Model-Constructing Satisfiability Calculus

Dejan Jovanović Clark Barrett Leonardo de Moura

SRI International NYU Microsoft Research

Satisfiability Modulo Theories and DPLL(T)

Problem

Check a given formula for satisfiability modulo the union of background theories.

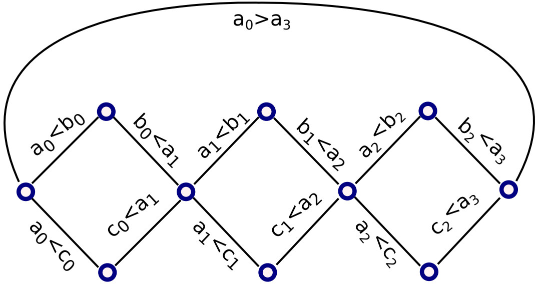
Example (QF_UFLRA)

$$(z = 1 \vee z = 0) \wedge (x - y + z = 1) \wedge (f(x) > f(y))$$

Main idea behind DPLL(T)

1. use a SAT solver to enumerate the Boolean structure,
2. check Boolean assignments with a decision procedure.

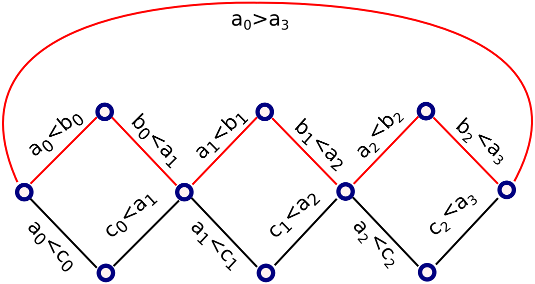
Satisfiability Modulo Theories and DPLL(T)



Example (Diamonds)

$$a_0 > a_n \wedge \bigwedge_{k=0}^{n-1} ((a_k < b_k \wedge b_k < a_{k+1}) \vee (a_k < c_k \wedge c_k < a_{k+1}))$$

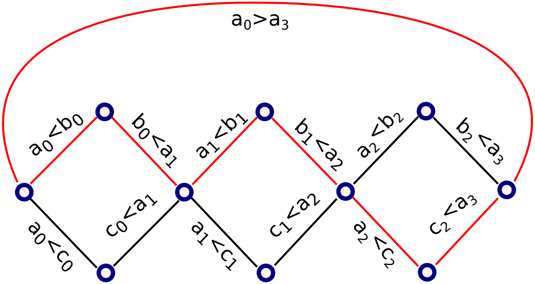
Satisfiability Modulo Theories and DPLL(T)



Example (Diamonds)

$$a_0 > a_n \wedge \bigwedge_{k=0}^{n-1} ((a_k < b_k \wedge b_k < a_{k+1}) \vee (a_k < c_k \wedge c_k < a_{k+1}))$$

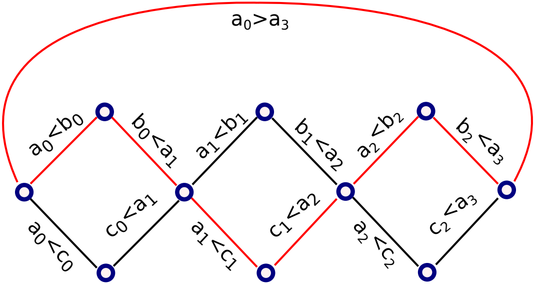
Satisfiability Modulo Theories and DPLL(T)



Example (Diamonds)

$$a_0 > a_n \wedge \bigwedge_{k=0}^{n-1} ((a_k < b_k \wedge b_k < a_{k+1}) \vee (a_k < c_k \wedge c_k < a_{k+1}))$$

Satisfiability Modulo Theories and DPLL(T)



Example (Diamonds)

$$a_0 > a_n \wedge \bigwedge_{k=0}^{n-1} ((a_k < b_k \wedge b_k < a_{k+1}) \vee (a_k < c_k \wedge c_k < a_{k+1}))$$

