Solving Non-linear Constraints in the CDCL style [1]

Franz Brauße[1] Konstantin Korovin[2] Margarita Korovina[3] Norbert Th. Müller[1]

[1] University of Trier, Germany

[2] The University of Manchester, UK

[3] IIS, Novosibirsk, Russia

[1] This project has received funding from the DFG grant WERA MU 1801/5-1, the DFG/RFBR grant CAVER BE 1267/14-1 and 14-01-91334 and from the EU's Horizon 2020 programme under the Marie Skłodowska-Curie grant agreement No 731143.

Main Problem

Checking satisfiability of (non-)linear constraints.

Linear:

$$5x - 10y - 2z \leq 1/2$$
$$6x - 1/3y + 2z > 0$$
$$-10x + 5y - 31z \geq 0$$

Main Problem

Checking satisfiability of (non-)linear constraints.

Polynomial:

$$
\begin{aligned}
&3x^2y - 10yzx - 2z \leq 5\\
&-5yz^2 - 1/3y + 2z > 1\\
&x + 5xy - 11xz \geq 7
\end{aligned}
$$

Main Problem

Checking satisfiability of (non-)linear constraints.

Non-linear with transcendental functions

$$
\begin{aligned}
&2\sin^2 x - 5\cos y^2 - 2z \leq 1/2 \quad \vee \quad e^{x^{-2}} + zy < y \\
&4x - 1/3y + 2zx > 0 \\
&x^2 - y^2 - z \geq 0
\end{aligned}
$$

Motivation:

- Verification: of hybrid; embedded systems; programs etc.
- Proof assistance for mathematics which rely on computations with non-linear constraints such as Hales proof of Kepler's conjecture.
- Curiosity: connected to many open problems in maths.

In most cases the problem of solving non-linear constraints is undecidable or relates to open problems in maths.

Overview of our approach

Main ingredients of our approach:

1. separated linear form $\mathcal{L} \wedge \mathcal{N}$
2. ksmt calculus – conflict-driven calculus for solving SPL
3. local linearisations for resolving non-linear conflicts
    - approximation of non-linear problem by incremental linearisations
    - related work [A. Cimatti, A. Griggio, A. Irfan, M. Roveri, and R. Sebastiani'18;. . .]

Overview of our approach

Main ingredients of our approach:

1. separated linear form $\mathcal{L} \wedge \mathcal{N}$
2. ksmt calculus – conflict-driven calculus for solving SPL
3. local linearisations for resolving non-linear conflicts
    - approximation of non-linear problem by incremental linearisations
    - related work [A. Cimatti, A. Griggio, A. Irfan, M. Roveri, and R. Sebastiani'18;. . .]

New class $\mathcal{F}_{\mathrm{DA}}$ – function with decidable rational approximations

- Checking "non-linear conflicts" is decidable for functions in $\mathcal{F}_{\mathrm{DA}}$
- inspired by computable analysis

Overview of our approach

Main ingredients of our approach:

1. separated linear form $\mathcal{L} \wedge \mathcal{N}$
2. ksmt calculus – conflict-driven calculus for solving SPL
3. local linearisations for resolving non-linear conflicts
    - approximation of non-linear problem by incremental linearisations
    - related work [A. Cimatti, A. Griggio, A. Irfan, M. Roveri, and R. Sebastiani'18;...]

New class $\mathcal{F}_{\mathrm{DA}}$ – function with decidable rational approximations

- Checking "non-linear conflicts" is decidable for functions in $\mathcal{F}_{\mathrm{DA}}$
- inspired by computable analysis
- $\mathcal{F}_{\mathrm{DA}}$ includes:
    - Multivariate polynomials x^2yz^5
    - Transcendental functions: $\exp, \ln, \log_b, \sin, \cos, \tan, \arctan \ldots$
    - Discontinuous functions: step-functions; piecewise linear/polynomial functions

From Logic to Arithmetic: The linear case

From Logic to Linear Arithmetic: Resolution

Motivation:

How to extend efficient SAT technology to other domains/theories ?

- Black-box: CDCL(T) – separate Boolean structure and theory
- SAT-encodings: bit-vectors etc.
- White-box: extend SAT calculi to other domains

From Logic to Linear Arithmetic: Resolution

propositional	linear arithmetic
clauses	linear inequalities
$\neg x_1 \vee x_2 \vee \cdots \vee x_n$	$-5x_1 + 3x_2 + \cdots + 0.5x_n + 17 \geq 0$
clause resolution	inequality resolution
$\dfrac{\neg x \vee C \quad x \vee D}{C \vee D}$	$\dfrac{-ax + p \geq 0 \quad bx + q \geq 0}{bp + aq \geq 0}$

Fourier-Motzkin

Example

$$\begin{array}{rcrcrcrcrcrcr} 2x_5 & - & 3x_4 & + & x_3 & - & 3x_2 & - & 2x_1 & + & 3 & \geq & 0 \\ 2x_5 & + & x_4 & - & 2x_3 & & & - & 2x_1 & + & 2 & \geq & 0 \\ -x_5 & & & & & + & 3x_2 & + & x_1 & + & 2 & \geq & 0 \\ -3x_5 & & & + & 2x_3 & & & - & 3x_1 & - & 2 & \geq & 0 \\ x_5 & - & 2x_4 & & & - & 2x_2 & + & 3x_1 & - & 2 & \geq & 0 \\ -2x_5 & + & 2x_4 & - & 3x_3 & - & x_2 & + & 2x_1 & + & 3 & > & 0 \\ 3x_5 & - & 2x_4 & + & 2x_3 & + & 3x_2 & + & 2x_1 & + & 1 & > & 0 \\ x_5 & & & & & & & + & 2x_1 & + & 2 & > & 0 \\ & & 2x_4 & - & x_3 & - & 3x_2 & - & x_1 & + & 3 & = & 0 \end{array}$$

Fourier-Motzkin: Generates over 280 million linear inequalities.

Combine model search and proof search

Conflict resolution – combination of model search and proof search

- Iteratively assign values (A) to variables $x_1 \mapsto 0 :: x_2 \mapsto 0.2 :: \ldots :: x_n \mapsto 5$
- If all constraints evaluate to true then – done
- Otherwise, we have a conflict
  1. resolve (R)
  2. backjump (B)
  3. refine assignment (A)

Combine model search and proof search

Conflict resolution – combination of model search and proof search

- Iteratively assign values (A) to variables $x_1 \mapsto 0 :: x_2 \mapsto 0.2 :: \ldots :: x_n \mapsto 5$
- If all constraints evaluate to true then – done
- Otherwise, we have a conflict
  1. resolve (R)
  2. backjump (B)
  3. refine assignment (A)

- Conflict Resolution [Korovin, Tsiskaridze, Voronkov, 2009]
- GDPLL [McMillan, Kuehlmann, Sagiv 2009]
- bound propagation [Korovin, Voronkov, 2011]
- MCSAT/NLSAT [Jovanović, de Moura, 2012/2013]
- CDSAT [Bonacina, Graham-Lengran, Shankar, 2017]
- ...

Example

$$
\begin{array}{rcrcrcrcrcl}
x_4 & - & 2x_3 & & & + & x_1 & + & 5 & \geq & 0 \quad (1)\\
x_4 & + & 2x_3 & + & x_2 & & & + & 3 & \geq & 0 \quad (2)\\
-\,x_4 & - & x_3 & - & 3x_2 & - & 3x_1 & + & 1 & \geq & 0 \quad (3)\\
-x_4 & + & 2x_3 & + & 2x_2 & + & x_1 & + & 6 & \geq & 0 \quad (4)\\
 & & x_3 & & & + & 3x_1 & - & 1 & \geq & 0 \quad (5)\\
 & & -x_3 & + & x_2 & - & 2x_1 & + & 5 & \geq & 0 \quad (6)
\end{array}
$$

variable				
bounds				
assignment				

Example

$$
\begin{array}{rcrcrcrcrcl}
x_4 & - & 2x_3 & & & + & x_1 & + & 5 & \geq & 0 \quad (1) \\
x_4 & + & 2x_3 & + & x_2 & & & + & 3 & \geq & 0 \quad (2) \\
-x_4 & - & x_3 & - & 3x_2 & - & 3x_1 & + & 1 & \geq & 0 \quad (3) \\
-x_4 & + & 2x_3 & + & 2x_2 & + & x_1 & + & 6 & \geq & 0 \quad (4) \\
 & & x_3 & & & + & 3x_1 & - & 1 & \geq & 0 \quad (5) \\
 & & -x_3 & + & x_2 & - & 2x_1 & + & 5 & \geq & 0 \quad (6)
\end{array}
$$

variable	x_1			
bounds				
assignment				

Example

$$
\begin{aligned}
x_4 - 2x_3 + x_1 + 5 &\geq 0 & (1)\\
x_4 + 2x_3 + x_2 + 3 &\geq 0 & (2)\\
-x_4 - x_3 - 3x_2 - 3x_1 + 1 &\geq 0 & (3)\\
-x_4 + 2x_3 + 2x_2 + x_1 + 6 &\geq 0 & (4)\\
x_3 + 3x_1 - 1 &\geq 0 & (5)\\
-x_3 + x_2 - 2x_1 + 5 &\geq 0 & (6)
\end{aligned}
$$

variable	x_1			
bounds	$(-\infty, \infty)$			
assignment				

Example

$$
\begin{aligned}
x_4 - 2x_3 + \cancel{x_1}\,0 + 5 &\geq 0 && (1)\\
x_4 + 2x_3 + x_2 + 3 &\geq 0 && (2)\\
-x_4 - x_3 - 3x_2 - \cancel{3x_1}\,0 + 1 &\geq 0 && (3)\\
-x_4 + 2x_3 + 2x_2 + \cancel{x_1}\,0 + 6 &\geq 0 && (4)\\
x_3 + \cancel{3x_1}\,0 - 1 &\geq 0 && (5)\\
-x_3 + x_2 - \cancel{2x_1}\,0 + 5 &\geq 0 && (6)
\end{aligned}
$$

