## Quantifier elimination in real closed fields : a formal proof

#### Cyril Cohen Assia Mahboubi

INRIA Saclay — Île-de-France LIX École Polytechnique INRIA Microsoft Research Joint Centre (cyril.cohen|assia.mahboubi)@inria.fr

#### September 9, 2011

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.

## $\forall x \in \mathbb{R}, (x > 0 \Rightarrow \exists y \in \mathbb{R}, (y^2 \le x \land y^5 - y + 3x = 0))$ Question : is it true or false ?

伺 ト イ ヨ ト イ ヨ ト

## $\forall x \in \mathbb{R}, (x > 0 \Rightarrow \exists y \in \mathbb{R}, (y^2 \le x \land y^5 - y + 3x = 0))$

Question : is it true or false ?

• Yes ! It is true or false

$$\forall x \in \mathbb{R}, (x > 0 \Rightarrow \exists y \in \mathbb{R}, (y^2 \le x \land y^5 - y + 3x = 0))$$

Question : is it true or false ?

- Yes ! It is true or false
- Can we decide this kind of problem ?

### $\forall x \in \mathbb{R}, (x > 0 \Rightarrow \exists y \in \mathbb{R}, (y^2 \le x \land y^5 - y + 3x = 0))$

#### Question : is it true or false ?

- Yes ! It is true or false
- Can we decide this kind of problem ?

### $\forall x \in \mathbb{R}, (x > 0 \Rightarrow \exists y \in \mathbb{R}, (y^2 \le x \land y^5 - y + 3x = 0))$

Question : is it true or false ?

- Yes ! It is true or false
- Can we decide this kind of problem ?
   ⇒ Yes, by eliminating quantifiers

Quantifier elimination procedure for **first order formulas** on *classical real numbers* and involving the following constructions:

- field operations (+, -,  $\times,$  ...)
- equality and comparison

Formalised and verified in Coq

We reduced the problem to eliminating " $\exists x$ " in :

$$\exists x, P(x) = 0 \land \bigwedge Q_i(x) > 0$$

We reduced the problem to eliminating " $\exists x$ " in :

$$\exists x, P(x) = 0 \land \bigwedge Q_i(x) > 0$$

Sketch of the solution from there:

- Count the number of roots x of P such that for all i, Q<sub>i</sub>(x) > 0
- if it is positive then it is true, else it is false

$$\exists x, P(x) = 0 \land \bigwedge Q_i(x) > 0$$
  
with  $P, \ Q_i \in R[X]$ 

- getting the roots : OK (root finding procedure)
- testing the signs of the  $Q_i$  : OK

$$\exists x, P(x) = 0 \land \bigwedge Q_i(x) > 0$$
  
with  $P, Q_i \in R[X_1, \dots, X_n][X]$ 

We need a characterisation of the existence of a solution, using an algebraic combinations of the variables.

#### Definition :

$$\operatorname{TQ}(P,Q) = \sum_{x \in \operatorname{roots}(P)} \operatorname{sign}(Q(x))$$

We showed we can characterise algebraically the sign of this quantity using the  $X_j$ 

### Constraints

So we have :

$$\mathrm{TQ}(P,Q) = \sum_{x \in \mathrm{roots}(P)} \mathrm{sign}\left(Q(x)\right)$$

And want to know whether :

$$\exists x, P(x) = 0 \land \bigwedge Q_i(x) > 0$$

• • = • • = •

### Constraints

So we have :

$$\mathrm{TQ}(P,Q) = \sum_{x \in \mathrm{roots}(P)} \mathrm{sign}\left(Q(x)\right)$$

And want to know whether :

$$\exists x, P(x) = 0 \land \bigwedge Q_i(x) > 0$$

i.e. whether

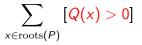
$$\left(\sum_{x\in \text{roots}(P)} [\forall i, Q_i(x) > 0]\right) > 0$$

with 
$$[true] = 1$$
 and  $[false] = 0$ 

3 🕨 🖌 3

#### $\exists x, P(x) = 0 \land Q(x) > 0$

We need :



