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.

An example

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

Question : is it true or false ?

An example

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

Question : is it true or false ?

- Yes ! It is true or false

An example

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

Question : is it true or false ?

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

An example

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

Question : is it true or false ?

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

An example

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

Question : is it true or false ?

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

The problem we would like to solve

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

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

Formalised and verified in Coq

Reducing the problem

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

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

Reducing the problem

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

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

Sketch of the solution from there:

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

Case of one variable

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

$$\text{with } P,\ Q_i \in R[X]$$

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

Case of multiple variables

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

$$\text{with } P,\ Q_i \in R[X_1, \ldots, X_n][X]$$

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

Tarski query

Definition :

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

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

Constraints

So we have :

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

And want to know whether :

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

Constraints

So we have :

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

And want to know whether :

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

i.e. whether

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

with $[\mathrm{true}] = 1$ and $[\mathrm{false}] = 0$

If only one Q_i

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

We need :

$$\sum_{x \in \mathrm{roots}(P)} [Q(x) > 0]$$

If only one Q_i

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

We need :

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

If only one Q_i

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

We need :

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

If only one Q_i

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

We need :

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

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

Relating TQ and C^{ε}

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

Relating TQ and C^{ε}

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

We omit Q for the sake of readability

Relating TQ and C^{ε}

$$\mathrm{TQ}_z \quad = \quad \sum_{x \in z} \mathrm{sign}\,(Q(x))$$

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

Relating TQ and C^{ε}

$$\mathrm{TQ}_z \quad = \sum_{x \in z \wedge Q(x) > 0} \mathrm{sign}\,(Q(x)) \;+ \sum_{x \in z \wedge Q(x) < 0} \mathrm{sign}\,(Q(x))$$

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

Relating TQ and C^{ε}

$$\mathrm{TQ}_z = \sum_{x \in z \wedge Q(x) > 0} 1 + \sum_{x \in z \wedge Q(x) < 0} -1$$

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

Relating TQ and C^{ε}

$$\mathrm{TQ}_z \quad = \quad \sum_{x \in z \wedge Q(x) > 0} 1 \; - \sum_{x \in z \wedge Q(x) < 0} 1$$

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

Relating TQ and C^{ε}

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

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

Relating TQ and C^{ε}

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

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

Relating TQ and C^{ε}

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

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

Relating TQ and C^{ε}

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

with $z = \mathrm{roots}(P)$
We restore the " printing" of Q

Relating TQ and C^{ε}

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

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

Relating TQ and C^{ε}

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

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

Matricial equation

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

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

Matricial equation

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

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

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

Matricial equation

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

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

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

For many Q_i

We generalise C^{ε} 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

$$\begin{pmatrix} \mathrm{TQ}_z(Q_1 Q_2) \\ \mathrm{TQ}_z(Q_1^2 Q_2) \\ \mathrm{TQ}_z(Q_2) \\ \mathrm{TQ}_z(Q_1 Q_2^2) \\ \mathrm{TQ}_z(Q_1^2 Q_2^2) \\ \mathrm{TQ}_z(Q_2^2) \\ \mathrm{TQ}_z(Q_1) \\ \mathrm{TQ}_z(Q_2^2) \\ \mathrm{TQ}_z(1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & -1 & -1 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 1 & -1 & 0 & 1 & -1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \mathrm{C}_z^{1,1}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,1}(Q_1, Q_2) \\ \mathrm{C}_z^{0,1}(Q_1, Q_2) \\ \mathrm{C}_z^{1,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{0,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{1,0}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,0}(Q_1, Q_2) \\ \mathrm{C}_z^{0,0}(Q_1, Q_2) \end{pmatrix}$$