Alternative: Model-Based Procedures

Linear Real Arithmetic

MKS 2009 Generalizing DPLL to Richer Logics

KTV 2009 Conflict Resolution

C 2010 Natural Domain SMT

Linear Integer Arithmetic

JdM 2011 Cutting to the Chase: Solving Linear Integer Arithmetic

Non-Linear Real Arithmetic

JdM 2012 Solving Non-Linear Arithmetic

Alternative: Model-Based Procedures

Goals

- General framework for model-based decision procedures
- Allow for Boolean structure
- Allow for multiple theories (QF_UFLRA)
- Efficient! (even for simple theories)

Boolean Satisfiability

$$x_n \vee \cdots \vee x_1 \vee \overline{y_m} \vee \cdots \vee \overline{y_1}$$

- **Resolution-Based procedure** by Davis, Putnam (1960)
- **Search-Based procedure** by Davis, Logemann, Loveland (1962)

Resolution (DP)

- Find a proof
- Saturation
- Exponential

Search (DLL)

- Find a model
- Search and backtracking
- Exponential

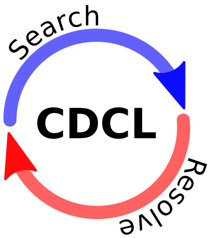
Boolean Satisfiability: CDCL

[1996] Marques-Silva, Sakallah
GRASP: A new search algorithm for satisfiabiliy

[2001] Moskewicz, Madigan, Zhao, Zhang, Malik
CHAFF: Engineering an efficient SAT solver

Conflict-Directed Clause Learning

- Use the search to guide resolution
- Use resolution to guide the search



Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ $\quad$ $x \vee \overline{y} \vee \overline{z}$ $\quad$ $\overline{x} \vee y \vee \overline{z}$ $\quad$ $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ $\quad$ $x \vee \overline{y} \vee z$ $\quad$ $\overline{x} \vee y \vee z$ $\quad$ $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$

⟦⟧

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ $x \vee \overline{y} \vee \overline{z}$ $\overline{x} \vee y \vee \overline{z}$ $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ $x \vee \overline{y} \vee z$ $\overline{x} \vee y \vee z$ $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$

$[\![x]\!]$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$	$x \vee \overline{y} \vee \overline{z}$	$\overline{x} \vee y \vee \overline{z}$	$\overline{x} \vee \overline{y} \vee \overline{z}$
$x \vee y \vee z$	$x \vee \overline{y} \vee z$	$\overline{x} \vee y \vee z$	$\overline{x} \vee \overline{y} \vee z$
$\overline{x} \vee \overline{y}$	$\overline{x}$		

$$[\![x, y]\!]$$

Boolean Satisfiability: CDCL

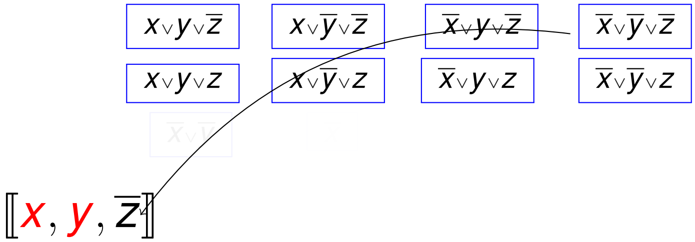
$x \vee y \vee \overline{z}$	$x \vee \overline{y} \vee \overline{z}$	$\overline{x} \vee y \vee \overline{z}$	$\overline{x} \vee \overline{y} \vee \overline{z}$
$x \vee y \vee z$	$x \vee \overline{y} \vee z$	$\overline{x} \vee y \vee z$	$\overline{x} \vee \overline{y} \vee z$
$\overline{x} \vee \overline{y}$	$\overline{x}$		

$[\![x, y]\!]$

Unit Propagation

($\overline{x} \vee \overline{y} \vee \overline{z}$) is unit, propagate $\overline{z}$.