variable	x_1			
bounds	$(-\infty, \infty)$			
assignment	$x_1 \mapsto 0$			

Example

$$
\begin{array}{rrrrrrrrrrrl}
x_4 & - & 2x_3 & & & + & \cancel{x_1}\ 0 & + & 5 & \geq & 0 & (1)\\
x_4 & + & 2x_3 & + & x_2 & & & + & 3 & \geq & 0 & (2)\\
-x_4 & - & x_3 & - & 3x_2 & - & \cancel{3x_1}\ 0 & + & 1 & \geq & 0 & (3)\\
-x_4 & + & 2x_3 & + & 2x_2 & + & \cancel{x_1}\ 0 & + & 6 & \geq & 0 & (4)\\
 & & x_3 & & & + & \cancel{3x_1}\ 0 & - & 1 & \geq & 0 & (5)\\
 & & -x_3 & + & x_2 & - & \cancel{2x_1}\ 0 & + & 5 & \geq & 0 & (6)
\end{array}
$$

variable	x_1	x_2		
bounds	$(-\infty, \infty)$			
assignment	$x_1 \mapsto 0$			

Example

$$
\begin{array}{rcrcrcrcrcl}
x_4 & - & 2x_3 & & & + & \cancel{x_1}\ 0 & + & 5 & \geq & 0 \quad (1)\\
x_4 & + & 2x_3 & + & x_2 & & & + & 3 & \geq & 0 \quad (2)\\
-\,x_4 & - & x_3 & - & 3x_2 & - & \cancel{3x_1}\ 0 & + & 1 & \geq & 0 \quad (3)\\
-x_4 & + & 2x_3 & + & 2x_2 & + & \cancel{x_1}\ 0 & + & 6 & \geq & 0 \quad (4)\\
 & & x_3 & & & + & \cancel{3x_1}\ 0 & - & 1 & \geq & 0 \quad (5)\\
 & & -x_3 & + & x_2 & - & \cancel{2x_1}\ 0 & + & 5 & \geq & 0 \quad (6)
\end{array}
$$

variable	x_1	x_2	
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	
assignment	$x_1 \mapsto 0$		

Example

$$
\begin{aligned}
x_4 - 2x_3 + \cancel{x_1}\,0 + 5 &\geq 0 && (1)\\
x_4 + 2x_3 + \cancel{x_2}\,0 + 3 &\geq 0 && (2)\\
-x_4 - x_3 - \cancel{3x_2}\,0 - \cancel{3x_1}\,0 + 1 &\geq 0 && (3)\\
-x_4 + 2x_3 + \cancel{2x_2}\,0 + \cancel{x_1}\,0 + 6 &\geq 0 && (4)\\
x_3 + \cancel{3x_1}\,0 - 1 &\geq 0 && (5)\\
-x_3 + \cancel{x_2}\,0 - \cancel{2x_1}\,0 + 5 &\geq 0 && (6)
\end{aligned}
$$

variable	x_1	x_2		
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$		
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$		

Example

$$
\begin{array}{rrrrrrrrrrrl}
x_4 & - & 2x_3 & & & + & \cancel{x_1}\ 0 & + & 5 & \geq & 0 & (1)\\
x_4 & + & 2x_3 & + & \cancel{x_2}\ 0 & & & + & 3 & \geq & 0 & (2)\\
-x_4 & - & x_3 & - & \cancel{3x_2}\ 0 & - & \cancel{3x_1}\ 0 & + & 1 & \geq & 0 & (3)\\
-x_4 & + & 2x_3 & + & \cancel{2x_2}\ 0 & + & \cancel{x_1}\ 0 & + & 6 & \geq & 0 & (4)\\
 & & x_3 & & & + & \cancel{3x_1}\ 0 & - & 1 & \geq & 0 & (5)\\
 & & -x_3 & + & \cancel{x_2}\ 0 & - & \cancel{2x_1}\ 0 & + & 5 & \geq & 0 & (6)
\end{array}
$$

variable	x_1	x_2	x_3
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	

Example

$$
\begin{array}{rrrrrrrrrrrl}
x_4 & - & 2x_3 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 & (1) \\
x_4 & + & 2x_3 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 & (2) \\
-x_4 & - & x_3 & - & \cancel{3x_2}\,0 & - & \cancel{3x_1}\,0 & + & 1 & \geq & 0 & (3) \\
-x_4 & + & 2x_3 & + & \cancel{2x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 & (4) \\
 & & x_3 & & & + & \cancel{3x_1}\,0 & - & 1 & \geq & 0 & (5) \\
 & & -x_3 & + & \cancel{x_2}\,0 & - & \cancel{2x_1}\,0 & + & 5 & \geq & 0 & (6)
\end{array}
$$

variable	x_1	x_2	x_3
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 5]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	

Example

$$
\begin{array}{rrrrrrrrrrrr}
x_4 & - & 2\cancel{x_3}\,4 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 & (1)\\
x_4 & + & 2\cancel{x_3}\,4 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 & (2)\\
-\,x_4 & - & \cancel{x_3}\,4 & - & \cancel{3x_2}\,0 & - & \cancel{3x_1}\,0 & + & 1 & \geq & 0 & (3)\\
-x_4 & + & 2\cancel{x_3}\,4 & + & \cancel{2x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 & (4)\\
 & & \cancel{x_3}\,4 & & & + & \cancel{3x_1}\,0 & - & 1 & \geq & 0 & (5)\\
 & & -\cancel{x_3}\,4 & + & \cancel{x_2}\,0 & - & \cancel{2x_1}\,0 & + & 5 & \geq & 0 & (6)
\end{array}
$$

variable	x_1	x_2	x_3
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 5]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 4$

Example

$$
\begin{array}{rrrrrrrrrrl}
x_4 & - & 2\cancel{x_3}\,4 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 \quad (1)\\
x_4 & + & 2\cancel{x_3}\,4 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 \quad (2)\\
-\,x_4 & - & \cancel{x_3}\,4 & - & 3\cancel{x_2}\,0 & - & 3\cancel{x_1}\,0 & + & 1 & \geq & 0 \quad (3)\\
-x_4 & + & 2\cancel{x_3}\,4 & + & 2\cancel{x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 \quad (4)\\
 & & \cancel{x_3}\,4 & & & + & 3\cancel{x_1}\,0 & - & 1 & \geq & 0 \quad (5)\\
 & & -\cancel{x_3}\,4 & + & \cancel{x_2}\,0 & - & 2\cancel{x_1}\,0 & + & 5 & \geq & 0 \quad (6)
\end{array}
$$

variable	x_1	x_2	x_3	x_4
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 5]$	
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 4$	

Example

$$
\begin{array}{rcrcrcrcrcr}
x_4 & - & 2\cancel{x_3}\;4 & & & + & \cancel{x_1}\;0 & + & 5 & \geq & 0 \quad (1)\\
x_4 & + & 2\cancel{x_3}\;4 & + & \cancel{x_2}\;0 & & & + & 3 & \geq & 0 \quad (2)\\
-\,x_4 & - & \cancel{x_3}\;4 & - & 3\cancel{x_2}\;0 & - & 3\cancel{x_1}\;0 & + & 1 & \geq & 0 \quad (3)\\
-x_4 & + & 2\cancel{x_3}\;4 & + & 2\cancel{x_2}\;0 & + & \cancel{x_1}\;0 & + & 6 & \geq & 0 \quad (4)\\
 & & \cancel{x_3}\;4 & & & + & 3\cancel{x_1}\;0 & - & 1 & \geq & 0 \quad (5)\\
 & & -\cancel{x_3}\;4 & + & \cancel{x_2}\;0 & - & 2\cancel{x_1}\;0 & + & 5 & \geq & 0 \quad (6)
\end{array}
$$

variable	x_1	x_2	x_3	x_4
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 5]$	$[3; -3]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 4$	

Example

$$
\begin{array}{rl}
x_4 - 2\cancel{x_3}\,4 + \cancel{x_1}\,0 + 5 \geq 0 & (1)\\
x_4 + 2\cancel{x_3}\,4 + \cancel{x_2}\,0 + 3 \geq 0 & (2)\\
-x_4 - \cancel{x_3}\,4 - 3\cancel{x_2}\,0 - 3\cancel{x_1}\,0 + 1 \geq 0 & (3)\\
-x_4 + 2\cancel{x_3}\,4 + 2\cancel{x_2}\,0 + \cancel{x_1}\,0 + 6 \geq 0 & (4)\\
\cancel{x_3}\,4 + 3\cancel{x_1}\,0 - 1 \geq 0 & (5)\\
-\cancel{x_3}\,4 + \cancel{x_2}\,0 - 2\cancel{x_1}\,0 + 5 \geq 0 & (6)
\end{array}
$$

variable	x_1	x_2	x_3	x_4
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 5]$	$[3; -3]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 4$	

Conflict: $\mathrm{res}_{x_4}((1), (3)) \rightsquigarrow (7);$

Example

$$
\begin{array}{rcrcrcrcrcl}
x_4 & - & 2x_3 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 \quad (1)\\
x_4 & + & 2x_3 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 \quad (2)\\
-\,x_4 & - & x_3 & - & \cancel{3x_2}\,0 & - & \cancel{3x_1}\,0 & + & 1 & \geq & 0 \quad (3)\\
-x_4 & + & 2x_3 & + & \cancel{2x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 \quad (4)\\
 & & x_3 & & & + & \cancel{3x_1}\,0 & - & 1 & \geq & 0 \quad (5)\\
 & & -x_3 & + & \cancel{x_2}\,0 & - & \cancel{2x_1}\,0 & + & 5 & \geq & 0 \quad (6)\\
 & & -\,x_3 & - & x_2 & - & \frac{2}{3}x_1 & + & 2 & \geq & 0 \quad (7)
\end{array}
$$

variable	x_1	x_2	x_3	x_4
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 5]$	$[3; -3]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 4$	

