Quantifier Elimination for Real and Complex fields

Andrei Giurgiu

November 18, 2010

Quantifier Elimination in General - Problem formulation

Given a formula

$$F(x_1, \ldots, x_k) = Qx_{k+1}.Qx_{k+2}.\ldots Qx_m.G(x_1, x_2, \ldots, x_m),$$

where G is *quantifier-free*,

find a *quantifier-free* formula $F'(x_1, \ldots, x_k)$,

such that F and F' are *equally satisfiable*.

Quantifier Elimination - General Strategy

It is enough if we do it on

$$\exists x_1 . L_1(x_1, \dots, x_k) \wedge L_2(x_1, \dots, x_k) \wedge \dots \wedge L_k(x_1, \dots, x_k),$$

where $L_i(x_1, \dots, x_k)$ are literals!

Quantifier Elimination - General Strategy

It is enough if we do it on

$$\exists x_1 . L_1(x_1, \ldots, x_k) \wedge L_2(x_1, \ldots, x_k) \wedge \ldots \wedge L_k(x_1, \ldots, x_k),$$

where $L_i(x_1, \ldots, x_k)$ are literals!

Why?

Real and Complex Fields: Signatures

- Real numbers: $(\{+_2, \cdot_2\}, \{=_2, <_2, >_2, \geq_2, \leq_2\})$
- Complex numbers: $(\{+_2, \cdot_2\}, \{=_2\})$

Real and Complex Fields: Signatures

- Real numbers: $(\{+_2, \cdot_2\}, \{=_2, <_2, >_2, \geq_2, \leq_2\})$
- Complex numbers: $(\{+_2, \cdot_2\}, \{=_2\})$

Atoms are just inequalities with multivariate polynomials!
For the reals:

$$f(x_1, \ldots, x_n) \bowtie 0, \text{with } \bowtie \in \{=_2, <_2, >_2, \geq_2, \leq_2\}$$

Some History

- Descartes 1637, *"rule of signs"*;
- Sturm 1835, rule to determine the number of roots of a polynomial;
- Tarski 1930's, published in 1948: first QE procedure for reals;
- Collins 1975, first QE procedure efficient enough to be implemented: Cylindrical Algebraic Decomposition (CAD);
- ...

The Complex Case is Simple

Lemma

All we need to do is QE on

$$\exists x. \bigwedge_{j=1}^{k} f_j(x, y_1, \ldots, y_n) = 0 \wedge \bigwedge_{j=k+1}^{k'} f_j(x, y_1, \ldots, y_n) \neq 0.$$

The Complex Case is Simple

Lemma

Let $f_1, \ldots, f_k \in \mathbb{R}(X_1, \ldots, X_n)$. *Then*

$$\bigwedge_{i=1}^{k} f_i(x_1, \ldots, x_n) \neq 0 \quad \Longleftrightarrow \quad \prod_{i=1}^{k} f_i(x_1, \ldots, x_n) \neq 0.$$

The Complex Case is Simple

Lemma (simple!)

Let $f, g \in \mathbb{R}(X)$, $d_f = \deg f$, $d_g = \deg g$. *Suppose* $d_f \geq d_g \geq 1$. *Then there is* $r \in \mathbb{R}X$ *with* $\deg r < d_f$, *such that Then*

$$f(x) = 0 \wedge g(x) = 0 \iff r(x) = 0 \wedge g(x) = 0.$$

Proof.

Pick r as the remainder of the division of f and g. $\square$

The Complex Case is Simple

Lemma (Pseudo-division)

Let $f, g \in \mathbb{R}(X, Y_1 \ldots, Y_n)$, $d_f = \deg_x f$, $d_g = \deg_x g$, *and fix* $y \in \mathbb{R}^n$. *Suppose* $d_f \geq d_g$ *and* $g(x, y) = \sum_{i=0}^{d_g} A_i(y) x^i$.