Boolean Satisfiability: CDCL



Boolean Satisfiability: CDCL

$$x \vee y \vee \overline{z} \qquad x \vee \overline{y} \vee \overline{z} \qquad \overline{x} \vee y \vee \overline{z} \qquad \overline{x} \vee \overline{y} \vee \overline{z}$$

$$x \vee y \vee z \qquad x \vee \overline{y} \vee z \qquad \overline{x} \vee y \vee z \qquad \overline{x} \vee \overline{y} \vee z$$

$$[\![x, y, \overline{z}]\!]$$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ | $x \vee \overline{y} \vee \overline{z}$ | $\overline{x} \vee y \vee \overline{z}$ | $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ | $x \vee \overline{y} \vee z$ | $\overline{x} \vee y \vee z$ | $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$

$[\![x, y, \overline{z}]\!]$

Resolve Conflict

$$\frac{\overline{x} \vee \overline{y} \vee z \qquad \overline{x} \vee \overline{y} \vee \overline{z}}{\overline{x} \vee \overline{y}}$$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ $\quad$ $x \vee \overline{y} \vee \overline{z}$ $\quad$ $\overline{x} \vee y \vee \overline{z}$ $\quad$ $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ $\quad$ $x \vee \overline{y} \vee z$ $\quad$ $\overline{x} \vee y \vee z$ $\quad$ $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ $\quad$ $\overline{x}$

$$[\![x, y, \overline{z}]\!]$$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ | $x \vee \overline{y} \vee \overline{z}$ | $\overline{x} \vee y \vee \overline{z}$ | $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ | $x \vee \overline{y} \vee z$ | $\overline{x} \vee y \vee z$ | $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ | $\overline{x}$

$[\![x]\!]$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ $x \vee \overline{y} \vee \overline{z}$ $\overline{x} \vee y \vee \overline{z}$ $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ $x \vee \overline{y} \vee z$ $\overline{x} \vee y \vee z$ $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ $\overline{x}$

$[\![x, \overline{y}]\!]$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ $\quad x \vee \overline{y} \vee \overline{z}$ $\quad \overline{x} \vee y \vee \overline{z}$ $\quad \overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ $\quad x \vee \overline{y} \vee z$ $\quad \overline{x} \vee y \vee z$ $\quad \overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ $\quad \overline{x}$

$$[\![x, \overline{y}, \overline{z}]\!]$$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ $\quad$ $x \vee \overline{y} \vee \overline{z}$ $\quad$ $\overline{x} \vee y \vee \overline{z}$ $\quad$ $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ $\quad$ $x \vee \overline{y} \vee z$ $\quad$ $\overline{x} \vee y \vee z$ $\quad$ $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ $\quad$ $\overline{x}$

$$[\![x, \overline{y}, \overline{z}]\!]$$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ $\quad$ $x \vee \overline{y} \vee \overline{z}$ $\quad$ $\overline{x} \vee y \vee \overline{z}$ $\quad$ $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ $\quad$ $x \vee \overline{y} \vee z$ $\quad$ $\overline{x} \vee y \vee z$ $\quad$ $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ $\quad$ $\overline{x}$

$[\![x, \overline{y}, \overline{z}]\!]$

Resolve Conflict

$$\dfrac{\dfrac{\overline{x} \vee y \vee z \qquad \overline{x} \vee y \vee \overline{z}}{\overline{x} \vee y} \qquad \overline{x} \vee \overline{y}}{\overline{x}}$$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ $\quad$ $x \vee \overline{y} \vee \overline{z}$ $\quad$ $\overline{x} \vee y \vee \overline{z}$ $\quad$ $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ $\quad$ $x \vee \overline{y} \vee z$ $\quad$ $\overline{x} \vee y \vee z$ $\quad$ $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ $\quad$ $\overline{x}$

$[\![x, \overline{y}, \overline{z}]\!]$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ | $x \vee \overline{y} \vee \overline{z}$ | $\overline{x} \vee y \vee \overline{z}$ | $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ | $x \vee \overline{y} \vee z$ | $\overline{x} \vee y \vee z$ | $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ | $\overline{x}$

$[\![\,]\!]$

Boolean Satisfiability: CDCL

$x \vee y \vee \overline{z}$ | $x \vee \overline{y} \vee \overline{z}$ | $\overline{x} \vee y \vee \overline{z}$ | $\overline{x} \vee \overline{y} \vee \overline{z}$

$x \vee y \vee z$ | $x \vee \overline{y} \vee z$ | $\overline{x} \vee y \vee z$ | $\overline{x} \vee \overline{y} \vee z$

$\overline{x} \vee \overline{y}$ | $\overline{x}$

$[\![\overline{x}]\!]$

Boolean Satisfiability: CDCL

Model Construction

Build partial model by assigning variables to values

$$[\![\ldots, x, \ldots, \overline{y}, \ldots, z, \ldots]\!] \ .$$

Unit Reasoning

Reason about unit constraints

$$(\overline{x} \vee y \vee \overline{z} \vee w) \ .$$

Explain Conflicts

Explain conflicts using clausal reasons

$$(\overline{x} \vee y \vee \overline{z}) \ .$$

Linear Real Arithmetic

Linear Arithmetic

$$a_1 x_1 + \cdots + a_n x_n \geq b \qquad a_1 x_1 + \cdots + a_n x_n = b$$

Current state-of-the-art: Simplex

A model builder for a conjunction of linear constraints.