Conflict: $\mathrm{res}_{x_4}((1),(3)) \rightsquigarrow (7)$; Backjump: x_2

Example

$$
\begin{array}{rrrrrrrrrrrrrl}
x_4 & - & 2x_3 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 & & (1)\\
x_4 & + & 2x_3 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 & & (2)\\
-\,x_4 & - & x_3 & - & \cancel{3x_2}\,0 & - & \cancel{3x_1}\,0 & + & 1 & \geq & 0 & & (3)\\
-x_4 & + & 2x_3 & + & \cancel{2x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 & & (4)\\
 & & x_3 & & & + & \cancel{3x_1}\,0 & - & 1 & \geq & 0 & & (5)\\
 & & -x_3 & + & \cancel{x_2}\,0 & - & \cancel{2x_1}\,0 & + & 5 & \geq & 0 & & (6)\\
 & & -\,x_3 & - & \cancel{x_2}\,0 & - & \tfrac{2}{3}\cancel{x_1}\,0 & + & 2 & \geq & 0 & & (7)
\end{array}
$$

variable	x_1	x_2	x_3
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	

Example

$$
\begin{array}{rrrrrrrrrrrl}
x_4 & - & 2x_3 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 & (1)\\
x_4 & + & 2x_3 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 & (2)\\
-x_4 & - & x_3 & - & \cancel{3x_2}\,0 & - & \cancel{3x_1}\,0 & + & 1 & \geq & 0 & (3)\\
-x_4 & + & 2x_3 & + & \cancel{2x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 & (4)\\
 & & x_3 & & & + & \cancel{3x_1}\,0 & - & 1 & \geq & 0 & (5)\\
 & & -x_3 & + & \cancel{x_2}\,0 & - & \cancel{2x_1}\,0 & + & 5 & \geq & 0 & (6)\\
 & & -x_3 & - & \cancel{x_2}\,0 & - & \cancel{\tfrac{2}{3}x_1}\,0 & + & 2 & \geq & 0 & (7)
\end{array}
$$

variable	x_1	x_2	x_3
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 2]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	

Example

$$
\begin{array}{rrrrrrrrrrl}
x_4 & - & 2\cancel{x_3}\,1 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 \qquad (1)\\
x_4 & + & 2\cancel{x_3}\,1 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 \qquad (2)\\
-\,x_4 & - & \cancel{x_3}\,1 & - & 3\cancel{x_2}\,0 & - & 3\cancel{x_1}\,0 & + & 1 & \geq & 0 \qquad (3)\\
-x_4 & + & 2\cancel{x_3}\,1 & + & 2\cancel{x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 \qquad (4)\\
 & & \cancel{x_3}\,1 & & & + & 3\cancel{x_1}\,0 & - & 1 & \geq & 0 \qquad (5)\\
 & & -\cancel{x_3}\,1 & + & \cancel{x_2}\,0 & - & 2\cancel{x_1}\,0 & + & 5 & \geq & 0 \qquad (6)\\
 & & -\,\cancel{x_3}\,1 & - & \cancel{x_2}\,0 & - & \frac{2}{3}\cancel{x_1}\,0 & + & 2 & \geq & 0 \qquad (7)
\end{array}
$$

variable	x_1	x_2	x_3
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 2]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 1$

Example

$$x_4 - 2\cancel{x_3}\,1 + \cancel{x_1}\,0 + 5 \geq 0 \tag{1}$$
$$x_4 + 2\cancel{x_3}\,1 + \cancel{x_2}\,0 + 3 \geq 0 \tag{2}$$
$$-x_4 - \cancel{x_3}\,1 - 3\cancel{x_2}\,0 - 3\cancel{x_1}\,0 + 1 \geq 0 \tag{3}$$
$$-x_4 + 2\cancel{x_3}\,1 + 2\cancel{x_2}\,0 + \cancel{x_1}\,0 + 6 \geq 0 \tag{4}$$
$$\cancel{x_3}\,1 + 3\cancel{x_1}\,0 - 1 \geq 0 \tag{5}$$
$$-\cancel{x_3}\,1 + \cancel{x_2}\,0 - 2\cancel{x_1}\,0 + 5 \geq 0 \tag{6}$$
$$-\cancel{x_3}\,1 - \cancel{x_2}\,0 - \tfrac{2}{3}\cancel{x_1}\,0 + 2 \geq 0 \tag{7}$$

variable	x_1	x_2	x_3	x_4
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 2]$	
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 1$	

Example

$$
\begin{array}{rcrcrcrcrcl}
x_4 & - & 2\cancel{x_3}\,1 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 \quad \color{red}{(1)} \\
x_4 & + & 2\cancel{x_3}\,1 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 \quad (2) \\
-\,x_4 & - & \cancel{x_3}\,1 & - & 3\cancel{x_2}\,0 & - & 3\cancel{x_1}\,0 & + & 1 & \geq & 0 \quad \color{blue}{(3)} \\
-x_4 & + & 2\cancel{x_3}\,1 & + & 2\cancel{x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 \quad (4) \\
 & & \cancel{x_3}\,1 & & & + & 3\cancel{x_1}\,0 & - & 1 & \geq & 0 \quad (5) \\
 & & -\cancel{x_3}\,1 & + & \cancel{x_2}\,0 & - & 2\cancel{x_1}\,0 & + & 5 & \geq & 0 \quad (6) \\
 & & -\,\cancel{x_3}\,1 & - & \cancel{x_2}\,0 & - & \frac{2}{3}\cancel{x_1}\,0 & + & 2 & \geq & 0 \quad (7)
\end{array}
$$

variable	x_1	x_2	x_3	x_4
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 2]$	$[\color{red}{-3}; \color{blue}{0}]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 1$	

Example

$$
\begin{array}{rrrrrrrrrrrrr}
\cancel{x_4}\,{-1} & - & 2\cancel{x_3}\,1 & & & + & \cancel{x_1}\,0 & + & 5 & \geq & 0 & & (1)\\
\cancel{x_4}\,{-1} & + & 2\cancel{x_3}\,1 & + & \cancel{x_2}\,0 & & & + & 3 & \geq & 0 & & (2)\\
-\cancel{x_4}\,{-1} & - & \cancel{x_3}\,1 & - & \cancel{3x_2}\,0 & - & \cancel{3x_1}\,0 & + & 1 & \geq & 0 & & (3)\\
-\cancel{x_4}\,{-1} & + & 2\cancel{x_3}\,1 & + & \cancel{2x_2}\,0 & + & \cancel{x_1}\,0 & + & 6 & \geq & 0 & & (4)\\
 & & \cancel{x_3}\,1 & & & + & \cancel{3x_1}\,0 & - & 1 & \geq & 0 & & (5)\\
 & & -\cancel{x_3}\,1 & + & \cancel{x_2}\,0 & - & \cancel{2x_1}\,0 & + & 5 & \geq & 0 & & (6)\\
 & & -\cancel{x_3}\,1 & - & \cancel{x_2}\,0 & - & \frac{2}{3}\cancel{x_1}\,0 & + & 2 & \geq & 0 & & (7)
\end{array}
$$

variable	x_1	x_2	x_3	x_4
bounds	$(-\infty, \infty)$	$(-\infty, \infty)$	$[1; 2]$	$[-3; 0]$
assignment	$x_1 \mapsto 0$	$x_2 \mapsto 0$	$x_3 \mapsto 1$	$x_4 \mapsto -1$

SAT

Conflict resolution

Conflict Resolution is correct and terminating.

Theorem. Let S be a set of linear constraints then:

- S is unsatisfiable iff conflict resolution derives $1 \leq 0$;
- S is satisfiable iff conflict terminates with a satisfying assignment.

[Korovin, Tsiskaridze, Voronkov; CP'09]

Fourier-Motzkin vs Conflict Resolution

Example:

$$
\begin{array}{rcrcrcrcrcrcl}
2x_5 & - & 3x_4 & + & x_3 & - & 3x_2 & - & 2x_1 & + & 3 & \geq & 0 \\
2x_5 & + & x_4 & - & 2x_3 & & & - & 2x_1 & + & 2 & \geq & 0 \\
-x_5 & & & & & + & 3x_2 & + & x_1 & + & 2 & \geq & 0 \\
-3x_5 & & & + & 2x_3 & & & - & 3x_1 & - & 2 & \geq & 0 \\
x_5 & - & 2x_4 & & & - & 2x_2 & + & 3x_1 & - & 2 & \geq & 0 \\
-2x_5 & + & 2x_4 & - & 3x_3 & - & x_2 & + & 2x_1 & + & 3 & > & 0 \\
3x_5 & - & 2x_4 & + & 2x_3 & + & 3x_2 & + & 2x_1 & + & 1 & > & 0 \\
x_5 & & & & & & & + & 2x_1 & + & 2 & > & 0 \\
 & & 2x_4 & - & x_3 & - & 3x_2 & - & x_1 & + & 3 & = & 0
\end{array}
$$

Fourier-Motzkin: Generates over 280 million linear inequalities.

Fourier-Motzkin vs Conflict Resolution

Example:

$$
\begin{array}{rcrcrcrcrcrcl}
2x_5 & - & 3x_4 & + & x_3 & - & 3x_2 & - & 2x_1 & + & 3 & \geq & 0 \\
2x_5 & + & x_4 & - & 2x_3 & & & - & 2x_1 & + & 2 & \geq & 0 \\
-x_5 & & & & & + & 3x_2 & + & x_1 & + & 2 & \geq & 0 \\
-3x_5 & & & + & 2x_3 & & & - & 3x_1 & - & 2 & \geq & 0 \\
x_5 & - & 2x_4 & & & - & 2x_2 & + & 3x_1 & - & 2 & \geq & 0 \\
-2x_5 & + & 2x_4 & - & 3x_3 & - & x_2 & + & 2x_1 & + & 3 & > & 0 \\
3x_5 & - & 2x_4 & + & 2x_3 & + & 3x_2 & + & 2x_1 & + & 1 & > & 0 \\
x_5 & & & & & & & + & 2x_1 & + & 2 & > & 0 \\
 & & 2x_4 & - & x_3 & - & 3x_2 & - & x_1 & + & 3 & = & 0
\end{array}
$$

Fourier-Motzkin: Generates over 280 million linear inequalities.

Conflict Resolution: Generates 21 linear inequalities.

Properties of conflict resolution

Properties of conflict resolution.

- Every conflict resolution inference is non-redundant;
- In particular, the same constraint is will never be added twice;
- Conflict resolution is exponentially more efficient than F-M (independently of initial assignments) on a class of problems.

[Korovin, Tsiskaridze, Voronkov; CP'09]

Properties of conflict resolution

Properties of conflict resolution.

- Every conflict resolution inference is non-redundant;
- In particular, the same constraint is will never be added twice;
- Conflict resolution is exponentially more efficient than F-M (independently of initial assignments) on a class of problems.

[Korovin, Tsiskaridze, Voronkov; CP'09]

Strategies:

- variable selection: tightest bound, VSIDS,...
- value selection: mid-pint, continued fraction approximations, ...
- conflict selection: maximal overlap, geometric relaxation, ...