・ 同 ト ・ ヨ ト ・ ヨ ト …

$$\exists x, P(x) = 0 \land Q(x) > 0$$

We need :

$$\sum_{x \in \text{roots}(P)} [\text{sign}(Q(x)) = 1]$$

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

▲御▶ ▲ 陸▶ ▲ 陸▶

$$\exists x, P(x) = 0 \land Q(x) > 0$$

We need :

$$C^{1}(P,Q) := \sum_{x \in \operatorname{roots}(P)} [\operatorname{sign} (Q(x)) = 1]$$

個 ト イヨト イヨト

$$\exists x, P(x) = 0 \land Q(x) > 0$$

We need :

$$C^{\varepsilon}(P,Q) := \sum_{x \in \text{roots}(P)} [\text{sign}(Q(x)) = \varepsilon]$$

with  $\pmb{\varepsilon} \in \{1,-1,0\}$ 

伺 ト イヨト イヨト

## $TQ(P, Q) = \sum_{x \in roots(P)} sign(Q(x))$

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

伺 ト イヨ ト イヨ ト

$$TQ(P) = \sum_{x \in roots(P)} sign(Q(x))$$

#### We omit Q for the sake of readability

→ < ∃ →</p>

$$TQ_z = \sum_{x \in z} sign(Q(x))$$

with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

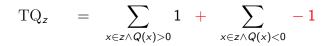
伺 ト イヨト イヨト

# $\mathrm{TQ}_z = \sum_{x \in z \land Q(x) > 0} \operatorname{sign} \left( Q(x) \right) + \sum_{x \in z \land Q(x) < 0} \operatorname{sign} \left( Q(x) \right)$

#### with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

• • = • • = •

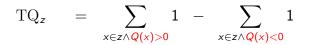


#### with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

伺 ト イヨ ト イヨ ト

## Relating TQ and $C^{\varepsilon}$



#### with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

伺 ト イヨ ト イヨ ト

## $\mathrm{TQ}_z \quad = \quad \sum_{x \in z} \left[ Q(x) > 0 \right] \quad - \quad \sum_{x \in z} \left[ Q(x) < 0 \right]$

#### with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

伺 ト イ ヨ ト イ ヨ ト

$$\mathrm{TQ}_z \quad = \quad \sum_{x \in z} \left[ \mathrm{sign} \left( Q(x) \right) = 1 \right] \quad - \quad \sum_{x \in z} \left[ \mathrm{sign} \left( Q(x) \right) = -1 \right]$$

#### with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

/□ ▶ ▲ 글 ▶ ▲ 글

## Relating TQ and $C^{\varepsilon}$

## $\mathrm{TQ}_z \quad = \quad \mathrm{C}_z^1 \quad - \quad \mathrm{C}_z^{-1}$

#### with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

伺 と く ヨ と く ヨ と …

## $\mathrm{TQ}_z(Q) = \mathrm{C}_z^1(Q) - \mathrm{C}_z^{-1}(Q)$

#### with z = roots(P)We restore the "printing" of Q

• • = • • = •

# $\begin{array}{rcl} \mathrm{TQ}_z(Q) &=& \mathrm{C}_z^1(Q) &-& \mathrm{C}_z^{-1}(Q) \\ \mathrm{TQ}_z(Q^2) &=& \mathrm{C}_z^1(Q) &+& \mathrm{C}_z^{-1}(Q) \end{array}$

#### with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

• • = • • = •

$$\begin{array}{rcl} \mathrm{TQ}_{z}(Q) & = & \mathrm{C}_{z}^{1}(Q) & - & \mathrm{C}_{z}^{-1}(Q) \\ \mathrm{TQ}_{z}(Q^{2}) & = & \mathrm{C}_{z}^{1}(Q) & + & \mathrm{C}_{z}^{-1}(Q) \\ \mathrm{TQ}_{z}(1) & = & \mathrm{C}_{z}^{1}(Q) & + & \mathrm{C}_{z}^{-1}(Q) & + & \mathrm{C}_{z}^{0}(Q) \end{array}$$

with z = roots(P)

