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 8th 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.

Aim of these talks

- Issues related to quantifier the theory of real closed fields.
- In the context of the formalization of these results in the Coq proof assistant.
- Sketch of the lectures:
  - Quantifier elimination, real closed fields
  - Projection of semi-algebraic sets, from algebra to logics
  - Cylindrical Algebraic Decomposition
  - Topics in formal proofs in real algebraic geometry

The language of ring

Terms are:

- Variables : $x, y, \ldots$
- Constants 0 and 1
- Opposites: $-t$
- Sums: $t_1 + t_2$
- Differences: $t_1 - t_2$
- Products: $t_1 * t_2$

Terms are polynomial expressions in the variables.

First order formulas in the language of ordered rings

Atoms are:

- Equalities: $t_1 = t_2$
- Inequalities: $t_1 \geq t_2$, $t_1 > t_2$, $t_1 \leq t_2$, $t_1 < t_2$

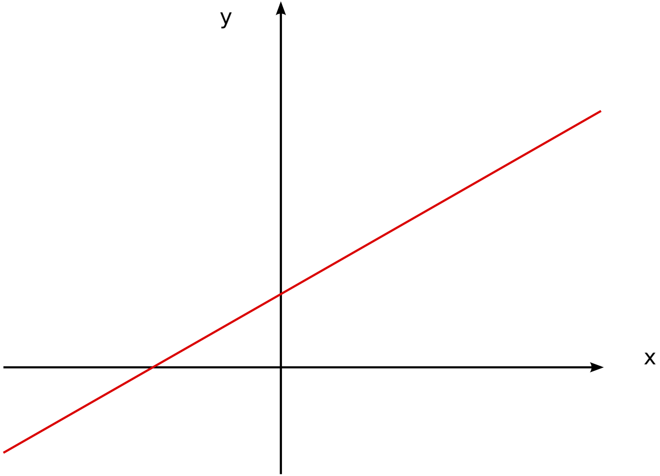
Formulas are:

- Atoms
- Conjunctions: $F_1 \wedge F_2$
- Disjunctions: $F_1 \vee F_2$
- Negations: $\neg F$
- Implications: $F_1 \Rightarrow F_2$
- Quantifications: $\exists x, F$, $\forall x, F$

Formulas are quantified systems of polynomial constraints.

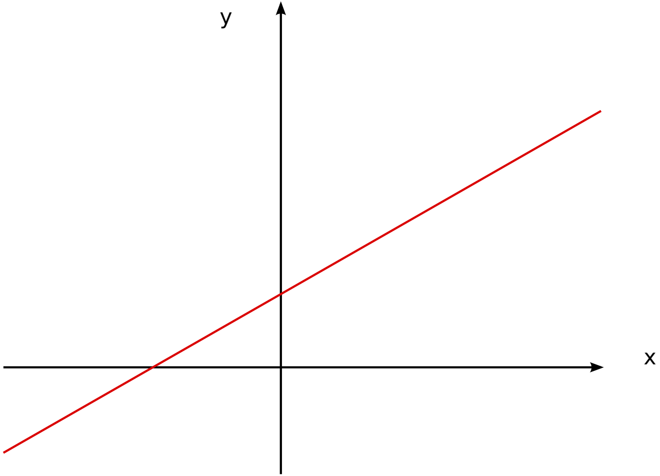
A taste of the first order language of ordered rings

"Any polynomial of degree one has a real root."



A taste of the first order language of ordered rings

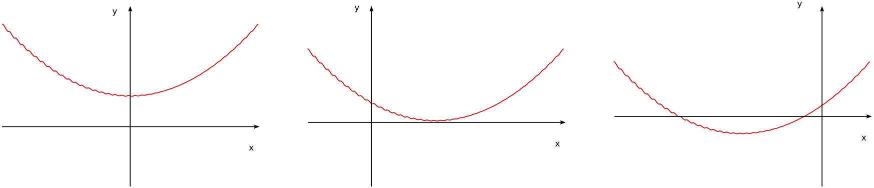
"Any polynomial of degree one has a real root."



$$\forall a \forall b, \exists x, a * x + b = 0$$

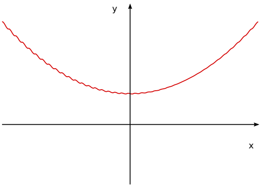
A taste of the first order language of ordered rings

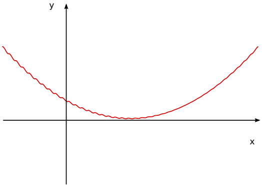
"Any polynomial of degree two has at most two real roots."