[KTV 2011, Dragan, Korovin, Kovács, Voronkov 2013]

ksmt calculus – extending conflict resolution to non-linear constraints

[Brauße, Korovin, Korovina, Müller, FroCoS'19]

Existentially quantified formula in CNF (i.e., $\bigwedge_i \bigvee_j \ell_{ij}$) where ℓ_{ij} are predicates or negated predicates over $(\mathbb{R}, \mathcal{F}_{\text{lin}} \cup \mathcal{F}_{\text{nl}}, \mathcal{P})$.

- $\mathcal{F}_{\text{lin}}$: constants $\in \mathbb{Q}$, addition, multiplication by constants $\in \mathbb{Q}$
- $\mathcal{F}_{\text{nl}}$: non-linear functions, incl. multiplication and transcendental functions
- $\mathcal{P} = \{<, \leq, >, \geq\}$ are predicates

Example

$$\exists x, y : \Big(((\sin x)^2 + (\cos x)^2 < 1) \vee (\exp x < y) \Big) \wedge \Big(4 \cdot x > y \Big)$$

An assignment $\alpha : V \to \mathbb{Q}$ is a solution to such a CNF $\mathcal{C}$ over variables V iff

- α assigns all quantified variables
- for each clause $C \in \mathcal{C}$ there is $\ell \in C$ with evaluates to true, in symbols: $[\![\ell]\!]^\alpha = \text{true}$

Problem: finding solution to $\mathcal{C}$ or showing that none exists.

Overview of the ksmt approach

Main ingredients of our approach:

1. separated linear form $\mathcal{L} \wedge \mathcal{N}$
2. ksmt calculus – conflict-driven calculus for solving SPL
3. local linearisations for resolving non-linear conflicts

Separated linear form

Separated linear form: $\mathcal{L} \wedge \mathcal{N}$

- $\mathcal{L}$ – linear inequalities: $q_1x_1 + q_2x_2 + \dots + q_nx_n + q_0 \diamond 0$

$$\begin{aligned} 2x - 4y - 2u - 2 &> 0 \\ -x + 2y + 3u + 1 &> 0 \\ 4y + 2u + 1 &\geq 0 \end{aligned}$$

- $\mathcal{N}$ – non-linear units: $x \diamond f(\bar{t})$

$$\begin{aligned} y &> sin(x^2) \\ u &\leq y^2x \\ x &\geq e^{-u} \end{aligned}$$

Linearisation

(L) Linearisation:
$(\alpha, \mathcal{L}, \mathcal{N}) \Rightarrow (\alpha, \mathcal{L} \cup L_{\alpha,\mathcal{N}}, \mathcal{N})$
$[\![\mathcal{L}]\!]^\alpha \neq$ false and
$[\![\mathcal{L} \cup L_{\alpha,\mathcal{N}}]\!]^\alpha =$ false.

Definition

A linear clause L is a linearisation of non-linear predicate P at assignment α iff

- $\forall \beta : [\![P]\!]^\beta =$ true $\rightarrow [\![L]\!]^\beta =$ true, and
- $[\![L]\!]^\alpha =$ false

$L_{\alpha,\mathcal{N}}$ contains (at least) one linearisation of a $P \in \mathcal{N}$ at α.

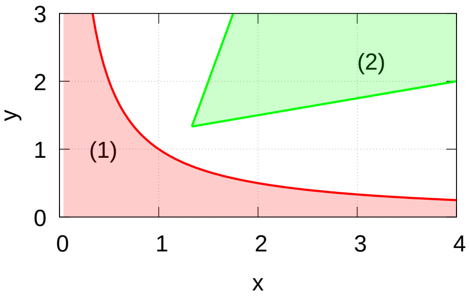
unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \leq 1/x)}_{P} \wedge (x/4 + 1 \leq y) \wedge (y \leq 4 \cdot (x-1))$$

Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \leq 1/d \ \vee \ y \leq d)$

rule	α	note



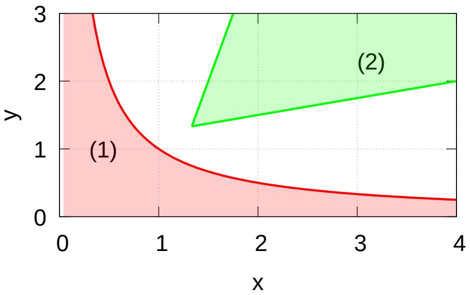
unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \le 1/x)}_{P} \wedge (x/4 + 1 \le y) \wedge (y \le 4 \cdot (x - 1))$$

Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = \big(x \le 1/d \ \vee \ y \le d\big)$

rule	α	note
(A)	$x \mapsto 2$	



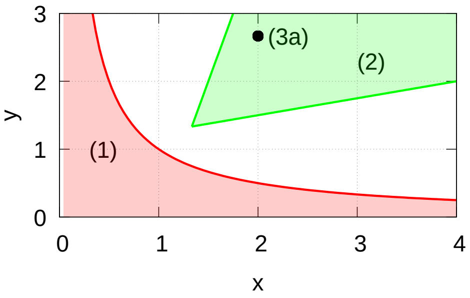
unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \le 1/x)}_{P} \wedge (x/4 + 1 \le y) \wedge (y \le 4 \cdot (x-1))$$

Linearisation of conflicts (x, y) at α here:

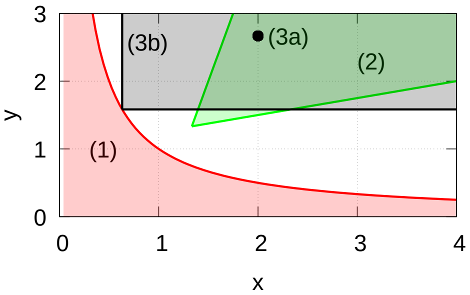
- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \le 1/d \ \vee \ y \le d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)



unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \leq 1/x)}_{P} \wedge (x/4 + 1 \leq y) \wedge (y \leq 4 \cdot (x-1)) \wedge \left((x \leq \tfrac{12}{19}) \vee (y \leq \tfrac{19}{12})\right)$$



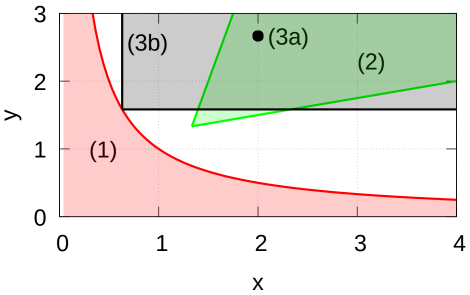
Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \leq 1/d \ \vee \ y \leq d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)

unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \le 1/x)}_{P} \wedge (x/4 + 1 \le y) \wedge (y \le 4 \cdot (x-1)) \wedge \left((x \le \tfrac{12}{19}) \vee (y \le \tfrac{19}{12})\right)$$



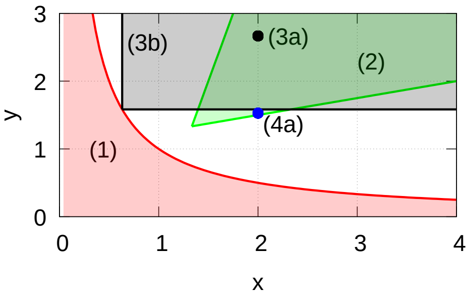
Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \le 1/d \;\vee\; y \le d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)
(B)	$x \mapsto 2$	

unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \le 1/x)}_{P} \wedge (x/4 + 1 \le y) \wedge (y \le 4 \cdot (x-1)) \wedge \left((x \le \tfrac{12}{19}) \vee (y \le \tfrac{19}{12})\right)$$



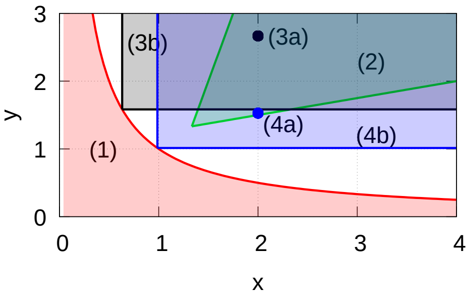
Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \le 1/d \ \vee \ y \le d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)
(B)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4a)

unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \leq 1/x)}_{P} \wedge (x/4 + 1 \leq y) \wedge (y \leq 4 \cdot (x-1)) \wedge \left((x \leq \tfrac{12}{19}) \vee (y \leq \tfrac{19}{12})\right) \wedge \left((x \leq \tfrac{220}{223}) \vee (y \leq \tfrac{223}{220})\right)$$



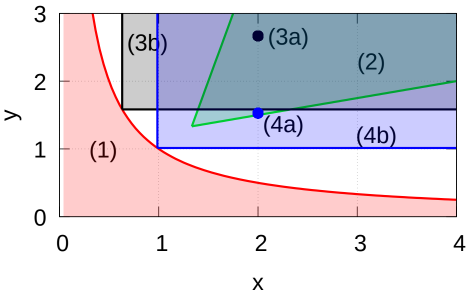
Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \leq 1/d \ \vee \ y \leq d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)
(B)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4a)
(L)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4b)

unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \leq 1/x)}_{P} \wedge (x/4 + 1 \leq y) \wedge (y \leq 4 \cdot (x-1))$$
$$\wedge \left((x \leq \tfrac{12}{19}) \vee (y \leq \tfrac{19}{12})\right)$$
$$\wedge \left((x \leq \tfrac{220}{223}) \vee (y \leq \tfrac{223}{220})\right)$$



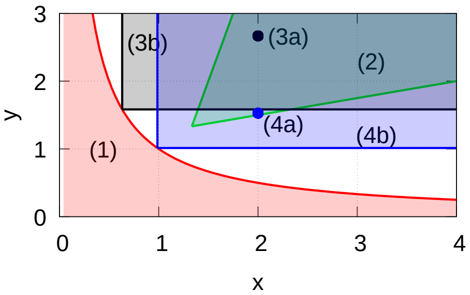
Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \leq 1/d \;\vee\; y \leq d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)
(B)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4a)
(L)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4b)
(B)	$x \mapsto 2$	

unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \le 1/x)}_{P} \wedge (x/4 + 1 \le y) \wedge (y \le 4 \cdot (x-1))$$
$$\wedge \left((x \le \tfrac{12}{19}) \vee (y \le \tfrac{19}{12})\right)$$
$$\wedge \left((x \le \tfrac{220}{223}) \vee (y \le \tfrac{223}{220})\right)$$
$$\wedge (\tfrac{4}{3} \le x) \wedge (x \le \tfrac{220}{223})$$