Cyril Cohen, Assia Mahboubi Quantifier elimination in real closed fields : a formal proof

→ < ∃ →</p>

э

## Matricial equation

$$\begin{pmatrix} \operatorname{TQ}_{z}(Q) \\ \operatorname{TQ}_{z}(Q^{2}) \\ \operatorname{TQ}_{z}(1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \operatorname{C}_{z}^{1}(Q) \\ \operatorname{C}_{z}^{-1}(Q) \\ \operatorname{C}_{z}^{0}(Q) \end{pmatrix}$$
  
with  $z = \operatorname{roots}(P)$ 

## Matricial equation

$$\begin{pmatrix} \mathrm{TQ}_{z}(Q) \\ \mathrm{TQ}_{z}(Q^{2}) \\ \mathrm{TQ}_{z}(1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \mathrm{C}_{z}^{1}(Q) \\ \mathrm{C}_{z}^{-1}(Q) \\ \mathrm{C}_{z}^{0}(Q) \end{pmatrix}$$

$$\text{with } z = \mathrm{roots}(P)$$

$$\begin{vmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{vmatrix} = 2$$

## Matricial equation

$$\begin{pmatrix} \operatorname{TQ}_{z}(Q) \\ \operatorname{TQ}_{z}(Q^{2}) \\ \operatorname{TQ}_{z}(1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \operatorname{C}_{z}^{1}(Q) \\ \operatorname{C}_{z}^{-1}(Q) \\ \operatorname{C}_{z}^{0}(Q) \end{pmatrix}$$

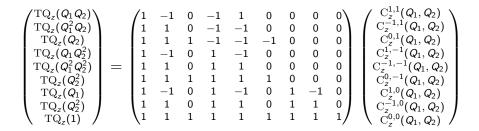
$$\text{with } z = \operatorname{roots}(P)$$

$$\begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \text{ is invertible}$$

We generalise  $C^{\varepsilon}$  again :

$$\mathrm{C}^{\varepsilon_1,\ldots,\varepsilon_n}(P,Q_1,\ldots,Q_n) = \sum_{x\in\mathrm{roots}(P)} [\forall i,\mathrm{sign}(Q_i(x)) = \varepsilon_i]$$

## Matricial system



with z = roots(P)

## Matricial system

Example with 2 polynomials  $Q_i$ 

$$\begin{pmatrix} \operatorname{TQ}_{z}(Q_{1}Q_{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}Q_{2}) \\ \operatorname{TQ}_{z}(Q_{1}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}$$

with z = roots(P)

# Matricial system

Example with 2 polynomials  $Q_i$ 

$$\begin{pmatrix} \operatorname{TQ}_{z}(Q_{1}Q_{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}Q_{2}) \\ \operatorname{TQ}_{z}(Q_{2}) \\ \operatorname{TQ}_{z}(Q_{1}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}) \\ \operatorname{TQ}_{z}(Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}) \\ \operatorname{TQ}_{z}(Q_{1}) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} ^{\otimes 2} \begin{pmatrix} \operatorname{C}_{z}^{1,1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,-1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{0,-1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{0,-1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,0}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,0}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,0}(Q_{1}, Q_{2}) \end{pmatrix}$$

with z = roots(P)

# Matricial system

Example with 2 polynomials  $Q_i$ 

$$\begin{pmatrix} \operatorname{TQ}_{z}(Q_{1}Q_{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}Q_{2}) \\ \operatorname{TQ}_{z}(Q_{2}) \\ \operatorname{TQ}_{z}(Q_{1}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}Q_{2}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}^{2}) \\ \operatorname{TQ}_{z}(Q_{1}) \\ \operatorname{TQ}_{z}(Q_{1}) \\ \operatorname{TQ}_{z}(Q_{1}) \\ \operatorname{TQ}_{z}(Q_{1}) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \otimes^{2} \begin{pmatrix} \operatorname{C}_{z}^{1,1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,-1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{0,-1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{0,-1}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,0}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,0}(Q_{1}, Q_{2}) \\ \operatorname{C}_{z}^{-1,0}(Q_{1}, Q_{2}) \end{pmatrix}$$

with z = roots(P)