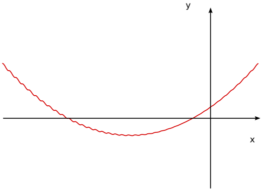


A taste of the first order language of ordered rings

"Any polynomial of degree two has at most two real roots."







$$\forall a \forall b, \forall c \forall x \forall y \forall z,$$

$$(ax^2 + bx + c = 0 \wedge ay^2 + by + c = 0 \wedge az^2 + bz + c = 0)$$

$$\Rightarrow (x = y \vee x = z \vee y = z)$$

A taste of the first order language of ordered rings

- ”Any two ellipses have at most four intersection points.”

A taste of the first order language of ordered rings

- "Any two ellipses have at most four intersection points."

  Similar to the previous example.

A taste of the first order language of ordered rings

- "Any two ellipses have at most four intersection points."
  Similar to the previous example.
- "Any polynomial of degree 18 has at least one root."

A taste of the first order language of ordered rings

- "Any two ellipses have at most four intersection points."

  Similar to the previous example.
- "Any polynomial of degree 18 has at least one root."

  Difficult to prove yet syntactically correct.

A taste of the first order language of ordered rings

- "Any polynomial has less roots than its degree."

A taste of the first order language of ordered rings

- "Any polynomial has less roots than its degree."

This demands higher order.

A taste of the first order language of ordered rings

- "Any polynomial has less roots than its degree."

  This demands higher order.

- "Any number is either rational or non rational."

A taste of the first order language of ordered rings

- "Any polynomial has less roots than its degree."

  This demands higher order.
- "Any number is either rational or non rational."

  The language is not precise enough.

Ordered rings, ordered fields

- The theory of discrete ordered rings is:
  - The theory of rings
  - A total order $\leq$
  - Compatibility of the order with ring operations

Ordered rings, ordered fields

- The theory of discrete ordered rings is:
  - The theory of rings
  - A total order $\leq$
  - Compatibility of the order with ring operations
- The theory of discrete ordered fields is:
  - Defined on an extended signature (inverse, quotient)
  - The theory of fields
  - A total order $\leq$
  - Compatibility of the order with field operations

Ordered rings, ordered fields

- The theory of discrete ordered rings is:
  - The theory of rings
  - A total order $\leq$
  - Compatibility of the order with ring operations
- The theory of discrete ordered fields is:
  - Defined on an extended signature (inverse, quotient)
  - The theory of fields
  - A total order $\leq$
  - Compatibility of the order with field operations

Any first order formula in discrete ordered fields has an equivalent in the theory of discrete ordered fields (possibly with more quantifiers).

Examples of real closed fields

- Real numbers
- Computable real numbers
- Real algebraic numbers
- The field of Puiseux series on a RCF R

First order theory of real closed fields

Theorem (Tarski (1948))

The classical theory of real closed fields admits quantifier elimination and is hence decidable.

There exists an algorithm which proves or disproves any theorem of real algebraic geometry (which can be expressed in this first order language).

Remarks

- We can decide whether an arbitrary given polynomial with rational coefficients has a root.

Remarks

- We can decide whether an arbitrary given polynomial with rational coefficients has a root.
- But we do not know whether this root is an integer or a rational.

Remarks

- We can decide whether an arbitrary given polynomial with rational coefficients has a root.
- But we do not know whether this root is an integer or a rational.
- There is indeed no algorithm to decide the solvability of diophantine equations (Matiyasevitch, 1970).

Remarks

There is an algorithm which determines:

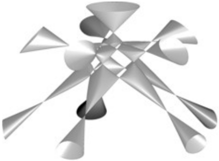
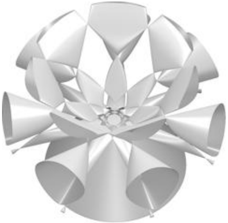
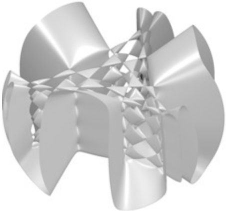
- If your piano can be moved through the stairs and then to your dinning room;
- If a (specified)robot can reach a desired position from an initial state;
- The solution to Birkhoff interpolation problem;
- ...

