SMT Solving: Past, Present and Future

Erika Ábrahám
RWTH Aachen University, Germany

Informatics Europe Webinar, 21 Oct 2021

RWTH AACHEN UNIVERSITY

The traveller Eve's problem

The traveller Eve's problem

After Covid lockdown, Eve is eager to make scientific visits again.

- She has 100 travel wishes $A_1, \ldots, A_{100}$.
- She is allowed to make only 5 travels.
- She wants to be physically at $A_1 = ECSS'21$.
- To coordinate a project, she needs to visit either A_2 or A_3.
- Travel A_i costs C_i EUR.
- Eve can spend up to C EUR.
- Travel A_i takes T_i days.
- Eve wants to travel at least T days.

The traveller Eve's problem

After Covid lockdown, Eve is eager to make scientific visits again.

- She has 100 travel wishes $A_1, \ldots, A_{100}$.
- She is allowed to make only 5 travels.
- She wants to be physically at $A_1 = ECSS'21$.
- To coordinate a project, she needs to visit either A_2 or A_3.
- Travel A_i costs C_i EUR.
- Eve can spend up to C EUR.
- Travel A_i takes T_i days.
- Eve wants to travel at least T days.

$$\left(\bigwedge_{i=1}^{100} \left((a_i = 0 \wedge c_i = 0 \wedge t_i = 0) \ \vee \ (a_i = 1 \wedge c_i = C_i \wedge t_i = T_i \ ) \right) \right) \wedge$$

$$\left(\sum_{i=1}^{100} a_i \leq 5 \right) \wedge (a_1 = 1) \wedge (a_2 = 1 \vee a_3 = 1) \wedge \left(\sum_{i=1}^{100} c_i \leq C \right) \wedge \left(\sum_{i=1}^{100} t_i \geq T \right)$$

The traveller Eve's problem

After Covid lockdown, Eve is eager to make scientific visits again.

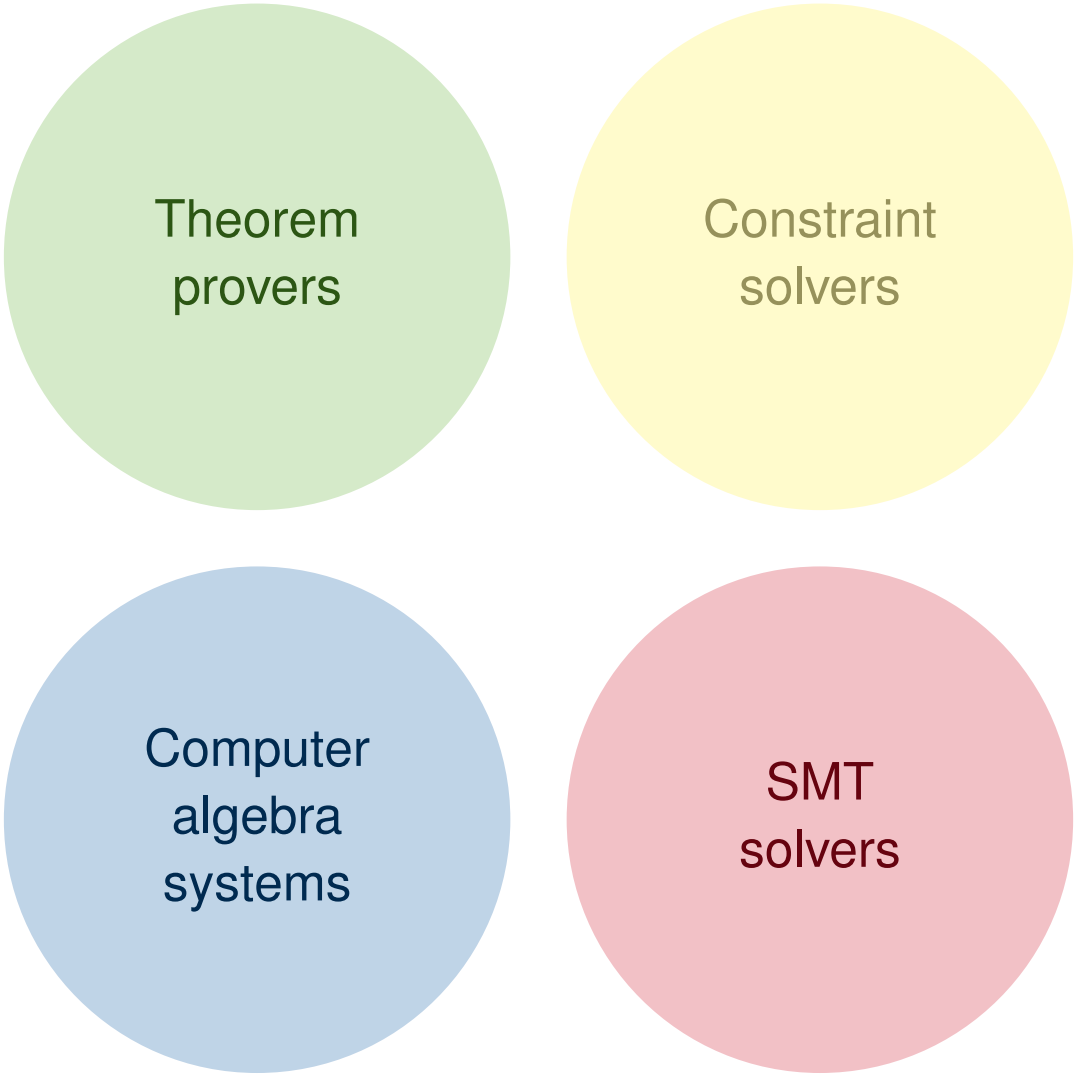
- She has 100 travel wishes $A_1, \ldots, A_{100}$.
- She is allowed to make only 5 travels.
- She wants to be physically at $A_1 = ECSS'21$.
- To coordinate a project, she needs to visit either A_2 or A_3.
- Travel A_i costs C_i EUR.
- Eve can spend up to C EUR.
- Travel A_i takes T_i days.
- Eve wants to travel at least T days.

$$\left(\bigwedge_{i=1}^{100} \left((a_i = 0 \wedge c_i = 0 \wedge t_i = 0) \ \vee \ (a_i = 1 \wedge c_i = C_i \wedge t_i = T_i \ ) \right) \right) \wedge$$

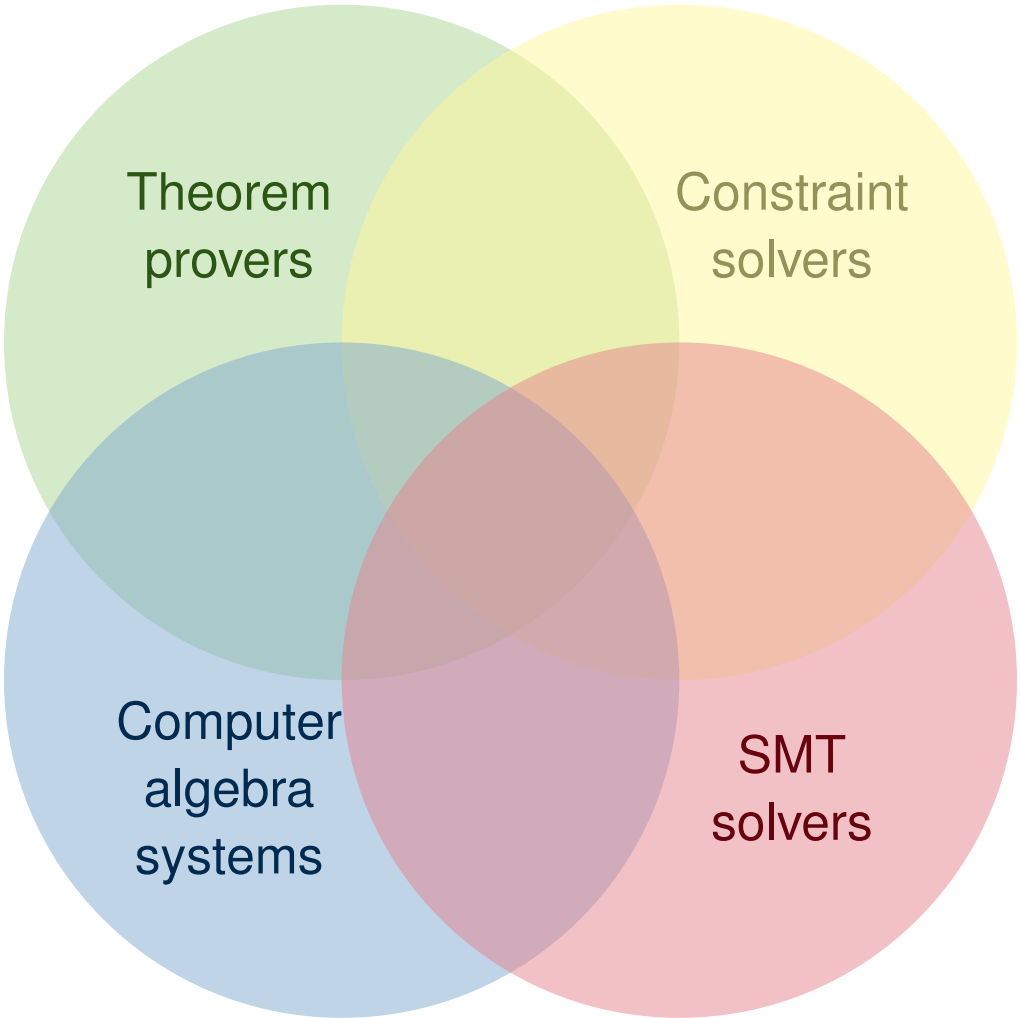
$$\left(\sum_{i=1}^{100} a_i \leq 5 \right) \wedge (a_1 = 1) \wedge (a_2 = 1 \vee a_3 = 1) \wedge \left(\sum_{i=1}^{100} c_i \leq C \right) \wedge \left(\sum_{i=1}^{100} t_i \geq T \right)$$

Logic: Linear real arithmetic.

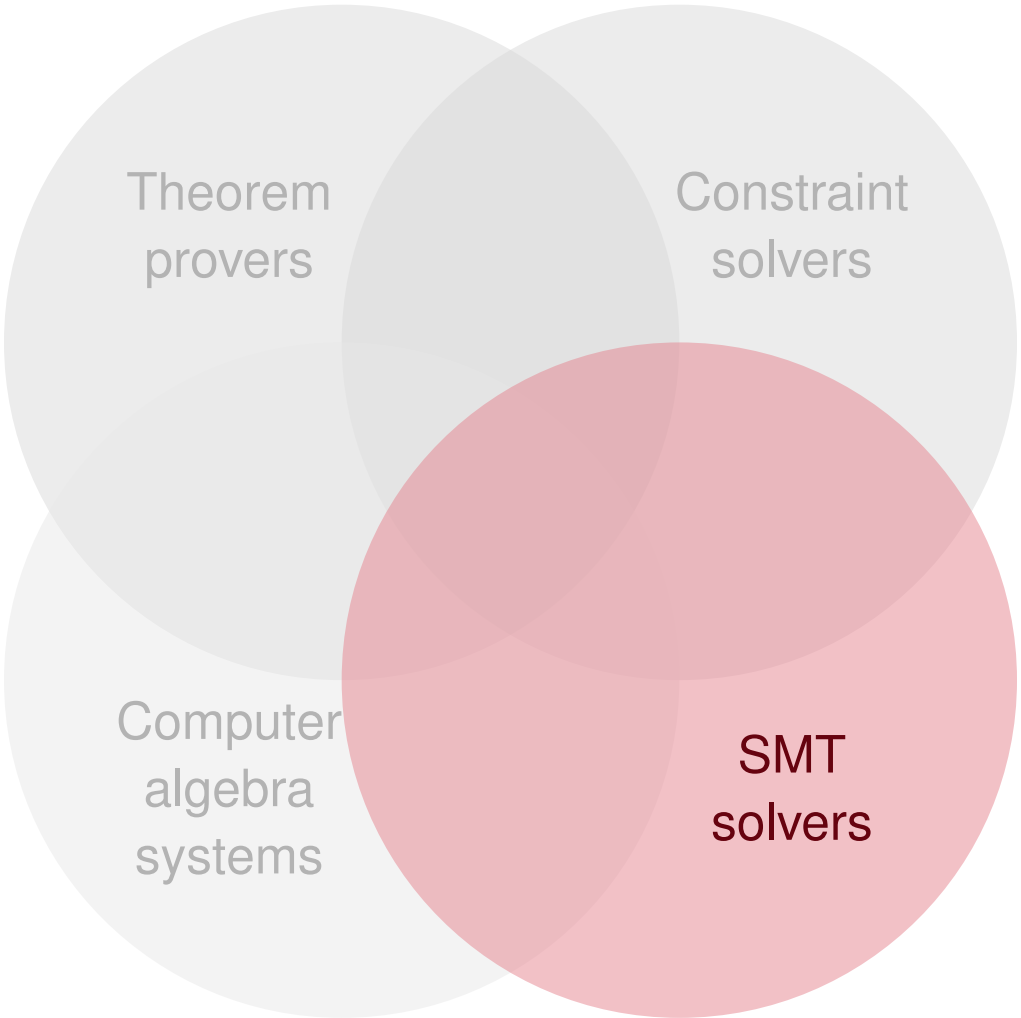
Some technologies for satisfiability checking