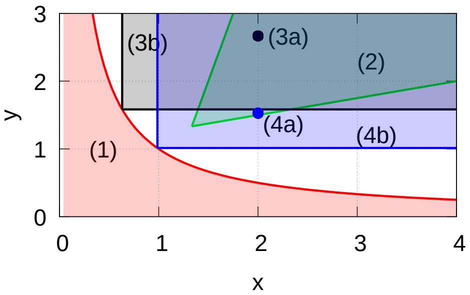
Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \le 1/d \ \vee \ y \le d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)
(B)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4a)
(L)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4b)
(B)	$x \mapsto 2$	
(R)	$x \mapsto 2$	on y

unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \le 1/x)}_{P} \wedge (x/4 + 1 \le y) \wedge (y \le 4 \cdot (x-1))$$
$$\wedge \left((x \le \tfrac{12}{19}) \vee (y \le \tfrac{19}{12})\right)$$
$$\wedge \left((x \le \tfrac{220}{223}) \vee (y \le \tfrac{223}{220})\right)$$
$$\wedge (\tfrac{4}{3} \le x) \wedge (x \le \tfrac{220}{223})$$



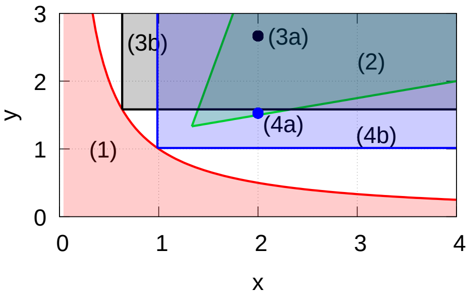
Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \le 1/d \ \vee \ y \le d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)
(B)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4a)
(L)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4b)
(B)	$x \mapsto 2$	
(R)	$x \mapsto 2$	on y
(B)		

unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \le 1/x)}_{P} \wedge (x/4 + 1 \le y) \wedge (y \le 4 \cdot (x-1))$$
$$\wedge \left((x \le \tfrac{12}{19}) \vee (y \le \tfrac{19}{12})\right)$$
$$\wedge \left((x \le \tfrac{220}{223}) \vee (y \le \tfrac{223}{220})\right)$$
$$\wedge (\tfrac{4}{3} \le x) \wedge (x \le \tfrac{220}{223})$$
$$\wedge (\tfrac{4}{3} \le \tfrac{220}{223})$$



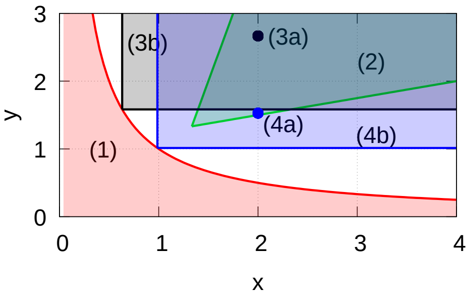
Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \le 1/d \ \vee \ y \le d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)
(B)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4a)
(L)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4b)
(B)	$x \mapsto 2$	
(R)	$x \mapsto 2$	on y
(B)		
(R)		on x

unsat example run using Interval linearisation

$$\mathcal{C} = \underbrace{(y \le 1/x)}_{P} \wedge (x/4 + 1 \le y) \wedge (y \le 4 \cdot (x-1))$$
$$\wedge \left((x \le \tfrac{12}{19}) \vee (y \le \tfrac{19}{12})\right)$$
$$\wedge \left((x \le \tfrac{220}{223}) \vee (y \le \tfrac{223}{220})\right)$$
$$\wedge (\tfrac{4}{3} \le x) \wedge (x \le \tfrac{220}{223})$$
$$\wedge (\tfrac{4}{3} \le \tfrac{220}{223})$$



Linearisation of conflicts (x, y) at α here:

- choose $d := (1/[\![x]\!]^\alpha + [\![y]\!]^\alpha)/2$,
- $L = (x \le 1/d \ \vee \ y \le d)$

rule	α	note
(A)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3a)
(L)	$x \mapsto 2,\ y \mapsto \frac{8}{3}$	(3b)
(B)	$x \mapsto 2$	
(A)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4a)
(L)	$x \mapsto 2,\ y \mapsto \frac{84}{55}$	(4b)
(B)	$x \mapsto 2$	
(R)	$x \mapsto 2$	on y
(B)		
(R)		on x
n/a		unsat

Some properties of the ksmt calculus

Some properties of the ksmt calculus

Corollary (Soundness)

If no rule can be applied to $(\alpha, \mathcal{L}, \mathcal{N})$, then $\begin{cases} [\![\mathcal{L}]\!]^\alpha = \text{true, and } \alpha \text{ is a solution to } \mathcal{C}, & \text{or} \\ \text{if } 1 < 0 \in \mathcal{L}, \text{ and } \mathcal{C} \text{ has no solution.} \end{cases}$

Some properties of the ksmt calculus

Corollary (Soundness)

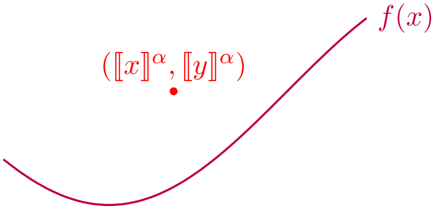
If no rule can be applied to $(\alpha, \mathcal{L}, \mathcal{N})$, then $\begin{cases} [\![\mathcal{L}]\!]^{\alpha} = \text{true, and } \alpha \text{ is a solution to } \mathcal{C}, & \text{or} \\ \text{if } 1 < 0 \in \mathcal{L}, \text{ and } \mathcal{C} \text{ has no solution.} \end{cases}$

Lemma (Progress)

After at most $n + 2$ steps the search space is reduced.

Deciding non-linear conflicts

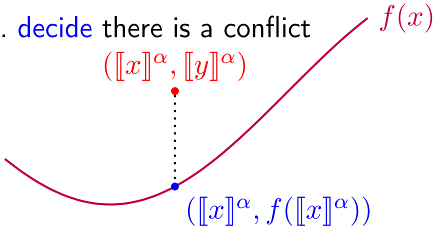
$f(x) \geq y$, $\alpha : V \to \mathbb{Q}$



Deciding non-linear conflicts

$f(x) \geq y$, $\alpha : V \to \mathbb{Q}$

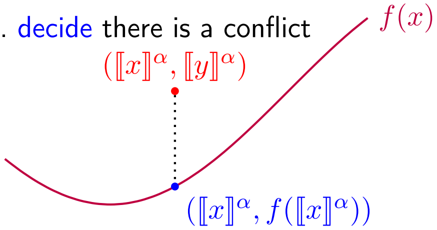
1. decide there is a conflict



Deciding non-linear conflicts

$f(x) \geq y$, $\alpha : V \to \mathbb{Q}$

1. decide there is a conflict



Computable Analysis: theory of computations on continuous structures: $\mathbb{R}$, $C([0,1],\mathbb{R})$, ...

- efficient implementation: iRRAM [Müller '00]

Definition (Cauchy representation of $\mathbb{R}$)

$x \in \mathbb{R}$ is computable iff $\tilde{x} : \mathbb{N} \to \mathbb{Q}$ is computable with $\forall n : |\tilde{x}(n) - x| \leq 2^{-n}$.

In general, $f(\llbracket x \rrbracket^\alpha) \geq \llbracket y \rrbracket^\alpha$ is not decidable, so we need more information about f.

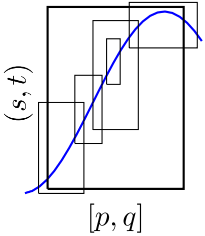
Approximability

Definition

A partial function $f : \mathbb{R} \to \mathbb{R}$ is called approximable iff

$$\{(p, q, s, t) : f([p, q]) \subset (s, t)\} \subset \mathbb{Q}^4$$

is computably enumerable.



Lemma

For total continuous real functions, approximability coincides with the notion of computability known from Computable Analysis.

The class $\mathcal{F}_{\mathrm{DA}}$

Definition

$\mathcal{F}_{\mathrm{DA}}$ – functions with decidable rational approximations; $g \in \mathcal{F}_{\mathrm{DA}}$ if

- $\mathrm{dom}\, g \cap \mathbb{Q}^n$ decidable,
- $\mathrm{graph}\, g \cap \mathbb{Q}^n \times \mathbb{Q}$ decidable and
- g approximable.

The class $\mathcal{F}_{\mathrm{DA}}$

Definition

$\mathcal{F}_{\mathrm{DA}}$ – functions with decidable rational approximations; $g \in \mathcal{F}_{\mathrm{DA}}$ if

- $\mathrm{dom}\, g \cap \mathbb{Q}^n$ decidable,
- $\mathrm{graph}\, g \cap \mathbb{Q}^n \times \mathbb{Q}$ decidable and
- g approximable.

- All multivariate polynomials
- Many elementary transcendental fn, e.g. $\exp, \ln, \log_q, \sin, \cos, \tan, \arctan$
- Many discontinuous fn, e.g. piecewise polynomials defined over a decidable set of rational intervals.

The class $\mathcal{F}_{\mathrm{DA}}$

Definition

$\mathcal{F}_{\mathrm{DA}}$ – functions with decidable rational approximations; $g \in \mathcal{F}_{\mathrm{DA}}$ if

- $\operatorname{dom} g \cap \mathbb{Q}^n$ decidable,
- $\operatorname{graph} g \cap \mathbb{Q}^n \times \mathbb{Q}$ decidable and
- g approximable.

- All multivariate polynomials
- Many elementary transcendental fn, e.g. $\exp, \ln, \log_q, \sin, \cos, \tan, \arctan$
- Many discontinuous fn, e.g. piecewise polynomials defined over a decidable set of rational intervals.

Theorem

For functions in $\mathcal{F}_{\mathrm{DA}}$, checking non-linear conflicts is decidable and linearisations are computable.

