Little Engines of Proof

N. Shankar, L. de Moura, H. Ruess, A. Tiwari
shankar@csl.sri.com
URL: http://www.csl.sri.com/~shankar/LEP.html

Computer Science Laboratory
SRI International
Menlo Park, CA

Recall

We discussed decision procedures based on Gröbner bases

- Gröbner basis gives canonical representation for sets of equations
- It can be used to decide the UWP and the CVP over ACFs

Most often, we need to decide formulas over the reals

Today: we show that the theory of real closed fields and ACFs admit quantifier elimination

Real-Closed Fields

Signature: $\Sigma_F = \langle 0, 1, +, -, *, < \rangle$

1. $\langle F, 0, 1, +, -, * \rangle$ is a field.
2. (a) $(x \not< x)$

   (b) $x < y \Rightarrow y < z \Rightarrow x < z$

   (c) $x < y \Rightarrow x + z < y + z$

   (d) $x, y > 0 \Rightarrow x * y > 0$

   (e) $x > 0 \vee x = 0 \vee 0 > x$
3. every positive element of F has a square root in F and every odd degree polynomial in $F[x]$ has a root in F.

The set of reals, $\Re$, form a real-closed field.

Quantifier Elimination Procedure for Reals

We only need to show how to eliminate one $\exists$ quantifier from a conjunction of literals. Why?

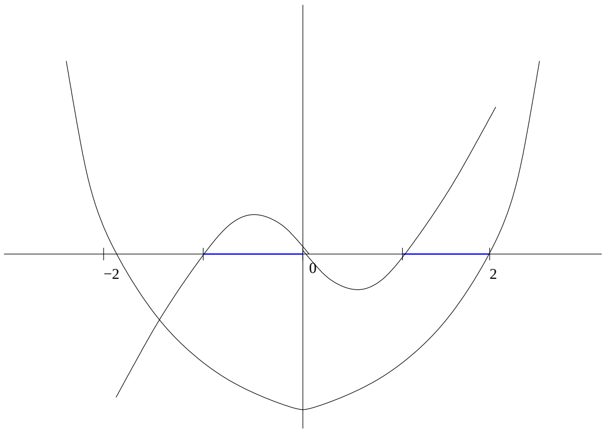
In case of $\Re$, this is:

$$\phi(\vec{y}) := \exists x.(p_1 \sim_1 0 \ \wedge \ p_2 \sim_2 0 \ \wedge \ \cdots \ \wedge \ p_l \sim_l 0)$$

where $\sim_i$ is either $<, =,$ or $>$ and $p_i \in \mathbb{Z}[\vec{y}][x]$

Geometric Intuition

Consider: $x^2 < 4 \wedge x^3 > x$



Geometric Intuition

The 1-D space $\Re^1$ is partitioned into finitely many sign-invariant regions:

$$(-\infty, -2), -2, (-2, -1), -1, (-1, 0), 0, (0, 1), 1, (1, 2), 2, (2, \infty)$$

The same happens in higher dimensions

This is because we only have polynomials

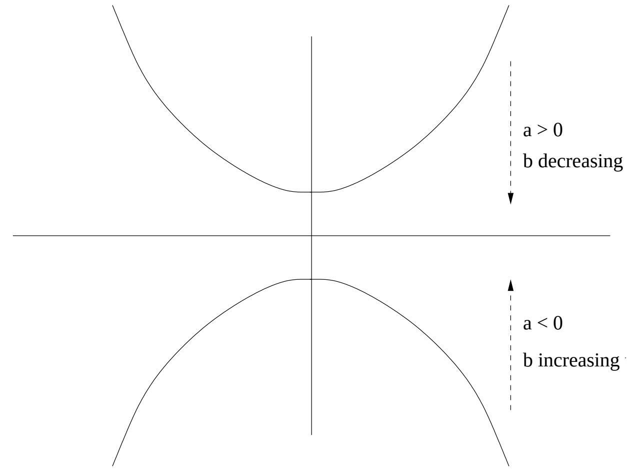
Inductively, if the $\Re^{n-1}$ is sufficiently partitioned, then we consider the cylinder above each region S;

And partition the space $-\infty < x_n < \infty$ accordingly

To get a partition of the cylinder $S \times (-\infty, \infty)$

QE Procedure for Reals: Example

Consider: $ax^2 + b > 0$



QE Procedure for Reals: Example

$\exists x. ax^2 + b > 0$

What are the relevant polynomials? Let p be $ax^2 + b$

a	:	leading coefficient of p, $\mathsf{LC}(p)$
b	:	remaining part of p, $\mathsf{RP}(p)$
$2ax$	:	derivative of p, p'
b	:	pseudo-remainder of p divided by $2ax$, $\mathsf{PR}(p, 2ax)$