Some technologies for satisfiability checking



Some technologies for satisfiability checking



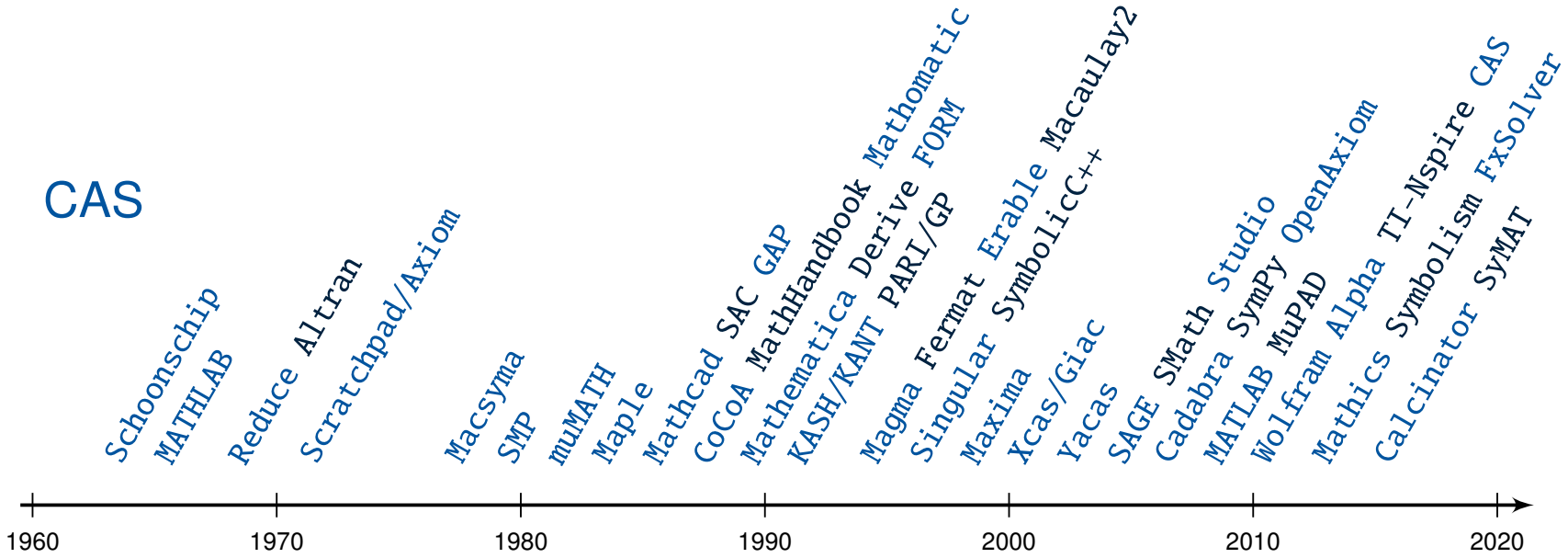
Contents

- SMT solving
- SMT-RAT
- Applications
- Future challenges

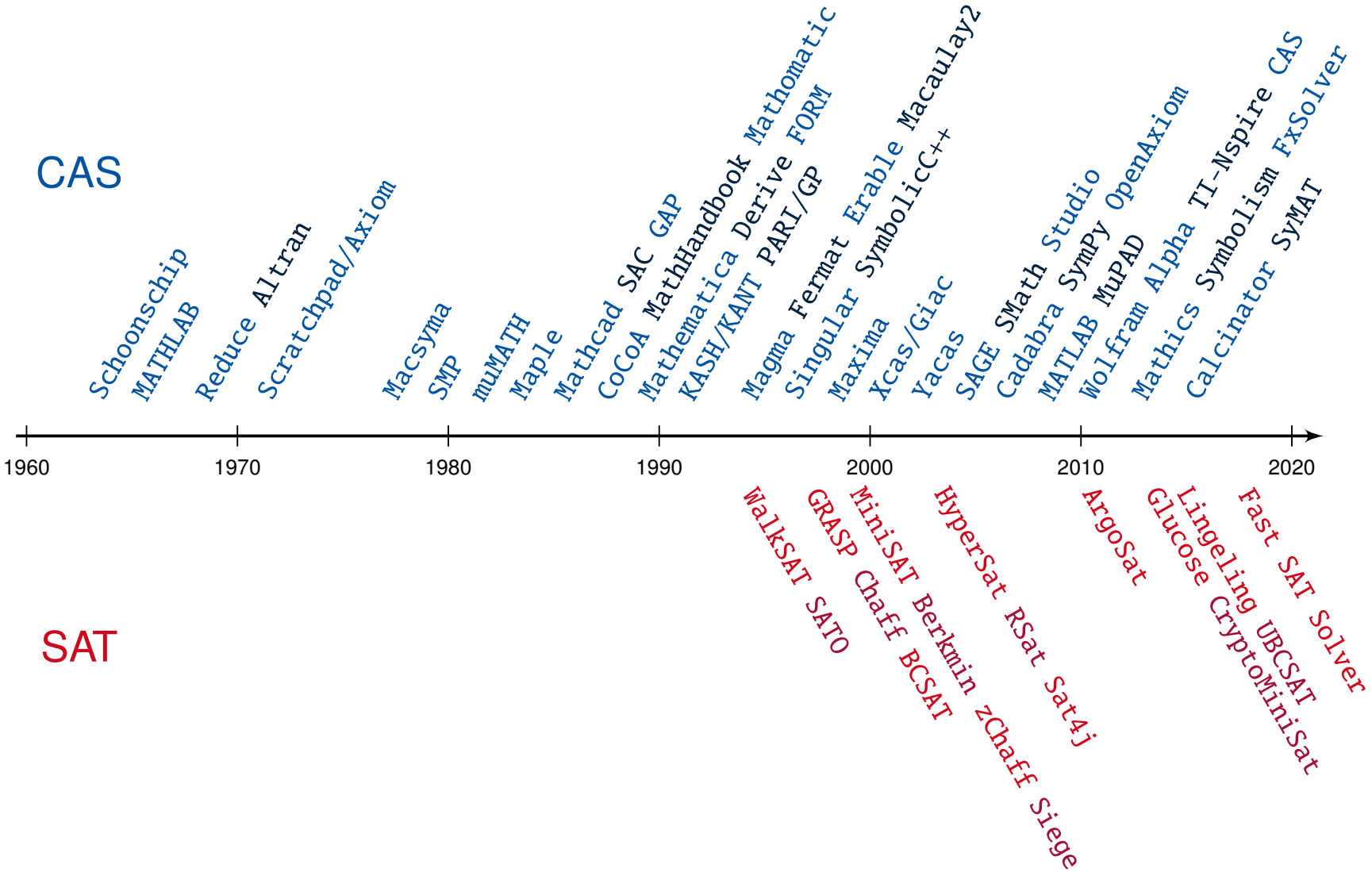
Contents

- SMT solving
- SMT-RAT
- Applications
- Future challenges

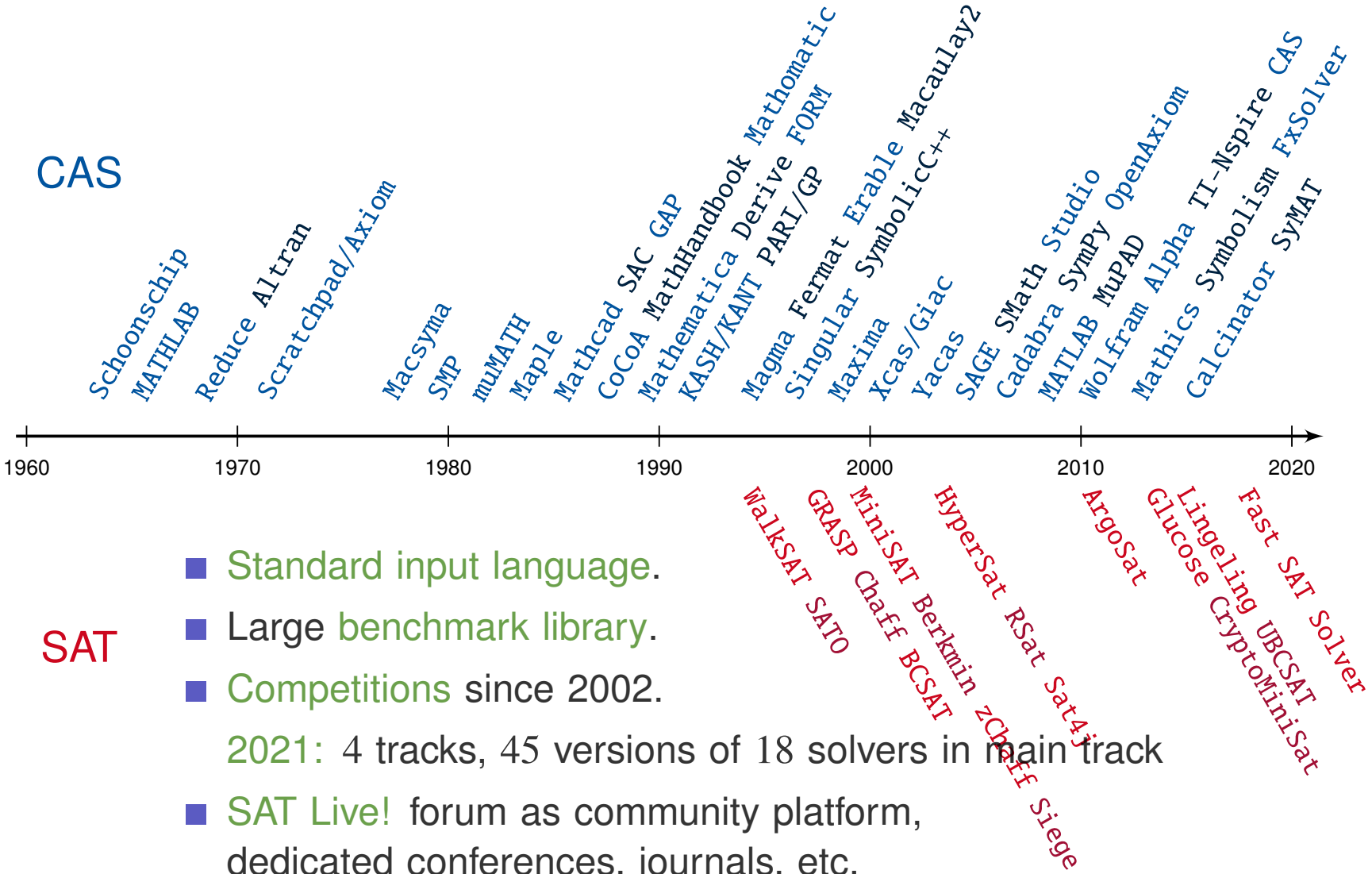
Tool development



Tool development



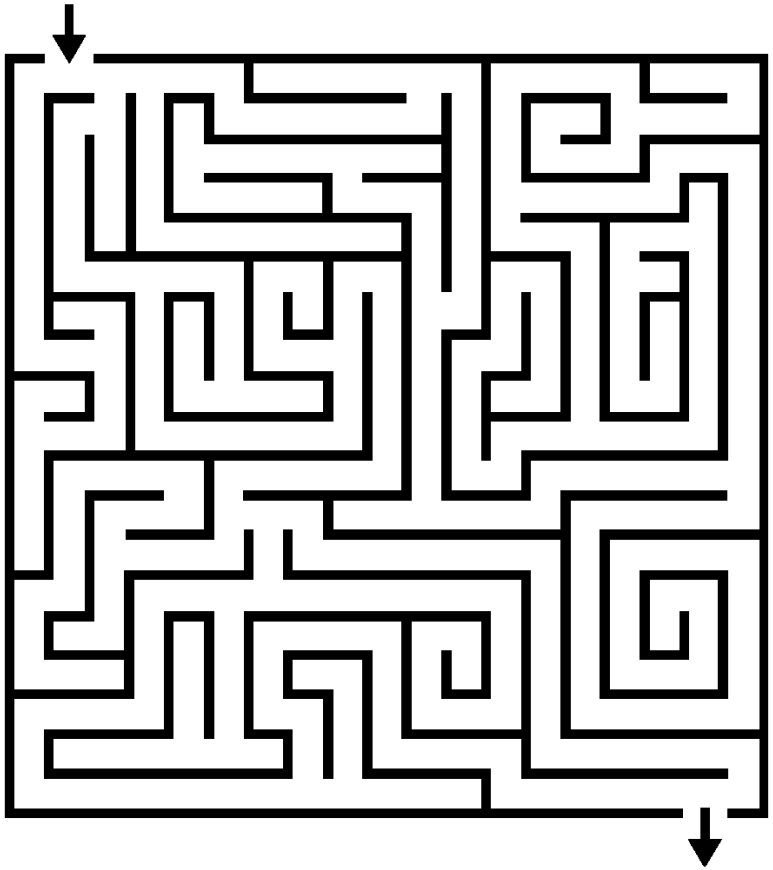
Tool development



- Standard input language.
- Large benchmark library.
- Competitions since 2002.

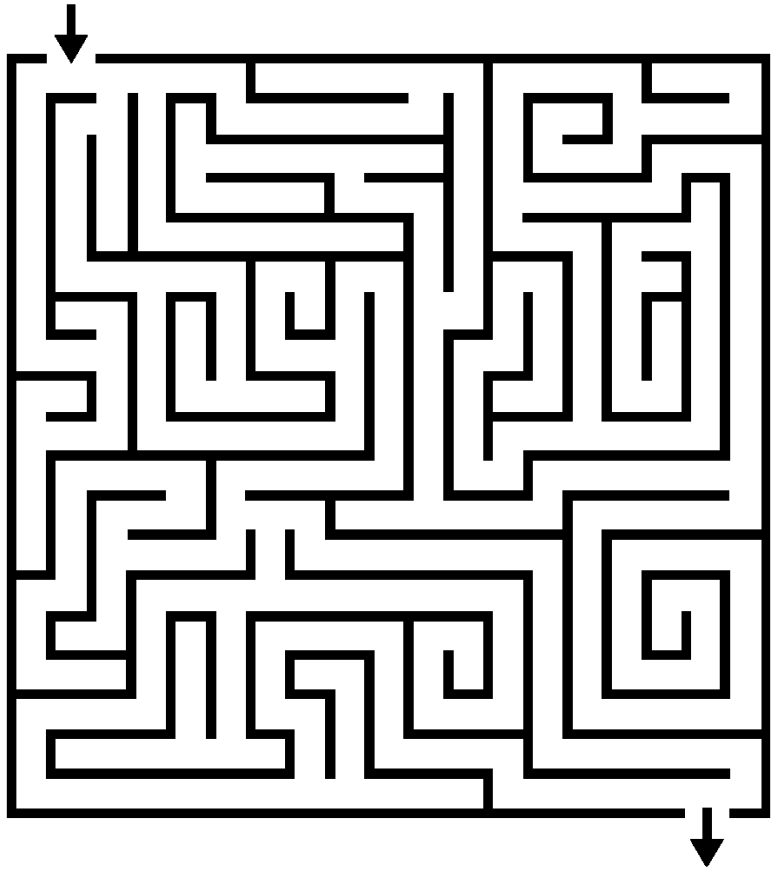
  2021: 4 tracks, 45 versions of 18 solvers in main track
- SAT Live! forum as community platform, dedicated conferences, journals, etc.

SAT solving: The DPLL+CDCL idea

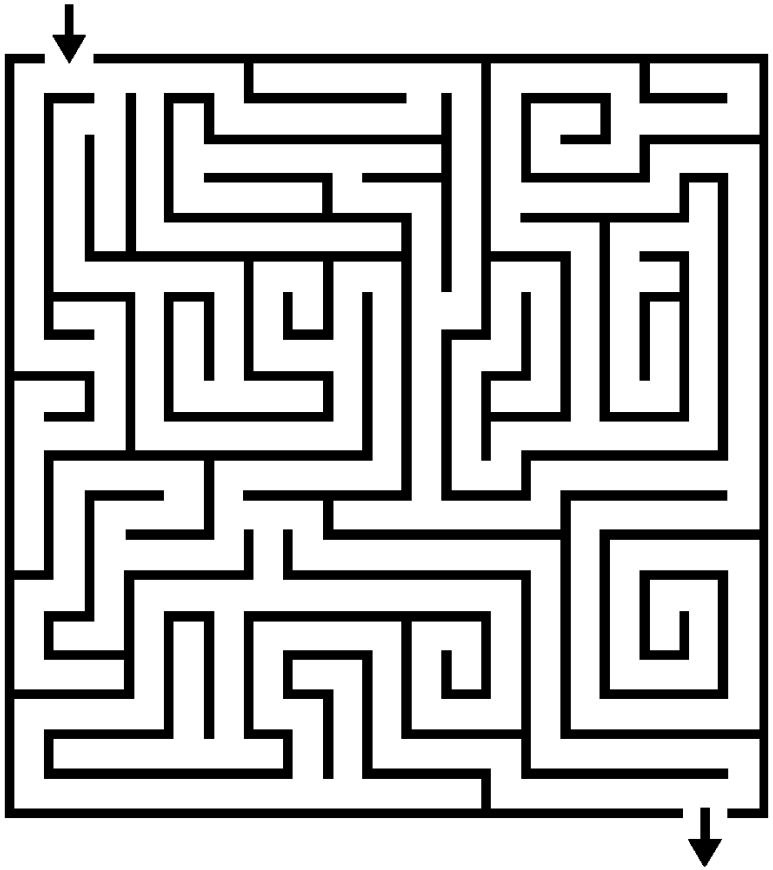


SAT solving: The DPLL+CDCL idea

Proof system



SAT solving: The DPLL+CDCL idea



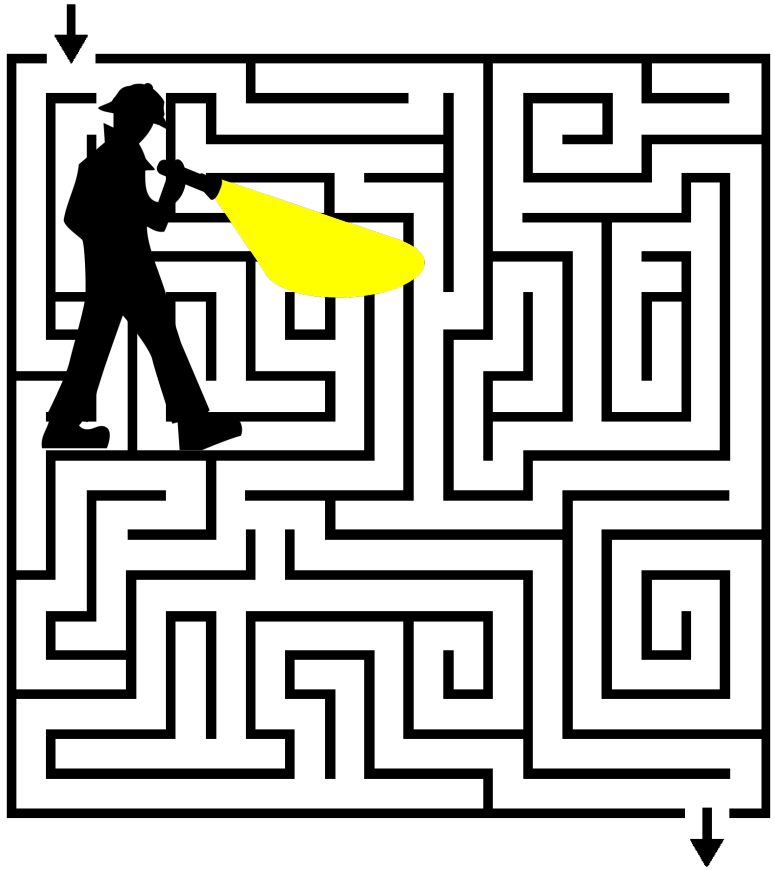
SAT solving: The DPLL+CDCL idea

Exploration

SAT solving: The DPLL+CDCL idea

Exploration

Look-ahead

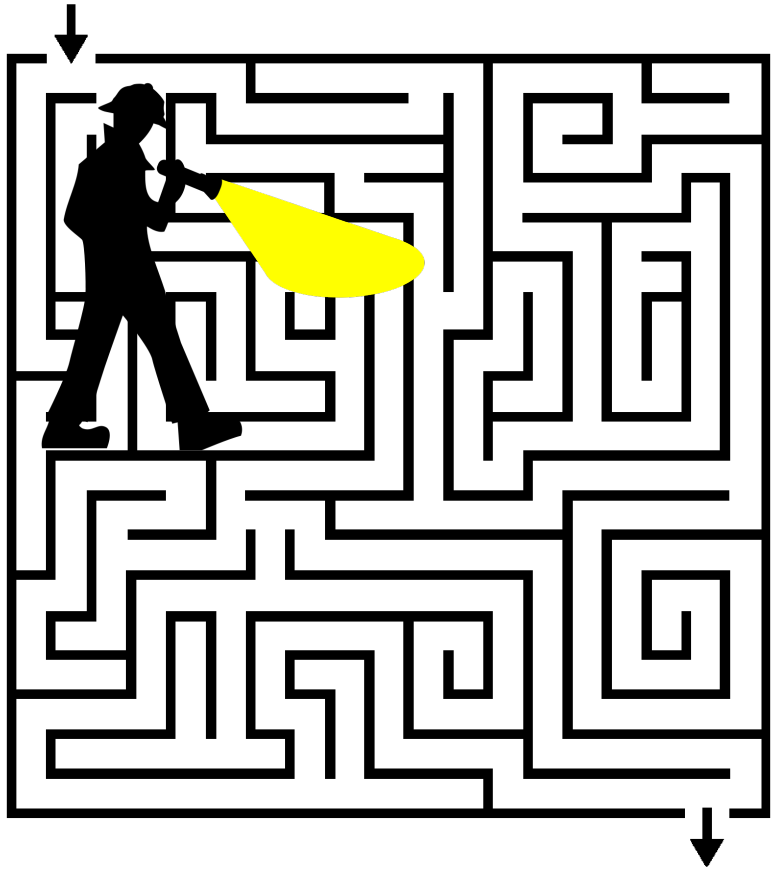


SAT solving: The DPLL+CDCL idea

Exploration

Look-ahead

Proof system



The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

$\mathbb{B}$-propagate -

The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$

The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$
$\mathbb{B}$-propagate	-

The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$
$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$b = \mathit{false}$

The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$
$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$b = \mathit{false}$
$\mathbb{B}$-propagate	$c = \mathit{true}$ 

The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

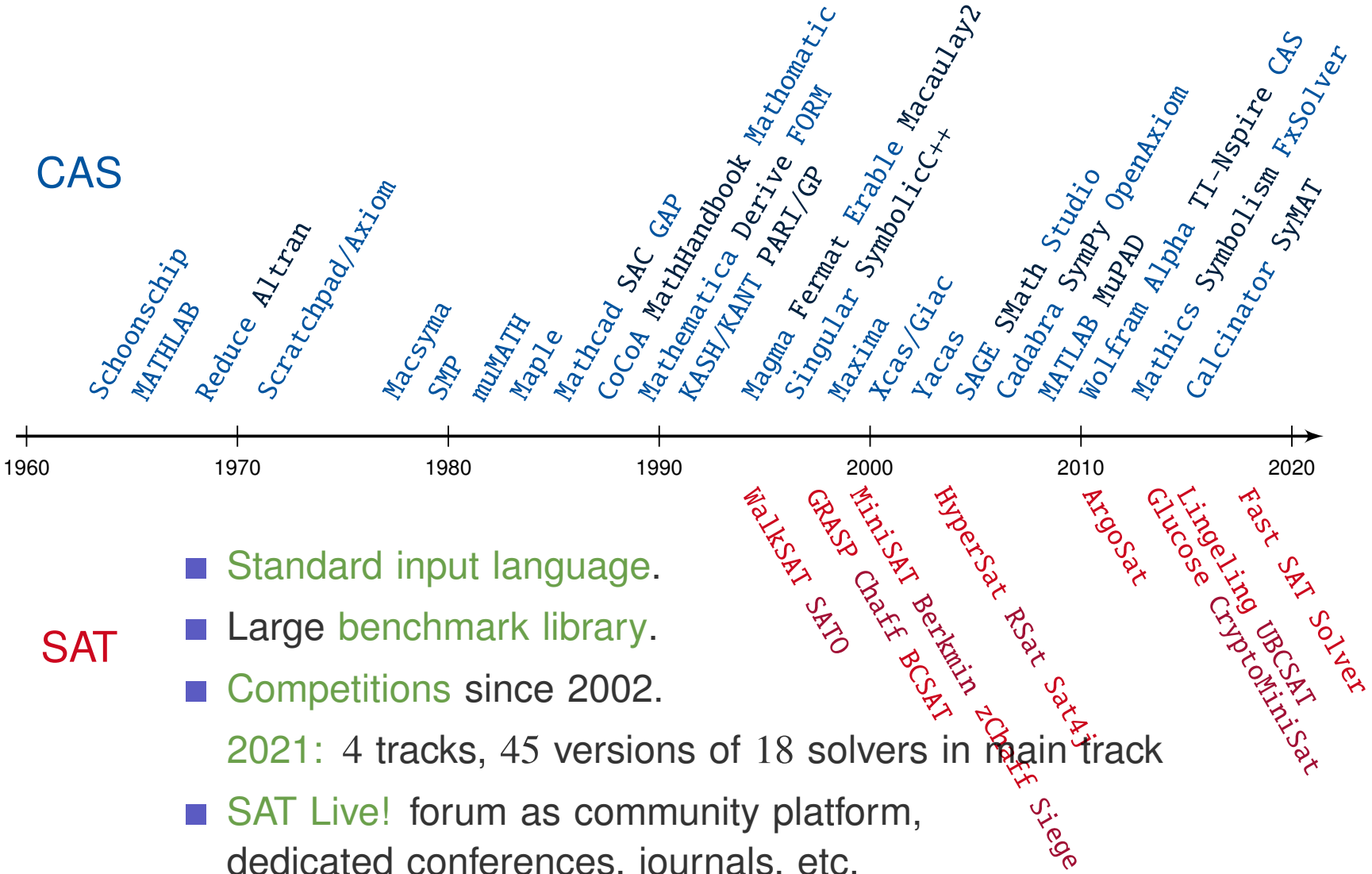
Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$
$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$b = \mathit{false}$
$\mathbb{B}$-propagate	$c = \mathit{true}$ 
$\mathbb{B}$-conflict resolution	$(a \vee b)$

