Satisfiability Checking

22 The virtual substitution method I

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 22/23

1 The idea

2 Test candidate generation for a single constraint

3 Test candidates for a set of constraints

4 Virtual substitution (next lecture)

Virtual substitution (VS)

In this lecture we handle [redacted]ly existentially quantified formulas, but note that the virtual substitution can handle also quantifier alternation.

Virtual substitution

For a real-algebraic formula $\exists x_1 . \ldots . \exists x_n . \varphi$ with $n > 0$ and φ quantifier-free, the virtual substitution method constructs a finite set $T \subset \mathbb{R}$ of test candidates with

$$\exists x_1 . \ldots . \exists x_n . \varphi \quad \equiv \quad \exists x_1 . \ldots . \exists x_{n-1} . \bigvee_{t \in T} \varphi[t /\!/ x_n] \ ,$$

where $[A /\!/ B]$ stays for virtually substituting A for B.

Intuitively, T contains representative points from sign-invariant regions.

To compute sign-invariant regions, we need...

...to identify the real roots of univariate polynomials, what can be done by...

...using solution equations, which exist up to polynomial degree 4.

In this lecture we handle only the quadratic case:

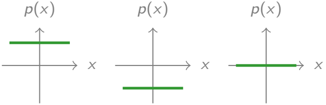
$$p \sim 0 \text{ constraint in } \varphi \quad \Rightarrow \quad \text{degree of } x_n \text{ in } p \text{ is at most 2.}$$

Sign-invariant regions

$p(x) := ax^2 + bx + c = 0$

constant:
$a = 0 \wedge b = 0$

degree = 0 0解

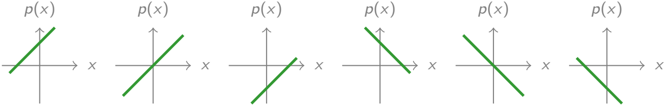


no zeros invariant zero

sign-invariant regions: $(-\infty, +\infty)$

linear:
$a = 0 \wedge b \neq 0$

degree = 1 1解

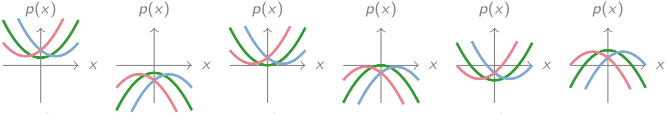


one zero ξ_0

sign-invariant regions: $(-\infty, \xi_0)$, $[\xi_0, \xi_0]$, $(\xi_0, +\infty)$

quadratic:
$a \neq 0$

degree = 2 2解



	$b^2 - 4ac < 0$	$b^2 - 4ac = 0$	$b^2 - 4ac > 0$
	no zeros	one zero ξ_1	two zeros ξ_1, ξ_2
sign-invariant regions:	$(-\infty, +\infty)$	$(-\infty, \xi_1)$, $[\xi_1, \xi_1]$, $(\xi_1, +\infty)$	$(-\infty, \xi_1)$, $[\xi_1, \xi_1]$, (ξ_1, ξ_2), $[\xi_2, \xi_2]$, $(\xi_2, +\infty)$

Real roots of univariate polynomials

For a polynomial $ax^2 + bx + c \in \mathbb{Z}[x]$, its real roots in x are

Case	*Real root*		*Side condition*
Constant in x : 多项式=0, 变量可取所有real number	*all real numbers*	, if	$a = 0 \wedge b = 0 \wedge c = 0$
Linear in x :	$\xi_0 = -\frac{c}{b}$	, if	$a = 0 \wedge b \neq 0$
Quadratic in x, 1^{st} solution:	$\xi_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}$	, if	$a \neq 0 \wedge b^2 - 4ac \geq 0$
Quadratic in x, 2^{nd} solution:	$\xi_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$	, if	$a \neq 0 \wedge b^2 - 4ac > 0$