We guess a sign assignment for polynomials not containing x

Say, we choose a to be negative and b to be positive

QE Procedure for Reals: Example

Full cylinder over $a < 0, b > 0$:

	$\gamma_{-\infty}$	$(\gamma_{-\infty}, \gamma_{\infty})$	γ_{∞}
a	$-$	$-$	$-$
b	$+$	$+$	$+$
$2ax$	$+$	$?$	$-$

	$\gamma_{-\infty}$	$(\gamma_{-\infty}, \gamma_0)$	γ_0	$(\gamma_0, \gamma_{\infty})$	γ_{∞}
a	$-$	$-$	$-$	$-$	$-$
b	$+$	$+$	$+$	$+$	$+$
$2ax$	$+$	$+$	0	$-$	$-$

QE Procedure for Reals: Example

	$\gamma_{-\infty}$	$(\gamma_{-\infty}, \gamma_0)$	γ_0	$(\gamma_0, \gamma_{\infty})$	γ_{∞}
a	$-$	$-$	$-$	$-$	$-$
b	$+$	$+$	$+$	$+$	$+$
$2ax$	$+$	$+$	0	$-$	$-$
ax^2+b	$-$	$?$	$+$	$?$	$-$

Fully decomposed cylinder over $a < 0, b > 0$:

	$\gamma_{-\infty}$	..	γ_{-1}	..	γ_0	..	γ_1	..	γ_{∞}
a	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$	$-$
b	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$	$+$
$2ax$	$+$	$+$	$+$	$+$	0	$-$	$-$	$-$	$-$
ax^2+b	$-$	$-$	0	$+$	$+$	$+$	0	$-$	$-$

QE Procedure for Reals: Example

Is there a column where $ax^2 + b > 0$?

Yes, so the guess $a < 0, b > 0$ is "part of the solution".

We consider the cylinder over the other 8 regions

In four cases, there is no column where $ax^2 + b > 0$:
$a < 0, b = 0$; $a < 0, b < 0$; $a = 0, b = 0$; $a = 0, b < 0$.

Hence, $\exists x.(ax^2 + b > 0)$ is equivalent to

$$a > 0 \ \vee \ (a = 0 \ \wedge \ b > 0) \ \vee \ (a < 0 \ \wedge \ b > 0)$$

Quantifier Elimination Procedure for Reals

Guess1	$\dfrac{\Gamma' \equiv \Gamma \cup \{p \sim 0\}}{\Gamma' \cup \{p' > 0\} \mid \Gamma' \cup \{p' = 0\} \mid \Gamma' \cup \{p' < 0\}}$
Guess2	$\dfrac{\Gamma' \equiv \Gamma \cup \{p \sim 0\}}{\Gamma' \cup \{\mathsf{LC}(p) > 0\} \mid \Gamma' \cup \{\mathsf{LC}(p) = 0\} \mid \Gamma' \cup \{\mathsf{LC}(p) < 0\}}$
Guess3	$\dfrac{\Gamma' \equiv \Gamma \cup \{p \sim 0\}}{\Gamma' \cup \{\mathsf{RP}(p) > 0\} \mid \Gamma' \cup \{\mathsf{RP}(p) = 0\} \mid \Gamma' \cup \{\mathsf{RP}(p) < 0\}}$
Guess4	$\dfrac{\Gamma' \equiv \Gamma \cup \{p_1 \sim_1 0, p_2 \sim_2 0\}}{\Gamma' \cup \{\mathsf{PR}(p_1, p_2) > 0\} \mid \ldots \mid \Gamma' \cup \{\mathsf{PR}(p_1, p_2) < 0\}}$

where $p' = \frac{\partial p}{\partial x}$, $\mathsf{LC}(p) =$ leading coefficient of p,
$p = \mathsf{LC}(p)x^i + \mathsf{RP}(p)$, and $\mathsf{LC}(q)^{n-m+1}p_1 = qp_2 + \mathsf{PR}(p_1, p_2)$.