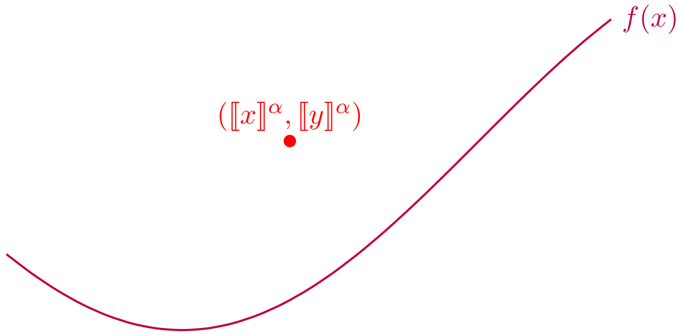
Using functions' known properties

Specialised linearisation algorithms for specific combinations of subclasses of functions $g \in \mathcal{F}_{\text{DA}}$ and point of conflict:

- **Differentiable g:** Use Tangent Space Linearisation.
- **Convex/Concave g:** Derive polytope R from computability of unique intersections
- **Piecewise g:** Meta-class: $\operatorname{dom} g$ partitioned by linear or non-linear predicates, each with a linearisation algorithm attached.
- **Rational $g(\boldsymbol{x})$:** Evaluate exactly in order to determine which linearisation to use.
- **Irrational $g(\boldsymbol{x})$:** Bound difference from below by a rational via successive approximations by the Computable Analysis implementation `iRRAM`.

Tangent space linearisation (schematic)

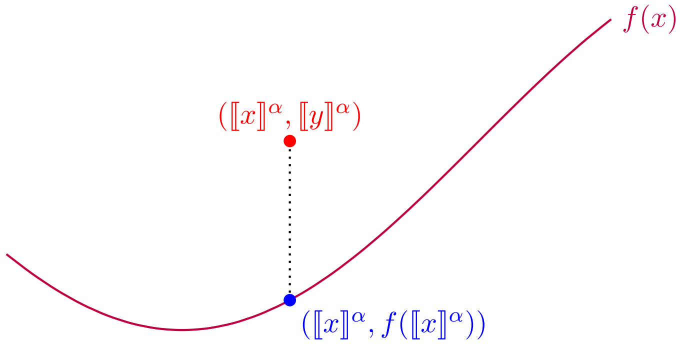
$\underbrace{f(x) \geq y}_{P}$, $\alpha : V \to \mathbb{Q}$



Tangent space linearisation (schematic)

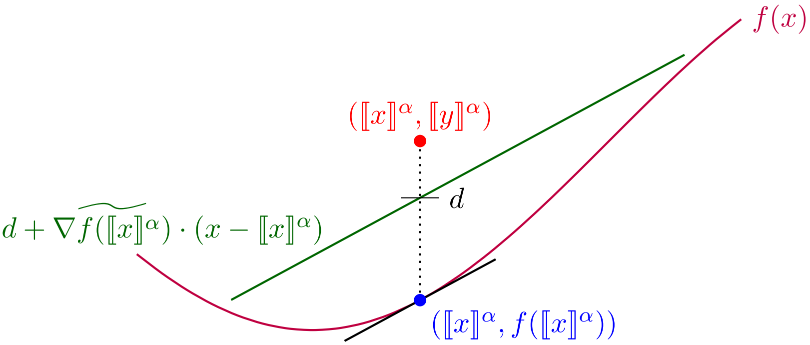
$\underbrace{f(x) \geq y}_{P}$, $\alpha : V \to \mathbb{Q}$

1. decide there is a conflict



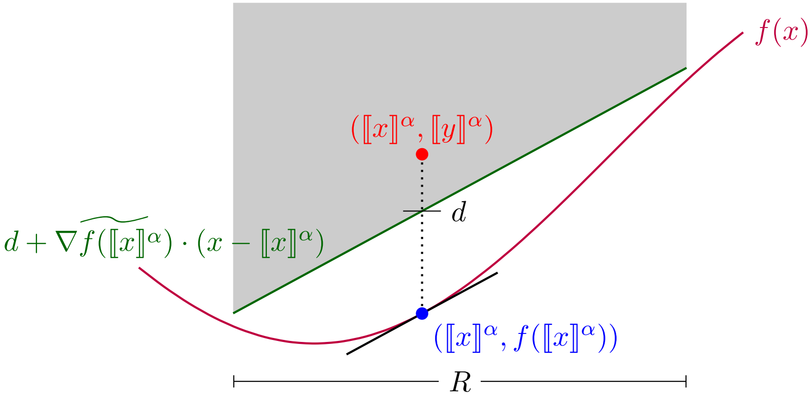
Tangent space linearisation (schematic)

$\underbrace{f(x) \geq y}_{P}$, $\alpha : V \to \mathbb{Q}$ 1. decide there is a conflict 2. compute linearization



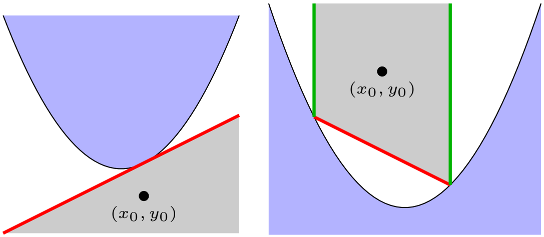
Tangent space linearisation (schematic)

$\underbrace{f(x) \geq y}_{P}$, $\alpha : V \to \mathbb{Q}$ 1. decide there is a conflict 2. compute linearization



Special classes: convex/concave

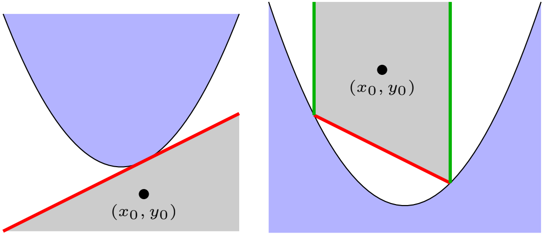
- f convex:



abs or $x \mapsto x^{2n}$ for $n \in \mathbb{N}$

Special classes: convex/concave

- f convex:

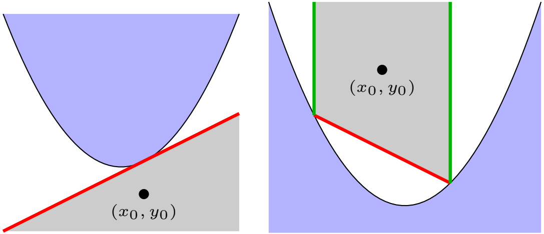


abs or $x \mapsto x^{2n}$ for $n \in \mathbb{N}$

- f concave $\iff$ $-f$ convex

Special classes: convex/concave

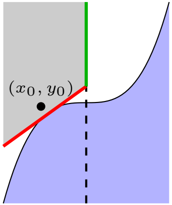
- f convex:



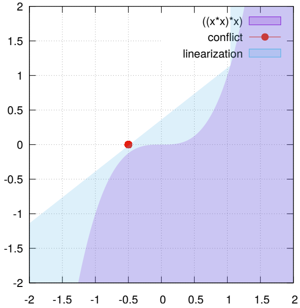
abs or $x \mapsto x^{2n}$ for $n \in \mathbb{N}$

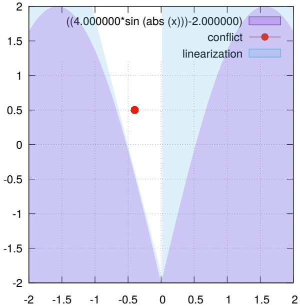
- f concave $\iff$ $-f$ convex

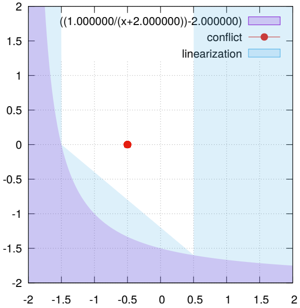
- f piecewise convex/-cave:

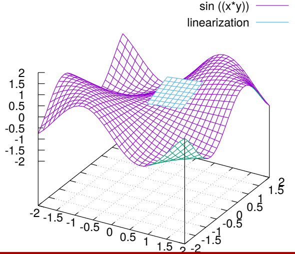


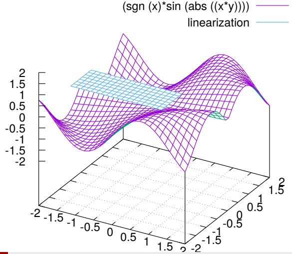
e.g. $x \mapsto x^{2n+1}$ for $n \in \mathbb{N}$

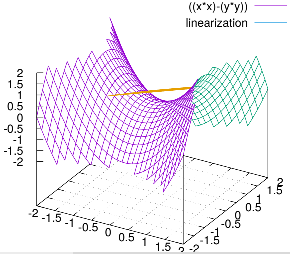

((x*x)*x)
conflict
linearization


((4.000000*sin (abs (x)))-2.000000)
conflict
linearization


((1.000000/(x+2.000000))-2.000000)
conflict
linearization


sin ((x*y))
linearization


(sgn (x)*sin (abs ((x*y))))
linearization


((x*x)-(y*y))
linearization

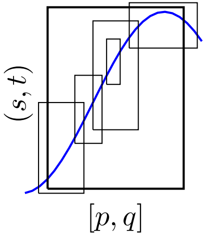
`ksmt` is a δ-complete decision procedure for non-linear constraints

[Brauße, Korovin, Korovina, Müller, CADE'21]

Computable Functions

Definition

A name for $\boldsymbol{x} \in \mathbb{R}^n$ is a rational sequence $\boldsymbol{\varphi} = (\boldsymbol{\varphi}_k)_k$ such that $\forall k : \|\boldsymbol{\varphi}_k - \boldsymbol{x}\| \leq 2^{-k}$.
A function $f : \mathbb{R}^n \to \mathbb{R}$ is computable iff there is a function-oracle Turing machine $M_f^?$ such that for all $\boldsymbol{x} \in \operatorname{dom} f$ and names $\boldsymbol{\varphi}$ for $\boldsymbol{x}$, $|M_f^{\boldsymbol{\varphi}}(p) - f(\boldsymbol{x})| \leq 2^{-p}$ holds for all $p \in \mathbb{N}$.