Remarks

This algorithm gives the complete topological description of semi-algebraic varieties.

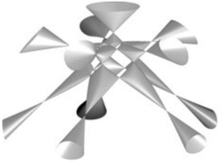
Remarks

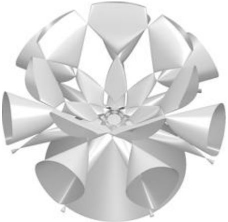
This algorithm gives the complete topological description of semi-algebraic varieties.

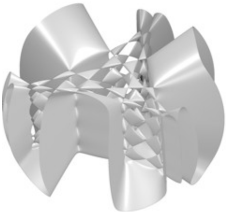




Remarks

This algorithm gives the complete topological description of semi-algebraic varieties.







Which seems a rather intricate problem...

Thanks to Oliver Labs for the pictures.

Formalization in the Coq system

The Coq system: a type theory based proof assistant.

- Coq is a (functional) programming language.
- Coq has such a rich type system that the types of objects can be theorem statements.
- In the absence of axiom, proofs should be intuitionistic.

Examples.

Quantifier Elimination

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

- for every formula $\phi(\vec{x}) \in \mathcal{F}(\Sigma, \mathcal{V})$,
- there exists a quantifier free formula $\psi(\vec{x}) \in \mathcal{F}(\Sigma, \mathcal{V})$
- such that:

$$T \vdash \forall \vec{x}, ((\phi(\vec{x}) \Rightarrow \psi(\vec{x})) \wedge (\psi(\vec{x}) \Rightarrow \phi(\vec{x})))$$

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
| Unit of term
| Not of formula
| And of formula & formula
| Or of formula & formula
| Implies of formula & formula
| Exists of nat & formula
| Forall of nat & formula.
```

Formal definition of the ring signature

Terms on the language of fields.

```
Inductive term : Type :=
| Var of nat
| Const0 : term
| Const1 : term
| Add of term & term
| Opp of term
| Mul of term & term
| Inv of term
```

Proving quantifier elimination on real closed fields

To state the theorem of quantifier elimination, we could:

- Build the list T of formulas describing the axioms of a real closed field structure.
- Formalize first order provability, $T \vdash \phi$, a predicate of type:

```
Definition entails
   (T : seq (formula R))(phi : formula R) : bool :=
      ...
```

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;
  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;
  ...}.
```

Theory of real closed fields, and models

Now we can equip a given type R with a structure of real closed field as soon as we have:

- implemented the required operations over this type
- proved the required specifications over these operations

To formalize a concrete instance of real closed field structure:

```
Definition R_rcf : RealClosedField R R0 R1 Radd ...
```

Theory of real closed fields, and models

Given an instance `R_rcf` of the real closed field structure , ie.
`R_rcf : rcf`

- We can interpret any element of the type `term` in the type of the domain:

```
Fixpoint eval (R_rcf : rcf)
  (ctxt : seq (carrier R_rcf))(t : term) : (carrier
    R_rcf) := ...
```

  - A variable `Var n` is interpreted by the `n`-th element of the context;
  - A term `(Plus t1 t2)` is interpreted by a sum in the real closed fields;
  - ...

Theory of real closed fields, and models

Given an instance `R_rcf` of the real closed field structure , ie.
`R_rcf : rcf`

- We can interpret any first order formula of type `(formula term)` as a first order Coq statement quantified over the type of the domain:

```
Fixpoint holds (R_rcf : rcf)
    (ctxt : seq (carrier R_rcf)) (f : formula term) :
        Prop := ...
```

  - An atom `(Leq t1 t2)` is interpreted by:

    `(eval R_rcf ctxt t1) <= (eval R_rcf ctxt t1)`

  - A formula `(Or f1 f2)` is interpreted by a Coq disjunction;
  - ...

Hence `(R_rcf : rcf)` can be understood as a formalization of:
"`R_rcf` is a model of the `rcf` theory of real closed fields".

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.