Real roots of univariate polynomials: Example

For the polynomial $4x^2 + 3x + 2 \in \mathbb{Z}[x]$, its real roots in x are

Case	*Real root*	*Side condition*
Constant in x :	*all real numbers*	if $4 = 0 \wedge 3 = 0 \wedge 2 = 0$
Linear in x :	$\xi_0 = -\frac{2}{3}$	if $4 = 0 \wedge 3 \neq 0$
Quadratic in x, 1^{st} sol.:	$\xi_1 = \frac{-3+\sqrt{3^2-4\cdot4\cdot2}}{2\cdot4}$	if $4 \neq 0 \wedge 3^2 - 4\cdot4\cdot2 \geq 0$
Quadratic in x, 2^{nd} sol.:	$\xi_2 = \frac{-3-\sqrt{3^2-4\cdot4\cdot2}}{2\cdot4}$	if $4 \neq 0 \wedge 3^2 - 4\cdot4\cdot2 > 0$

For the polynomial -4 $x^2 + 3x + 2 \in \mathbb{Z}[x]$, its real roots in x are

Case	*Real root*	*Side condition*
Constant in x :	*all real numbers*	if $-4 = 0 \wedge 3 = 0 \wedge 2 = 0$
Linear in x :	$\xi_0 = -\frac{2}{3}$	if $-4 = 0 \wedge 3 \neq 0$
Quadratic in x, 1^{st} sol.:	$\xi_1 = \frac{-3+\sqrt{3^2-4\cdot(-4)\cdot2}}{2\cdot(-4)}$	if $-4 \neq 0 \wedge 3^2 - 4\cdot(-4)\cdot2 \geq 0$
Quadratic in x, 2^{nd} sol.:	$\xi_2 = \frac{-3-\sqrt{3^2-4\cdot(-4)\cdot2}}{2\cdot(-4)}$	if $-4 \neq 0 \wedge 3^2 - 4\cdot(-4)\cdot2 > 0$

Real roots of multivariate polynomials

- What about multivariate polynomials?
- They can be seen as univariate polynomials with polynomial coefficients.

$$5\,y^3z^2x^2 \quad +3\,zx \quad +5\,y^2\,-3 \quad \in \mathbb{Z}[y,z,x] \quad \rightsquigarrow$$

$$5y^3z^2\,x^2 \quad +3z\,x \quad +5y^2-3 \quad \in \mathbb{Z}[y,z]\,[x]$$

multivariate ⇒ 把其他变量当成系数

- So we can use the same solution equations but symbolically, parameterized in the values of the variables in the coefficients.

Real roots of univariate polynomials: Example

For the polynomial $3v^3x^2 + 2u^2vx + 5ab \in \mathbb{Z}[v, u, a, b][x]$, its real roots in x are

Case	*Real root*	*Side condition*
Constant in x :	*all real numbers*	if $3v^3 = 0 \wedge 2u^2v = 0 \wedge 5ab = 0$
Linear in x :	$\xi_0 = -\frac{5ab}{2u^2v}$	if $3v^3 = 0 \wedge 2u^2v \neq 0$
Quadratic in x, 1^{st} sol.:	$\xi_1 = \frac{-2u^2v+\sqrt{(2u^2v)^2-4\cdot 3v^3\cdot 5ab}}{2\cdot 3v^3}$	if $3v^3 \neq 0 \wedge (2u^2v)^2 - 4 \cdot 3v^3 \cdot 5ab \geq 0$
Quadratic in x, 2^{nd} sol.:	$\xi_2 = \frac{-2u^2v-\sqrt{(2u^2v)^2-4\cdot 3v^3\cdot 5ab}}{2\cdot 3v^3}$	if $3v^3 \neq 0 \wedge (2u^2v)^2 - 4 \cdot 3v^3 \cdot 5ab > 0$

Real roots of univariate polynomials: Example

For the polynomial $\boxed{2}\,x^2 + 2u^2vx + 5ab \in \mathbb{Z}[v,u,a,b][x]$, its real roots in x are

