:

$$\{x \in R^{k+1} \mid P(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

we want to show that its projection on R^k is still a semi-algebraic set.

Back to quantifier elimination

Given a basic semi-algebraic set:

$$\{x \in R^{k+1} \mid P(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x) > 0\}$$

we want to show that its projection on R^k is still a semi-algebraic set. This problem is different from the unidimensional case:

$$\{(y, x) \in R^{k+1} \mid P(y)(x) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(y)(x) > 0\}$$

where $P, Q \in \mathbb{Q}[X_1, \ldots, X_k][X_{k+1}]$.

Back to quantifier elimination

Obtain a semi-algebraic description of

$$\{x \in R^k \mid \exists y \in R \mid P(x)(y) = 0 \wedge \bigwedge_{Q \in \mathcal{Q}} Q(x)(y) > 0\}$$

where $P, Q \in \mathbb{Q}[X_1, \ldots, X_k][X_{k+1}]$.

- Coefficients are no more in a field but in a ring. Yet euclidean division can be replaced by pseudo-euclidean division.

  Harmless

- The output semi-algebraic description depends on the values of the parameters.

  Example

Back to quantifier elimination

- We need a model-independent description of a finite partition of the space of parameters R^k into semi-algebraic cells.
- Each cell corresponds to a possible value for the quantifier free equivalent formula.
- This description is obtained by analyzing the tree of successive zero tests performed when computing the degrees and the pseudo divisions involved in the Tarski Queries.
- What about the (formal) formula construction?