QE in Reals: Phase 2

Verify1 $$\frac{\Gamma \cup \{p_1 \sim_1 0,\ \mathsf{LC}(p_1) = 0,\ \mathsf{RP}(p_1) \sim_2 0\}}{\bot} \quad \text{if } \sim_1 \not\equiv \sim_2$$

Verify2 $$\frac{\Gamma \cup \{p_1 \sim_1 0,\ p_2 = 0,\ \mathsf{PR}(p_1, p_2) \sim_2 0, \mathsf{LC}(p_2) > 0\}}{\bot} \quad \text{if } \sim_1 \not\equiv \sim_2$$

$\vdots$

QE in Reals: Phase 3

Assert1 $$\frac{\Gamma}{\Gamma \cup \{\gamma_{-\infty} < x, x < \gamma_\infty\} \cup \Gamma_{-\infty} \cup \Gamma_\infty}$$

where $\Gamma_\infty = \{p[x := \gamma_\infty] \sim' 0 : p \sim 0 \in \Gamma\}$ and $\sim'$ is computed correctly using continuity.

IVT $$\frac{\Gamma \cup \{p \sim 0, p(\gamma_i) < 0, p(\gamma_{i+1}) > 0, \gamma_i < x < \gamma_{i+1}\}}{\Gamma' \cup \{\gamma_i < x < \gamma < \gamma_{i+1}, p(\gamma) = 0\} \cup \Gamma'_\gamma \mid \Gamma'_\gamma \mid \ \ldots}$$

IVT is applied to p only if it can not be applied to lower degree polynomials

Example

$$\frac{\frac{\frac{\{x^2 - 4 < 0,\ x^3 - x > 0\}}{\{x^2 - 4 < 0,\ x^3 - x > 0,\ 2x > 0\} \mid \ldots}}{\{x^2 - 4 < 0,\ x^3 - x > 0,\ 2x > 0,\ 3x^2 - 1 > 0\} \mid \ldots}}{\begin{array}{l}\gamma_{-\infty}^2 - 4 > 0,\ \gamma_{-\infty}^3 - \gamma_{-\infty} < 0,\ 2\gamma_{-\infty} < 0,\ 3\gamma_{-\infty}^2 - 1 > 0 \\ \gamma_\infty^2 - 4 > 0,\ \gamma_\infty^3 - \gamma_\infty > 0,\ 2\gamma_\infty > 0,\ 3\gamma_\infty^2 - 1 > 0, \gamma_{-\infty} < x < \gamma_\infty\end{array}}$$

Using IVT, in order, we introduce

- γ_0 s.t. $2\gamma_0 = 0$.
- γ_2 and γ_{-2} s.t. $\gamma_{-\infty} < \gamma_{-2} < \gamma_0 < \gamma_2 < \gamma_\infty$ and $\gamma_{\pm 2}^2 - 4 = 0$
- $\gamma_{1/\sqrt{3}}$ and $\gamma_{-1/\sqrt{3}}$
- γ_{-1} and γ_1 s.t. $\gamma_{-2} < \gamma_{-1} < \gamma_{-1/\sqrt{3}} < \gamma_0 < \gamma_{1/\sqrt{3}} < \gamma_1 < \ldots$ and $\gamma_{\pm 1}^3 - \gamma_{\pm 1} = 0$

Example Contd

x is a point/in an open interval, in different branches

Consider the IVT step that introduces γ_2:

$$\frac{\begin{array}{l}\gamma_0 < x < \gamma_\infty, \\ x^2 - 4 < 0,\ x^3 - x > 0,\ 2x > 0,\ 3x^2 - 1 > 0 \\ \gamma_0^2 - 4 < 0,\ \gamma_0^3 - \gamma_0 = 0,\ 2\gamma_0 = 0,\ 3\gamma_0^2 - 1 < 0 \\ \gamma_\infty^2 - 4 > 0,\ \gamma_\infty^3 - \gamma_\infty > 0,\ 2\gamma_\infty > 0,\ 3\gamma_\infty^2 - 1 > 0\end{array}}{\begin{array}{l}\ldots, \\ \gamma_2^2 - 4 = 0,\ \gamma_2^3 - \gamma_2 > 0,\ 2\gamma_2 > 0,\ 3\gamma_2^2 - 1 > 0 \\ \gamma_0 < x < \gamma_2\end{array}}$$

Note how we deduced the blue operators

Quantifier Elimination in Reals

Termination:

- Phase1 rules: Adding only lower degree polynomials
- Phase2 rules: Trivially terminate
- Phase3 rules: IVT can be applied only finitely many times

Soundness: All inference rules are sound w.r.t the theory of reals

Completeness: Can read off a model from an irreducible non-$\perp$ state?