- Search for a model
- Escape conflicts through pivoting
- Built for the DPLL(T) framework

[DdM 2006] A fast linear-arithmetic solver for DPLL(T)

Linear Real Arithmetic

Linear Arithmetic

$$a_1 x_1 + \cdots + a_n x_n \geq b \qquad a_1 x_1 + \cdots + a_n x_n = b$$

Fourier-Motzkin Resolution

$$\dfrac{\dfrac{2x + 3y - z \geq -1}{6x + 9y - 3z \geq -3} \qquad \dfrac{-3x - 2y + 4z \geq 2}{-6x - 4y + 8z \geq 4}}{5y + 5z \geq 1}$$

- Feels like Boolean resolution (elimination).
- Behaves like Boolean resolution (exponential).

Linear Real Arithmetic

Model Construction

Build partial model by assigning variables to values

$$[\![\ldots, C_1, C_2, \ldots, x \mapsto 1/2, \ldots, y \mapsto 1/2, \ldots, z \mapsto -1, \ldots]\!] \ .$$

Unit Reasoning

Reason about unit constraints

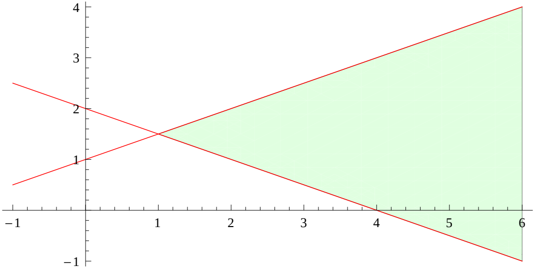
$$C_1 \equiv (x + y + z + w \geq 0) \qquad C_2 \equiv (x + y + z - w > 0) \ .$$

Explain Conflicts

Explain conflicts using valid clausal reasons

$$(\overline{C_1} \vee \overline{C_2} \vee x + y + z > 0) \ .$$

Linear Real Arithmetic

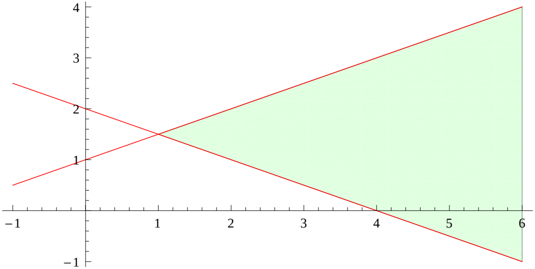


$$\overbrace{2y - x - 2 < 0}^{C_1} \;\wedge\; \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$\Downarrow$$

Explanation $C_1 \wedge C_2 \implies x \neq 0.5$

Linear Real Arithmetic

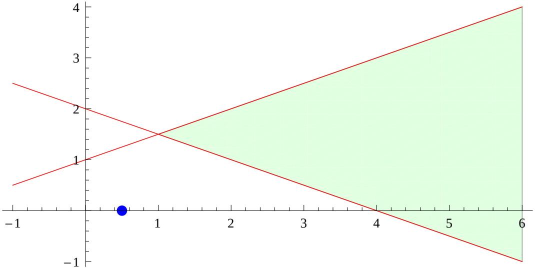


$$\overbrace{2y - x - 2 < 0}^{C_1} \wedge \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2]\!]$$

Explanation $C_1 \wedge C_2 \implies x \neq 0.5$

Linear Real Arithmetic

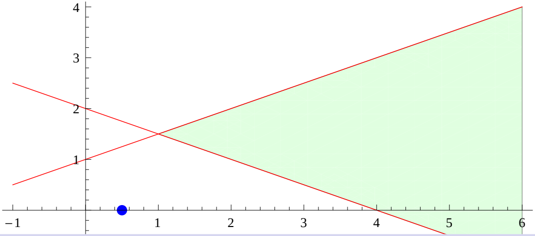


$$\overbrace{2y - x - 2 < 0}^{C_1} \;\wedge\; \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x \mapsto 0.5]\!]$$

Explanation $C_1 \wedge C_2 \implies x \neq 0.5$

Linear Real Arithmetic



Unit Constraint Reasoning

$$2y - x - 2 < 0 \Longrightarrow (y < 1.25)$$

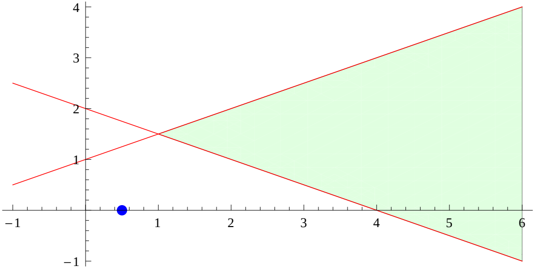
$$-2y - x + 4 < 0 \Longrightarrow (y > 1.75)$$

$$(2y - x - 2 < 0) \wedge (-2y - x + 4 < 0)$$

$$[\![C_1, C_2, x \mapsto 0.5]\!]$$

Explanation $C_1 \wedge C_2 \implies x \neq 0.5$

Linear Real Arithmetic

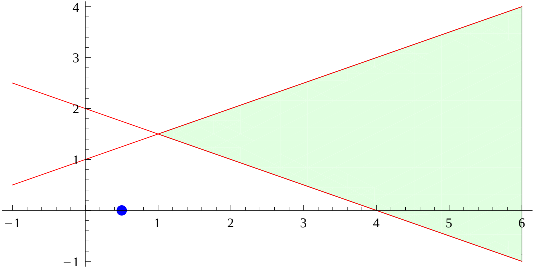


$$\overbrace{2y - x - 2 < 0}^{C_1} \wedge \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x \mapsto 0.5]\!]$$

Explanation $C_1 \wedge C_2 \implies x \neq 0.5$

Linear Real Arithmetic

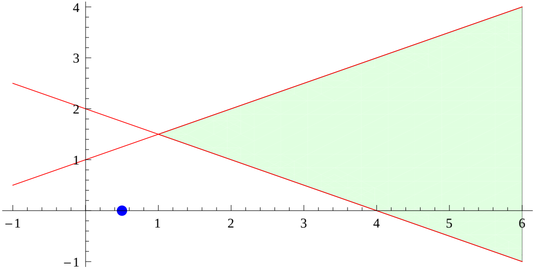


$$\overbrace{2y - x - 2 < 0}^{C_1} \wedge \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x \mapsto 0.5]\!]$$

Explanation $C_1 \wedge C_2 \implies$

Linear Real Arithmetic



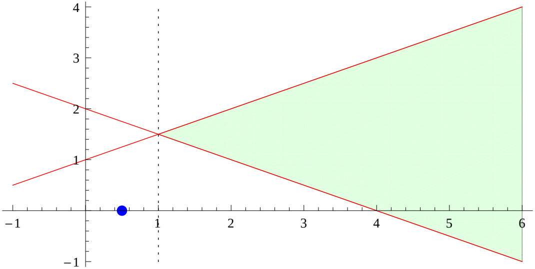
Fourier-Motzkin

$$\frac{2y - x - 2 < 0 \qquad -2y - x + 4 < 0}{-2x + 2 < 0}$$

$$[\![C_1, C_2, x \mapsto 0.5]\!]$$

Explanation $C_1 \wedge C_2 \implies$

Linear Real Arithmetic



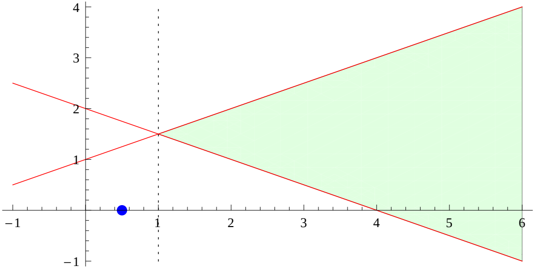
Fourier-Motzkin

$$\frac{2y - x - 2 < 0 \qquad -2y - x + 4 < 0}{-2x + 2 < 0}$$

$$[\![C_1, C_2, x \mapsto 0.5]\!]$$

Explanation $C_1 \wedge C_2 \implies x > 1$

Linear Real Arithmetic

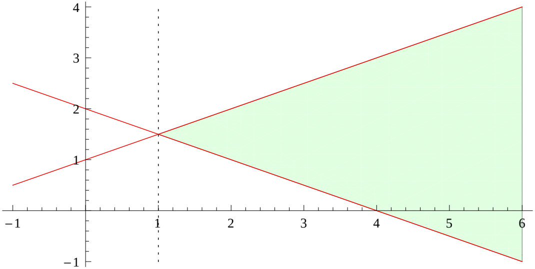


$$\overbrace{2y - x - 2 < 0}^{C_1} \;\wedge\; \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x \mapsto 0.5]\!]$$

Explanation $\overline{C_1} \vee \overline{C_2} \vee (x > 1)$

Linear Real Arithmetic

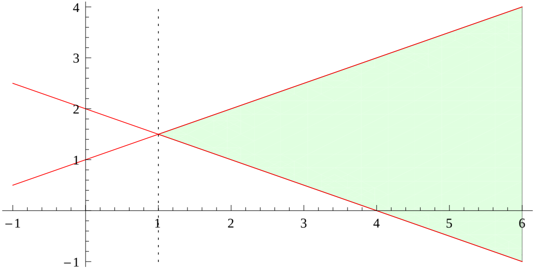


$$\overbrace{2y - x - 2 < 0}^{C_1} \;\wedge\; \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2]\!]$$

Explanation $\overline{C_1} \vee \overline{C_2} \vee (x > 1)$

Linear Real Arithmetic

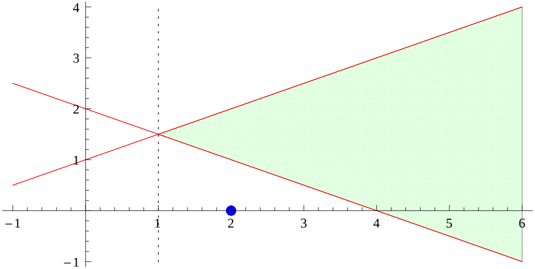


$$\overbrace{2y - x - 2 < 0}^{C_1} \ \wedge \ \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x > 1]\!]$$

Explanation $\overline{C_1} \vee \overline{C_2} \vee (x > 1)$

Linear Real Arithmetic

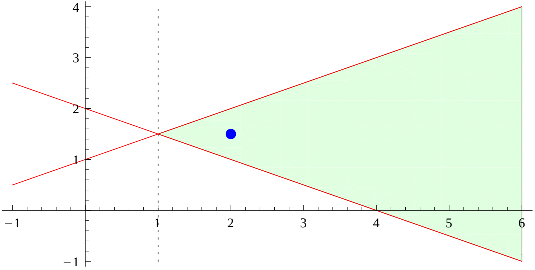


$$\overbrace{2y - x - 2 < 0}^{C_1} \;\wedge\; \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x > 1, x \mapsto 2]\!]$$

Explanation $\overline{C_1} \vee \overline{C_2} \vee (x > 1)$

Linear Real Arithmetic

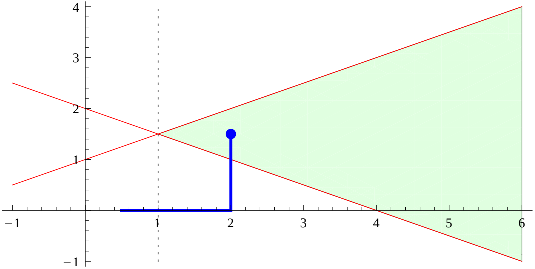


$$\overbrace{2y - x - 2 < 0}^{C_1} \wedge \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x > 1, x \mapsto 2, y \mapsto 1.5]\!]$$

Explanation $\overline{C_1} \vee \overline{C_2} \vee (x > 1)$

Linear Real Arithmetic

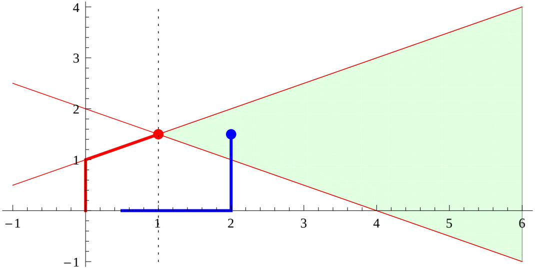


$$\overbrace{2y - x - 2 < 0}^{C_1} \wedge \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x > 1, {\color{red} x \mapsto 2, y \mapsto 1.5}]\!]$$

$$\text{Explanation } \overline{C_1} \vee \overline{C_2} \vee (x > 1)$$

Linear Real Arithmetic

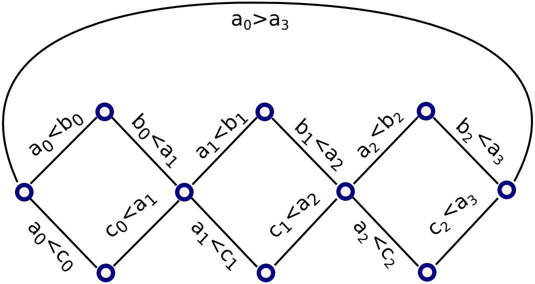


$$\overbrace{2y - x - 2 < 0}^{C_1} \wedge \overbrace{-2y - x + 4 < 0}^{C_2}$$

$$[\![C_1, C_2, x > 1, x \mapsto 2, y \mapsto 1.5]\!]$$

Explanation $\overline{C_1} \vee \overline{C_2} \vee (x > 1)$

Linear Real Arithmetic: Results



Example (Diamonds)

$$a_0 > a_n \wedge \bigwedge_{k=0}^{n-1} ((a_k < b_k \wedge b_k < a_{k+1}) \vee (a_k < c_k \wedge c_k < a_{k+1}))$$

Linear Real Arithmetic: Results

	mcsat		cvc4		z3		mathsat5		yices	
set	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)
clocksynchro (36)	**36**	**123.11**	36	1166.55	36	1828.74	36	1732.59	36	1093.80
DTPScheduling (91)	**91**	**31.33**	91	72.92	91	100.55	89	1980.96	91	926.22
miplib (42)	8	97.16	**27**	**3359.40**	23	3307.92	19	5447.46	23	466.44
sal (107)	107	12.68	107	13.46	107	6.37	107	7.99	**107**	**2.45**
sc (144)	144	1655.06	144	1389.72	144	954.42	144	880.27	**144**	**401.64**
spiderbenchmarks (42)	42	2.38	42	2.47	42	1.66	42	1.22	**42**	**0.44**
TM (25)	25	1125.21	25	82.12	**25**	**51.64**	25	1142.98	25	55.32
ttastartup (72)	70	4443.72	72	1305.93	72	1647.94	72	2607.49	**72**	**1218.68**
uart (73)	73	5244.70	73	1439.89	73	1379.90	73	1481.86	**73**	**679.54**
	596	12735.35	**617**	**8832.46**	613	9279.14	607	15282.82	613	4844.53

Uninterpreted Functions

$x = y$ $x \neq y$ $x = f(y, z)$

Current state-of-the art: Congruence Closure

- Incremental algorithms for congruence closure.
- Propagation of entailed equalities.
- Combination through Nelson-Oppen style procedures.

Alternative: Ackermannization

$$\frac{}{x_1 = y_1 \wedge x_2 = y_2 \implies f(x_1, x_2) = f(y_1, y_2)}$$

Uninterpreted Functions

$$x = y \qquad x \neq y \qquad x = f(y, z)$$

Current state-of-the art: Congruence Closure

- Incremental algorithms for congruence closure.
- Propagation of entailed equalities.
- Combination through Nelson-Oppen style procedures.

Alternative: Ackermannization

$$\overline{x_1 = y_1 \wedge x_2 = y_2 \implies f(x_1, x_2) = f(y_1, y_2)}$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$\llbracket\ \rrbracket$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y)]\!]$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y), \quad f(x) \mapsto 0]\!]$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y),\ \ f(x) \mapsto 0,\ \ f(y) \mapsto 1]\!]$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y),\ \ f(x) \mapsto 0,\ \ f(y) \mapsto 1,\ \ x \mapsto 0]\!]$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y),\ \ f(x) \mapsto 0,\ \ f(y) \mapsto 1,\ \ x \mapsto 0,\ \ y \mapsto 0]\!]$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y),\ \ f(x) \mapsto 0,\ \ f(y) \mapsto 1,\ \ x \mapsto 0,\ \ y \mapsto 0]\!]$$

Explain Conflict: Ackermanization

$$\frac{}{x = y \implies f(x) = f(y)}$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y),\ \ f(x) \mapsto 0,\ \ f(y) \mapsto 1,\ \ x \mapsto 0,\ \ y \mapsto 0]\!]$$

Explain Conflict: Ackermanization

$$\frac{}{x \neq y \vee f(x) = f(y)}$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y), \quad f(x) \mapsto 0, \quad f(y) \mapsto 1]\!]$$

Explain Conflict: Ackermanization

$$\frac{}{x \neq y \vee f(x) = f(y)}$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y),\ \ f(x) \mapsto 0,\ \ f(y) \mapsto 1,\ \ x \neq y]\!]$$

Explain Conflict: Ackermanization

$$\frac{}{x \neq y \vee f(x) = f(y)}$$

Uninterpreted Functions: Example

$$f(x) < f(y)$$

$$[\![f(x) < f(y),\ \ f(x) \mapsto 0,\ \ f(y) \mapsto 1,\ \ x \neq y,\ \ x \mapsto 0]\!]$$

Explain Conflict: Ackermanization

$$\frac{}{x \neq y \vee f(x) = f(y)}$$

Uninterpreted Functions: Example

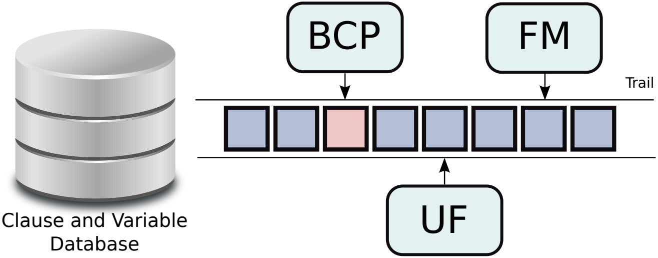
$$f(x) < f(y)$$

$$[\![f(x) < f(y),\ \ f(x) \mapsto 0,\ \ f(y) \mapsto 1,\ \ x \neq y,\ \ x \mapsto 0,\ \ y \mapsto 1]\!]$$

Explain Conflict: Ackermanization

$$\frac{}{x \neq y \vee f(x) = f(y)}$$

Implementation Details



- Source available
  https://github.com/dddejan/CVC4/tree/mcsat

Uninterpreted Functions (QF_UFLRA): Results

	mcsat		cvc4		z3		mathsat5		yices	
set	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)
EufLaArithmetic (33)	33	39.57	33	49.11	**33**	**2.53**	33	20.18	33	4.61
Hash (198)	198	34.81	198	10.60	198	7.18	198	1330.88	**198**	**2.64**
RandomCoupled (400)	400	68.04	400	35.90	400	31.44	**400**	**18.56**	384	39903.78
RandomDecoupled (500)	500	34.95	500	40.63	500	30.98	**500**	**21.86**	500	3863.79
Wisa (223)	223	9.18	223	87.35	223	10.80	223	65.27	**223**	**2.80**
wisas (108)	**108**	**40.17**	108	5221.37	108	443.36	106	1737.41	108	736.98
	1462	**226.72**	1462	5444.96	1462	526.29	1460	3194.16	1446	44514.60

Conclusions/Future Work

Conclusion

- General framework for model-based decision procedures
- Allows Boolean structure
- Allows multiple theories
- Simple and efficient!

Future Work

- New theories: bit-vectors, arrays
- Old theories: integers, non-linear arithmetic, simplex
- Extend the API to “incremental” solving
- More expressive fragments: $\exists\forall$

Thank You!

Questions?

Leonardo de Moura and Dejan Jovanović.
A model-constructing satisfiability calculus.
In *VMCAI*, 2013.

Dejan Jovanović, Clark Barrett, and Leonardo de Moura.
Design and implementation of the model-constructing satisfiability calculus.
In *FMCAD*, 2013.