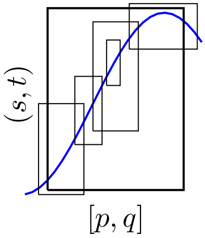
Proposition

A computable function $f : \mathbb{R}^n \to \mathbb{R}$ total on a compact $D \subset \mathbb{R}^n$ has a computable *uniform modulus of continuity* $\mu : \mathbb{N} \to \mathbb{N}$ on D:

$$\forall k \in \mathbb{N}\, \forall \boldsymbol{y}, \boldsymbol{z} \in D : \|\boldsymbol{y} - \boldsymbol{z}\| \leq 2^{-\mu(k)} \to |f(\boldsymbol{y}) - f(\boldsymbol{z})| \leq 2^{-k}.$$

Computable Functions

Computability of a real function corresponds to interval-like computations with convergence insurance.
Formalisation can be done by oracle Turing machines or Type-2 Weihrauch machines.
All of them give the same class of computable functions.



Proposition

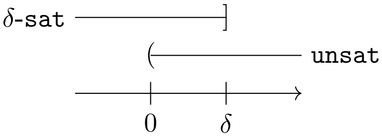
A computable function $f:\mathbb{R}^n \to \mathbb{R}$ total on a compact $D \subset \mathbb{R}^n$ has a computable *uniform modulus of continuity* $\mu:\mathbb{N}\to\mathbb{N}$ on D:

$$\forall k \in \mathbb{N}\, \forall \boldsymbol{y},\boldsymbol{z} \in D : \|\boldsymbol{y}-\boldsymbol{z}\| \le 2^{-\mu(k)} \to |f(\boldsymbol{y}) - f(\boldsymbol{z})| \le 2^{-k}.$$

δ-decidability

Let $\delta > 0$ be rational. The δ-relaxation P_δ of a constraint $P : f(\boldsymbol{x}) \diamond 0$ is

- $P_\delta : |f(\boldsymbol{x})| \leq \delta$ when $\diamond \in \{=\}$,
- $P_\delta : f(\boldsymbol{x}) \diamond \delta$ when $\diamond \in \{<, \leq\}$, and
- $P_\delta : f(\boldsymbol{x}) \diamond -\delta$ when $\diamond \in \{>, \geq\}$.

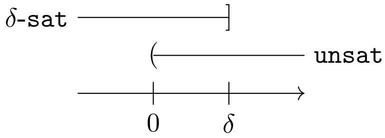


$P : f(\boldsymbol{x}) \leq 0.$

δ-decidability

Let $\delta > 0$ be rational. The δ-relaxation P_δ of a constraint $P : f(\boldsymbol{x}) \diamond 0$ is

- $P_\delta : |f(\boldsymbol{x})| \leq \delta$ when $\diamond \in \{=\}$,
- $P_\delta : f(\boldsymbol{x}) \diamond \delta$ when $\diamond \in \{<, \leq\}$, and
- $P_\delta : f(\boldsymbol{x}) \diamond -\delta$ when $\diamond \in \{>, \geq\}$.



$P : f(\boldsymbol{x}) \leq 0.$

Definition [S. Gao, J. Avigad, E. Clarke, '12]

δ-deciding a formula F denotes computing

- δ-sat, if there is α s.t. $[\![F_\delta]\!]^\alpha =$ true.
- unsat, if F is unsatisfiable.

In case both answers are valid, either output is acceptable.

For ksmt, just relaxing the non-linear part for δ-sat suffices: $\mathcal{L}_0 \wedge \mathcal{N}_\delta$.

δ-ksmt calculus

- Transition rules define relation $\Rightarrow$ on states $(\alpha, \mathcal{L}, \mathcal{N})$.
  - (partial) assignment α
  - linear inequalities $\mathcal{L}$
  - non-linear units $\mathcal{N}$
- initial state is $(\mathrm{nil}, \mathcal{L}_0, \mathcal{N}_0)$ for formula in separated linear form $\mathcal{L}_0 \wedge \mathcal{N}_0$.
- sat, $unsat$ and δ-sat are final states.

δ-ksmt calculus

Rules	$(\alpha, \mathcal{L}, \mathcal{N}) \Rightarrow \circ$	

δ-ksmt calculus

Rules	$(\alpha, \mathcal{L}, \mathcal{N}) \Rightarrow \circ$	
(A) assign	$(\alpha :: z \mapsto q, \mathcal{L}, \mathcal{N})$	z unassigned, $q \in \mathbb{Q}$ and no linear conflict

δ-ksmt calculus

Rules	$(\alpha, \mathcal{L}, \mathcal{N}) \Rightarrow \circ$	
(A) assign	$(\alpha :: z \mapsto q, \mathcal{L}, \mathcal{N})$	z unassigned, $q \in \mathbb{Q}$ and no linear conflict
(R) resolve	$(\alpha, \mathcal{L} \cup R, \mathcal{N})$	R resolvent excluding the linear conflict

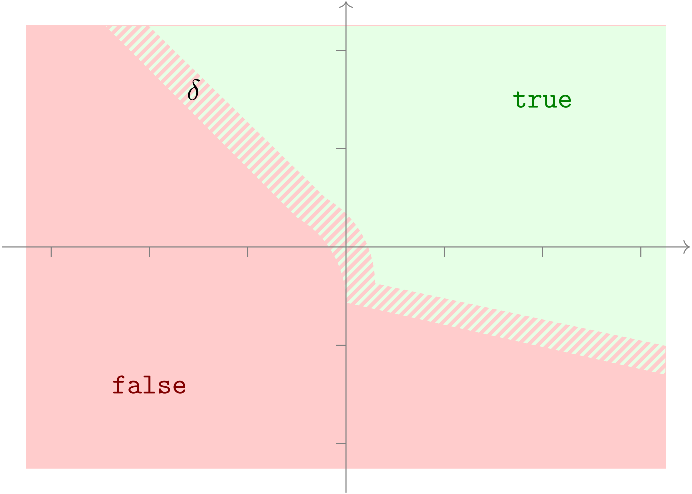
δ-ksmt calculus

Rules	$(\alpha, \mathcal{L}, \mathcal{N}) \Rightarrow \circ$	
(A) assign	$(\alpha :: z \mapsto q, \mathcal{L}, \mathcal{N})$	z unassigned, $q \in \mathbb{Q}$ and no linear conflict
(R) resolve	$(\alpha, \mathcal{L} \cup R, \mathcal{N})$	R resolvent excluding the linear conflict
(B) backjump	$(\gamma, \mathcal{L}, \mathcal{N})$	to γ maximal conflict-free prefix of α

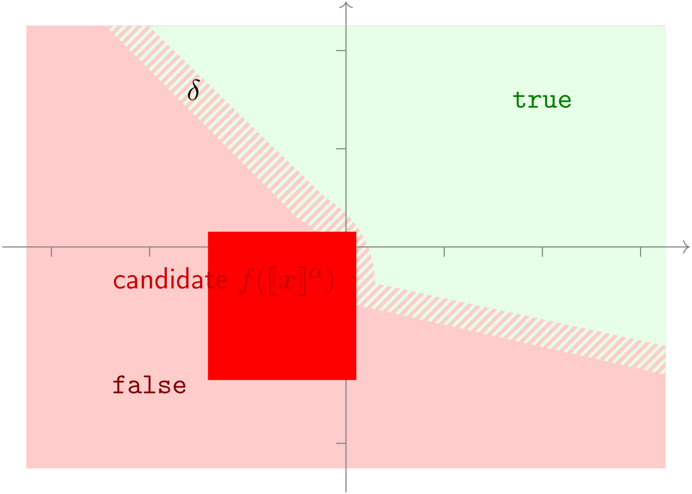
δ-ksmt calculus

Rules	$(\alpha, \mathcal{L}, \mathcal{N}) \Rightarrow \circ$	
(A) assign	$(\alpha :: z \mapsto q, \mathcal{L}, \mathcal{N})$	z unassigned, $q \in \mathbb{Q}$ and no linear conflict
(R) resolve	$(\alpha, \mathcal{L} \cup R, \mathcal{N})$	R resolvent excluding the linear conflict
(B) backjump	$(\gamma, \mathcal{L}, \mathcal{N})$	to γ maximal conflict-free prefix of α
(L) linearise	$(\alpha, \mathcal{L} \cup L, \mathcal{N})$	L linearisation, excluding the non-linear conflict
(F^{sat})	sat	all variables are assigned, no linear conflict and (A), (R), (B), (L) are not applicable
(F^{unsat})	$unsat$	$[\![\mathcal{L}]\!]^{nil} =$ false
(F_δ^{sat})	$\delta\text{-}sat$	all variables are assigned and $[\![\mathcal{L} \wedge \mathcal{N}_\delta]\!]^\alpha =$ true

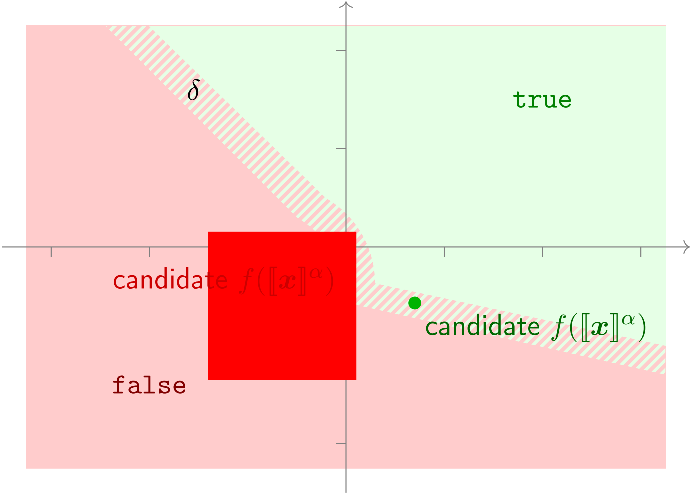
δ-ksmt candidates and linearisations



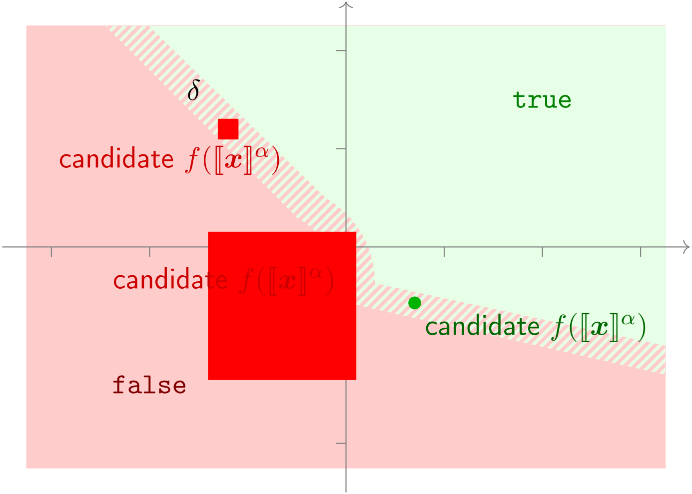
δ-ksmt candidates and linearisations



δ-ksmt candidates and linearisations



δ-ksmt candidates and linearisations



Theorem

Soundness of `ksmt` carries over to δ-`ksmt`.