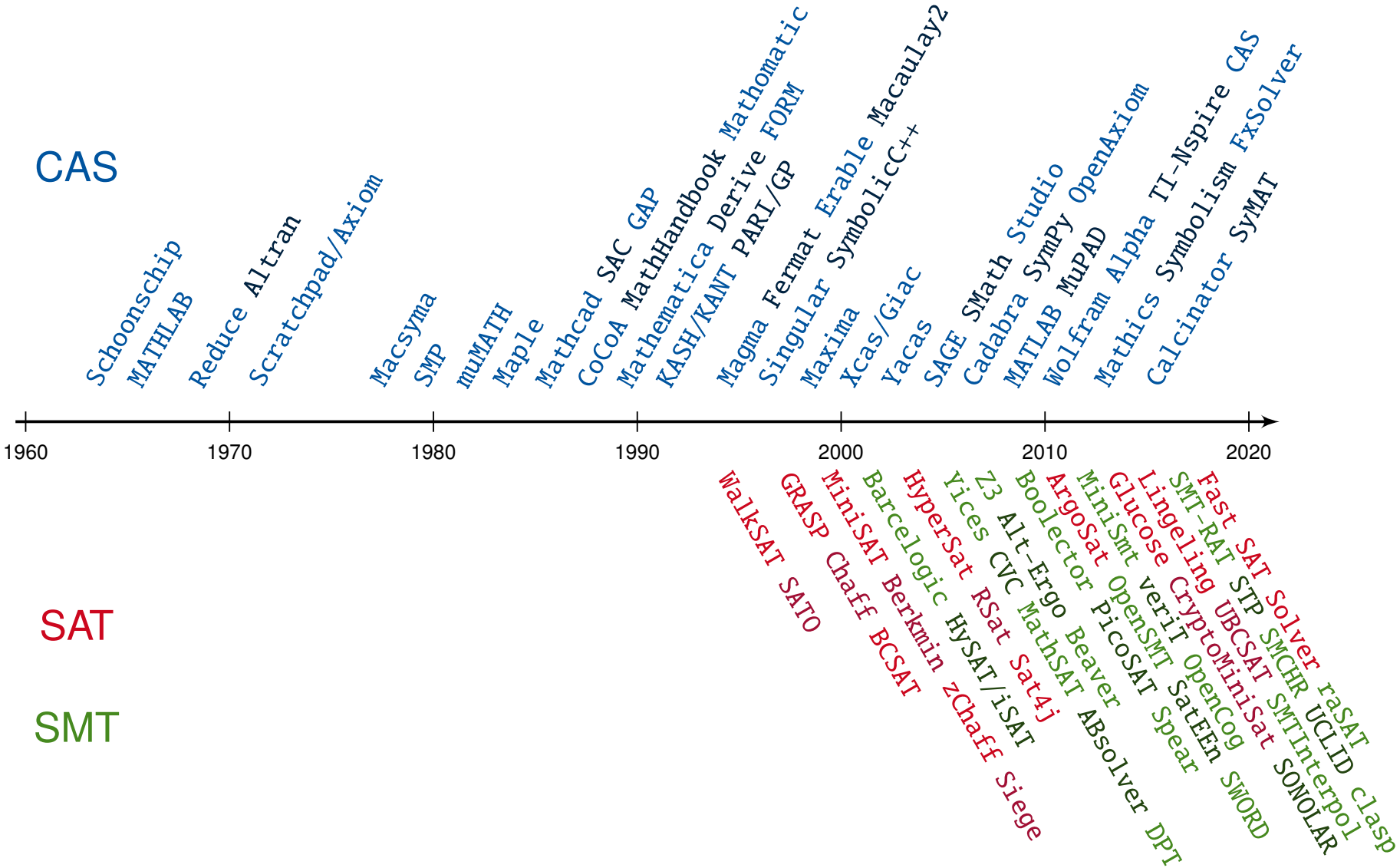
Tool development



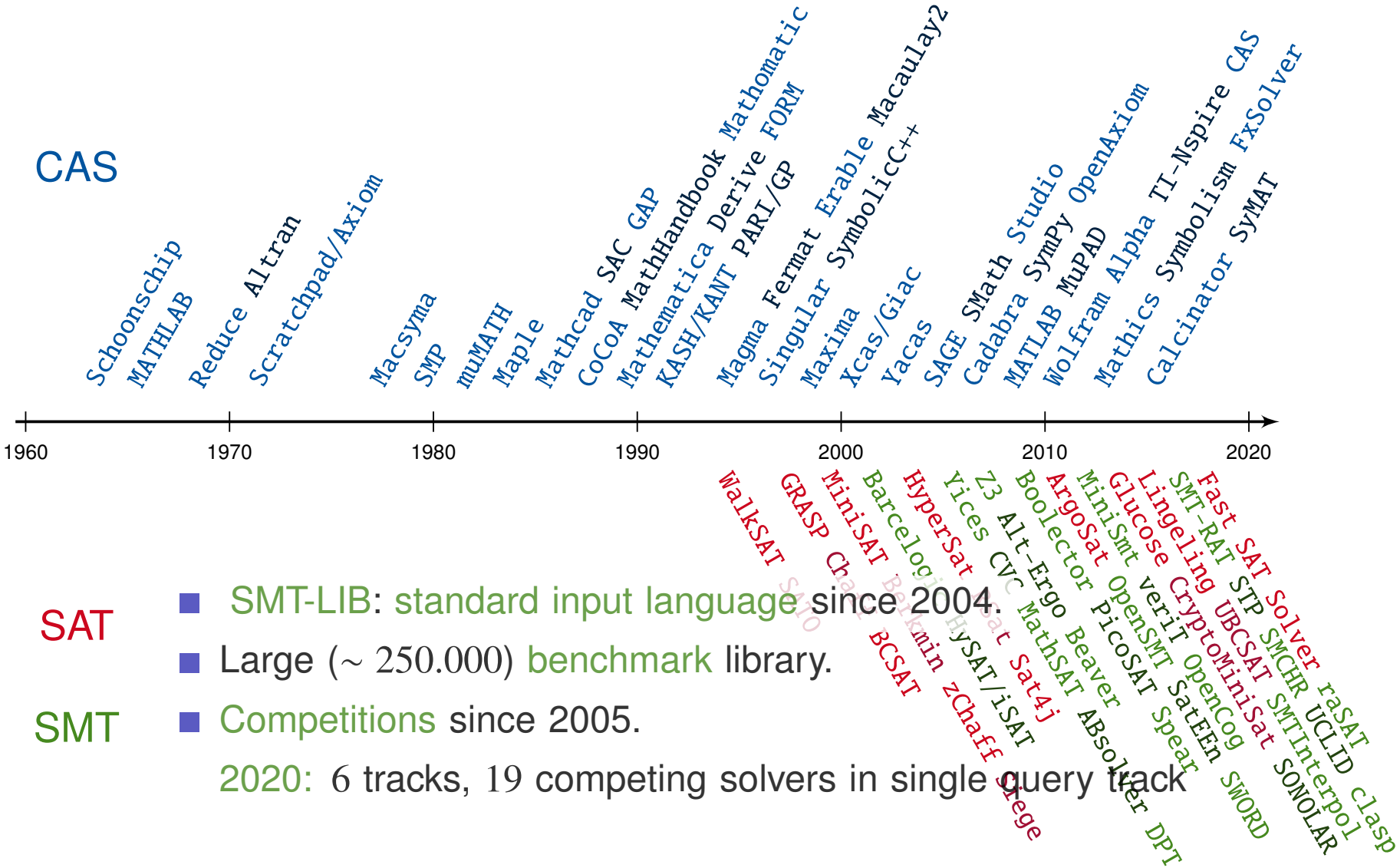
- Standard input language.
- Large benchmark library.
- Competitions since 2002.

  2021: 4 tracks, 45 versions of 18 solvers in main track
- SAT Live! forum as community platform, dedicated conferences, journals, etc.

Tool development



Tool development

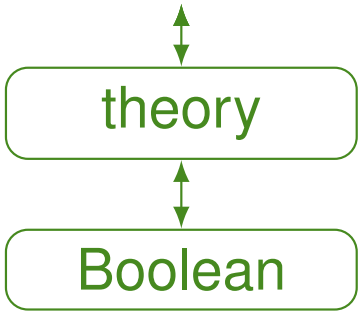


- SMT-LIB: standard input language since 2004.
- Large (~ 250.000) benchmark library.
- Competitions since 2005.

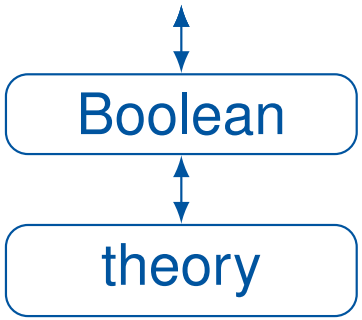
  2020: 6 tracks, 19 competing solvers in single query track

Three SMT solving approaches

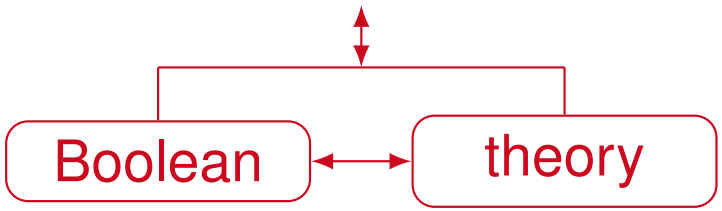
Eager SMT solving



Lazy SMT solving

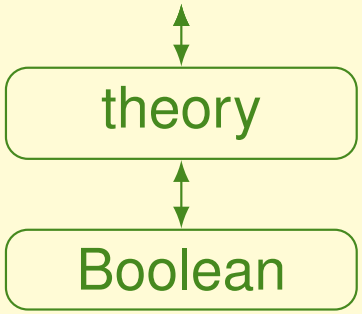


Model-constructing satisfiability calculus (MCSAT)

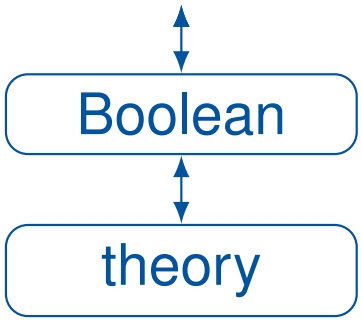


Three SMT solving approaches

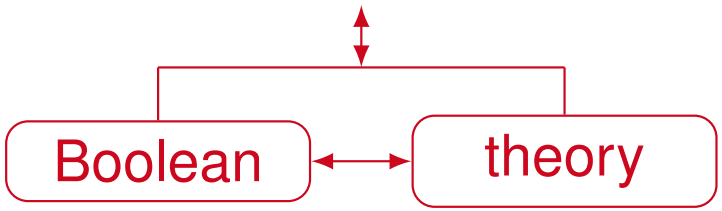
Eager SMT solving



Lazy SMT solving



Model-constructing satisfiability calculus (MCSAT)



Eager example [Bryant and Velev, 2000]

$$\varphi^E = x_1 = x_2 \wedge x_2 = x_3 \wedge x_1 \neq x_3$$

Eager example [Bryant and Velev, 2000]

$$\varphi^E = x_1 = x_2 \wedge x_2 = x_3 \wedge x_1 \neq x_3$$

$\varphi^{prop} :=$

φ^E *is satisfiable* *iff* φ^{prop} *is satisfiable*

Eager example [Bryant and Velev, 2000]

$$\varphi^E = x_1 = x_2 \wedge x_2 = x_3 \wedge x_1 \neq x_3$$

$$\varphi^{prop} := \underbrace{e_1 \wedge e_2 \wedge \neg e_3}_{\textit{Boolean abstraction}} \wedge$$

φ^E *is satisfiable* *iff* φ^{prop} *is satisfiable*

Eager example [Bryant and Velev, 2000]

$$\varphi^E = x_1 = x_2 \wedge x_2 = x_3 \wedge x_1 \neq x_3$$

$$\varphi^{prop} := \underbrace{e_1 \wedge e_2 \wedge \neg e_3}_{\textit{Boolean abstraction}} \wedge \underbrace{((e_1 \wedge e_2) \rightarrow e_3)}_{\textit{transitivity constraint}}$$

φ^E *is satisfiable* *iff* φ^{prop} *is satisfiable*

Eager example [Bryant and Velev, 2000]

$$\varphi^E = x_1 = x_2 \wedge x_2 = x_3 \wedge x_1 \neq x_3$$

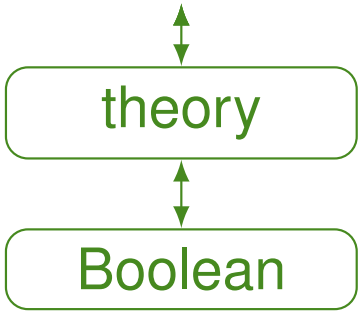
$$\varphi^{prop} := \underbrace{e_1 \wedge e_2 \wedge \neg e_3}_{\textit{Boolean abstraction}} \wedge \underbrace{((e_1 \wedge e_2) \rightarrow e_3)}_{\textit{transitivity constraint}}$$

φ^E *is satisfiable* *iff* φ^{prop} *is satisfiable*

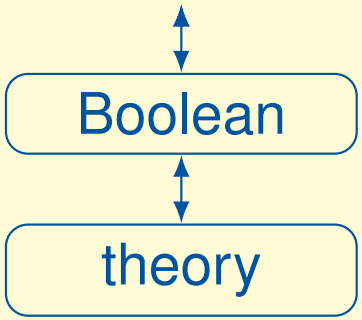
Similar approaches are available for uninterpreted functions, bit-vector arithmetic ("bit-blasting"), floating-point arithmetic and others.

Three SMT solving approaches

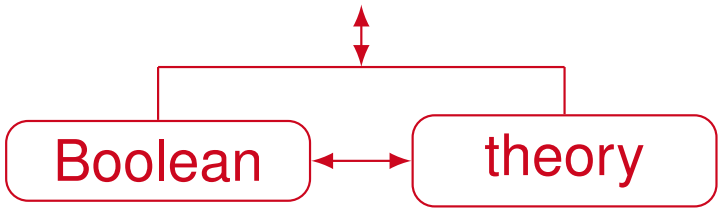
Eager SMT solving



Lazy SMT solving



Model-constructing satisfiability calculus (MCSAT)



Less lazy SMT solving

Less lazy SMT solving

$$(x < 0 \vee x > 2) \wedge (x^2 = 1 \vee x^2 < 0)$$

Less lazy SMT solving

$$(x < 0 \vee x > 2) \wedge (x^2 = 1 \vee x^2 < 0)$$

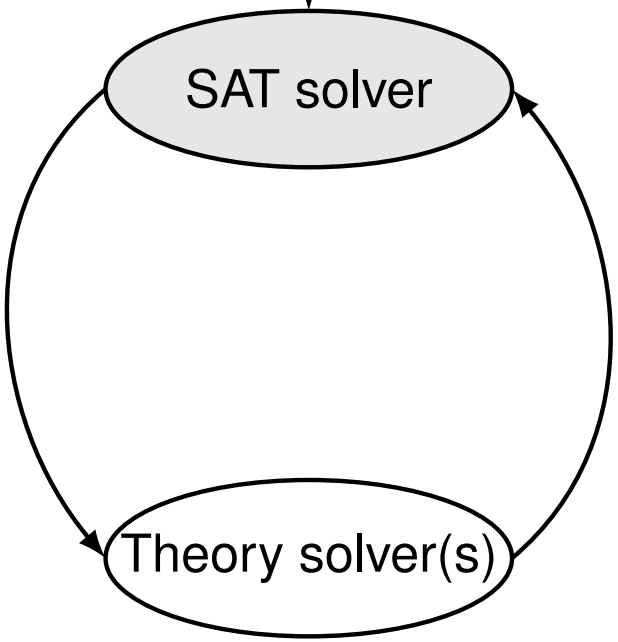
$$\downarrow$$

$$(\ a\ \vee\ b\ ) \wedge (\ c\ \vee\ d\ )$$

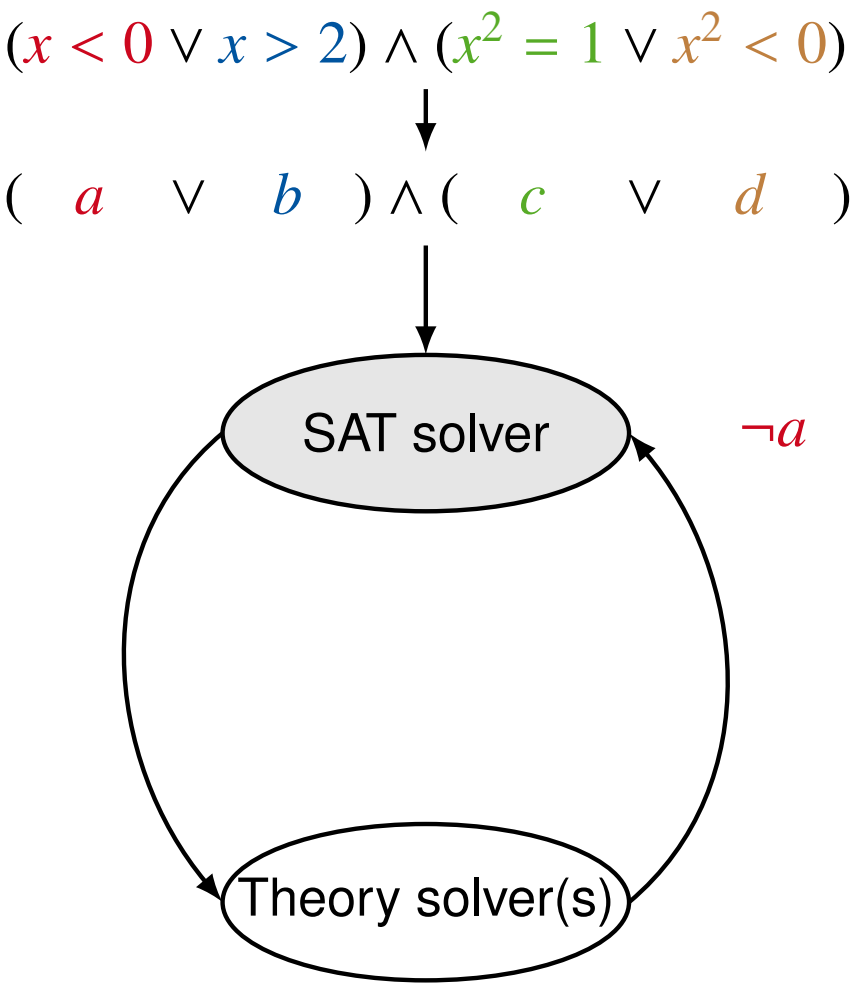
Less lazy SMT solving

$$(x < 0 \vee x > 2) \wedge (x^2 = 1 \vee x^2 < 0)$$

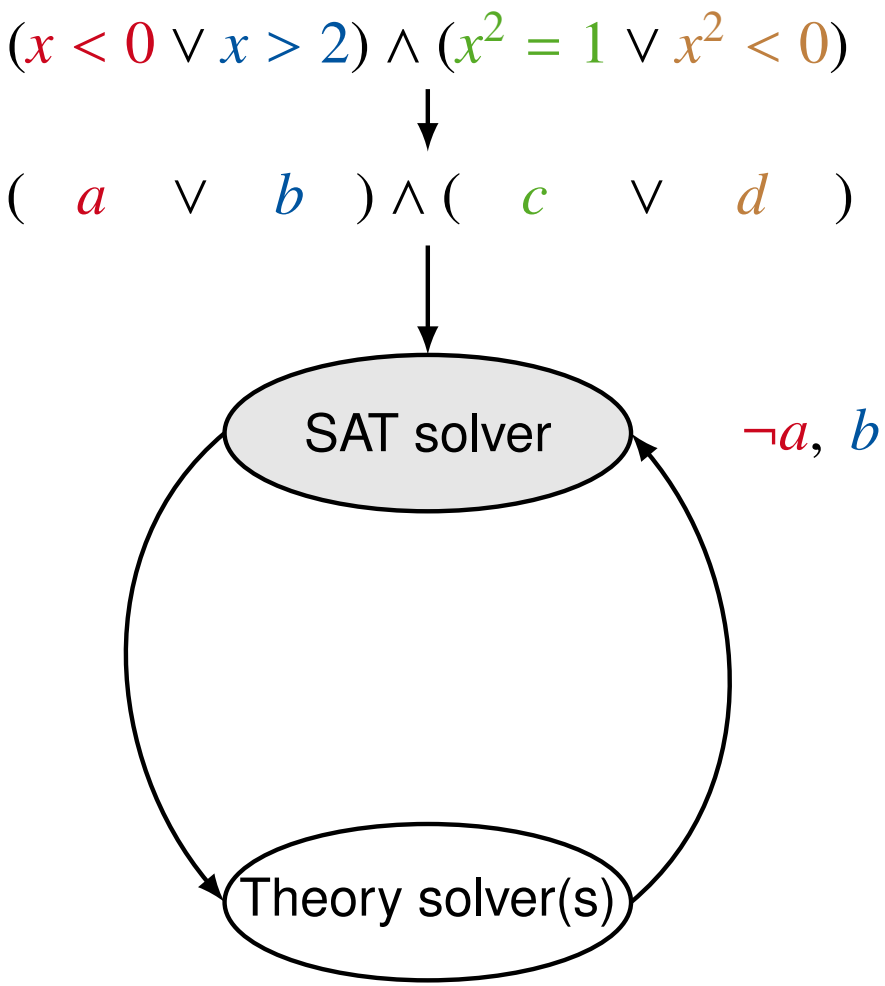
$$(\ a\ \vee\ b\ ) \wedge (\ c\ \vee\ d\ )$$



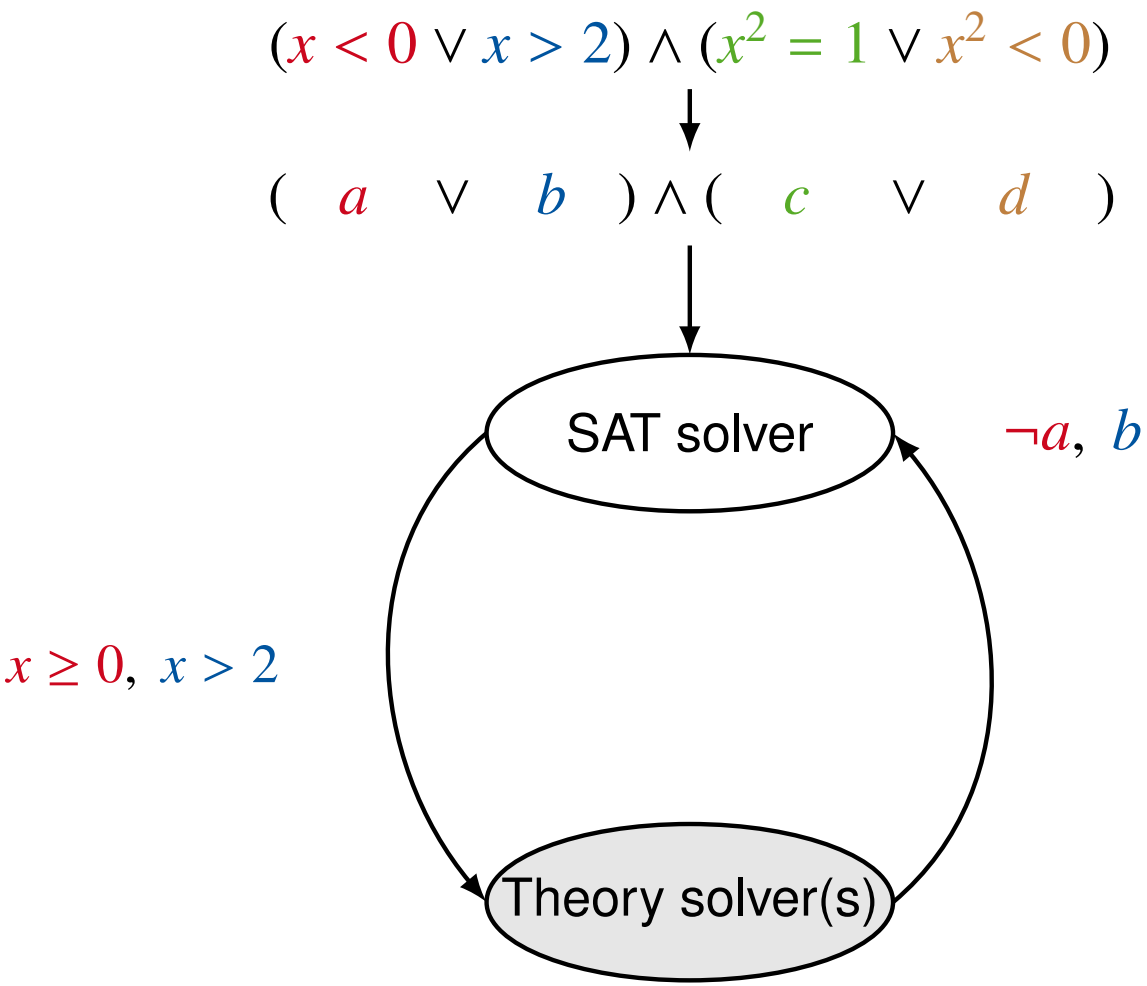
Less lazy SMT solving



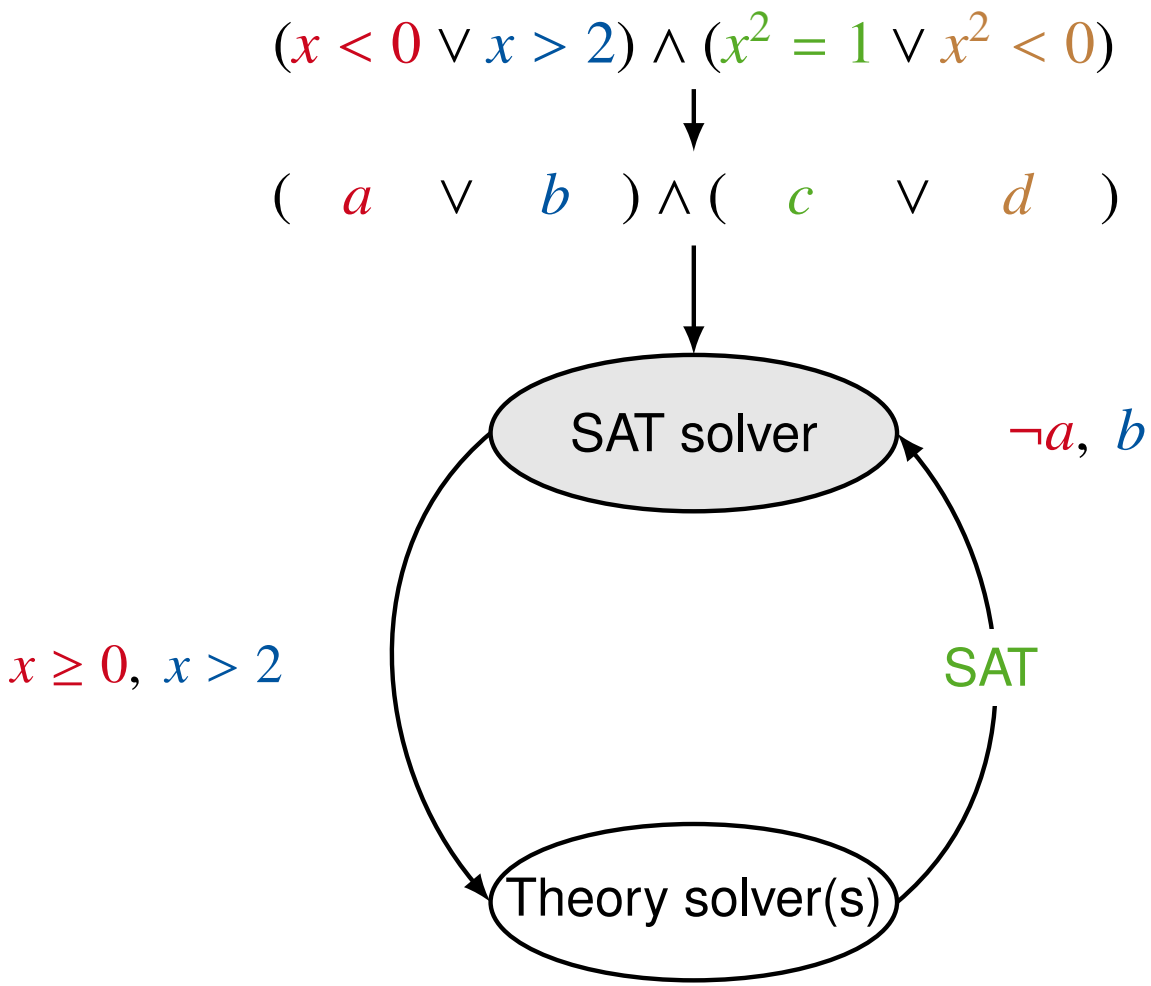
Less lazy SMT solving



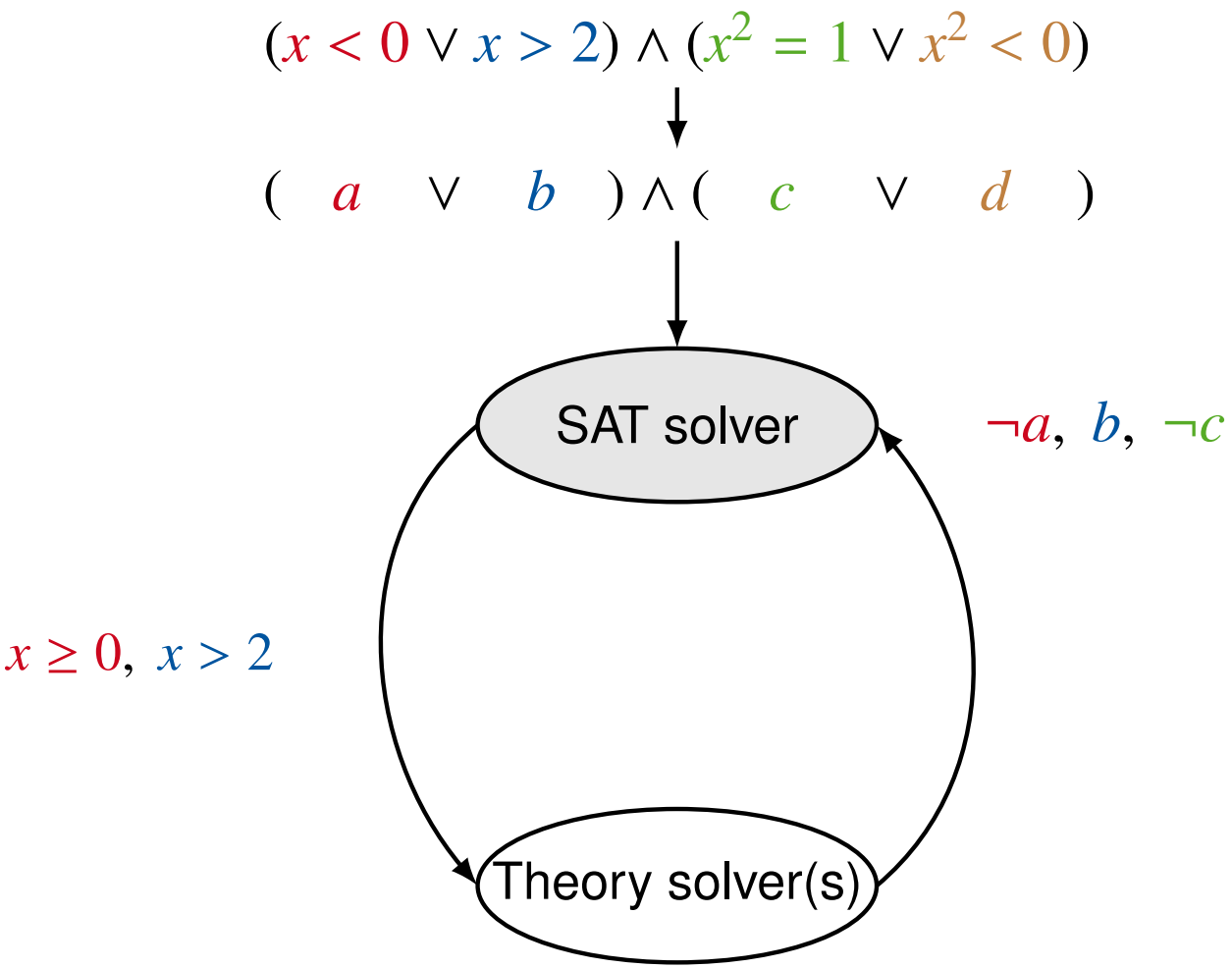
Less lazy SMT solving



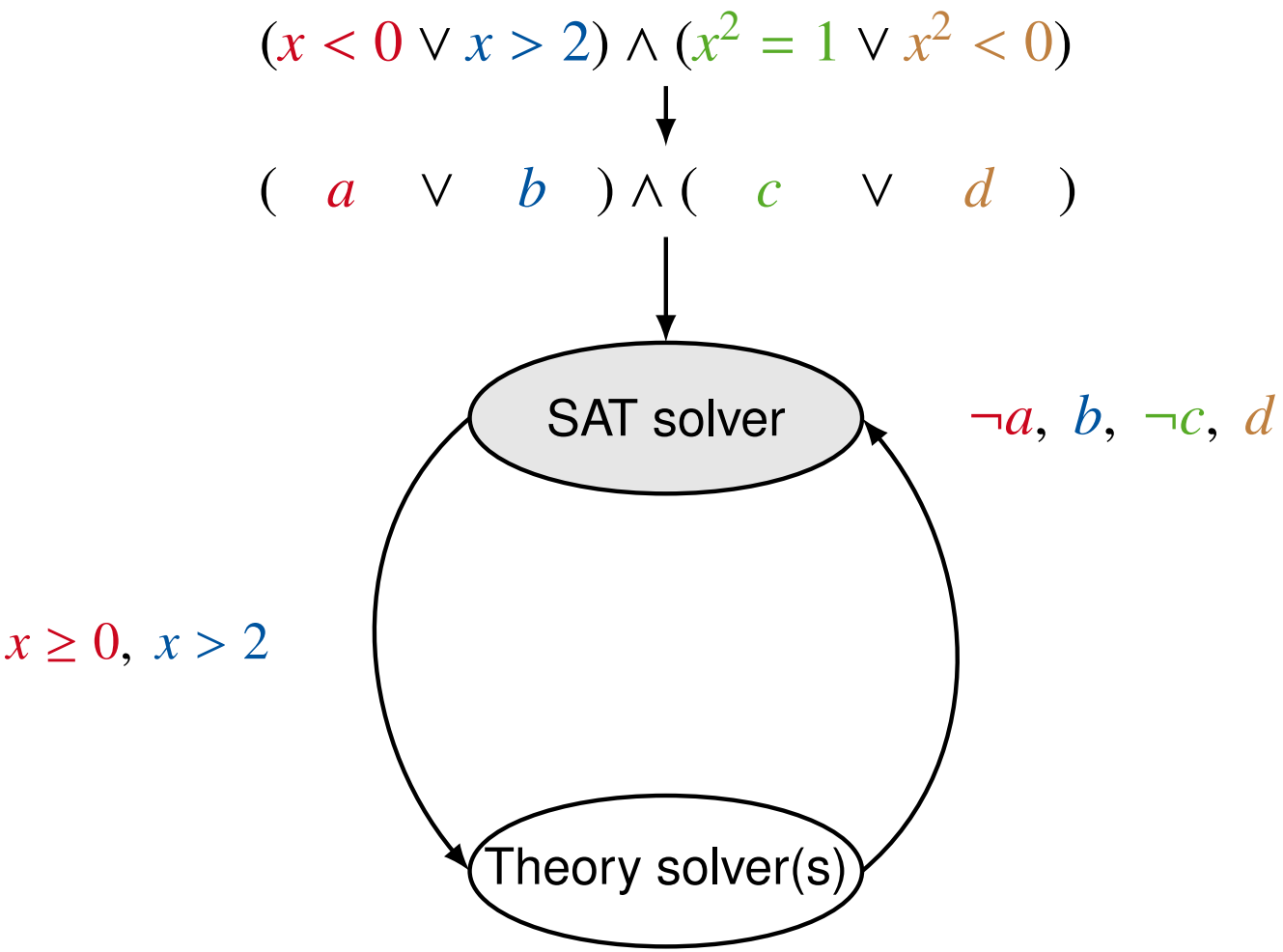
Less lazy SMT solving



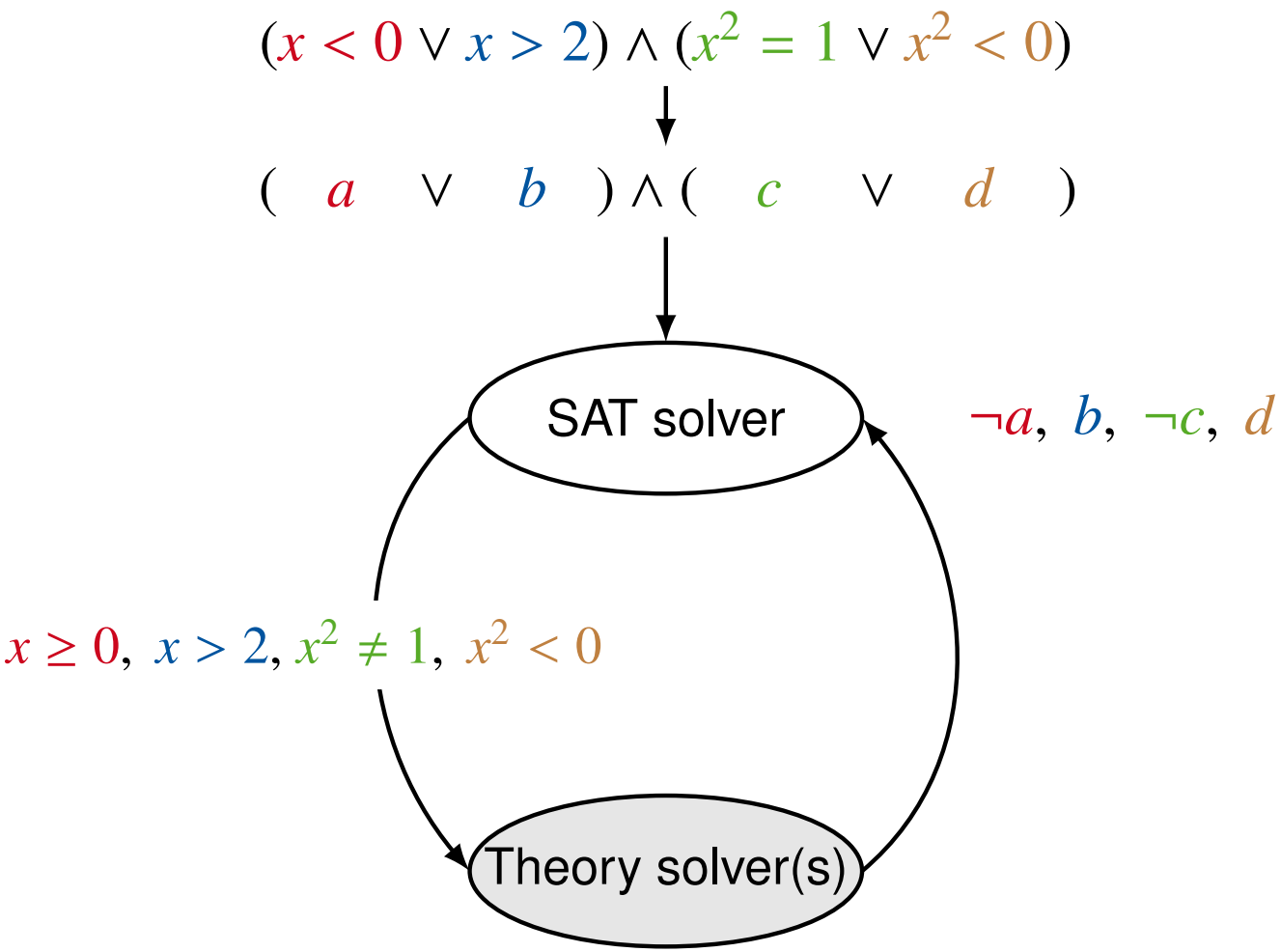
Less lazy SMT solving



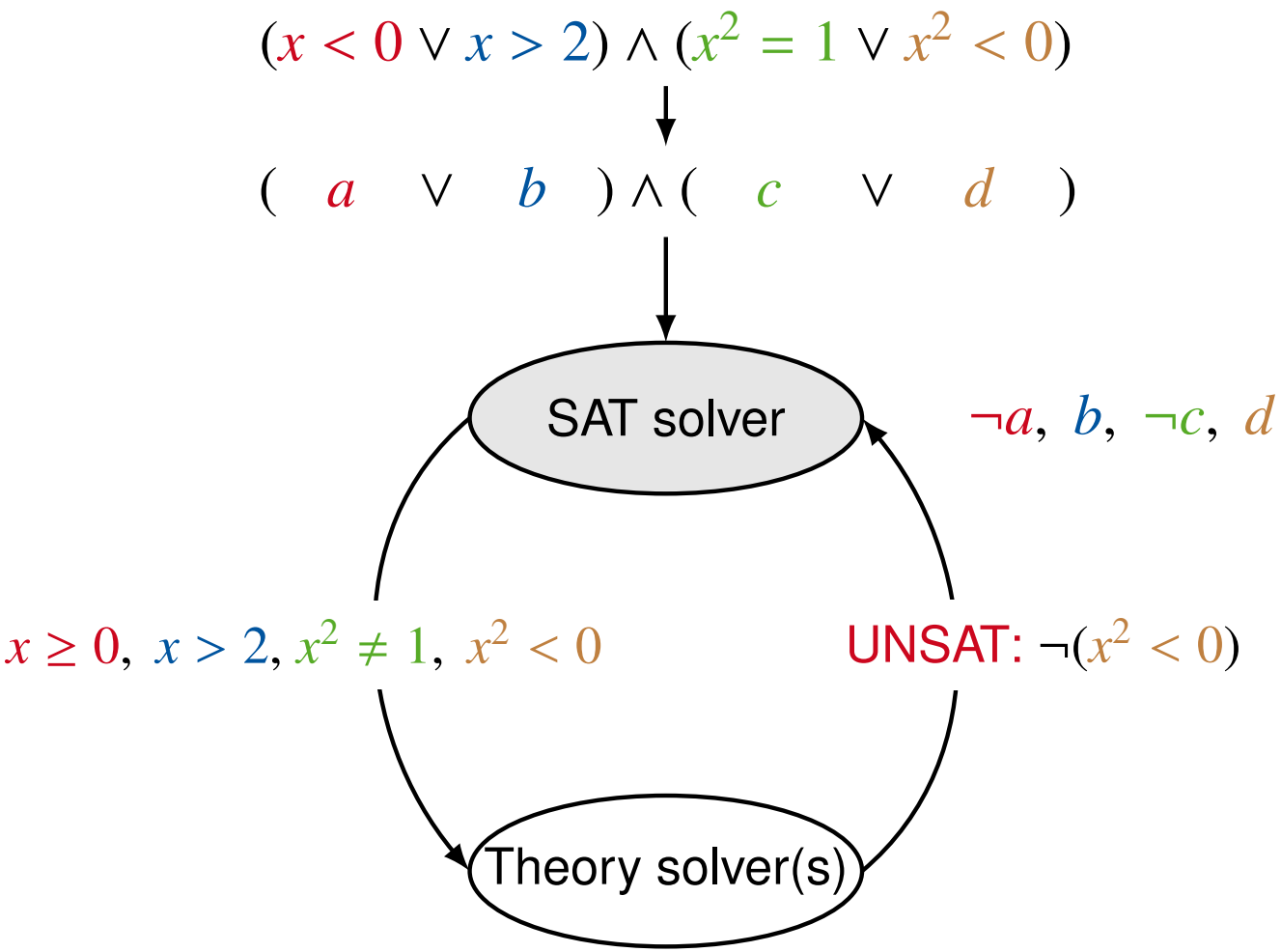
Less lazy SMT solving



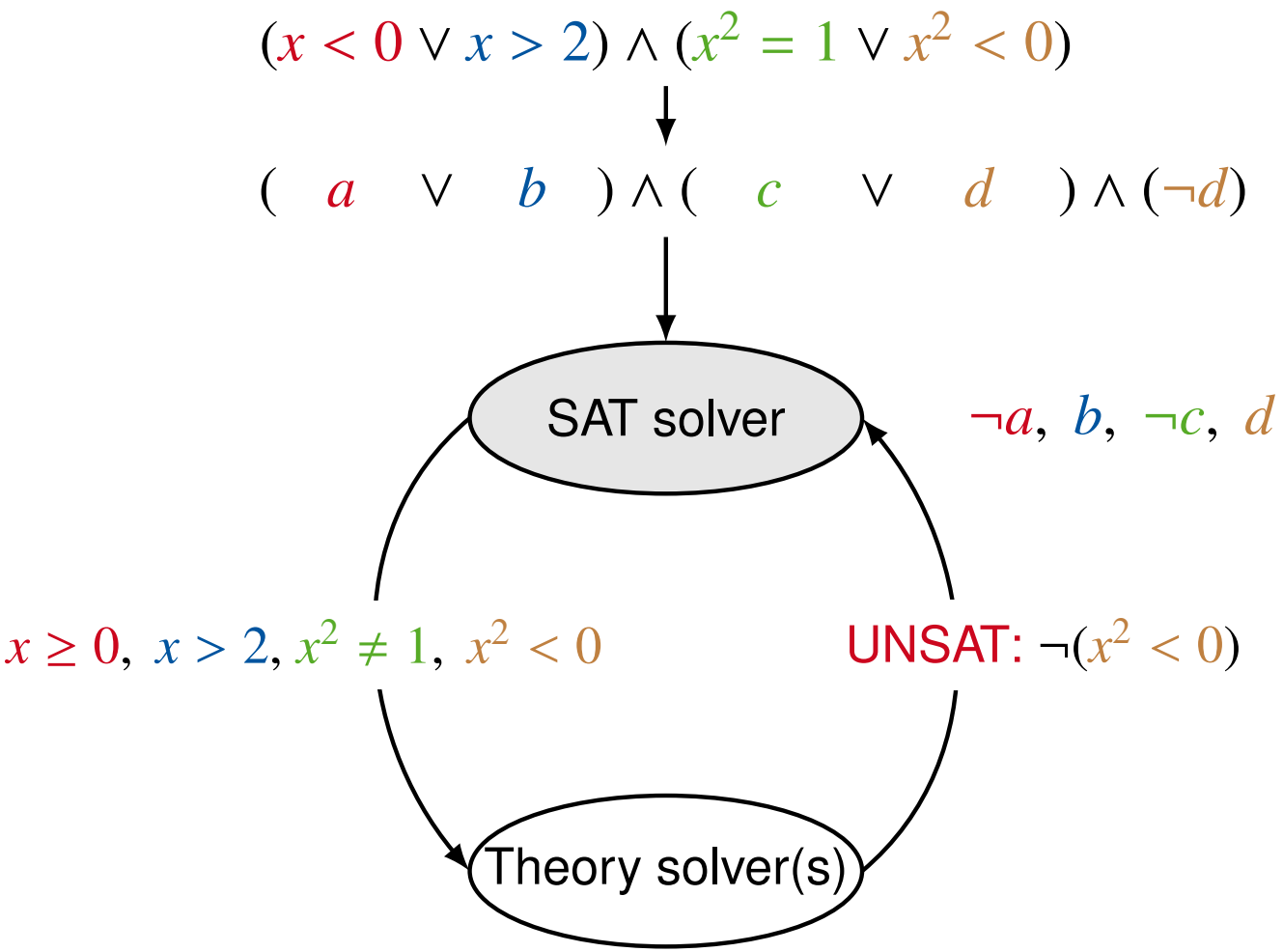
Less lazy SMT solving



Less lazy SMT solving

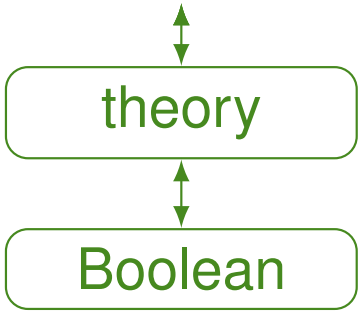


Less lazy SMT solving

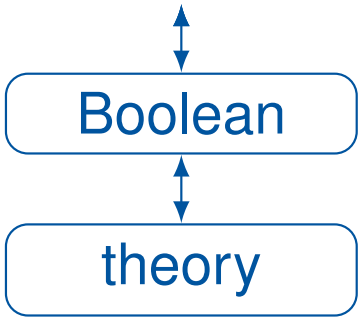


Three SMT solving approaches

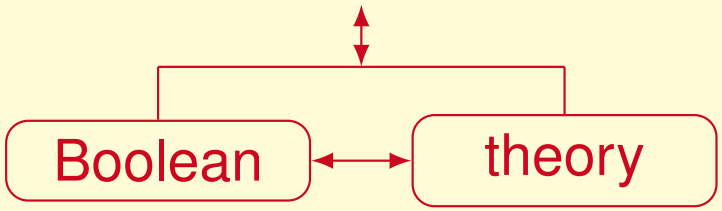
Eager SMT solving



Lazy SMT solving



Model-constructing satisfiability calculus (MCSAT)



The DPLL+CDCL idea [Davis et al., '60/61] [Marques-Silva et al., '96]

Exploration: $\mathbb{B}$-decision

Look-ahead: $\mathbb{B}$-propagation

Proof system: $\mathbb{B}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$
$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$b = \mathit{false}$
$\mathbb{B}$-propagate	$c = \mathit{true}$ 
$\mathbb{B}$-conflict resolution	$(a \vee b)$

The MCSAT idea [de Moura, Jovanović, VMCAI'13]

	$\mathbb{B}$	$\mathbb{T}$
Exploration:	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Look-ahead:	$\mathbb{B}$-propagation	$\mathbb{T}$-propagation
Proof system:	$\mathbb{B}$-conflict resolution	$\mathbb{T}$-conflict resolution

$$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$$

$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$
$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$b = \mathit{false}$
$\mathbb{B}$-propagate	$c = \mathit{true}$ ↯
$\mathbb{B}$-conflict resolution	$(a \vee b)$

The MCSAT idea [de Moura, Jovanović, VMCAI'13]

	$\mathbb{B}$	$\mathbb{T}$
Exploration:	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Look-ahead:	$\mathbb{B}$-propagation	$\mathbb{T}$-propagation
Proof system:	$\mathbb{B}$-conflict resolution	$\mathbb{T}$-conflict resolution

$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$ $\quad\quad$ $\ldots\ x \cdot y^2 < 0\ \ldots$

$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$
$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$b = \mathit{false}$
$\mathbb{B}$-propagate	$c = \mathit{true}$ ↯
$\mathbb{B}$-conflict resolution	$(a \vee b)$

The MCSAT idea [de Moura, Jovanović, VMCAI'13]

Exploration:	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Look-ahead:	$\mathbb{B}$-propagation	$\mathbb{T}$-propagation
Proof system:	$\mathbb{B}$-conflict resolution	$\mathbb{T}$-conflict resolution

$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$ $\quad\quad$ $\ldots\ x \cdot y^2 < 0\ \ldots$

$\mathbb{B}$-propagate	-	$\mathbb{B}$-propagate -
$\mathbb{B}$-decision	$a = \mathit{false}$	
$\mathbb{B}$-propagate	-	
$\mathbb{B}$-decision	$b = \mathit{false}$	
$\mathbb{B}$-propagate	$c = \mathit{true}$	
$\mathbb{B}$-conflict resolution	$(a \vee b)$	

The MCSAT idea [de Moura, Jovanović, VMCAI'13]

	$\mathbb{B}$	$\mathbb{T}$
Exploration:	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Look-ahead:	$\mathbb{B}$-propagation	$\mathbb{T}$-propagation
Proof system:	$\mathbb{B}$-conflict resolution	$\mathbb{T}$-conflict resolution

$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$ $\quad\quad$ $\ldots\ x \cdot y^2 < 0\ \ldots$

$\mathbb{B}$-propagate	-	$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$	$\mathbb{B}$-decision	$x \cdot y^2 < 0$
$\mathbb{B}$-propagate	-		
$\mathbb{B}$-decision	$b = \mathit{false}$		
$\mathbb{B}$-propagate	$c = \mathit{true}$ ↯		
$\mathbb{B}$-conflict resolution	$(a \vee b)$		

The MCSAT idea [de Moura, Jovanović, VMCAI'13]

	$\mathbb{B}$	$\mathbb{T}$
Exploration:	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Look-ahead:	$\mathbb{B}$-propagation	$\mathbb{T}$-propagation
Proof system:	$\mathbb{B}$-conflict resolution	$\mathbb{T}$-conflict resolution

$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$ $\quad\quad$ $\ldots\ x \cdot y^2 < 0\ \ldots$

$\mathbb{B}$-propagate	-	$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$	$\mathbb{B}$-decision	$x \cdot y^2 < 0$
$\mathbb{B}$-propagate	-	$\mathbb{T}$-propagate	$x \in (-\infty, \infty)$
$\mathbb{B}$-decision	$b = \mathit{false}$		
$\mathbb{B}$-propagate	$c = \mathit{true}$ ↯		
$\mathbb{B}$-conflict resolution	$(a \vee b)$		

The MCSAT idea [de Moura, Jovanović, VMCAI'13]

	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Exploration:	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Look-ahead:	$\mathbb{B}$-propagation	$\mathbb{T}$-propagation
Proof system:	$\mathbb{B}$-conflict resolution	$\mathbb{T}$-conflict resolution

$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$ $\quad\quad$ $\ldots\ x \cdot y^2 < 0\ \ldots$

$\mathbb{B}$-propagate	-	$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$	$\mathbb{B}$-decision	$x \cdot y^2 < 0$
$\mathbb{B}$-propagate	-	$\mathbb{T}$-propagate	$x \in (-\infty, \infty)$
$\mathbb{B}$-decision	$b = \mathit{false}$	$\mathbb{T}$-decision	$x = 1$
$\mathbb{B}$-propagate	$c = \mathit{true}$ ↯		
$\mathbb{B}$-conflict resolution	$(a \vee b)$		

The MCSAT idea [de Moura, Jovanović, VMCAI'13]

	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Exploration:	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Look-ahead:	$\mathbb{B}$-propagation	$\mathbb{T}$-propagation
Proof system:	$\mathbb{B}$-conflict resolution	$\mathbb{T}$-conflict resolution

$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$ $\quad\quad$ $\ldots\ x \cdot y^2 < 0\ \ldots$

$\mathbb{B}$-propagate	-	$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$	$\mathbb{B}$-decision	$x \cdot y^2 < 0$
$\mathbb{B}$-propagate	-	$\mathbb{T}$-propagate	$x \in (-\infty, \infty)$
$\mathbb{B}$-decision	$b = \mathit{false}$	$\mathbb{T}$-decision	$x = 1$
$\mathbb{B}$-propagate	$c = \mathit{true}$ ↯	$\mathbb{T}$-propagate	$y \in \emptyset$ ↯
$\mathbb{B}$-conflict resolution	$(a \vee b)$		

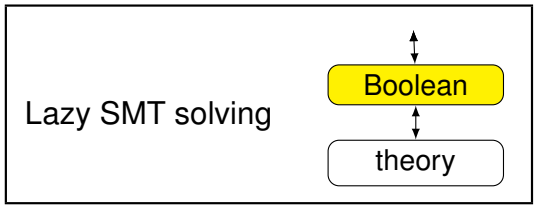
The MCSAT idea [de Moura, Jovanović, VMCAI'13]

Exploration:	$\mathbb{B}$-decision	$\mathbb{T}$-decision
Look-ahead:	$\mathbb{B}$-propagation	$\mathbb{T}$-propagation
Proof system:	$\mathbb{B}$-conflict resolution	$\mathbb{T}$-conflict resolution

$(a \vee b \vee c) \wedge (a \vee b \vee \neg c)$ $\quad\quad$ $\ldots\ x \cdot y^2 < 0\ \ldots$

$\mathbb{B}$-propagate	-	$\mathbb{B}$-propagate	-
$\mathbb{B}$-decision	$a = \mathit{false}$	$\mathbb{B}$-decision	$x \cdot y^2 < 0$
$\mathbb{B}$-propagate	-	$\mathbb{T}$-propagate	$x \in (-\infty, \infty)$
$\mathbb{B}$-decision	$b = \mathit{false}$	$\mathbb{T}$-decision	$x = 1$
$\mathbb{B}$-propagate	$c = \mathit{true}$ ↯	$\mathbb{T}$-propagate	$y \in \emptyset$ ↯
$\mathbb{B}$-conflict resolution	$(a \vee b)$	$\mathbb{T}$-conflict resolution	$(x \cdot y^2 < 0 \rightarrow x < 0)$

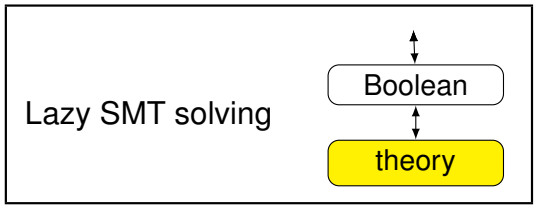
Fourier-Motzkin as theory solver in lazy SMT



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$

$x_1 \leq 2x_2$ $\quad x_2 \leq 0$

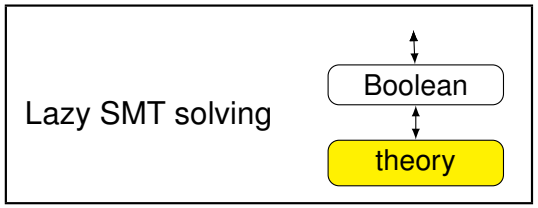
Fourier-Motzkin as theory solver in lazy SMT



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$

$x_1 \leq 2x_2$ $\quad x_2 \leq 0$

Fourier-Motzkin as theory solver in lazy SMT

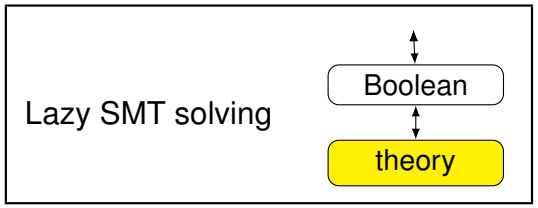


$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

x_2: $\quad x_2 \leq 0$

Fourier-Motzkin as theory solver in lazy SMT

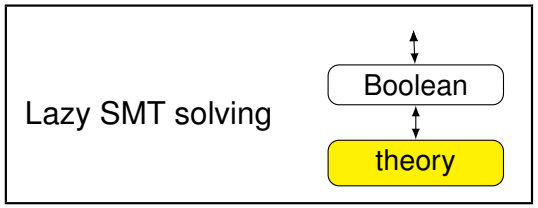


$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

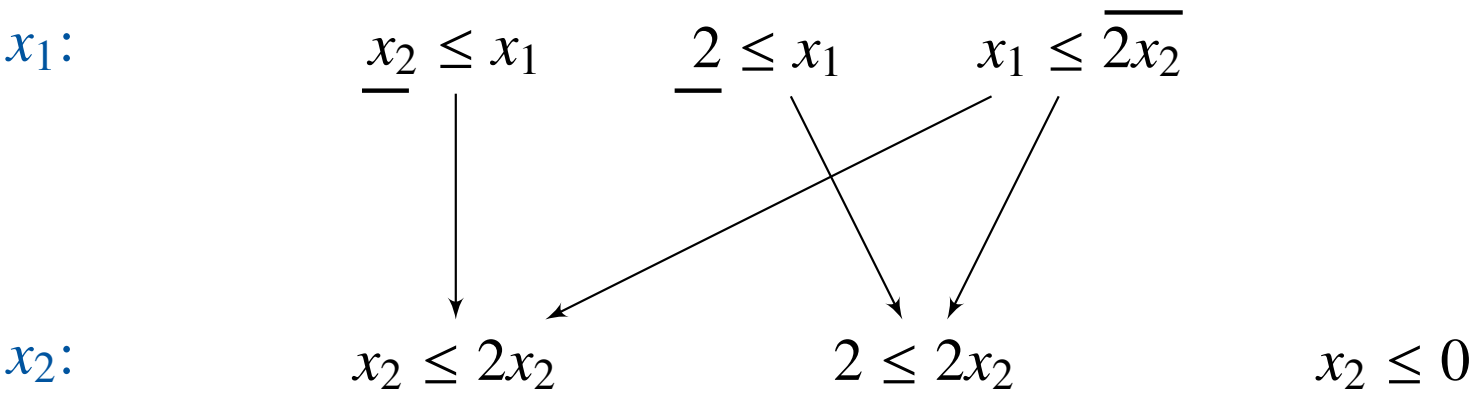
x_1: $\quad \underline{x_2} \leq x_1 \quad \underline{2} \leq x_1 \quad x_1 \leq \overline{2x_2}$

x_2: $\quad x_2 \leq 0$

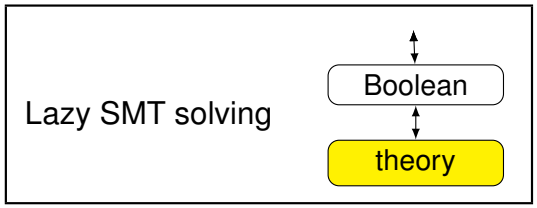
Fourier-Motzkin as theory solver in lazy SMT



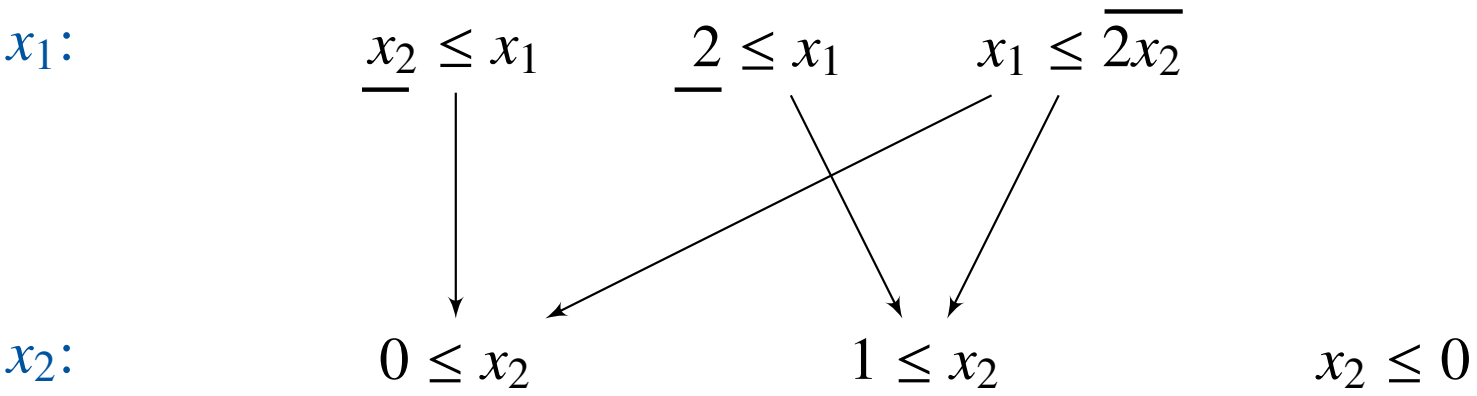
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$



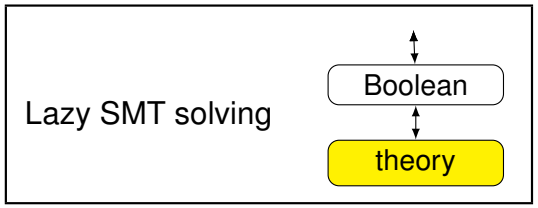
Fourier-Motzkin as theory solver in lazy SMT



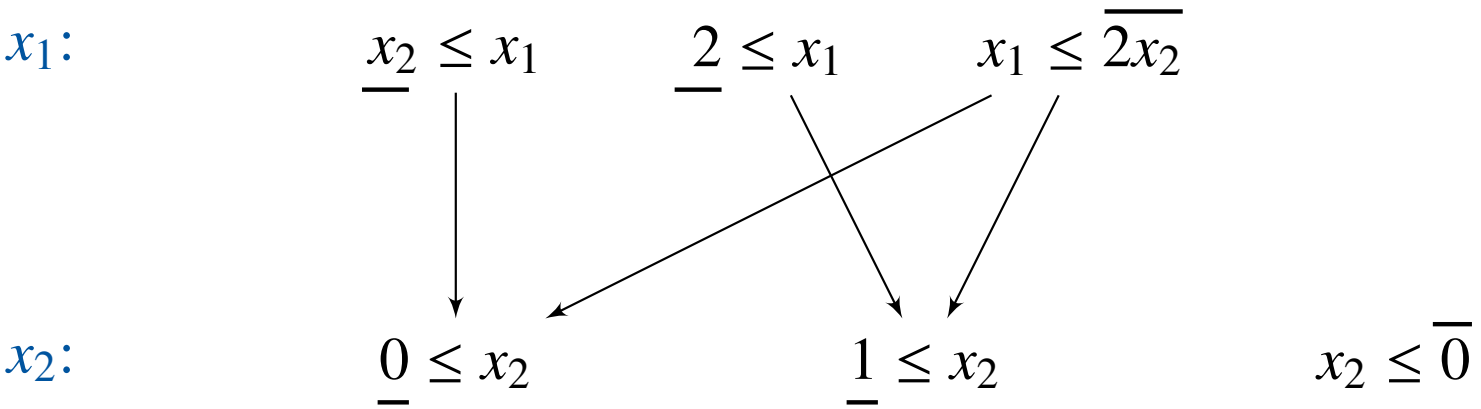
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$



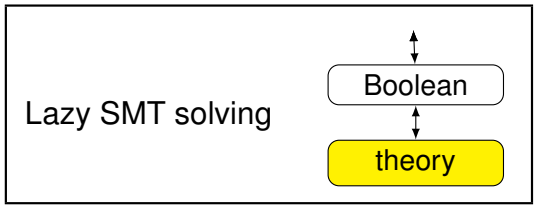
Fourier-Motzkin as theory solver in lazy SMT



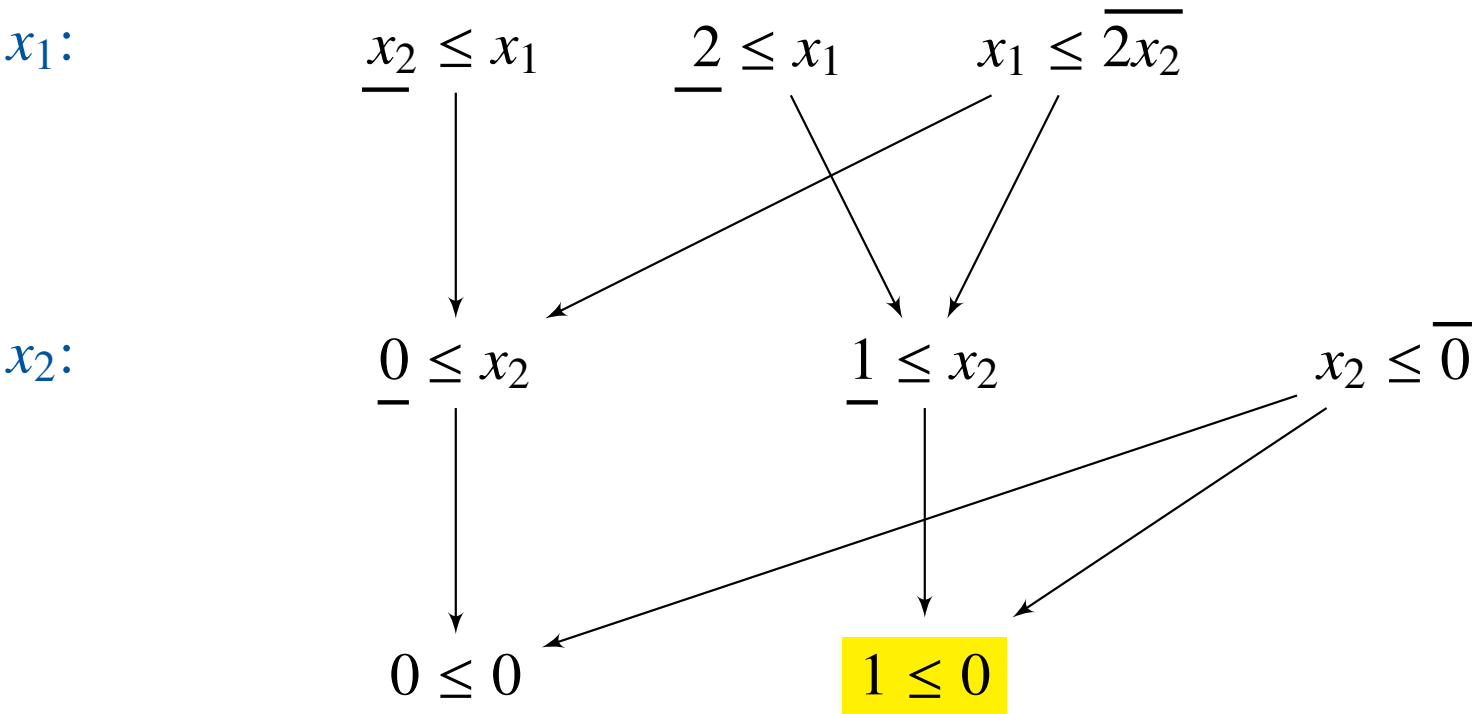
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$



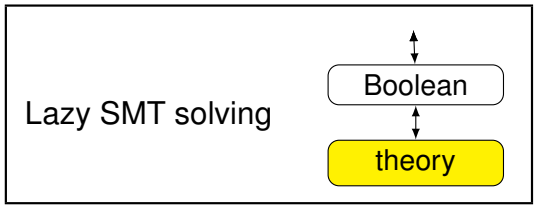
Fourier-Motzkin as theory solver in lazy SMT



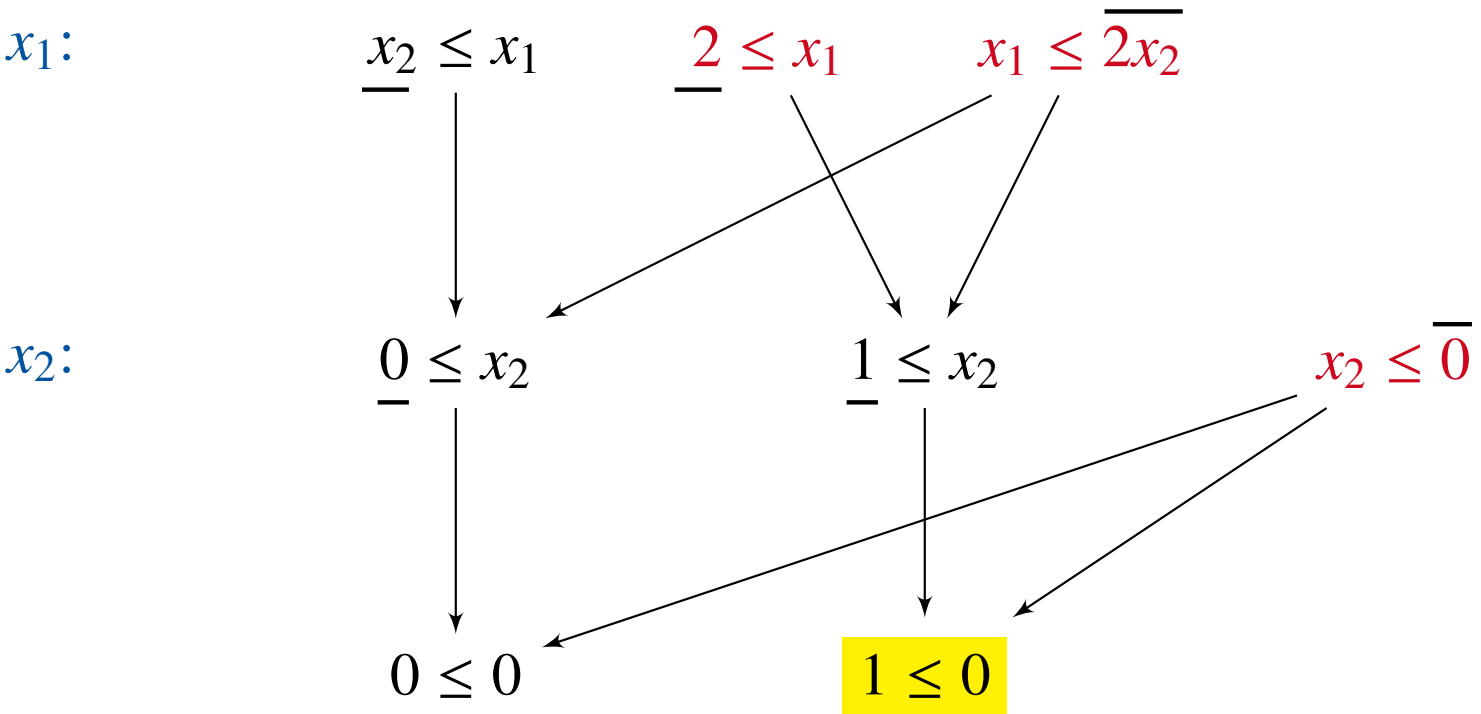
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$



Fourier-Motzkin as theory solver in lazy SMT



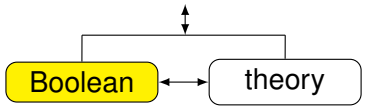
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$



return UNSAT with explanation $\neg(2 \leq x_1 \wedge x_1 \leq 2x_2 \wedge x_2 \leq 0)$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)

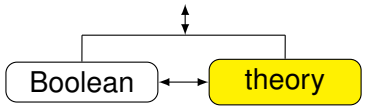


$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$

$x_1 \leq 2x_2$ $\quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)

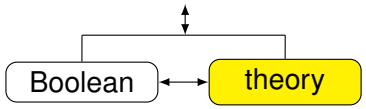


$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$

$x_1 \leq 2x_2$ $\quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



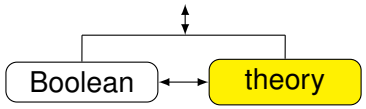
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

x_2: $\quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

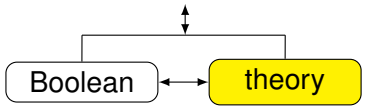
$\mathbb{T}$-prop.: $x_2 \in ?$

x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

x_2: $\quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

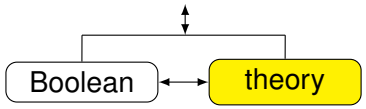
$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$

x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

x_2: $\quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

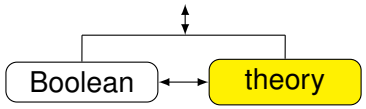
$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$

x_1: $\quad \underset{0}{x_2 \leq x_1}$ $\quad 2 \leq x_1$ $\quad \underset{0}{x_1 \leq 2x_2}$

x_2: $\quad \underset{0}{x_2 \leq 0}$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

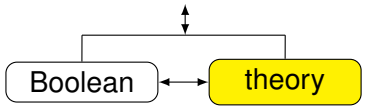
$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$ $\quad$ $\mathbb{T}$-prop.: $x_1 \in ?$

x_1: $\quad x_2 \leq x_1$ (0) $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ (0)

x_2: $\quad x_2 \leq 0$ (0)

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

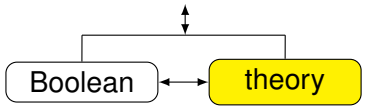
$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$ $\quad$ $\mathbb{T}$-prop.: $x_1 \in \emptyset$

x_1: $\quad x_2 \leq x_1$ (0) $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ (0)

x_2: $\quad x_2 \leq 0$ (0)

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

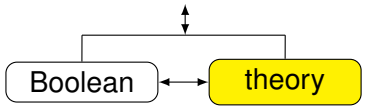
$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$ $\quad$ $\mathbb{T}$-prop.: $x_1 \in \emptyset$

x_1: $\quad x_2 \leq x_1$ (0) $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ (0)

x_2: $\quad (2 \leq x_1 \wedge x_1 \leq 2x_2) \rightarrow 2 \leq 2x_2$ $\quad x_2 \leq 0$ (0)

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

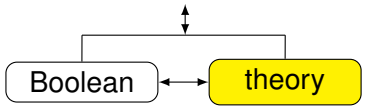
$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$ $\quad$ $\mathbb{T}$-prop.: $x_1 \in \emptyset$

x_1: $\quad x_2 \leq x_1$ (0) $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ (0)

x_2: $\quad (2 \leq x_1 \wedge x_1 \leq 2x_2) \rightarrow 1 \leq x_2$ $\quad x_2 \leq 0$ (0)

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



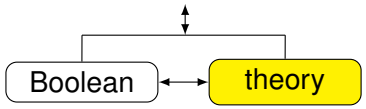
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

x_1: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

x_2: $(2 \leq x_1 \wedge x_1 \leq 2x_2) \rightarrow 1 \leq x_2$ $\quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

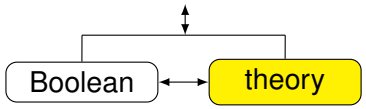
$\mathbb{B}$-prop.: $1 \leq x_2$

x_1: $\quad x_2 \leq x_1 \quad 2 \leq x_1 \quad x_1 \leq 2x_2$

x_2: $\quad (2 \leq x_1 \wedge x_1 \leq 2x_2) \rightarrow 1 \leq x_2 \quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)

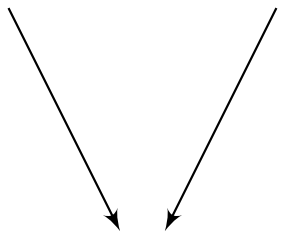


$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{B}$-prop.: $1 \leq x_2$

$\mathbb{T}$-prop.: $x_2 \in ?$

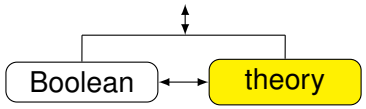
x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$



x_2: $\quad (2 \leq x_1 \wedge x_1 \leq 2x_2) \rightarrow 1 \leq x_2$ $\quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)

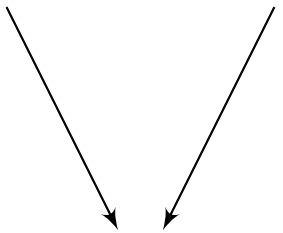


$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{B}$-prop.: $1 \leq x_2$

$\mathbb{T}$-prop.: $x_2 \in \emptyset$

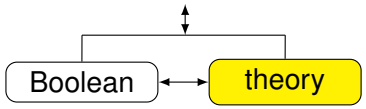
x_1: $\quad x_2 \leq x_1 \quad 2 \leq x_1 \quad x_1 \leq 2x_2$



x_2: $\quad (2 \leq x_1 \wedge x_1 \leq 2x_2) \rightarrow 1 \leq x_2 \quad x_2 \leq 0$

Fourier-Motzkin in MCSAT

Model-constructing satisfiability calculus (MCSAT)



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{B}$-prop.: $1 \leq x_2$

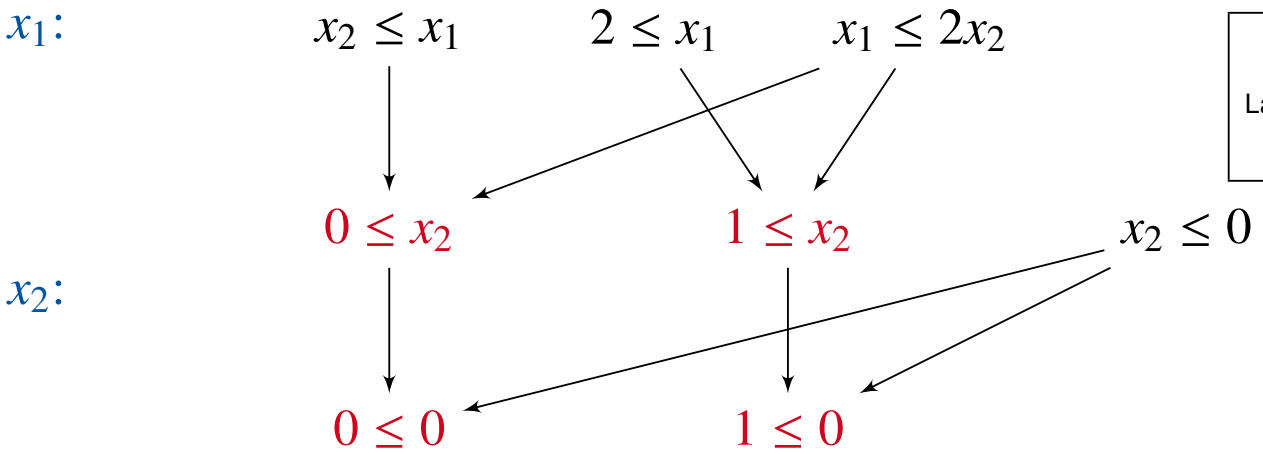
$\mathbb{T}$-prop.: $x_2 \in \emptyset$

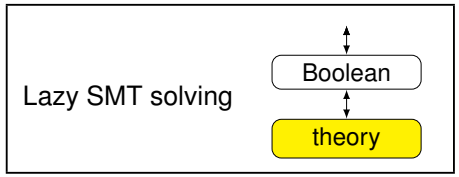
x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

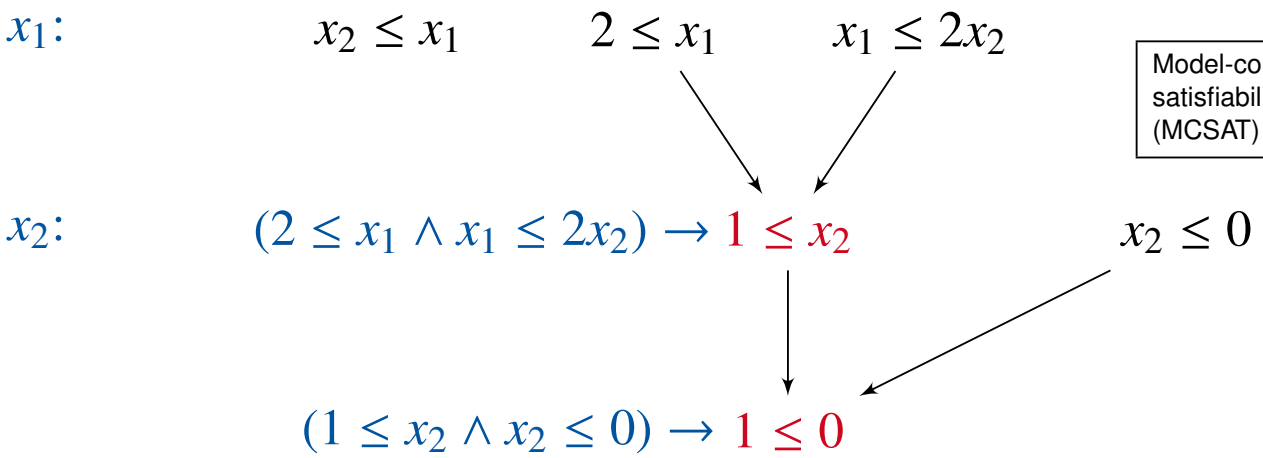
x_2: $\quad (2 \leq x_1 \wedge x_1 \leq 2x_2) \rightarrow 1 \leq x_2$ $\quad x_2 \leq 0$

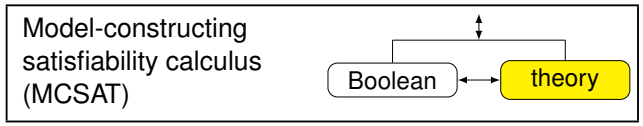
$(1 \leq x_2 \wedge x_2 \leq 0) \rightarrow 1 \leq 0$

Fourier-Motzkin: Lazy SMT vs MCSAT

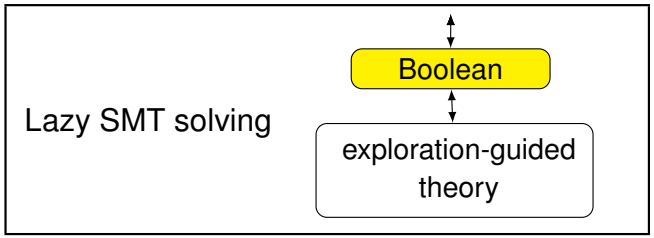








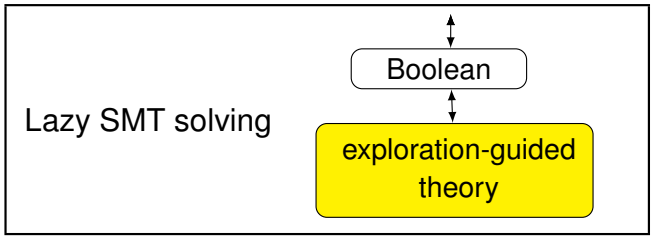
Exploration-guided Fourier-Motzkin



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$

$x_1 \leq 2x_2$ $\quad x_2 \leq 0$

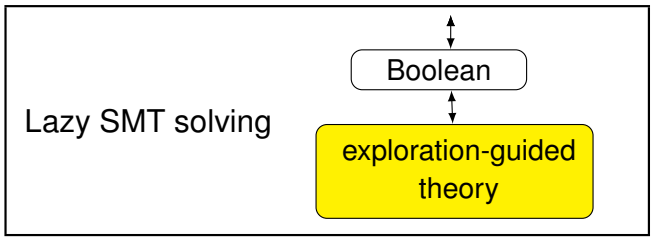
Exploration-guided Fourier-Motzkin



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$

$x_1 \leq 2x_2$ $\quad x_2 \leq 0$

Exploration-guided Fourier-Motzkin

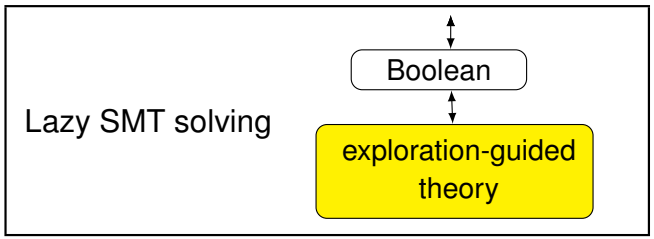


$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

x_2: $\quad x_2 \leq 0$

Exploration-guided Fourier-Motzkin



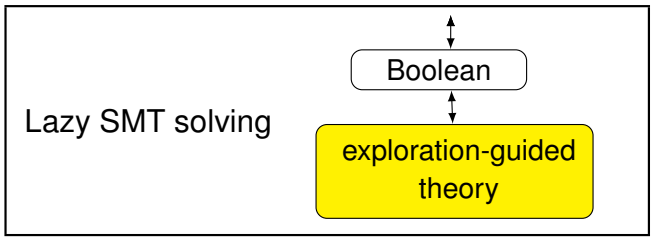
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$
$x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{T}$-prop.: $x_2 \in ?$

x_1: $\quad x_2 \leq x_1 \quad 2 \leq x_1 \quad x_1 \leq 2x_2$

x_2: $\quad x_2 \leq 0$

Exploration-guided Fourier-Motzkin



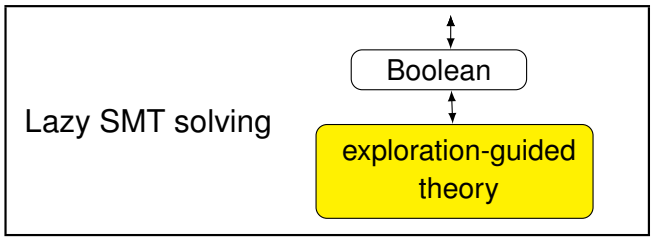
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$
$x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$

x_1: $\quad x_2 \leq x_1 \quad 2 \leq x_1 \quad x_1 \leq 2x_2$

x_2: $\quad x_2 \leq 0$

Exploration-guided Fourier-Motzkin



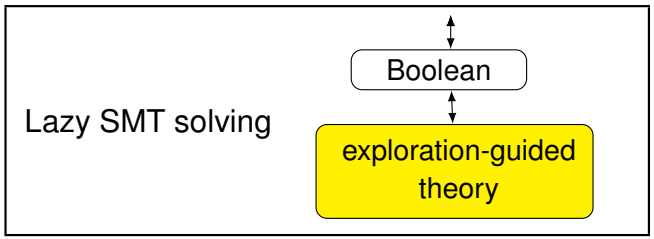
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$

x_1: $\quad \underset{0}{x_2 \leq x_1}$ $\quad 2 \leq x_1$ $\quad \underset{0}{x_1 \leq 2x_2}$

x_2: $\quad \underset{0}{x_2 \leq 0}$

Exploration-guided Fourier-Motzkin



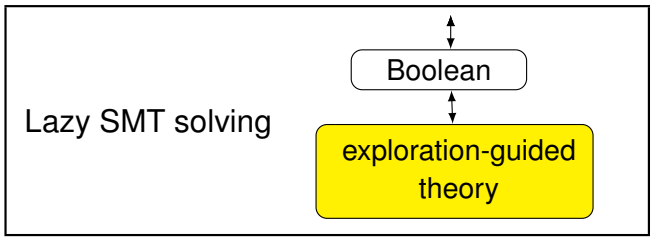
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$ $\quad$ $\mathbb{T}$-prop.: $x_1 \in ?$

x_1: $\quad \underset{0}{x_2 \leq x_1}$ $\quad 2 \leq x_1$ $\quad \underset{0}{x_1 \leq 2x_2}$

x_2: $\quad \underset{0}{x_2 \leq 0}$

Exploration-guided Fourier-Motzkin



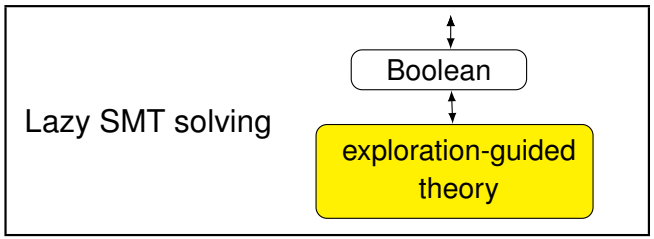
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$ $\quad$ $\mathbb{T}$-prop.: $x_1 \in \emptyset$

x_1: $\quad \underset{0}{x_2 \leq x_1}$ $\quad 2 \leq x_1$ $\quad \underset{0}{x_1 \leq 2x_2}$

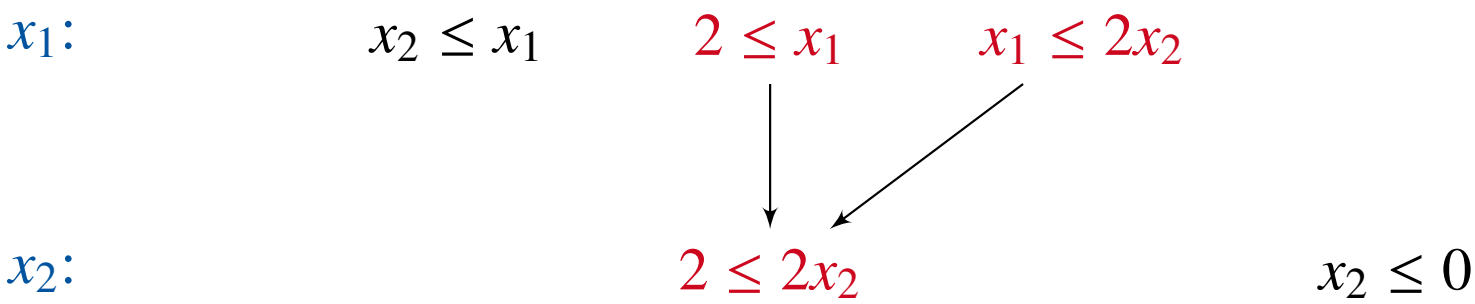
x_2: $\quad \underset{0}{x_2 \leq 0}$

Exploration-guided Fourier-Motzkin

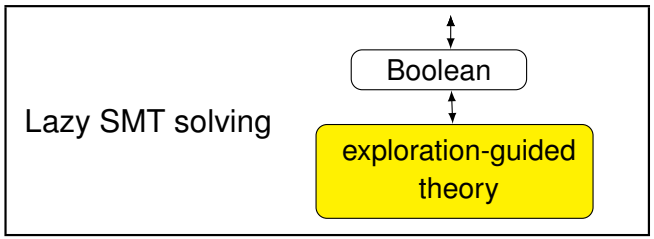


$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$ $\quad$ $\mathbb{T}$-prop.: $x_1 \in \emptyset$



Exploration-guided Fourier-Motzkin



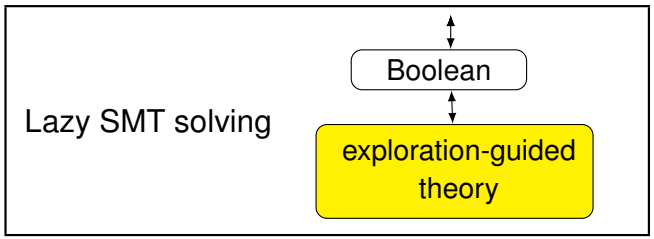
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{T}$-prop.: $x_2 \in (-\infty, 0]$ $\quad$ $\mathbb{T}$-dec.: $x_2 = 0$ $\quad$ $\mathbb{T}$-prop.: $x_1 \in \emptyset$

x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

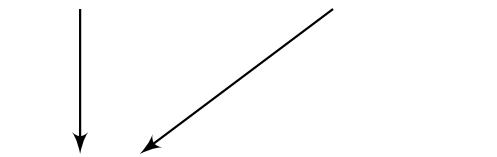
x_2: $\quad 1 \leq x_2$ $\quad x_2 \leq 0$

Exploration-guided Fourier-Motzkin



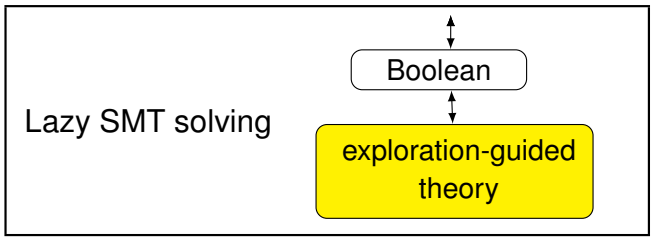
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$



x_2: $\quad 1 \leq x_2$ $\quad x_2 \leq 0$

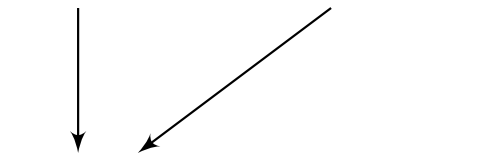
Exploration-guided Fourier-Motzkin



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

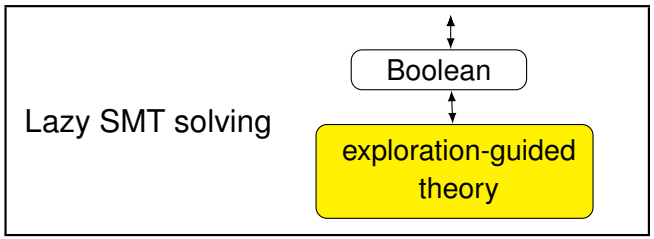
$\mathbb{T}$-prop.: $x_2 \in ?$

x_1: $\quad x_2 \leq x_1 \quad 2 \leq x_1 \quad x_1 \leq 2x_2$



x_2: $\quad 1 \leq x_2 \quad x_2 \leq 0$

Exploration-guided Fourier-Motzkin



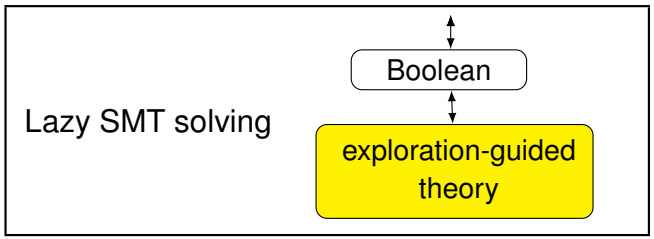
$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

$\mathbb{T}$-prop.: $x_2 \in \emptyset$

x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

x_2: $\quad 1 \leq x_2$ $\quad x_2 \leq 0$

Exploration-guided Fourier-Motzkin



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

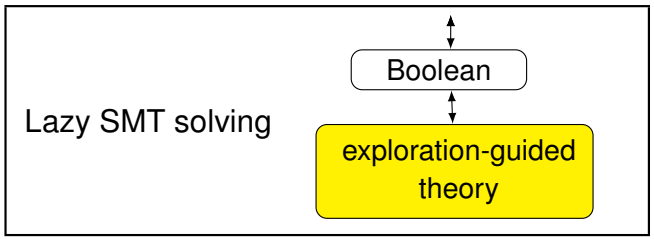
$\mathbb{T}$-prop.: $x_2 \in \emptyset$

x_1: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

x_2: $1 \leq x_2$ $\quad x_2 \leq 0$

$1 \leq 0$

Exploration-guided Fourier-Motzkin



$\mathbb{B}$-decisions: $x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$ $\quad x_2 \leq 0$

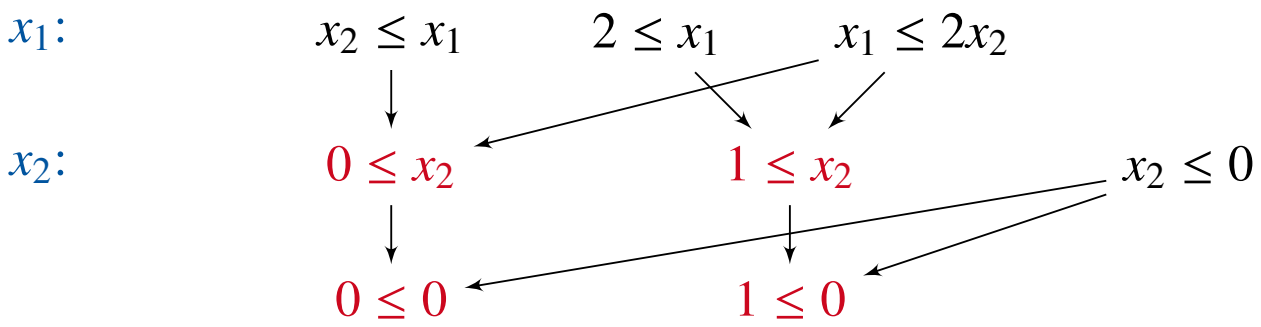
$\mathbb{T}$-prop.: $x_2 \in \emptyset$

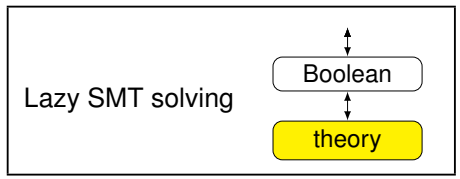
x_1: $\quad x_2 \leq x_1$ $\quad 2 \leq x_1$ $\quad x_1 \leq 2x_2$

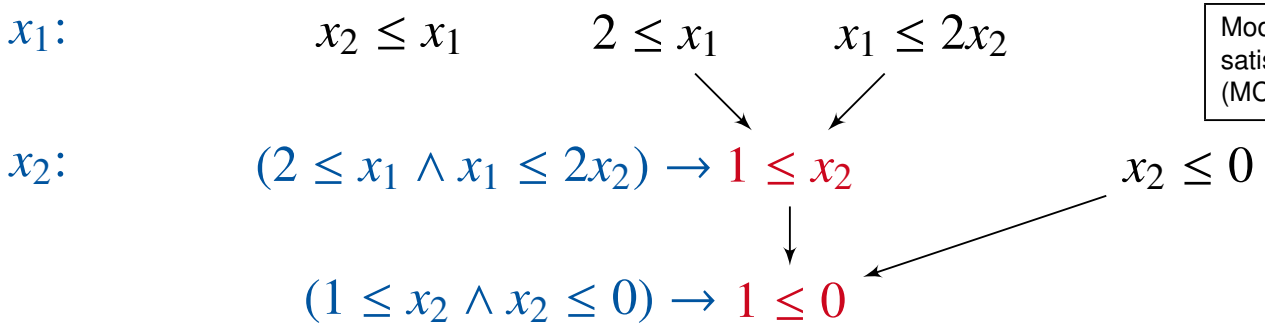
x_2: $\quad 1 \leq x_2$ $\quad x_2 \leq 0$

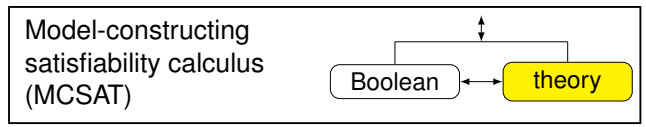
$1 \leq 0$

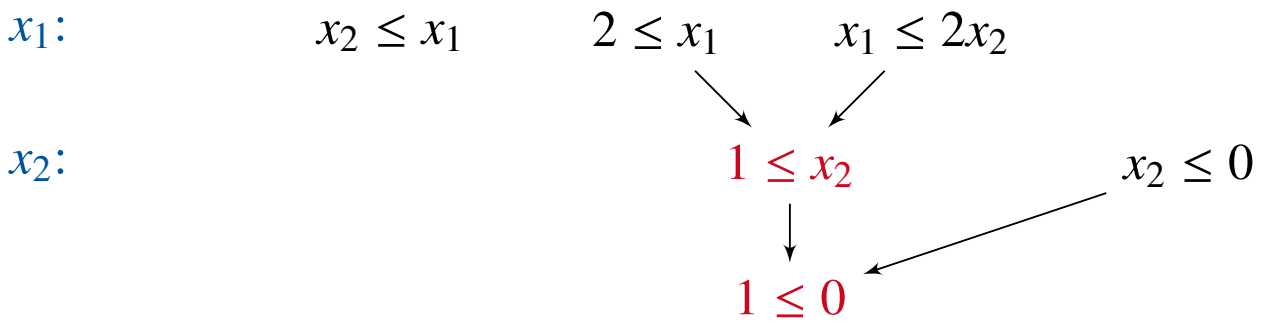
return UNSAT with explanation $\neg(2 \leq x_1 \wedge x_1 \leq 2x_2 \wedge x_2 \leq 0)$

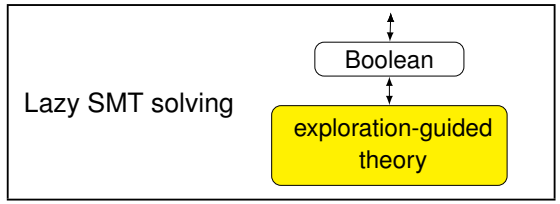

x_1:
$x_2 \le x_1$
$2 \le x_1$
$x_1 \le 2x_2$
x_2:
$0 \le x_2$
$1 \le x_2$
$x_2 \le 0$
$0 \le 0$
$1 \le 0$


Lazy SMT solving
Boolean
theory


x_1:
$x_2 \le x_1$
$2 \le x_1$
$x_1 \le 2x_2$
x_2:
$(2 \le x_1 \wedge x_1 \le 2x_2) \rightarrow 1 \le x_2$
$x_2 \le 0$
$(1 \le x_2 \wedge x_2 \le 0) \rightarrow 1 \le 0$

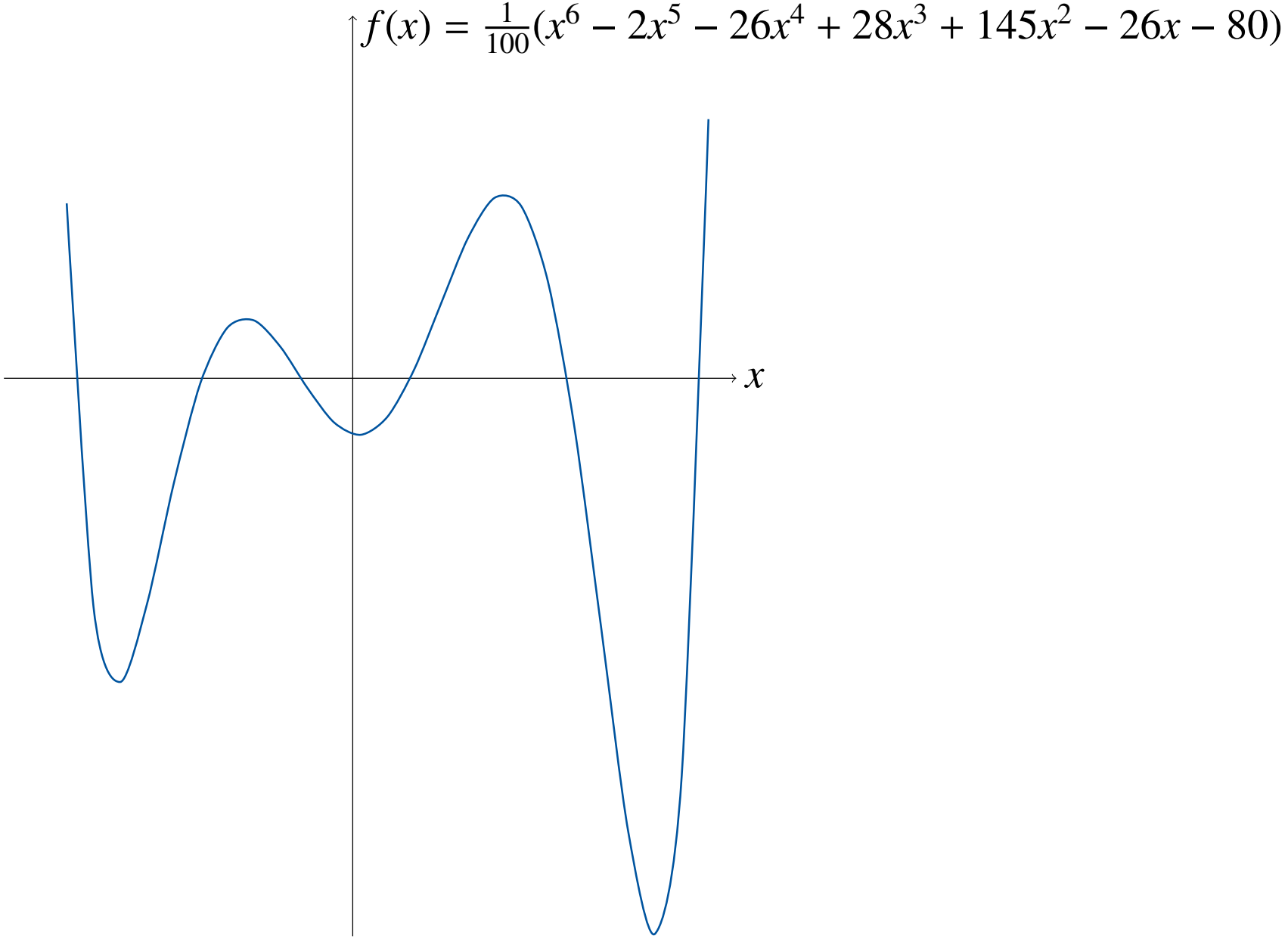

Model-constructing
satisfiability calculus
(MCSAT)
Boolean
theory


x_1:
$x_2 \le x_1$
$2 \le x_1$
$x_1 \le 2x_2$
x_2:
$1 \le x_2$
$x_2 \le 0$
$1 \le 0$


Lazy SMT solving
Boolean
exploration-guided
theory

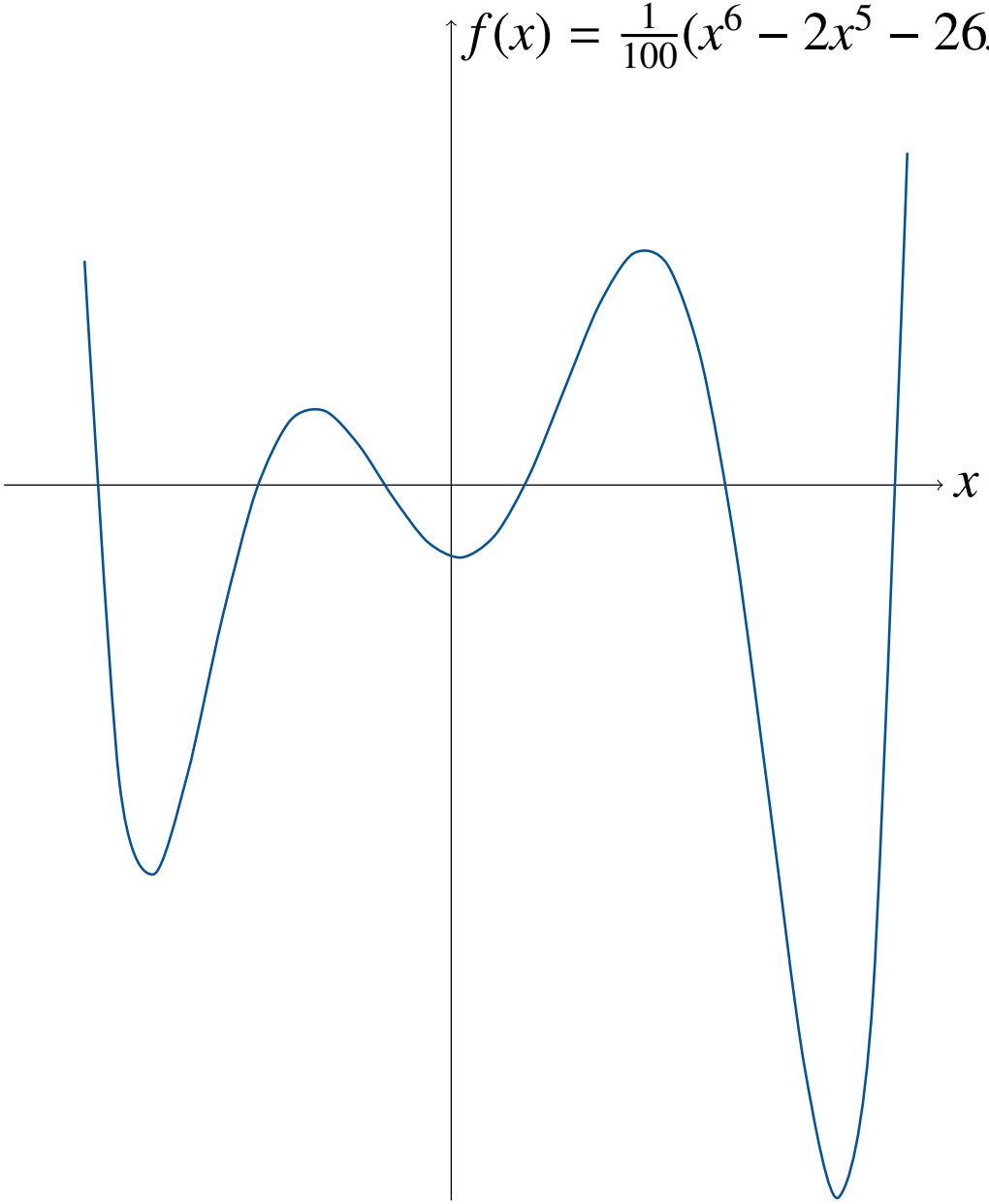
The key to decidability of NRA: Sign-invariant regions

The key to decidability of NRA: Sign-invariant regions



The key to decidability of NRA: Sign-invariant regions

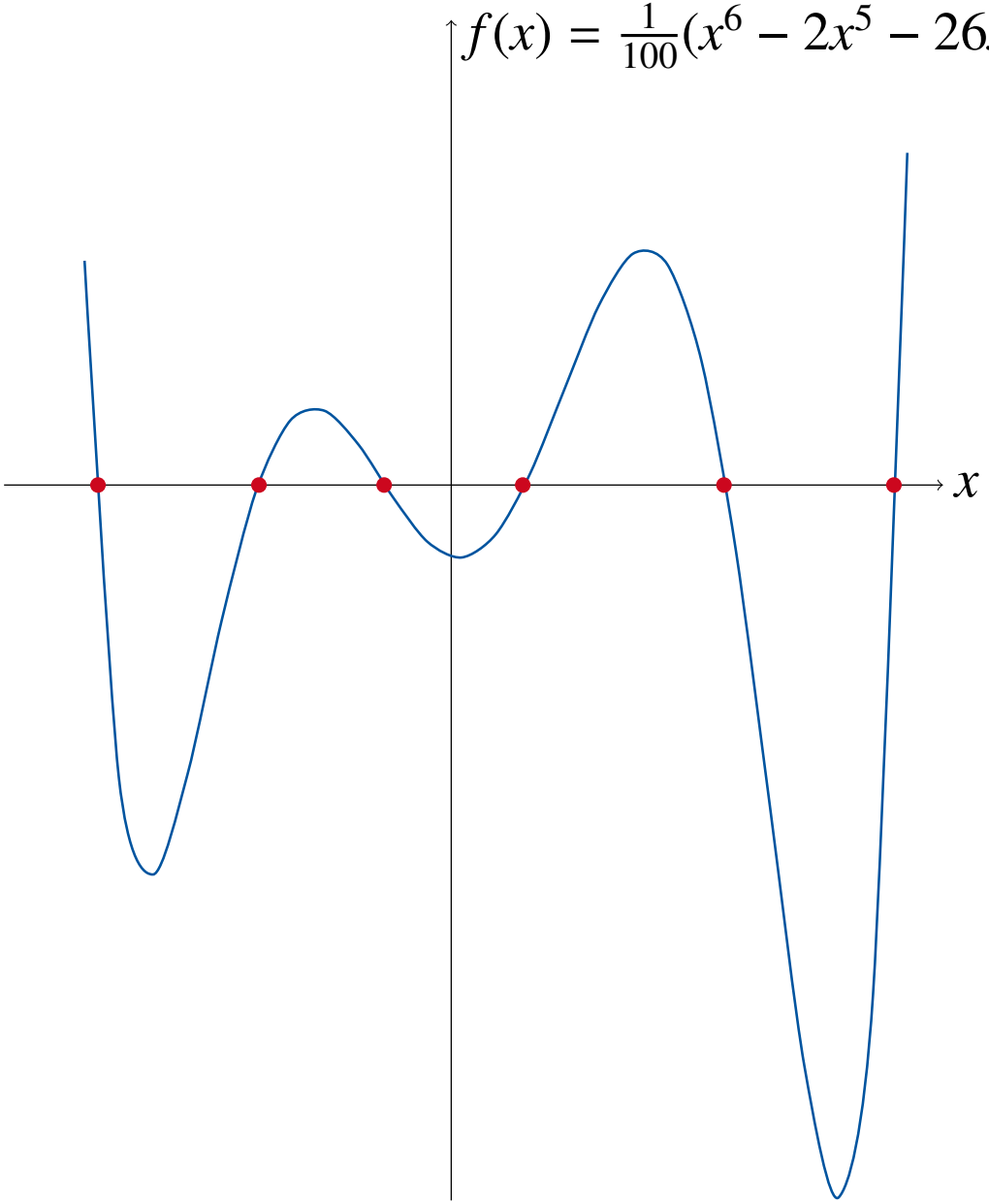
$$f(x) = \frac{1}{100}(x^6 - 2x^5 - 26x^4 + 28x^3 + 145x^2 - 26x - 80)$$



Is
$f(x) < 0$
satisfiable?

The key to decidability of NRA: Sign-invariant regions

$$f(x) = \frac{1}{100}(x^6 - 2x^5 - 26x^4 + 28x^3 + 145x^2 - 26x - 80)$$



Is
$f(x) < 0$
satisfiable?

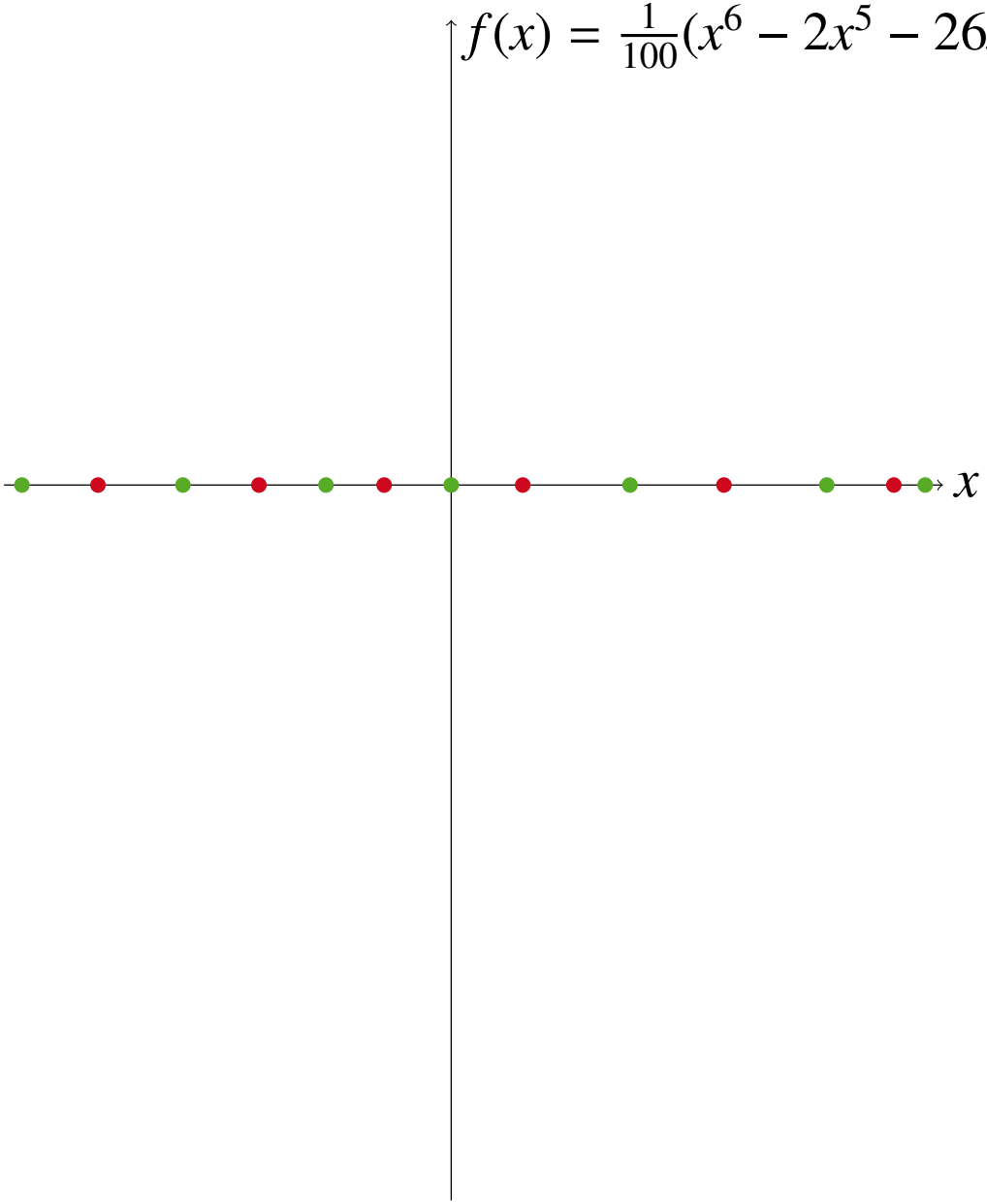
The key to decidability of NRA: Sign-invariant regions

$$f(x) = \frac{1}{100}(x^6 - 2x^5 - 26x^4 + 28x^3 + 145x^2 - 26x - 80)$$

Is
$f(x) < 0$
satisfiable?

The key to decidability of NRA: Sign-invariant regions

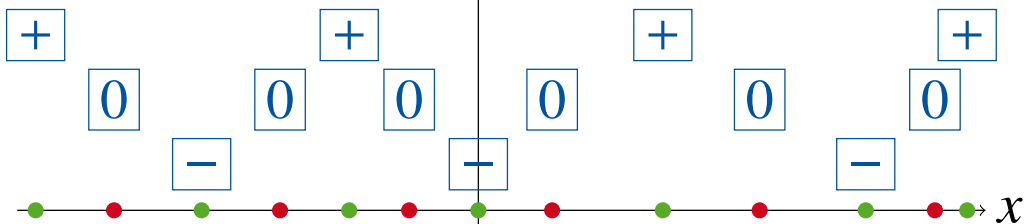
$$f(x) = \frac{1}{100}(x^6 - 2x^5 - 26x^4 + 28x^3 + 145x^2 - 26x - 80)$$



Is
$f(x) < 0$
satisfiable?

The key to decidability of NRA: Sign-invariant regions

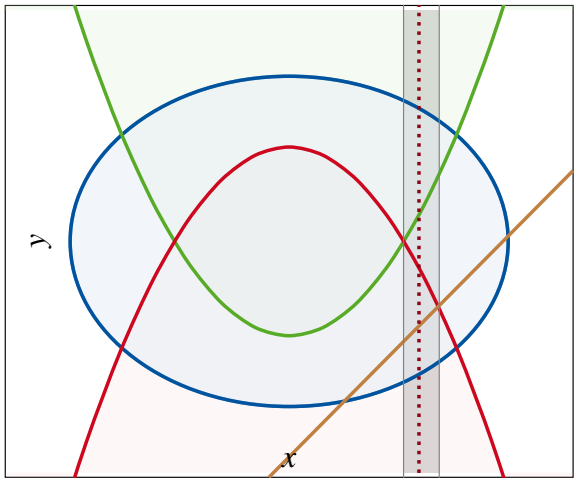
$$f(x) = \frac{1}{100}(x^6 - 2x^5 - 26x^4 + 28x^3 + 145x^2 - 26x - 80)$$

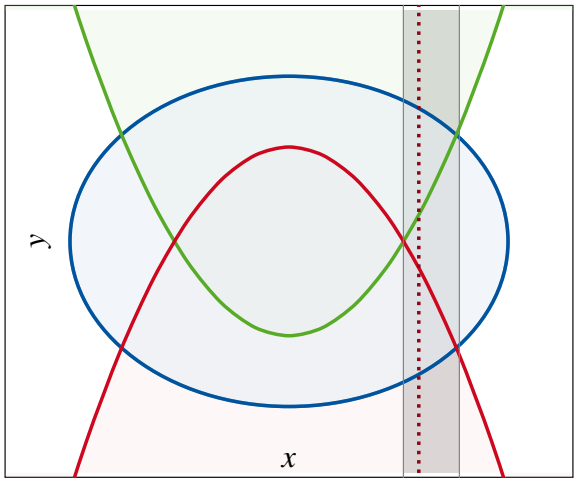


Is
$f(x) < 0$
satisfiable?

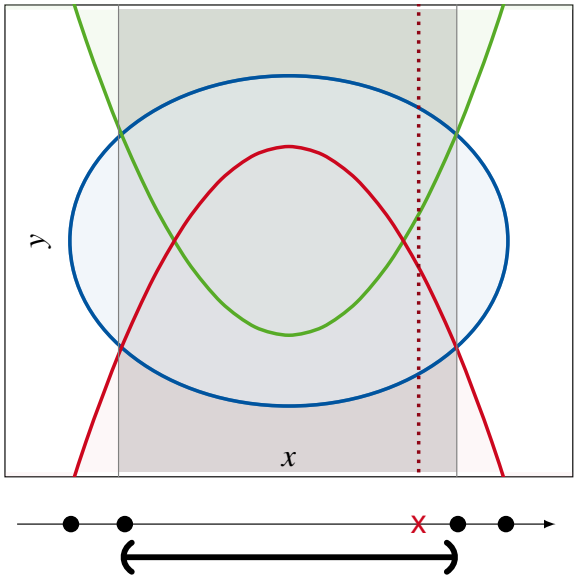
One-cell construction for MCSAT

Naive CAD cell





nlsat cell
[Jovanovic, de Moura, IJCAR'12]
Single-cell
[Brown, Kosta, JSC'15]



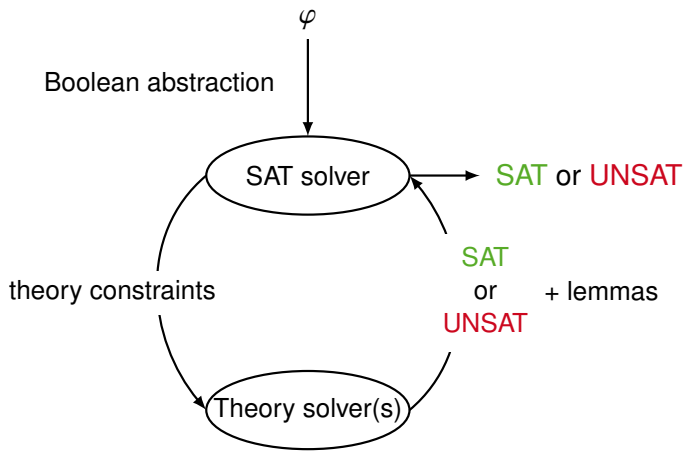
Covering-cell
[Ábrahám, Davenport, England, Kremer, JLAMP'21]

Contents

- SMT solving
- SMT-RAT
- Applications
- Future challenges

Problem solved?

Can we simply plug in available implementations of existing methods as theory solvers into an SMT solver?

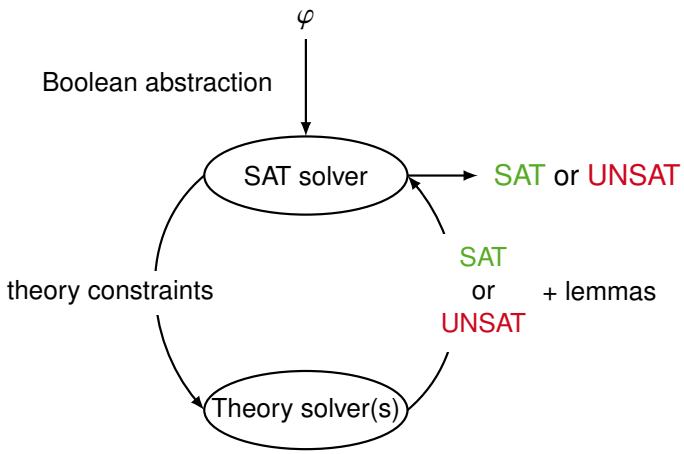


Problem solved?

Can we simply plug in available implementations of existing methods as theory solvers into an SMT solver?

Theory solvers should be SMT-compliant, i.e., they should

- work incrementally,
- generate lemmas explaining inconsistencies, and
- be able to backtrack.

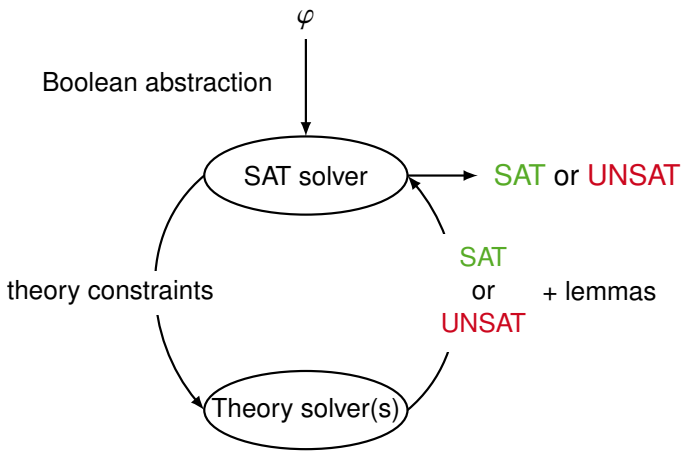


Problem solved?

Can we simply plug in available implementations of existing methods as theory solvers into an SMT solver?

Theory solvers should be SMT-compliant, i.e., they should

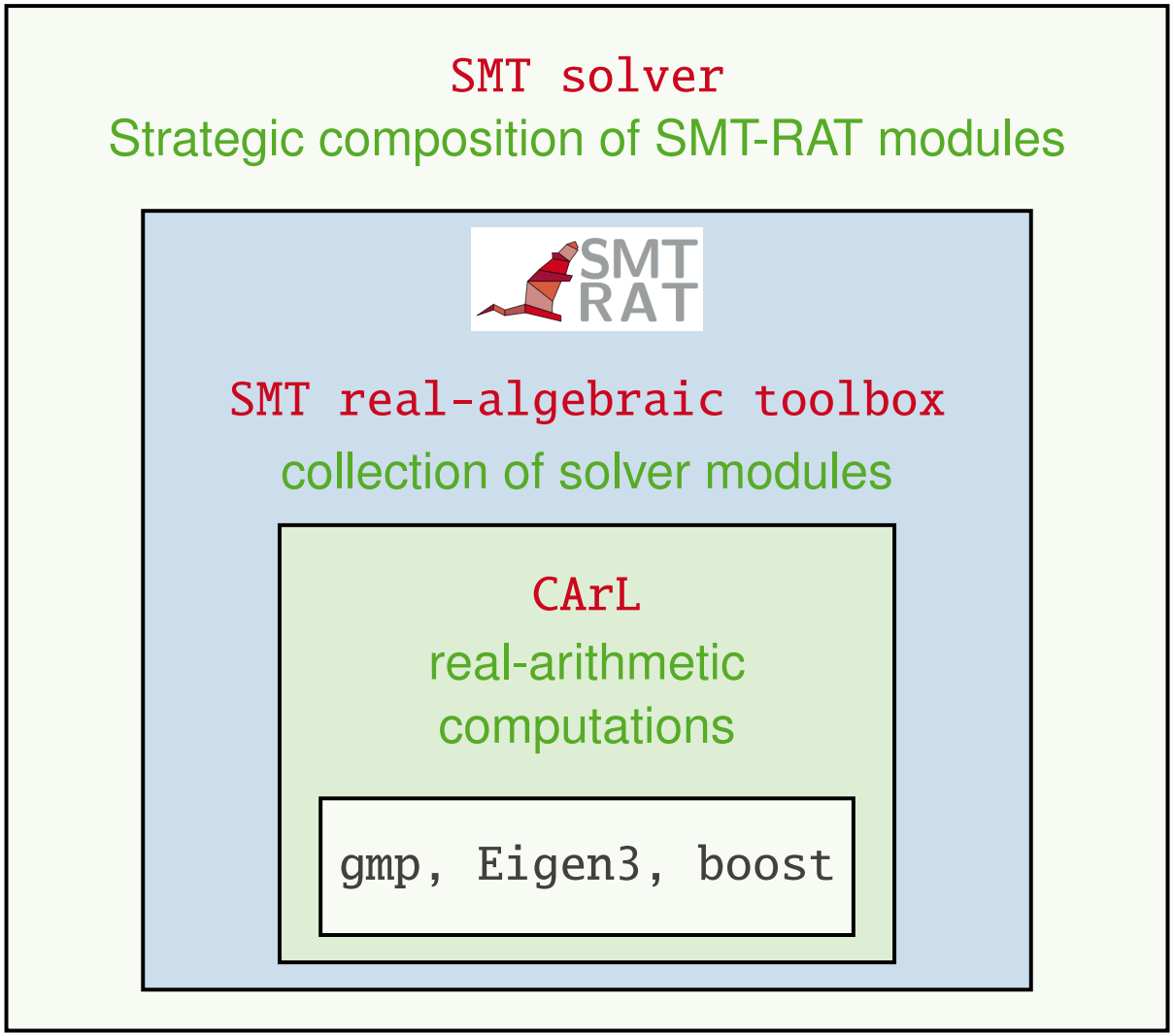
- work incrementally,
- generate lemmas explaining inconsistencies, and
- be able to backtrack.



Originally, the mentioned methods are not SMT-compliant.

SMT-adaptations can be tricky, but can lead to beautiful novel algorithms.

Our SMT-RAT library [SAT'12, SAT'15]



- MIT licensed source code: `github.com/smtrat/smtrat`
- Documentation: `smtrat.github.io`

Solver modules in SMT-RAT [SAT'12, SAT'15]

CArL library: basic arithmetic datatypes and computations [Sapientia'18, NFM'11, CAI'11]

Basic modules

- SAT solver
- CNF converter
- Preprocessing/simplifying modules

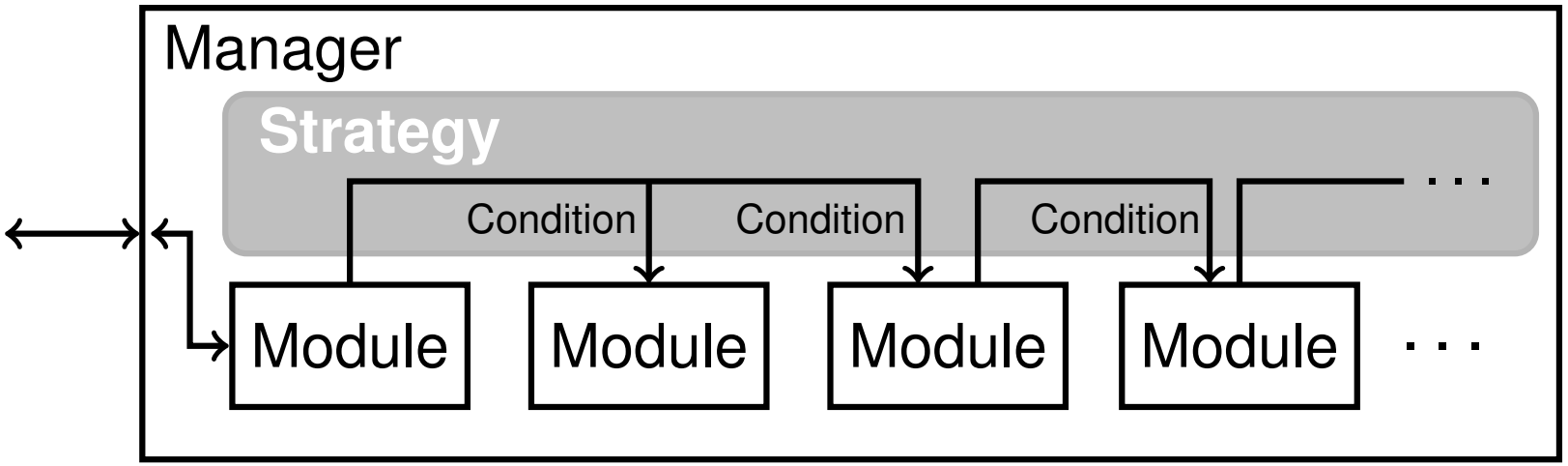
Non-algebraic decision procedures

- