Solving Non-Linear Real Arithmetic Formulas with Virtual Substitution

Author: Aklima Zaman
Supervision: Erika Ábrahám

Theory of Hybrid Systems - Informatik 2 - RWTH-Aachen

Satisfiability Checking Seminar, Winter-16/17

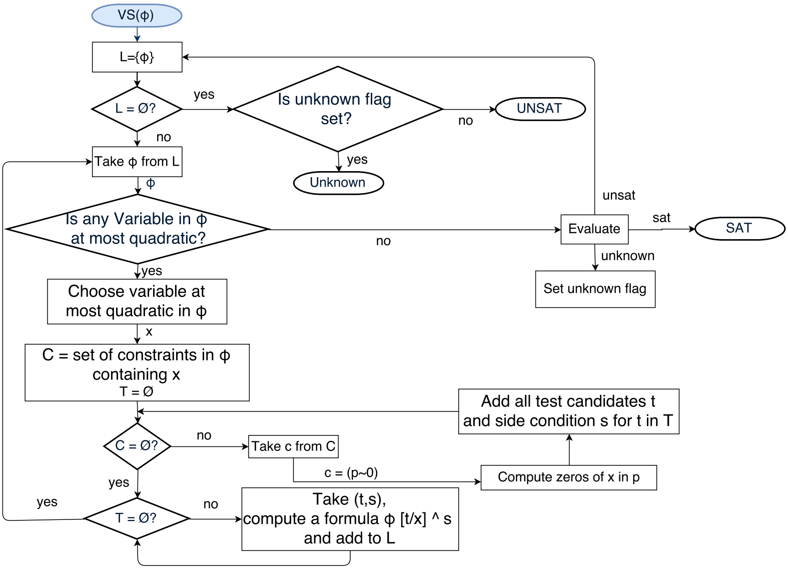
Outline

- Motivation
- Real Arithmetic Formula
- Virtual Substitution
  - Sign Invariant Regions
  - Compute Zeros
  - Compute Test Candidates
  - Virtual Substitution Rules

Motivation

- Other related methods
  - interval constraint propagation
  - cylindrical algebraic decomposition
- Virtual substitution
  - applicable only to sub-language
  - eliminates quantified variables up to degree 4

Flow Chart of Virtual Substitution



Real Arithmetic Formula

- Real arithmetic (RA) formula has the following syntax:

  terms: $t := \; 0 \;\mid\; 1 \;\mid\; x \;\mid\; t + t \;\mid\; t - t \;\mid\; t \cdot t$

  constraints: $c := \; t < t$

  formulas: $\varphi := \; c \;\mid\; \neg\varphi \;\mid\; \varphi \wedge \varphi \;\mid\; \exists x \cdot \varphi$

Real Arithmetic Formula

- Real arithmetic (RA) formula has the following syntax:

  terms: $t := \; 0 \;\mid\; 1 \;\mid\; x \;\mid\; t + t \;\mid\; t - t \;\mid\; t \cdot t$

  constraints: $c := \; t < t$

  formulas: $\varphi := \; c \;\mid\; \neg\varphi \;\mid\; \varphi \wedge \varphi \;\mid\; \exists x \cdot \varphi$

Real Arithmetic Formula

- Real arithmetic (RA) formula has the following syntax:

  terms: $t := \quad 0 \mid 1 \mid x \mid t + t \mid t - t \mid t \cdot t$

  constraints: $c := \quad t < t$

  formulas: $\varphi := \quad c \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \cdot \varphi$

Real Arithmetic Formula

- Real arithmetic (RA) formula has the following syntax:
  terms: $t := \ 0 \mid 1 \mid x \mid t + t \mid t - t \mid t \cdot t$
  constraints: $c := \ t < t$
  formulas: $\varphi := \ c \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \cdot \varphi$

Real Arithmetic Formula

- Real arithmetic (RA) formula has the following syntax:
  terms: $t := \; 0 \;|\; 1 \;|\; x \;|\; t+t \;|\; t-t \;|\; t \cdot t$
  constraints: $c := \; t < t$
  formulas: $\varphi := \; c \;|\; \neg\varphi \;|\; \varphi \wedge \varphi \;|\; \exists x \cdot \varphi$

- Polynomial $p(x) \in Z[x_1 \ldots, x_n][x]$ normal form:

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 x^0$$

Example:

$$\varphi = (\underbrace{(x^2 + 2x + 4z)}_{p_1} \leq 0 \vee \underbrace{(yx^2 + 6y^3 x + 4z)}_{p_2} = 0)$$

Real Arithmetic Formula

- Real arithmetic (RA) formula has the following syntax:
  terms: $t := \quad 0 \mid 1 \mid x \mid t+t \mid t-t \mid t \cdot t$
  constraints: $c := \quad t < t$
  formulas: $\varphi := \quad c \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \cdot \varphi$

- Polynomial $p(x) \in Z[x_1 \ldots, x_n][x]$ normal form:

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 x^0$$

Example:

$$\varphi = ((\underbrace{x^2 + 2x + 4z}_{p_1}) \leq 0 \vee (\underbrace{yx^2 + 6y^3 x + 4z}_{p_2}) = 0)$$

Real Arithmetic Formula

- Real arithmetic (RA) formula has the following syntax:
  terms: $t := \ 0 \mid 1 \mid x \mid t+t \mid t-t \mid t\cdot t$
  constraints: $c := \ t < t$
  formulas: $\varphi := \ c \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \cdot \varphi$

- Polynomial $p(x) \in Z[x_1 \ldots, x_n][x]$ normal form:

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 x^0$$

Example:

$$\varphi = ((\underbrace{x^2 + 2x + 4z)}_{p_1} \leq 0 \vee \underbrace{(yx^2 + 6y^3 x + 4z)}_{p_2} = 0)$$

Real Arithmetic Formula

- Real arithmetic (RA) formula has the following syntax:
  terms: $t := 0 \mid 1 \mid x \mid t + t \mid t - t \mid t \cdot t$
  constraints: $c := t < t$
  formulas: $\varphi := c \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists x \cdot \varphi$

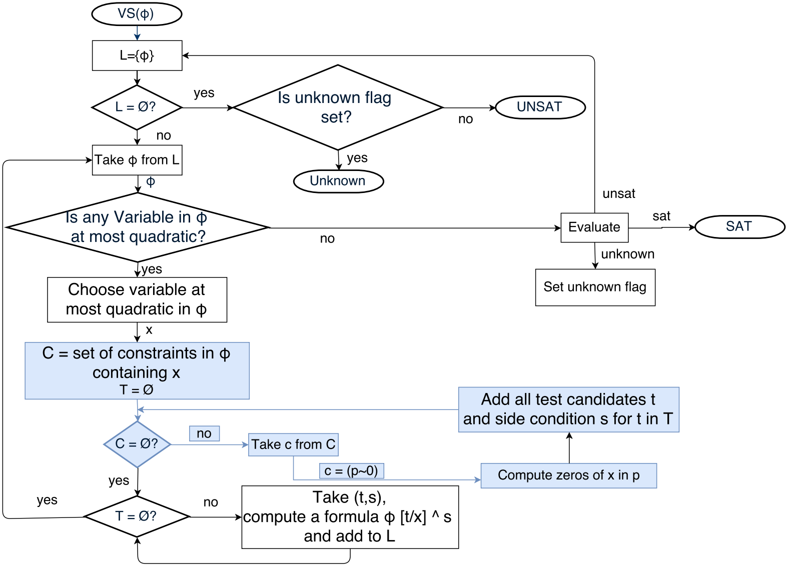
- Polynomial $p(x) \in Z[x_1 \ldots, x_n][x]$ normal form:

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 x^0$$

Example:

$$\varphi = (\underbrace{(x^2 + 2x + 4z)}_{p_1} \leq 0 \vee \underbrace{(yx^2 + 6y^3 x + 4z)}_{p_2} = 0)$$

Flow Chart of Virtual Substitution



Virtual Substitution

- Quantifier elimination procedure:

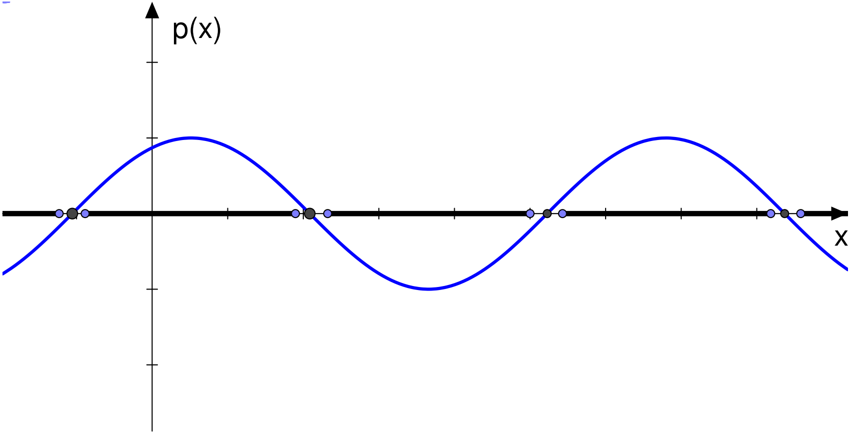
$$\exists x_1 \ldots \exists x_n \cdot \varphi \equiv \exists x_1 \ldots \exists x_{n-1} \cdot \psi$$

  where φ, ψ quantifier free.

- Quantifier elimination by virtual substitution:

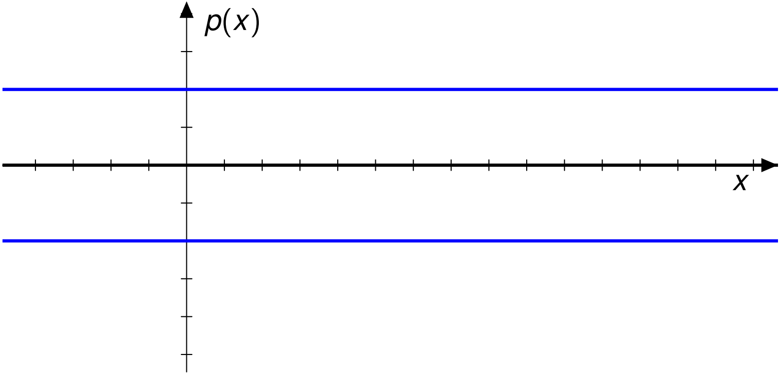
$$\exists x_1 \ldots \exists x_n \cdot \varphi \equiv \exists x_1 \ldots \exists x_{n-1} \cdot \bigvee_{t \in T} (\varphi[t//x] \wedge S_t)$$

Sign Invariant Regions



Compute Zeros

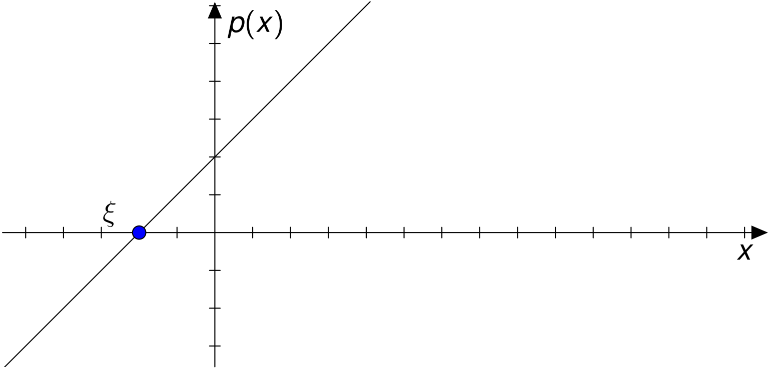
$p(x) = ax^2 + bx + c$ side condition: $a = 0 \wedge b = 0$



constant polynomial $\Rightarrow$ constant zero or non zeros

Compute Zeros

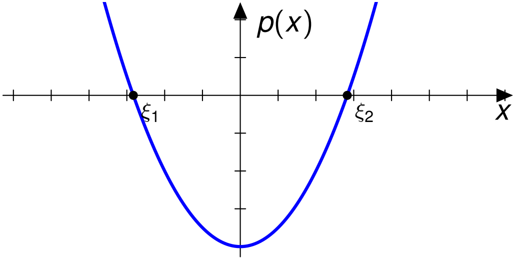
$p(x) = ax^2 + bx + c$ side condition: $a = 0 \wedge b \neq 0$



$\xi = -b/c$

Compute Zeros

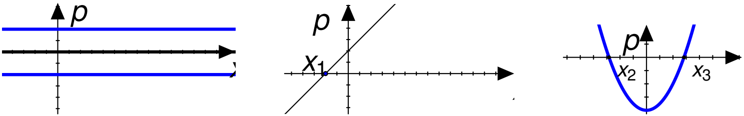
$p(x) = ax^2 + bx + c$ side condition: $a \neq 0 \wedge b^2 - 4ac \geq 0$



$\xi_1 = \frac{-b-\sqrt{b^2-4ac}}{2a}$, $\xi_2 = \frac{-b+\sqrt{b^2-4ac}}{2a}$

Compute Test Candidates

Possible solution intervals for x on $p \sim 0$:



Constraints	$-\infty$	x_1	$x_1+\epsilon$	x_2	$x_2+\epsilon$	x_3	$x_3+\epsilon$
$p=0$	-	✓	-	✓	-	✓	-
$p>0$, $p<0$, $p\neq 0$	✓	-	✓	-	✓	-	✓
$p\geqslant 0, p\leqslant 0$	✓	✓	-	✓	-	✓	-

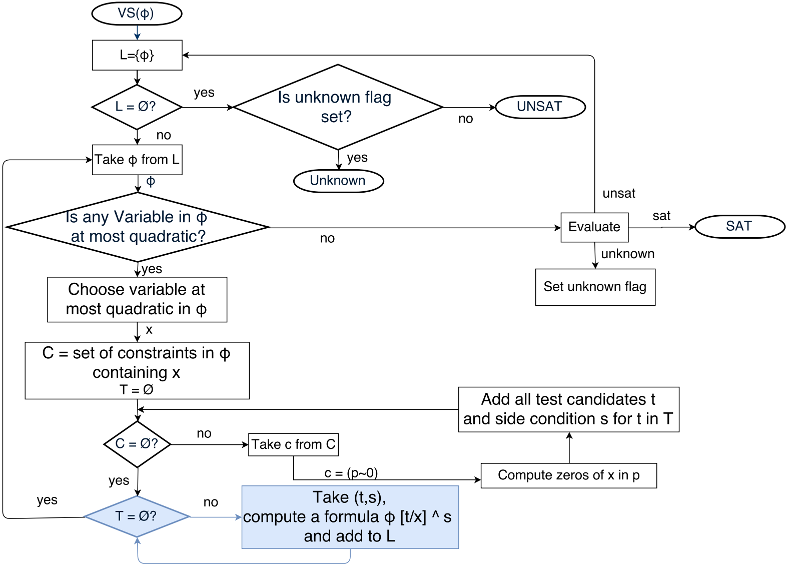
Example

$$\varphi := ((\underbrace{xy - 1}_{p_1} = 0) \wedge \underbrace{y^2 - 1}_{p_2} < 0)$$

Elimination of y:

	constraints	test candidates
1.	from all constraints	$-\infty$
2.	$p_1 = 0$	$1/x$ if $x \neq 0$
3.	$p_2 < 0$	$1 + \epsilon$
4.	$p_2 < 0$	$-1 + \epsilon$

Example



VS(ϕ)
L={ϕ}
L = Ø?
yes
no
Is unknown flag set?
no
UNSAT
yes
Unknown
Take ϕ from L
ϕ
Is any Variable in ϕ at most quadratic?
no
Evaluate
unsat
sat
SAT
unknown
Set unknown flag
yes
Choose variable at most quadratic in ϕ
x
C = set of constraints in ϕ containing x
T = Ø
Add all test candidates t and side condition s for t in T
C = Ø?
no
Take c from C
c = (p~0)
Compute zeros of x in p
yes
yes
T = Ø?
no
Take (t,s), compute a formula ϕ [t/x] ^ s and add to L

Example

$$\varphi := ((\underbrace{xy - 1}_{p_1} = 0) \wedge \underbrace{y^2 - 1}_{p_2} < 0)$$

Elimination of y:

	constraints	test candidates
1.	from all constraints	$-\infty$
2.	$p_1 = 0$	$1/x$ if $x \neq 0$
3.	$p_2 < 0$	$1 + \epsilon$
4.	$p_2 < 0$	$-1 + \epsilon$

$$\begin{array}{llll} \exists x \cdot \exists y \cdot \varphi \quad \leftrightarrow \quad \exists x \cdot & (\varphi[-\infty/y]) & & \vee \\ & (\varphi[\frac{1}{x}/y] & \wedge x \neq 0) & \vee \\ & (\varphi[1 + \epsilon/y]) & & \vee \\ & (\varphi[-1 + \epsilon/y]) & & \end{array}$$

Substitution of Square Root Expression

A square root expression has following form:

$$k = \frac{u + q\sqrt{r}}{s} \quad \text{with } u, q, r, s \text{ polynomials.}$$