Case	*Real root*	*Side condition*
Constant in x :	*all real numbers*	if $\boxed{2 = 0} \wedge 2u^2v = 0 \wedge$ $5ab = 0$
Linear in x :	$\xi_0 = -\frac{5ab}{2u^2v}$	if $\boxed{2 = 0} \wedge 2u^2v \neq 0$
Quadratic in x, 1^{st} sol.:	$\xi_1 = \frac{-2u^2v+\sqrt{(2u^2v)^2-4\cdot 2\cdot 5ab}}{2\cdot 2}$	if $\boxed{2 \neq 0} \wedge$ $(2u^2v)^2 - 4\cdot 2\cdot 5ab \geq 0$
Quadratic in x, 2^{nd} sol.:	$\xi_2 = \frac{-2u^2v-\sqrt{(2u^2v)^2-4\cdot 2\cdot 5ab}}{2\cdot 2}$	if $\boxed{2 \neq 0} \wedge$ $(2u^2v)^2 - 4\cdot 2\cdot 5ab > 0$

Possible solution intervals for a single constraint

Given: $p \sim 0$, $\quad p = ax^2 + bx + c \in \mathbb{Z}[\vec{y}][x]$, $\sim \in \{=, <, >, \leq, \geq, \neq\}$.

Goal: Check satisfiability, return a solution or an explanation for unsatisfiability

I. If p has no real roots then it is sign-invariant over $x \in (-\infty, +\infty)$.

II. Otherwise, the finite endpoints of p's sign-invariant regions are p's real roots:

Case	*Real root*		*Side condition*
Linear in x :	$\xi_0 = -\frac{c}{b}$	, if	$a = 0 \wedge b \neq 0$
Quadratic in x, 1^{st} solution:	$\xi_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}$	, if	$a \neq 0 \wedge b^2 - 4ac \geq 0$
Quadratic in x, 2^{nd} solution:	$\xi_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$	, if	$a \neq 0 \wedge b^2 - 4ac > 0$

Constraint	Test sign-invariant regions $(0 \leq i, j \leq 2, i \neq j)$ $(-\infty, \xi_i)$	$[\xi_i, \xi_i]$	(ξ_i, ξ_j)	$(\xi_i, +\infty)$	$(-\infty, +\infty)$
$p = 0$		✓			✓
$p \leq 0 \quad p \geq 0$	✓	✓	✓	✓	✓
$p < 0 \quad p > 0 \quad p \neq 0$	✓		✓	✓	✓

Gray cases may contain solutions, but do not need to be tested: if a solution exists then we find one in the black cases.

Test candidates for a single constraint $p \sim 0$

Constraint	Test sign-invariant regions ($0 \leq i,\ j \leq 2,\ i \neq j$)				
	$(-\infty, \xi_i)$	$[\xi_i, \xi_i]$	(ξ_i, ξ_j)	$(\xi_i, +\infty)$	$(-\infty, +\infty)$
$p = 0 \quad p \leq 0 \quad p \geq 0$		✓			✓
$p < 0 \quad p > 0 \quad p \neq 0$	✓		✓	✓	✓

- We test the "smallest" value from each of these regions.
- Problem: The endpoints are symbolic expressions.
- Solution: We introduce a "sufficiently small" value $-\infty$ and an infinitesimal ϵ to refer to the "smallest" values.

We use the following test candidates:

$p = 0$, $p \leq 0$, $p \geq 0$:
包含等号
1. Each real root of p
2. $-\infty$

$p < 0$, $p > 0$, $p \neq 0$:
不包含等号
1. Each real root of p plus an infinitesimal ϵ
2. $-\infty$

Test candidates for a single constraint: Example

We use the following test candidates:

$p = 0,\ p \leq 0,\ p \geq 0$:
1. Each real root of p
2. $-\infty$

$p < 0,\ p > 0,\ p \neq 0$:
1. Each real root of p plus an infinitesimal ϵ
2. $-\infty$

$\varphi \quad := \quad y \cdot x^2 + z \cdot x \geq 0$, eliminate x

Case	Real root	Side conditions
Linear	0	$y = 0 \wedge z \neq 0$
Quadratic I	0	$y \neq 0 \wedge z^2 \geq 0$
Quadratic II	$-\frac{z}{y}$	$y \neq 0 \wedge z^2 > 0$