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

Matricial system

Example with 2 polynomials Q_i

$$\begin{pmatrix} \mathrm{TQ}_z(Q_1 Q_2) \\ \mathrm{TQ}_z(Q_1^2 Q_2) \\ \mathrm{TQ}_z(Q_2) \\ \mathrm{TQ}_z(Q_1 Q_2^2) \\ \mathrm{TQ}_z(Q_1^2 Q_2^2) \\ \mathrm{TQ}_z(Q_2^2) \\ \mathrm{TQ}_z(Q_1) \\ \mathrm{TQ}_z(Q_2^2) \\ \mathrm{TQ}_z(1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} \mathrm{C}_z^{1,1}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,1}(Q_1, Q_2) \\ \mathrm{C}_z^{0,1}(Q_1, Q_2) \\ \mathrm{C}_z^{1,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{0,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{1,0}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,0}(Q_1, Q_2) \\ \mathrm{C}_z^{0,0}(Q_1, Q_2) \end{pmatrix}$$

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

Matricial system

Example with 2 polynomials Q_i

$$\begin{pmatrix} \mathrm{TQ}_z(Q_1 Q_2) \\ \mathrm{TQ}_z(Q_1^2 Q_2) \\ \mathrm{TQ}_z(Q_2) \\ \mathrm{TQ}_z(Q_1 Q_2^2) \\ \mathrm{TQ}_z(Q_1^2 Q_2^2) \\ \mathrm{TQ}_z(Q_2^2) \\ \mathrm{TQ}_z(Q_1) \\ \mathrm{TQ}_z(Q_2^2) \\ \mathrm{TQ}_z(1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}^{\otimes 2} \begin{pmatrix} \mathrm{C}_z^{1,1}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,1}(Q_1, Q_2) \\ \mathrm{C}_z^{0,1}(Q_1, Q_2) \\ \mathrm{C}_z^{1,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{0,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{1,0}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,0}(Q_1, Q_2) \\ \mathrm{C}_z^{0,0}(Q_1, Q_2) \end{pmatrix}$$

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

Matricial system

Example with 2 polynomials Q_i

$$\begin{pmatrix} \mathrm{TQ}_z(Q_1 Q_2) \\ \mathrm{TQ}_z(Q_1^2 Q_2) \\ \mathrm{TQ}_z(Q_2) \\ \mathrm{TQ}_z(Q_1 Q_2^2) \\ \mathrm{TQ}_z(Q_1^2 Q_2^2) \\ \mathrm{TQ}_z(Q_2^2) \\ \mathrm{TQ}_z(Q_1) \\ \mathrm{TQ}_z(Q_2^2) \\ \mathrm{TQ}_z(1) \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}^{\otimes 2} \begin{pmatrix} \mathrm{C}_z^{1,1}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,1}(Q_1, Q_2) \\ \mathrm{C}_z^{0,1}(Q_1, Q_2) \\ \mathrm{C}_z^{1,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{0,-1}(Q_1, Q_2) \\ \mathrm{C}_z^{1,0}(Q_1, Q_2) \\ \mathrm{C}_z^{-1,0}(Q_1, Q_2) \\ \mathrm{C}_z^{0,0}(Q_1, Q_2) \end{pmatrix}$$

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

We formalised in Coq

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 TQ

Issues during the formalisation

Amongst others :

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

Paper proof Imprecision

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

- Need to compute all the expressions the form
  - $\mathrm{TQ}_z(Q_1^{\sigma_1} Q_2^{\sigma_2} \dots Q_n^{\sigma_n})$ for $\sigma \in \{0, 1, 2\}$.
  - $\mathrm{C}_z^{\varepsilon_1, \dots, \varepsilon_n}(Q_1, \dots, Q_n)$ for $\varepsilon \in \{1, -1, 0\}$.

  And organise them properly inside the matrices
- Induction hypothesis non-trivial and omitted in the paper
  " with $z = \mathrm{roots}(P)$" $\longrightarrow$ " for any z"

Matrix data-structure

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

Matrix data-structure

Matrices encoded as finite functions (Ssreflect library)

- `M : 'M[R]_(m, n)`
- `forall A i j, A = B <-> A i j = B i j`

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

Dependent types issues

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)

Reduction is locked

- Ssreflect matrices are locked
  $\Rightarrow$ 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

Context

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

An example

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

Question : is it true or false ?

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

An example

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

Question : is it true or false ?

- Yes ! It is true or false
- Can we decide this kind of problem ?
  $\Rightarrow$ 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 and future work

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

The End

Thank you for your attention. Questions ?