Substitution of Square Root Expression

A square root expression has following form:

$$k = \frac{u + q\sqrt{r}}{s} \quad \text{with } u, q, r, s \text{ polynomials.}$$

Assume, $p(x) = 0$ and test candidate is $\frac{u+q\sqrt{r}}{s}$

Substitution of Square Root Expression

A square root expression has following form:

$$k = \frac{u + q\sqrt{r}}{s} \quad \text{with } u, q, r, s \text{ polynomials.}$$

Assume, $p(x) = 0$ and test candidate is $\frac{u+q\sqrt{r}}{s}$

1. $(p(x) = 0)[\frac{u+q\sqrt{r}}{s}//x]$ to be computed.

Substitution of Square Root Expression

A square root expression has following form:

$$k = \frac{u + q\sqrt{r}}{s} \quad \text{with } u, q, r, s \text{ polynomials.}$$

Assume, $p(x) = 0$ and test candidate is $\frac{u+q\sqrt{r}}{s}$

1. $(p(x) = 0)[\frac{u+q\sqrt{r}}{s}//x]$ to be computed.
2. Transform the result to $\frac{u'+q'\sqrt{r}}{s'} = 0$ where u', q', s' are polynomials.

Substitution of Square Root Expression

A square root expression has following form:

$$k = \frac{u + q\sqrt{r}}{s} \quad \text{with } u, q, r, s \text{ polynomials.}$$

Assume, $p(x) = 0$ and test candidate is $\frac{u+q\sqrt{r}}{s}$

1. $(p(x) = 0)[\frac{u+q\sqrt{r}}{s}//x]$ to be computed.
2. Transform the result to $\frac{u'+q'\sqrt{r}}{s'} = 0$ where u', q', s' are polynomials.
3. $\frac{u'+q'\sqrt{r}}{s'} = 0$

Substitution of Square Root Expression

A square root expression has following form:

$$k = \frac{u + q\sqrt{r}}{s} \quad \text{with } u, q, r, s \text{ polynomials.}$$

Assume, $p(x) = 0$ and test candidate is $\frac{u+q\sqrt{r}}{s}$

1. $(p(x) = 0)[\frac{u+q\sqrt{r}}{s}//x]$ to be computed.
2. Transform the result to $\frac{u'+q'\sqrt{r}}{s'} = 0$ where u', q', s' are polynomials.
3. $\frac{u'+q'\sqrt{r}}{s'} = 0$
   $\iff u' + q'\sqrt{r} = 0$

Substitution of Square Root Expression

A square root expression has following form:

$$k = \frac{u + q\sqrt{r}}{s} \quad \text{with } u, q, r, s \text{ polynomials.}$$

Assume, $p(x) = 0$ and test candidate is $\frac{u+q\sqrt{r}}{s}$

1. $(p(x) = 0)[\frac{u+q\sqrt{r}}{s}//x]$ to be computed.
2. Transform the result to $\frac{u'+q'\sqrt{r}}{s'} = 0$ where u', q', s' are polynomials.
3. $\frac{u'+q'\sqrt{r}}{s'} = 0$
   $\iff u' + q'\sqrt{r} = 0$
   $\iff u'q' \leq 0 \;\wedge\; \mid u' \mid = \mid q'\sqrt{r} \mid$

Substitution of Square Root Expression

A square root expression has following form:

$$k = \frac{u + q\sqrt{r}}{s} \quad \text{with } u, q, r, s \text{ polynomials.}$$

Assume, $p(x) = 0$ and test candidate is $\frac{u+q\sqrt{r}}{s}$

1. $(p(x) = 0)[\frac{u+q\sqrt{r}}{s}//x]$ to be computed.
2. Transform the result to $\frac{u'+q'\sqrt{r}}{s'} = 0$ where u', q', s' are polynomials.
3. $\frac{u'+q'\sqrt{r}}{s'} = 0$
$\iff u' + q'\sqrt{r} = 0$
$\iff u'q' \leq 0 \ \wedge \ \mid u' \mid = \mid q'\sqrt{r} \mid$
$\iff u'q' \leq 0 \ \wedge \ u'^2 - q'^2\sqrt{r} = 0$

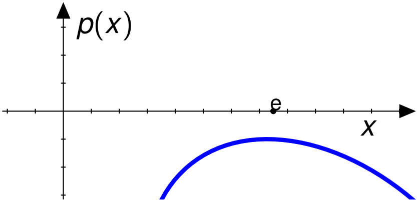
Substitution of Infinitesimal Expressions