We provide algorithms computing ϵ-full linearisations via:

- Linearise$_\delta$ (uniform) modulus of continuity, and
- LineariseLocal$_\delta$ local modulus of continuity extracted from computability of f.

Theorem

On bounded instances, there is $\epsilon > 0$ such that δ-`ksmt` runs with linearisations computed by Linearise$_\delta$ and LineariseLocal$_\delta$ are ϵ-full.

Theorem

δ-`ksmt` is a δ-complete decision procedure.

LineariseLocal$_\delta$

ksmt implementation/evaluation

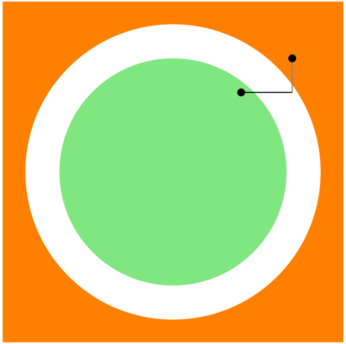
ksmt implementation

ksmt system:

- SMT solver for non-linear arithmetic
- Model guided architecture in the spirit of conflict resolution/MCSAT
- Including SAT/linear/non-linear in one incremental framework
- Integrates iRRAM – system for exact real arithmetic based on computable analysis developed by Norbert Th. Müller and colleagues.
- Open source: `http://informatik.uni-trier.de/~brausse/ksmt`

BB: $\exists \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^3 : \|\boldsymbol{x}\|_2 \leq r \wedge \|\boldsymbol{y}\|_2 \geq \sqrt{64} \wedge \|\boldsymbol{x} - \boldsymbol{y}\|_\infty \leq \frac{1}{100}$.

BB: $\exists \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^3 : \|\boldsymbol{x}\|_2 \leq r \wedge \|\boldsymbol{y}\|_2 \geq \sqrt{64} \wedge \|\boldsymbol{x} - \boldsymbol{y}\|_\infty \leq \frac{1}{100}$.



BB: $\exists \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^3 : \|\boldsymbol{x}\|_2 \leq r \wedge \|\boldsymbol{y}\|_2 \geq \sqrt{64} \wedge \|\boldsymbol{x} - \boldsymbol{y}\|_\infty \leq \frac{1}{100}$.

s : 'sat'
δ : 'δ-sat', $\delta = 10^{-3}$
u : 'unsat'
? : 'unknown'
> : timeout

r	ksmt		cvc4		z3		mathsat		yices		dReal		raSAT	
$\sqrt{37}$	u	0.07s	u	0.76s	u	510.67s	u	40.55s	u	0.07s	u	0.01	>	8h
$\sqrt{49}$	u	0.40s	u	2.46s	u	23211.20s	u	6307.18s	u	0.11s	u	0.03	>	8h
$\sqrt{62}$	u	11.61s	u	5.07s	u	210.16s	>	14.5h	u	76.82s	u	2.00	>	8h
$\sqrt{63}$	u	55.84s	?	0.48s	u	3925.65s	>	14.5h	u	0.10s	u	12.38	>	8h
$\sqrt{64}$	s	0.01s	?	0.01s	s	0.00s	>	21.6h	s	0.00s	δ	0.01	>	8h

Timings on Linux, Core-i7 3.6GHz, (all except mathsat: g++-7.3.0)

BB: $\exists \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^3 : \|\boldsymbol{x}\|_2 \leq r \wedge \|\boldsymbol{y}\|_2 \geq \sqrt{64} \wedge \|\boldsymbol{x} - \boldsymbol{y}\|_\infty \leq \frac{1}{100}$.

s: 'sat'
δ: 'δ-sat', $\delta = 10^{-3}$
u: 'unsat'
?: 'unknown'
$>$: timeout

r	ksmt		cvc4		z3		mathsat		yices		dReal		raSAT	
$\sqrt{37}$	u	0.07s	u	0.76s	u	510.67s	u	40.55s	u	0.07s	u	0.01	$>$	8h
$\sqrt{49}$	u	0.40s	u	2.46s	u	23211.20s	u	6307.18s	u	0.11s	u	0.03	$>$	8h
$\sqrt{62}$	u	11.61s	u	5.07s	u	210.16s	$>$	14.5h	u	76.82s	u	2.00	$>$	8h
$\sqrt{63}$	u	55.84s	?	0.48s	u	3925.65s	$>$	14.5h	u	0.10s	u	12.38	$>$	8h
$\sqrt{64}$	s	0.01s	?	0.01s	s	0.00s	$>$	21.6h	s	0.00s	δ	0.01	$>$	8h

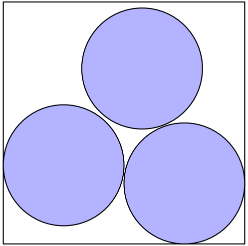
KK: $\exists \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathbb{R}^d : \bigwedge_{1 \leq i \leq n} \|\boldsymbol{x}_i\|_\infty \leq 1 \wedge \bigwedge_{1 \leq i < j \leq n} \|\boldsymbol{x}_i - \boldsymbol{x}_j\|_2 > 2$

BB: $\exists \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^3 : \|\boldsymbol{x}\|_2 \leq r \wedge \|\boldsymbol{y}\|_2 \geq \sqrt{64} \wedge \|\boldsymbol{x} - \boldsymbol{y}\|_\infty \leq \frac{1}{100}$.

s : 'sat'
δ : 'δ-sat', $\delta = 10^{-3}$
u : 'unsat'
? : 'unknown'
$>$: timeout

r	ksmt		cvc4		z3		mathsat		yices		dReal		raSAT	
$\sqrt{37}$	u	0.07s	u	0.76s	u	510.67s	u	40.55s	u	0.07s	u	0.01	$>$	8h
$\sqrt{49}$	u	0.40s	u	2.46s	u	23211.20s	u	6307.18s	u	0.11s	u	0.03	$>$	8h
$\sqrt{62}$	u	11.61s	u	5.07s	u	210.16s	$>$	14.5h	u	76.82s	u	2.00	$>$	8h
$\sqrt{63}$	u	55.84s	?	0.48s	u	3925.65s	$>$	14.5h	u	0.10s	u	12.38	$>$	8h
$\sqrt{64}$	s	0.01s	?	0.01s	s	0.00s	$>$	21.6h	s	0.00s	δ	0.01	$>$	8h

KK: $\exists \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathbb{R}^d : \bigwedge_{1 \leq i \leq n} \|\boldsymbol{x}_i\|_\infty \leq 1 \wedge \bigwedge_{1 \leq i < j \leq n} \|\boldsymbol{x}_i - \boldsymbol{x}_j\|_2 > 2$



BB: $\exists \boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^3 : \|\boldsymbol{x}\|_2 \leq r \wedge \|\boldsymbol{y}\|_2 \geq \sqrt{64} \wedge \|\boldsymbol{x} - \boldsymbol{y}\|_\infty \leq \frac{1}{100}$.

s: 'sat'
δ: 'δ-sat', $\delta = 10^{-3}$
u: 'unsat'
?: 'unknown'
>: timeout

r	ksmt		cvc4		z3		mathsat		yices		dReal		raSAT	
$\sqrt{37}$	u	0.07s	u	0.76s	u	510.67s	u	40.55s	u	0.07s	u	0.01	>	8h
$\sqrt{49}$	u	0.40s	u	2.46s	u	23211.20s	u	6307.18s	u	0.11s	u	0.03	>	8h
$\sqrt{62}$	u	11.61s	u	5.07s	u	210.16s	>	14.5h	u	76.82s	u	2.00	>	8h
$\sqrt{63}$	u	55.84s	?	0.48s	u	3925.65s	>	14.5h	u	0.10s	u	12.38	>	8h
$\sqrt{64}$	s	0.01s	?	0.01s	s	0.00s	>	21.6h	s	0.00s	δ	0.01	>	8h

KK: $\exists \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathbb{R}^d : \bigwedge_{1 \leq i \leq n} \|\boldsymbol{x}_i\|_\infty \leq 1 \wedge \bigwedge_{1 \leq i < j \leq n} \|\boldsymbol{x}_i - \boldsymbol{x}_j\|_2 > 2$

d	n	ksmt		cvc4		z3		mathsat		yices		dreal		rasat	
	2	s	0.01s	?	0.03s	s	0.01s	s	0.02s	s	0.01s	δ	0.01	s	0.02
	3	s	0.03s	?	0.08s	>	60m	s	0.24s	s	0.03s	δ	0.02	>	8h
2	4	>	8h	u	1474.16s	>	60m	u	8.11s	>	17h	δ	0.05	>	8h
	5	u	1.43s	u	0.45s	>	8h	u	0.28s	>	8h	u	3581.96	>	8h
	6	u	5.00s	u	0.75s	>	8h	u	0.40s	>	166m	>	8h	>	8h
3	5	s	0.93s	?	465.45s	>	8h	s	0.12s	s	0.06s	>	8h	>	8h
	6	s	6.02s	>	143m	>	7h	>	8h	>	6h	>	8h	>	8h
	5	s	0.38s	?	1544.87s	s	2165.78s	s	0.10s	s	7.34s	>	8h	>	8h
4	6	s	0.57s	>	91m	>	8h	s	0.23s	s	0.38s	>	8h	>	8h
	7	s	14.27s	>	160m	>	8h	s	0.18s	>	8h	>	8h	>	8h

Timings on Linux, Core-i7 3.6GHz, (all except `mathsat`: g++-7.3.0)

Conclusions and future work

Sound `ksmt` calculus:

- model-guided search & resolution of non-linear conflicts via local linearisation
- prototypical implementation with promising results
- identified broad class of functions $\mathcal{F}_{\mathrm{DA}}$ for which conflicts are decidable

Future:

- more precise linearisations for specific functions
- analyze complexity of deciding conflicts
- more extensive evaluation
- theoretical properties of calculus:
  - completeness in restricted settings
  - δ-completeness