Then if $A_{d_g}(y) = 0$, *there are some* $k \in \mathbb{N}$, $q, r \in \mathbb{R}(X, Y_1 \ldots, Y_n)$ *with* $\deg_x r < d_g$, *such that*

$$A_{d_g}(y)^k f(x, y) = g(x, y) q(x, y) + r(x, y)$$

Proof.

See blackboard. □

The Complex Case is Simple

Lemma (complicated!)

Let $f, g \in \mathbb{R}(X, Y_1 \ldots, Y_n)$, $d_f = \deg_x f$, $d_g = \deg_x g$. *Suppose* $d_f \geq d_g$ *and*
$g(x, y) = \sum_{i=0}^{d_g} A_i(y)x^i$..

Set
$g_t(x, y) = \sum_{i=0}^{d_g - 1} A_i(y)x^i$.

Then there is $r \in \mathbb{R}(X, Y_1 \ldots, Y_n)$ *with* $\deg_x r < d_g$*, such that*

$$\begin{aligned} & f(x,y) = 0 \wedge g(x,y) = 0 \iff \\ A_{d_f}(y) = 0 \wedge \quad & f(x,y) = 0 \wedge g_t(x,y) = 0 \quad \vee \\ A_{d_f}(y) \neq 0 \wedge \quad & r(x,y) = 0 \wedge g(x,y) = 0. \end{aligned}$$

Proof.

Use pseudo-division.

The Complex Case is Simple

We have managed to prove that

$$\exists x. \bigwedge_{j=1}^{k} f_j(x, y_1, \ldots, y_n) = 0 \wedge \bigwedge_{j=k+1}^{k'} f_j(x, y_1, \ldots, y_n) \neq 0.$$

is equally satisfiable with

$$\bigvee_i P_i(y_1, \ldots, y_n) \wedge (\exists x. f(x, y_1, \ldots, y_n) = 0 \wedge g(x, y_1, \ldots, y_n) \neq 0),$$

for some predicates P_i depending only on $y_1, \ldots, y_n$.

The red part above is equivalent to

$$\neg \forall x. f(x, y_1, \ldots, y_n) = 0 \rightarrow g(x, y_1, \ldots, y_n) = 0.$$

The Complex Case is Simple

Lemma

The formula

$$\forall x. f(x, y_1, \dots, y_n) = 0 \rightarrow g(x, y_1, \dots, y_n) = 0$$

is equisatisfiable with

$$f(\cdot, y_1, \dots, y_n) | g^{d_f}(\cdot, y_1, \dots, y_n).$$

Proof.

Fundamental Theorem of Algebra! $\square$

The Complex Case is Simple

There are $q, r \in \mathbb{R}(X, Y_1, \ldots, Y_n)$ with $\deg_x(r) < \deg_x(f)$, such that

$$A_{d_g}(y)f(x,y) = g(x,y)q(x,y) + r(x,y).$$

Lemma

Given that $A_{d_g} \neq 0$,

$$f(\cdot, y_1, \ldots, y_n) | g^{d_f}(\cdot, y_1, \ldots, y_n) \iff r(x,y) \equiv 0.$$

The Complex Case is Simple

There are $q, r \in \mathbb{R}(X, Y_1, \ldots, Y_n)$ with $\deg_x(r) < \deg_x(f)$, such that

$$A_{d_g}(y) f(x, y) = g(x, y) q(x, y) + r(x, y).$$

Lemma

Given that $A_{d_g} \neq 0$,

$$f(\cdot, y_1, \ldots, y_n) | g^{d_f}(\cdot, y_1, \ldots, y_n) \iff r(x, y) \equiv 0.$$

We are done!!