Assume $p(x) < 0$ and test candidate is $e + \epsilon$

Substitution of Infinitesimal Expressions

Assume $p(x) < 0$ and test candidate is $e + \epsilon$

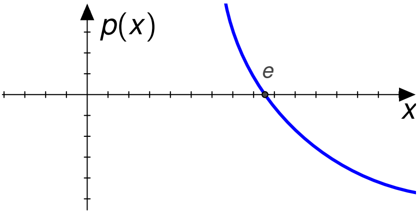
$$
\begin{aligned}
(p < 0)[e + \epsilon/x] \quad = & \ \underbrace{((p < 0)[e/x])}_{\text{Case 1}} & \vee \\
& \underbrace{((p = 0)[e/x] \wedge (p' < 0)[e/x])}_{\text{Case 2}} & \vee \\
& \underbrace{((p = 0)[e/x] \wedge (p' = 0)[e/x] \wedge (p'' < 0[e/x])}_{\text{Case 3}} & \vee
\end{aligned}
$$



Substitution of Infinitesimal Expressions

Assume $p(x) < 0$ and test candidate is $e + \epsilon$

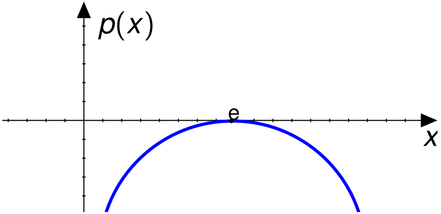
$$
\begin{aligned}
(p < 0)[e + \epsilon/x] \quad = \; & \underbrace{((p < 0)[e/x])}_{\text{Case 1}} & \vee \\
& \underbrace{((p = 0)[e/x] \wedge (p' < 0)[e/x])}_{\text{Case 2}} & \vee \\
& \underbrace{((p = 0)[e/x] \wedge (p' = 0)[e/x] \wedge (p'' < 0[e/x])}_{\text{Case 3}} & \vee
\end{aligned}
$$



Substitution of Infinitesimal Expressions

Assume $p(x) < 0$ and test candidate is $e + \epsilon$

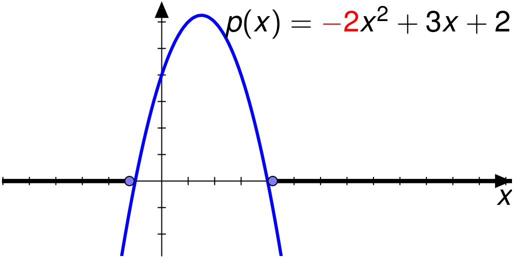
$$
\begin{aligned}
(p < 0)[e + \epsilon/x] \quad = & \underbrace{((p < 0)[e/x])}_{\text{Case 1}} & \vee \\
& \underbrace{((p = 0)[e/x] \wedge (p' < 0)[e/x])}_{\text{Case 2}} & \vee \\
& \underbrace{((p = 0)[e/x] \wedge (p' = 0)[e/x] \wedge (p'' < 0[e/x])}_{\text{Case 3}} & \vee
\end{aligned}
$$



Substitution of a Minus Infinity

Assume $(p(x) = ax^2 + bx + c) < 0$ and test candidate is $-\infty$

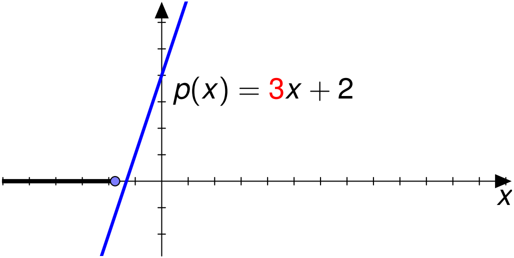
$$p(x) < 0[-\infty/x] \quad = \quad \underbrace{a < 0}_{\text{Case 1}} \quad \vee \quad \underbrace{a = 0 \wedge b > 0}_{\text{Case 2}} \quad \vee \quad \underbrace{a = 0 \wedge b = 0 \wedge c < 0}_{\text{Case 3}}$$



