Non-linear Real Arithmetic: Virtual Substitution

Prof. Dr. Erika Ábrahám and Florian Corzilius

January 22, 2012

Non-linear real arithmetic (NRA)

Real algebra

First-order theory of $(\mathbb{R}, +, \cdot, 0, 1, <)$

Syntax:

$$
\begin{array}{rrcccccccccc}
\text{Terms:} & t & := & 0 & | & 1 & | & x & | & t + t & | & t \cdot t \\
\text{Constraints:} & c & := & t < t & & & & & & & & \\
\text{Formulas:} & \varphi & := & c & | & \neg\varphi & | & \varphi \wedge \varphi & | & \exists x \varphi & &
\end{array}
$$

where x is a variable.

The term non-linear real arithmetic is mainly used in the SMT community and is the non-linear existential fragment of real algebra.

Real algebra: applications

- Systems of linear real constraints:

$$\exists x \; (\; Ax \leq b \;)$$

- Linear real optimization:

$$\exists x \; \big(\; Ax \leq b \;\wedge\; x \geq 0 \;\wedge\; \forall y \; (\; Ay \leq b \;\wedge\; y \geq 0 \rightarrow y \geq x \;) \; \big)$$

- Geometric problems: intersection, union, ... of geometric shapes e.g.

$$\exists x, y \; (\; x^2 + 4y^2 = 1 \;\wedge\; x - y = 1 \;)$$

Real algebra: on the border of decidability

Theorem (Alfred Tarski 1948)

FO *theory of* $(\mathbb{R}, +, \cdot, 0, 1, <)$ *is decidable.*

- The proof was first published in the book [Tarski1948].
- Time-complexity of a decision procedure in the number of variables would be "greater than all finite towers of powers of 2" [Feferman2006].

Already undecidable

FO theory of $(\mathbb{R}, +, \cdot, \sin, 0, 1, <)$

Real algebra: some historic facts

1637 Descartes' rule of signs

1835 Jaques Charles François Sturm's theorem

1948 Alfred Tarski's "A decision method for elementary algebra and geometry"

1975 Cylindrical algebraic decomposition (CAD) method by George E. Collins

1979–80 First implementation of the CAD method by Dennis S. Arnon

1988 Virtual substitution by Volker Weispfenning

1990 First implementation of virtual substitution (Klaus-Dieter Burhenne)

1993 Gröbner bases approach by P. Pedersen, M.-F. Roy, A. Szpirglas, later extended by V. Weispfenning

1994 Implementation of the Gröbner bases approach (Andreas Dolzmann)

Real algebra: implementations

Virtual substitution

- Computer logic system `Redlog` (package of `Reduce`)

Cylindrical algebraic decomposition

- `QEPCAD`, `Redlog`, ...

Gröbner bases

- `Maple`, `Mathematica`, `Singular`, `Maxima`, `CoCoA`, `Reduce`, ...

Other methods

- Interval arithmetic (`Ariadne` or `HySAT`)

The idea of quantifier elimination

Given: φ (FO sentence over $(\mathbb{R}, +, \cdot, 0, 1, <)$ containing n quantifiers)

1. Transform φ into prenex normal form:

$$\varphi \quad \equiv \quad Q_1 x_1 \ldots Q_n x_n \varphi', \quad \text{with} \quad \varphi' \quad \text{quantifier free}$$

2. Eliminate iteratively the quantifiers $Q_1 \ldots Q_n$ and thus the quantified variables.

The idea of quantifier elimination

What if we can only eliminate existential quantifier?

$$
\begin{array}{rl}
 & \exists x_1 \exists x_2\, \forall x_3\, \exists x_4\, \forall x_5\, \forall x_6\, \exists x_7\, \exists x_8 \quad \varphi' \\
\equiv & \exists x_1\, \exists x_2\, \neg(\exists x_3\, \neg(\exists x_4\, \neg(\exists x_5\, \neg(\neg(\exists x_6\, \neg(\exists x_7\, \exists x_8 \quad \varphi' \quad)))))) \\
\equiv & \exists x_1\, \exists x_2\, \neg(\exists x_3\, \neg(\exists x_4\, \neg(\exists x_5\, \exists x_6\, \neg(\exists x_7\, \exists x_8 \quad \varphi' \quad))))
\end{array}
$$