The Real Case is also Simple

We do QE on

$$\exists x. \bigwedge_{i=1}^{k} f_i(x, y_1, \ldots, y_n) \bowtie 0, \text{with } \bowtie \in \{=_2, <_2, >_2, \geq_2, \leq_2\}.$$

The Real Case is also Simple

Simplest case, polynomials are univariate.
We would like to have something like this:

	$(-\infty, x_1)$	x_1	(x_1, x_2)	x_2	(x_2, x_3)	x_3	(x_3, x_4)	x_4	(x_4, x_5)	x_5	$(x_5, +\infty)$
$f_1(x)$	$+$	0	$+$	$+$	$+$	0	$-$	$-$	$-$	0	$+$
$f_2(x)$	$+$	$+$	$+$	0	$-$	$-$	$-$	$-$	$-$	$-$	$-$
$f_3(x)$	$-$	0	$+$	0	$+$	0	$-$	0	$+$	0	$+$
$f_4(x)$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	0	$-$	0	$+$

Then we can readily decide whether the formula is true or false! It is clear from the table that there is a solution that satisfies the constraints or not.

The Real Case is also Simple

Task: build table for $f, f_1, f_2, \ldots, f_k \in \mathbb{R}(X)$.
Do this with recursion! Assume we already have a table for

$$
\begin{aligned}
&f_0 = f' \\
&f_1 \\
&\vdots \\
&f_k \\
&f \mod f_0 \\
&f \mod f_1 \\
&\vdots \\
&f \mod f_k
\end{aligned}
$$

The Real Case is also Simple

How to transform the table:

- If $f_j(x) = 0$ then we can infer the sign of $f(x)$ from the sign of $(f \mod f_j)(x)$.
- Let $\tilde{x}$ and $\tilde{x}'$ be two consecutive roots of f'. Then in the interval $[\tilde{x}, \tilde{x}']$ there is at most one root of f. Also, the sign of f changes at most once.
- The head coefficient of f gives the sign at $+\infty$ and $-\infty$.
- Drop polynomials $f', f \mod f_0, f \mod f_1, \dots, f \mod f_k$, since they do not appear in the final table.
- Whenever the sign of f changes between two consecutive points in the table, introduce a new point corresponding to a root of f, and infer the signs of the other polynomials in the table.

The Real Case is also Simple

Generalize for more variables: consider $y_1, \ldots, y_n$ as constants, and eliminate x in the following way.

- Use pseudo-division instead of normal (univariate) polynomial division.
- Note that the signs of the polynomials in the table depend directly on the coefficients of polynomials.
- Branch on the sign of each coefficient that appears while creating the table (thereby creating predicates of the form $A(y_1, \ldots, y_n)$), to determine the sign table.
- Use this to create the formula on $y_1, \ldots, y_n$ with no quantifiers.

The Real Case is also Simple

Generalize for more variables: consider $y_1, \ldots, y_n$ as constants, and eliminate x in the following way.

- Use pseudo-division instead of normal (univariate) polynomial division.
- Note that the signs of the polynomials in the table depend directly on the coefficients of polynomials.
- Branch on the sign of each coefficient that appears while creating the table (thereby creating predicates of the form $A(y_1, \ldots, y_n)$, to determine the sign table.
- Use this to create the formula on $y_1, \ldots, y_n$ with no quantifiers.
- Done!

Cylindrical Algebraic Decomposition

Define a *cell* recursively:

- In 1-D: a cell is either a point or an interval.
- In $\mathbb{R}^k$: a set $S \in \mathbb{R}^k$ is a cell if there is a $k-1$-dimensional cell $D \subset \mathbb{R}^{k-1}$ and functions $f, g : \mathbb{R}^{k-1} \to \mathbb{R}$ such that there are polynomials $F, G \in \mathbb{R}(X, Y_1, \dots, Y_{k-1})$ with

$$F(f(y_1, \dots, y_{k-1}), y_1, \dots, y_{k-1}) = 0,$$
$$G(g(y_1, \dots, y_{k-1}), y_1, \dots, y_{k-1}) = 0,$$

and

$$S = \{(x, y_1, \dots, y_{k-1}) : (y_1, \dots, y_{k-1}) \in D, f(y) < x < g(y)\}.$$

Cylindrical Algebraic Decomposition

Our QE method generates a Cylindrical Algebraic Decomposition: see blackboard!

Thanks for listening!