$\rightsquigarrow$

Test candidates	Side conditions
$-\infty$	*true*
0	$y = 0 \wedge z \neq 0$
0	$y \neq 0 \wedge z^2 \geq 0$
$-\frac{z}{y}$	$y \neq 0 \wedge z^2 > 0$

$\rightsquigarrow$

$$
\begin{aligned}
\exists x.\exists y.\exists z.\varphi \quad \leftrightarrow \quad \exists y.\exists z.\ & (\varphi[-\infty /\!/ x]) && \vee \\
& (\varphi[0 /\!/ x] \quad \wedge (y = 0 \wedge z \neq 0)) && \vee \\
& (\varphi[0 /\!/ x] \quad \wedge (y \neq 0 \wedge z^2 \geq 0)) && \vee \\
& (\varphi[-\tfrac{z}{y} /\!/ x] \quad \wedge (y \neq 0 \wedge z^2 > 0))
\end{aligned}
$$

22 The virtual substitution method I

1. The idea
2. Test candidate generation for a single constraint
3. Test candidates for a set of constraints
4. Virtual substitution (next lecture)

Test candidates for a set of constraints

Assume now several polynomial QFNRA constraints.

- Now the sign-invariant regions are intersections of the individual sign-invariant regions.
- The endpoints of these intersections are endpoints of the intersected intervals.
- Thus the "smallest" values in the intersections are the test candidates of the individual polynomials.

For each constraint $p \sim 0$ we add the following test candidates:

$p = 0$, $p \leq 0$, $p \geq 0$:
1. Each real root of p
2. $-\infty$

$p < 0$, $p > 0$, $p \neq 0$:
1. Each real root of p plus an infinitesimal ϵ
2. $-\infty$

Test candidates for a set of constraints: Example

$\varphi := ((\ xy - 1 = 0 \quad \vee \quad y - x \geq 0\ ) \quad \wedge \quad y^2 - 1 < 0\ )$, eliminate y

Test candidates:

1.	$-\infty$		*from all constraints*
2.	$\frac{1}{x}$	*if* $x \neq 0$	*from* $xy - 1 = 0$ 包含等号时直接使用real root
3.	x		*from* $y - x = 0$
4.	$1 + \epsilon$		*from* $y^2 - 1 < 0$ strict inequality时使用real root+ε
5.	$-1 + \epsilon$		*from* $y^2 - 1 < 0$

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

对φ中的y进行替换的选择

$-\infty \vee \frac{1}{x} \vee x \vee 1+\varepsilon \vee -1+\varepsilon$

不是具体的替换过程

Test candidates for a set of constraints: Example

$$\varphi \quad := \quad (\underbrace{y = 0}_{-\infty} \ \vee \ \underbrace{y^2 + 1 < 0}_{-\infty}) \ \wedge \ \underbrace{\overset{1 \neq 0}{} x - 3 \leq 0}_{-\infty} \ \wedge \ \underbrace{x\overset{y \neq 0}{y} + 1 < 0}_{-\infty}, \text{ eliminate } \boxed{x}$$

Test candidates:

$\xi_0 = 3$ if $\underbrace{1 \neq 0}_{\text{linear 系数} \neq 0}$ $\quad$ $\xi_0 = -\frac{1}{y} + \varepsilon$ if $y \neq 0$

1.	$-\infty$		*from all constraints*
2.	3	*if* $1 \neq 0$	*from* $x - 3 \leq 0$
3.	$-\frac{1}{y} + \epsilon$	*if* $y \neq 0$	*from* $xy + 1 < 0$

$$\exists x . \exists y . \varphi \quad \leftrightarrow \quad \exists y . \quad \begin{array}{ll} (\varphi[-\infty /\!/ x]) & \vee \\ (\varphi[3 /\!/ x]) & \vee \\ (\varphi[-\frac{1}{y} + \epsilon /\!/ x] \quad \wedge \ y \neq 0) & \end{array}$$

Learning target

- What is the basic idea of the virtual substitution?
- How to compute the test candidates?
- How to apply virtual substitution?
- Is the virtual substitution method complete?