Substitution of a Minus Infinity

Assume $(p(x) = ax^2 + bx + c) < 0$ and test candidate is $-\infty$

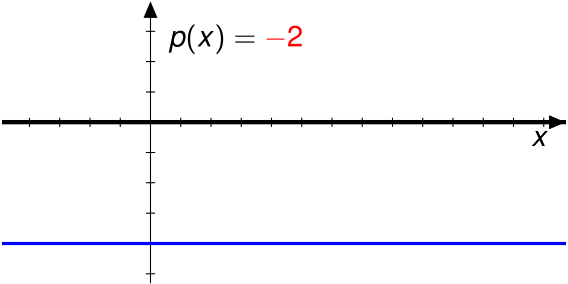
$$p(x) < 0[-\infty/x] \quad = \quad \underbrace{a < 0}_{\text{Case 1}} \vee \underbrace{a = 0 \wedge b > 0}_{\text{Case 2}} \vee \underbrace{a = 0 \wedge b = 0 \wedge c < 0}_{\text{Case 3}}$$



Substitution of a Minus Infinity

Assume $(p(x) = ax^2 + bx + c) < 0$ and test candidate is $-\infty$

$$p(x) < 0[-\infty/x] \quad = \quad \underbrace{a < 0}_{\text{Case 1}} \quad \vee \quad \underbrace{a = 0 \wedge b > 0}_{\text{Case 2}} \quad \vee \quad \underbrace{a = 0 \wedge b = 0 \wedge c < 0}_{\text{Case 3}}$$



Example

$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$

Elimination of y:

1.Test candidate: $-\infty$

$$\begin{array}{lll} \exists x \cdot & (& (xy - 1 = 0)[-\infty/y] \\ & \wedge & (y^2 - 1 < 0)[-\infty/y]\ ) \end{array}$$

Example

$$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$$

Elimination of y:

1.Test candidate: $-\infty$

$$\begin{array}{lll} \exists x\cdot & (& (xy - 1 = 0)[-\infty/y] \\ & \wedge & (y^2 - 1 < 0)[-\infty/y]\ ) \\ \Leftrightarrow \exists x\cdot & (& (x = 0 \wedge -1 = 0) \end{array}$$

Example

$$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$$

Elimination of y:

1.Test candidate: $-\infty$

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

Example

$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$

Elimination of y:

1. Test candidate: $-\infty$

$$
\begin{array}{rll}
\exists x \cdot & (& (xy - 1 = 0)[-\infty/y] \\
 & \wedge & (y^2 - 1 < 0)[-\infty/y]\ ) \\
\Leftrightarrow \exists x \cdot & (& (x = 0 \wedge -1 = 0) \\
 & \wedge & (1 < 0 \vee (1 = 0 \wedge 0 > 0) \vee (1 = 0 \wedge 0 = 0 \wedge -1 < 0))) \\
\Leftrightarrow \exists x \cdot & & (\textbf{false})
\end{array}
$$

Example

$$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$$

Elimination of y:

2.Test candidate: $\frac{1}{x}$ *if* $x \neq 0$

$$\begin{array}{lll} \exists x \cdot & (& (xy - 1 = 0)[\frac{1}{x}/y] \\ & \wedge & (y^2 - 1 < 0)[\frac{1}{x}/y] \\ & \wedge & x \neq 0 \ ) \end{array}$$

Example

$$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$$

Elimination of y:

2.Test candidate: $\frac{1}{x}$ *if* $x \neq 0$

$$\begin{array}{lll} \exists x\cdot & (& (xy - 1 = 0)[\frac{1}{x}/y] \\ & \wedge & (y^2 - 1 < 0)[\frac{1}{x}/y] \\ & \wedge & x \neq 0\ ) \\ \Leftrightarrow \exists x\cdot & (& (0 = 0) \end{array}$$

Example

$$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$$

Elimination of y:

2.Test candidate: $\frac{1}{x}$ *if* $x \neq 0$

$$\begin{array}{lll} \exists x \cdot & (& (xy - 1 = 0)[\frac{1}{x}/y] \\ & \wedge & (y^2 - 1 < 0)[\frac{1}{x}/y] \\ & \wedge & x \neq 0 \ ) \\ \Leftrightarrow \exists x \cdot & (& (0 = 0) \\ & \wedge & ((1 > 0) \wedge 1 - x^2 < 0 \vee (1 < 0 \wedge 1 - x^2 < 0)) \end{array}$$

Example

$$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$$

Elimination of y:

2.Test candidate: $\frac{1}{x}$ *if* $x \neq 0$

$$\begin{array}{lll} \exists x \cdot & (& (xy - 1 = 0)[\frac{1}{x}/y] \\ & \wedge & (y^2 - 1 < 0)[\frac{1}{x}/y] \\ & \wedge & x \neq 0 \;) \\ \Leftrightarrow \exists x \cdot & (& (0 = 0) \\ & \wedge & ((1 > 0) \wedge 1 - x^2 < 0 \vee (1 < 0 \wedge 1 - x^2 < 0)) \\ & \wedge & x \neq 0 \;) \end{array}$$

Example

$$\exists x \cdot \exists y \cdot ((xy - 1 = 0) \wedge y^2 - 1 < 0)$$

Elimination of y:

2.Test candidate: $\frac{1}{x}$ *if* $x \neq 0$

$$\begin{array}{lll}
\exists x \cdot & (& (xy - 1 = 0)[\frac{1}{x}/y] \\
& \wedge & (y^2 - 1 < 0)[\frac{1}{x}/y] \\
& \wedge & x \neq 0\ ) \\
\Leftrightarrow \exists x \cdot & (& (0 = 0) \\
& \wedge & ((1 > 0) \wedge 1 - x^2 < 0 \vee (1 < 0 \wedge 1 - x^2 < 0)) \\
& \wedge & x \neq 0\ ) \\
\Leftrightarrow \exists x \cdot & (& (1 - x^2 < 0) \\
& \wedge & x \neq 0\ )
\end{array}$$

Example

$\exists x \cdot (\; 1 - x^2 < 0 \; \wedge x \neq 0 \;)$

Elimination of x:

1. Test candidate: $-\infty$

$$
\begin{aligned}
& (1 - x_2 < 0)[-\infty/x] \\
= \quad & (-1 < 0 \vee (-1 = 0 \wedge 0 > 0) \vee (-1 = 0 \wedge 0 = 0 \wedge 1 < 0)) \\
= \quad & \textbf{true}
\end{aligned}
$$

Example

$\exists x \cdot (\ \textbf{true} \wedge x \neq 0 \ )$

Elimination of x:

1. Test candidate: $-\infty$

$$
\begin{aligned}
& (x \neq 0)[-\infty/x] \\
= \quad & (1 \neq 0 \vee 0 \neq 0) \\
= \quad & \textbf{true}
\end{aligned}
$$

Example

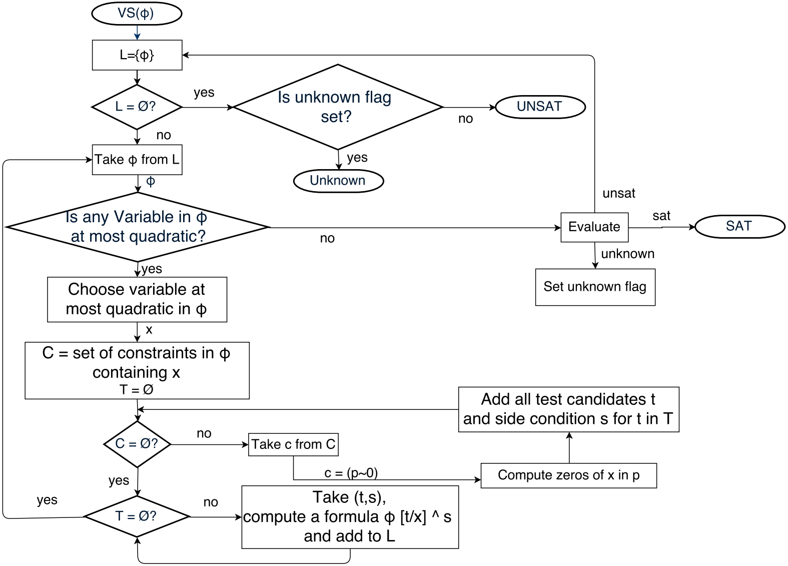
$\exists x \cdot ($ **true** $\wedge$ **true** $)$

Elimination of x:

1. Test candidate: $-\infty$

$$
\begin{aligned}
& (x \neq 0)[-\infty/x] \\
= \quad & (1 \neq 0 \vee 0 \neq 0) \\
= \quad & \textbf{true}
\end{aligned}
$$

Flow Chart of Virtual Substitution



Example: Search Tree

$$\varphi := ((\underbrace{xy - 1}_{p_1} = 0) \wedge \underbrace{y^2 - 1}_{p_2} < 0)$$