Ordered structures :

- lots of lemmas : good statements and good naming conventions
- intervals and neighbourhoods infrastructure

Polynomials

- properties about pseudo-division
- properties about roots and multiplicity
- root finding using dichotomy, neighbourhoods
- Cauchy index
  - $\Rightarrow$  gives the algebraic characterisation for  $\mathrm{TQ}$

Amongst others :

- Imprecision of the paper proof (*Algorithms in Real Algebraic Geometry*)
- Problems with dependent types and data-structures

Relation between the  $\mathrm{TQ}_z(ar{Q}^{ar{\sigma}})$  and  $\mathrm{C}_z^{ar{\varepsilon}}(ar{Q})$ 

- Need to compute all the expressions the form
  - $\operatorname{TQ}_{z}(Q_{1}^{\sigma_{1}}Q_{2}^{\sigma_{2}}\ldots Q_{n}^{\sigma_{n}})$  for  $\sigma \in \{0, 1, 2\}$ .
  - $C_z^{\varepsilon_1,\ldots,\varepsilon_n}(Q_1,\ldots,Q_n)$  for  $\varepsilon \in \{1,-1,0\}$ .

And organise them properly inside the matrices

• Induction hypothesis non-trivial and omitted in the paper "with z = roots(P)"  $\longrightarrow$  " for any z" Matrices encoded as finite functions (Ssreflect library)

- type is dependent on the size of the matrix
- forall A i j, A = B <-> A i j = B i j

Thanks to the dependent type, we can easily express block matrices

Matrices encoded as finite functions (Ssreflect library)

• M : 'M[R]\_(<u>m</u>, <u>n</u>)

• forall A i j, A = B <-> A i j = B i j

Thanks to the dependent type, we can easily express block matrices

# Nine block $3^n$ -matrices put together gives a $3^n + 3^n + 3^n$ -matrix.

Not convertible to  $3^{n+1}$ -matrix (as such)

- Ssreflect matrices are locked
   ⇒ Prevents unwanted partial evaluation
- No computation for a simple 3-matrix determinant :

$$\begin{pmatrix} 1 & -1 & 0 \ 1 & 1 & 0 \ 1 & 1 & 1 \end{pmatrix}$$

• done using rewriting lemmas

- Proof done on any discrete **real closed field** (with decidable comparison)
- Procedure by reflection : reification of the logic

## $\forall x \in \mathbb{R}, (x > 0 \Rightarrow \exists y \in \mathbb{R}, (y^2 \le x \land y^5 - y + 3x = 0))$

#### Question : is it true or false ?

- Yes ! It is true or false
- Can we decide this kind of problem ?
   ⇒ Yes, by eliminating quantifiers
- Is there an efficient algorithm ?

## $\forall x \in \mathbb{R}, (x > 0 \Rightarrow \exists y \in \mathbb{R}, (y^2 \le x \land y^5 - y + 3x = 0))$

#### Question : is it true or false ?

- Yes ! It is true or false
- Can we decide this kind of problem ?
   ⇒ Yes, by eliminating quantifiers
- Is there an efficient algorithm ?

## Effective computation and related work

- Would executable if data-structures allowed it.
- Not efficient

Related work :

- Tactic for HOL Light (different spirit) : John Harisson
- Cylindrical Algebraic Decomposition in Coq (no completed proof yet): Assia Mahboubi

Conclusion :

- Makes first order theory of real closed fields decidable
- Opens the way to proving the Cylindrical Algebraic Decomposition (CAD)

Future work :

- Integrate automation (fourier, ring) to the development
- Prove CAD correctness

#### Thank you for your attention. Questions ?

→ < ∃ →</p>