Quantifier Elimination in Reals

For completeness, the inference rules have to be applied recursively

But non-recursive procedure already gives a quantifier elimination method:

- Let Γ^0 be all literals in Γ that do not contain x (and any of the γ_i's)
- Let final state be $\Gamma_1 \mid \Gamma_2 \mid \ldots \mid \Gamma_m$
- Then original formula $\exists x.\phi(\vec{y})(x)$ is equivalent to $\phi_{\Gamma_1^0} \vee \ldots \vee \phi_{\Gamma_m^0}$

Qn. Why did we add derivatives in the Guess phase?

Algebraically Closed Fields

There is no ordering relation $>$ here

Polynomials of degree d have exactly d roots counted with multiplicity

Literals: $p = 0$ or $p \neq 0$

Define p', $\mathsf{LC}(p)$, $\mathsf{RP}(p)$, and $\mathsf{PR}(p_1, p_2)$ as before

QE in Alg Closed Fields

Guess1	$\dfrac{\Gamma' \equiv \Gamma \cup \{p \sim 0\}}{\Gamma' \cup \{p' \neq 0\} \mid \Gamma' \cup \{p' = 0\}}$
Guess2	$\dfrac{\Gamma' \equiv \Gamma \cup \{p \sim 0\}}{\Gamma' \cup \{\mathsf{LC}(p) \neq 0\} \mid \Gamma' \cup \{\mathsf{LC}(p) = 0\}}$
Guess3	$\dfrac{\Gamma' \equiv \Gamma \cup \{p \sim 0\}}{\Gamma' \cup \{\mathsf{RP}(p) \neq 0\} \mid \Gamma' \cup \{\mathsf{RP}(p) = 0\}}$
Guess4	$\dfrac{\Gamma' \equiv \Gamma \cup \{p_1 \sim_1 0, p_2 \sim_2 0\}}{\Gamma' \cup \{\mathsf{PR}(p_1, p_2) \neq 0\} \mid \Gamma' \cup \{\mathsf{PR}(p_1, p_2) = 0\}}$

QE in Alg Closed Fields

Verify1 $\dfrac{\Gamma \cup \{p_1 \sim_1 0,\ \text{LC}(p_1) = 0,\ \text{RP}(p_1) \sim_2 0\}}{\perp}$ if $\sim_1 \not\equiv \sim_2$

Verify2 $\dfrac{\Gamma \cup \{p_1 \sim_1 0,\ p_2 = 0,\ \text{PR}(p_1, p_2) \sim_2 0, \text{LC}(p_2) \neq 0\}}{\perp}$ if $\sim_1 \not\equiv \sim_2$

Verify3 $\dfrac{\Gamma \cup \{p_1 = 0,\ p_1 \neq 0\}}{\perp}$

QE in Alg Closed Fields

Instead of the Intermediate Value Theorem, we use the Fundamental Theorem of Algebra

FTA $\dfrac{\Gamma \cup \{p \sim 0, x \neq \gamma_1, \ldots, x \neq \gamma_k\}}{\Gamma' \cup \{p \neq 0, x \neq \gamma_{k+1}\} \mid \Gamma'_{\gamma_{k+1}} \mid \ldots}$

if $deg(p) > \sum_{i=1}^{k} \mu_i$, where μ_i is the multiplicity of γ_i as a root of p.

FTA is applied to p only after it has applied to all lower degree polynomials

Check that side condition can be verified

The state $\Gamma'_{\gamma_{k+1}}$ can be computed

QE in Alg Closed Fields

Termination, Soundness, and Correctness follow reasoning similar to the case of real closed fields

As in the case of real closed fields, we get a quantifier elimination procedure for ACFs

Example

Consider $\exists x.(xy = 0\ \wedge\ xy \neq x)$

Phase1 guess gives us 4 cases: $y \sim_1 0,\ y - 1 \sim_2 0$.

Consider the case $y \neq 0, y - 1 \neq 0$:

$$\frac{yx = 0,\ (y-1)x \neq 0,\ y \neq 0,\ y - 1 \neq 0}{\perp}$$

because $\text{PR}((y-1)x, yx) = 0$ (Verify2 rule)

Only the case $y = 0, y - 1 \neq 1$ results in a consistent state.

Hence, $\exists x.(xy = 0\ \wedge\ xy \neq x)$ is equivalent to the QFF $y = 0$.

Summary

The theory of real closed fields admits QE

The theory of algebraically closed fields admits QE

QE procedures decide satisfiability of the full FO theory

QE procedures for reals is simple to describe, but computationally expensive

Lots of ongoing research in developing theoretically and practically better algorithms and implementations