Satisfiability Checking

Non-linear Real Arithmetic: Virtual Substitution

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 14/15

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 φ', ψ' 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.

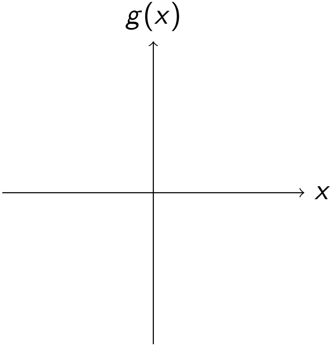
Virtual substitution

Virtual substitution constructs a finite set $T \subset \mathcal{R}$ 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

$g(x) := ax^2 + bx + c$



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 check only the 'smallest value' in the constraints' solution spaces, respectively.

- We know ..
  - .. that the solution space of all constraints together is a set of intervals.
  - .. the endpoints of these intervals.
- Hence, the 'smallest value' in a constraint's solution space 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 check only the 'smallest value' in the constraints' solution spaces, respectively.

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

- $p = 0, \; p \leq 0, \; p \geq 0$
  1. Zeros of the polynomial p
  2. $-\infty$ $\quad$ (:= sufficient small value)
- $p < 0, \; p > 0, \; p \neq 0$
  1. Zeros of the polynomial p plus an infinitesimal ϵ
  2. $-\infty$
- Example: $xy + 1 < 0$

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

eliminate x

$\equiv$

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

Side condition

eliminate y

$\equiv$

$\ldots$

Substitution of 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 $(\mathcal{R}, +, \cdot, 0, 1, <)$ 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. $\hat{r}\neq 0 \;\wedge\; \frac{\hat{q}+\hat{r}\sqrt{t}}{\hat{s}}=0 \quad\Leftrightarrow\quad \hat{r}\neq 0 \;\wedge\; \hat{q}+\hat{r}\sqrt{t}=0$

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

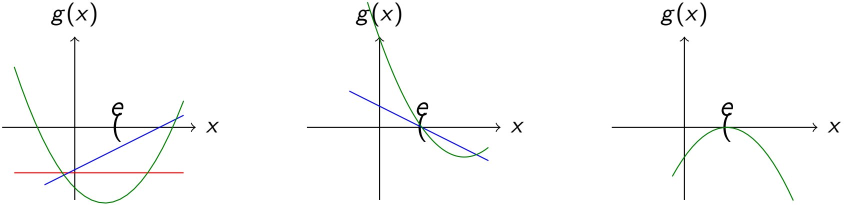
Substitution of a variable by a test candidate in a constraint

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: $-\infty$

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

1. Test candidate: $-\infty$

$$\begin{array}{llll} \exists x(& (& & (x = 0 \;\wedge\; -1 = 0) \\ & & \vee & (1 < 0 \;\vee\; (1 = 0 \;\wedge\; x \geq 0)) \qquad) \end{array}$$

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.