Existential quantifier elimination: Brute force

- Given: $\varphi = \exists x_1 \ldots \exists x_n \varphi'$, where φ' is an quantifier-free FO sentence over $(\mathbb{R}, +, \cdot, 0, 1, <)$
- Brute force: (elimination of one quantifier)

$$\exists x_1 \ldots \exists x_n\ \varphi' \quad \equiv \quad \exists x_1 \ldots \exists x_{n-1} \bigvee_{r \in \mathbb{R}} \varphi'[r/x].$$

- But: $\mathbb{R}$ is infinite.
- Idea: Find a finite set $T \subset \mathbb{R}$ with

$$\exists t \in T:\ \varphi[t/x] \quad \Leftrightarrow \quad \exists r \in \mathbb{R}:\ \varphi[r/x].$$

Virtual substitution

- Is an existential quantifier elimination procedure:

$$\exists x_1 \ldots \exists x_n \varphi' \quad \rightarrow \quad \exists x_1 \ldots \exists x_{n-1} \psi',$$

where $\varphi', \ \psi'$ quantifier free and $\exists x_1 \ldots \exists x_n \varphi' \ \equiv \ \exists x_1 \ldots \exists x_{n-1} \psi'$.

- Restricted in the degree of the variable to eliminate:

$p(x) \sim 0$ constraint of $\varphi \quad \Rightarrow \quad$ degree of x in $p(x)$ must be ≤ 2.

Virtual substitution

Virtual substitution constructs a finite set $T \subset \mathbb{R}$ of **test candidates** with

$$\exists x_1 \ldots \exists x_n \ \varphi' \quad \equiv \quad \exists x_1 \ldots \exists x_{n-1} \bigvee_{t \in T} \varphi'[t/x].$$

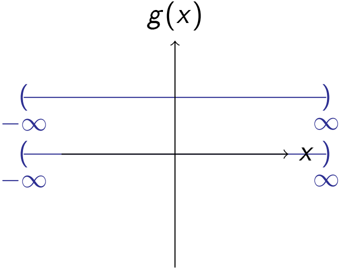
Construction of the set of test candidates T

1.) $g(x) = ax^2 + bx + c$ constant in x $\quad (a = 0 \ \wedge \ b = 0)$

Consider the constraint: $g(x) = 0$ or $g(x) \leq 0$ or $g(x) < 0$ $g(x) \geq 0$ or $g(x) > 0$ or $g(x) \neq 0$ $g(x) = 0$ or $g(x) \leq 0$ or $g(x) \geq 0$ $g(x) < 0$ or $g(x) > 0$ or $g(x) \neq 0$

$c \ngeq 0$:

($c < 0$ analog)

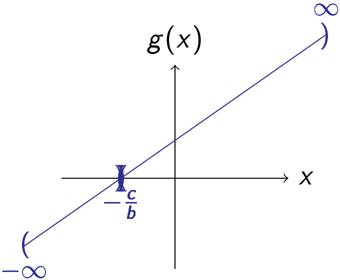


2.) $g(x) = ax^2 + bx + c$ linear in x $\quad (a = 0 \ \wedge \ b \neq 0)$

Consider the constraint: $g(x) = \ \leq \ < \ \geq \ > \ \neq 0$

$b > 0$:

($b < 0$ analog)



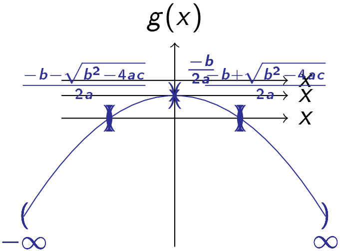
3.) $g(x) = ax^2 + bx + c$ quadratic in x $(a \neq 0)$

Consider the constraint: $g(x) = 0$ or $g(x) \geq 0$ or $g(x) > 0$ $g(x) \leq 0$ or $g(x) < 0$ or $g(x) \neq 0$ $g(x) \geq 0$ or $g(x) > 0$ $g(x) = 0$ $g(x) \leq 0$ $g(x) < 0$ or $g(x) \neq 0$ $g(x) = 0$ $g(x) \leq 0$ $g(x) \geq 0$ $g(x) < 0$ $g(x) > 0$ $g(x) \neq 0$

$a < 0$:

($a > 0$ analog)

$b^2 - 4ac \gtreqless 0$



Construction of the set of test candidates T

Given: A constraint $p \sim 0$. $\quad (p = ax^2 + bx + c,\ \sim \in \{=, <, >, \leq, \geq, \neq\})$.

The finite endpoints of its non-empty solution intervals are the zeros of p:

Linear in x :	$x_0 = -\frac{c}{b}$	, if	$a = 0 \ \wedge \ b \neq 0$
Quadratic in x, first solution:	$x_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}$	, if	$a \neq 0 \ \wedge \ b^2 - 4ac \geq 0$
Quadratic in x, second solution:	$x_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$	, if	$a \neq 0 \ \wedge \ b^2 - 4ac > 0$

All possible non-empty solution intervals for x in $p \sim 0$:

constraints		possible solution intervals ($0 \leq i,\ j \leq 2,\ i \neq j$)				
$p = 0$			$[x_i,\ x_i]$			$(-\infty,\ \infty)$
$p < 0$	$p > 0$	$(-\infty,\ x_i)$		$(x_i,\ x_j)$	$(x_i,\ \infty)$	$(-\infty,\ \infty)$
$p \neq 0$		$(-\infty,\ x_i)$			$(x_i,\ \infty)$	$(-\infty,\ \infty)$
$p \leq 0$	$p \geq 0$	$(-\infty,\ x_i]$	$[x_i,\ x_i]$	$[x_i,\ x_j]$	$[x_i,\ \infty)$	$(-\infty,\ \infty)$

Construction of the set of test candidates T

- Consider we have two constraints:

$$p^1 \sim^1 0 \quad \text{and} \quad p^2 \sim^2 0.$$

- When do they both hold?
- If the intersection of their solution intervals is not empty!
- Then the intersection consists of at least one non-empty interval.
- The interval's endpoints are endpoints of the intersected intervals.

Construction of the set of test candidates T

We search for a value fullfilling several constraints.

Idea: We search for the 'smallest value' fulfilling the constraints.

- We know ..
  - .. that the solution space of the constraints is a set of intervals.
  - .. the endpoints of these intervals.
- Hence, the 'smallest value' fullfilling the constraints is
  - either a left endpoint of an left closed interval
  - or a left endpoint of an left opened interval plus an infinitesimal.

Construction of the set of test candidates T

Idea: We search for the 'smallest value' fulfilling the constraints.

The constraints provide finitely many **test candidates**:

- $p = 0$
  1. Zeros of the polynomial p
- $p \leq 0, \ p \geq 0$
  1. Zeros of the polynomial p
  2. $-\infty$ (:= sufficient small value)
- $p < 0, \ p > 0, \ p \neq 0$
  1. Zeros of the polynomial p plus an infinitesimal ϵ
  2. $-\infty$
- Example: $xy + 1 < 0 \quad \rightarrow \quad \begin{cases} \frac{1}{y} + \epsilon & \text{if } y \neq 0 \\ -\infty \end{cases}$

Construction of the set of test candidates T

Example: $y \cdot x^2 + z \cdot x \geq 0$

- The finite endpoints are: $x_0 = x_1 = 0$ and $x_2 = -\frac{z}{y}$.
- The possible solution intervals are:

Case	Solution interval	Side condition
Constant	$(-\infty,\ \infty)$	$y = z = 0$
Linear	$(-\infty,\ 0]$ or $[0,\ \infty)$	$y = 0\ \wedge\ z \neq 0$
Quadratic	$(-\infty,\ 0]$ or $[0,\ \infty)$	$y \neq 0\ \wedge\ z^2 \geq 0$
Quadratic	$(-\infty,\ -\frac{z}{y}]$ or $[-\frac{z}{y},\ \infty)$	$y \neq 0\ \wedge\ z^2 > 0$

- The test candidates are:

Test candidate	Side condition
$-\infty$	none
0	$y = 0\ \wedge\ z \neq 0$
0	$y \neq 0$
$-\frac{z}{y}$	$y \neq 0$

Construction of the set of test candidates T

Example: $\exists y \exists x : \ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0$

Test candidates

$$\overset{\text{eliminate x}}{\equiv}$$

$$\begin{array}{llll}
\exists y : & & & (\ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0 \ )[-\infty / \mathbf{x}] \\
& \vee & & (\ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0 \ )[\mathbf{3} / \mathbf{x}] \\
& \vee \ (\ \mathbf{y \neq 0} & \wedge & (\ (y = 0 \ \vee \ y^2 + 1 < 0) \ \wedge \ x - 3 \leq 0 \ \wedge \ xy + 1 < 0 \ )[-\frac{\mathbf{1}}{\mathbf{y}} + \epsilon / \mathbf{x}] \ ) \ )
\end{array}$$

$$\overset{\text{eliminate y}}{\equiv}$$

Side condition

$\ldots$

How to substitute a variable by a test candidate in a constraint

- Standard substitution $\rightarrow$ expressions with ϵ, ∞, $\sqrt{}$ or division.
- Virtual Substitution defines rules, which give an equivalent FO sentence over $(\mathbb{R}, +, \cdot, 0, 1, <)$ to the expression resulting by the above standard substitution.
- The substitution rules distinguish between
  - the constraint's relation symbol
  - the test candidate's type ($-\infty$, $+\epsilon$, contains $\sqrt{}$)

Substitution of a variable by a test candidate in a constraint

Example: $(g(x) = 0)[\frac{q+r\sqrt{t}}{s}/x]$

Result: $(\hat{r} = 0 \wedge \hat{q} = 0) \vee (\hat{r} \neq 0 \wedge \hat{q}\hat{r} \leq 0 \wedge \hat{q}^2 - \hat{r}^2 t = 0)$,

where $\hat{q}$, $\hat{r}$, and $\hat{s}$ are polynomials.

Explanation:

1. Substitute x by $\frac{q+r\sqrt{t}}{s}$ in $g = 0$ in the common way.
2. Transform the result to $\frac{\hat{q}+\hat{r}\sqrt{t}}{\hat{s}} = 0$ where $\hat{q}$, $\hat{r}$, and $\hat{s}$ are polynomials (always possible, proof exercise)
3. Compare:
    1. $\hat{r} = 0 \;\wedge\; \frac{\hat{q}+\hat{r}\sqrt{t}}{\hat{s}} = 0 \;\Leftrightarrow\; \hat{r} = 0 \;\wedge\; \frac{\hat{q}}{\hat{s}} = 0 \;\Leftrightarrow\; \hat{r} = 0 \;\wedge\; \hat{q} = 0$
    2. $\hat{r} \neq 0 \;\wedge\; \frac{\hat{q}+\hat{r}\sqrt{t}}{\hat{s}} = 0 \quad\Leftrightarrow\quad \hat{r} \neq 0 \;\wedge\; \hat{q} + \hat{r}\sqrt{t} = 0$

       $\Leftrightarrow\; \hat{r} \neq 0 \;\wedge\; \hat{r}\hat{q} \leq 0 \;\wedge\; \|\hat{q}\| = \|\hat{r}\sqrt{t}\|$

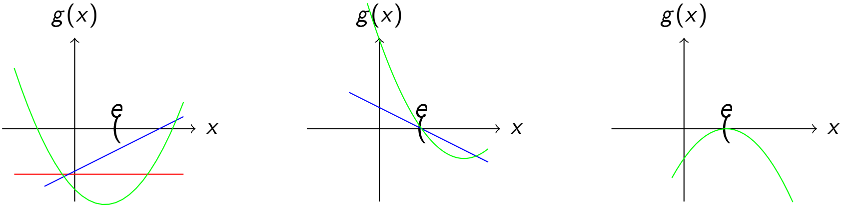
Substitution of a variable by a test candidate in a constraint

Example: $(g(x) < 0)[e + \epsilon/x]$

Result:

$$\underbrace{g[e/x] < 0}_{\text{Case 1}} \vee \underbrace{g[e/x] = 0 \wedge g'[e/x] < 0}_{\text{Case 2}} \vee \underbrace{g[e/x] = 0 \wedge g'[e/x] = 0 \wedge g''[e/x] < 0}_{\text{Case 3}}$$

Explanation:



Case 1 Case 2 Case 3

Virtual Substitution: Example

$$\exists x, y \; ((\; xy - 1 = 0 \quad \vee \quad y - x \geq 0 \;) \quad \wedge \quad y^2 - 1 < 0 \;)$$

Eliminate y:

1. Test candidate: $-\infty$

$$\begin{aligned} \exists x(\quad (\quad & (xy - 1 = 0)[-\infty/y] \\ \vee \quad & (y - x \geq 0)[-\infty/y] \quad) \\ \wedge \quad & (y^2 - 1 < 0)[-\infty/y] \quad) \end{aligned}$$

1. Test candidate: $-\infty$

$$\begin{aligned} \exists x(\quad (\quad & (y = 0 \;\wedge\; -1 = 0) \\ \vee \quad & (1 < 0 \;\vee\; (1 = 0 \;\wedge\; -x \geq 0)) \quad) \end{aligned}$$

Virtual Substitution: Example

$\exists x\ (((x > 0 \text{False} \wedge x - x^2 \geq 0) \vee (x < 0 \text{True} \wedge x - x^2 \leq 0 \text{True})) \wedge 1 - x^2 < 0 \text{True} \wedge x \neq 0 \text{True})$

Eliminate x:

1. Test candidate: $-\infty$

$$
\begin{aligned}
& (x > 0)[-\infty/x] \\
= \quad & (1 < 0 \ \vee \ (1 = 0 \ \wedge \ 0 > 0)) \\
= \quad & \text{False}
\end{aligned}
$$

1. Test candidate: $-\infty$

$$(x < 0)[-\infty/x]$$

Complexity

We consider in the following the elimination of one existential quantifier (existentially quantified variable):

$$\exists x_1 \ldots \exists x_n\ \varphi' \quad \equiv \quad \exists x_1 \ldots \exists x_{n-1} \bigvee_{t \in T} \varphi'[t/x].$$

- Degree of a remaining variable x_i, $1 \leq i < n$, in φ', i.e. $D(x_i,\ \varphi')$:

$$D(x_i,\ \bigvee_{t \in T} \varphi'[t/x]) \ \in \ \mathcal{O}(6D(x_i,\ \varphi') - 8)$$

- Number of atoms in φ', i.e. $at(\varphi')$:

$$at(\bigvee_{t \in T} \varphi'[t/x]) \ \in \ \mathcal{O}(8at(\varphi') + at(\varphi')(8 + 63at(\varphi')))$$

References

- S. Feferman. *Tarski's influence on computer science*. Logical Methods in Computer Science, 2006.
- A. Dolzmann, T. Sturm, V. Weispfenning. *Real Quantifier Elimination in Practice*. 1997.
- Alfred Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1948.
- Christopher W. Brown and James H. Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In Dongming Wang, editor, *ISSAC*, pages 54–60. ACM, 2007.
- M. O. Rabin. *A simple method for undecidability proofs and some applications*. Logic, Methodology and Philosophy of Science II, 1965.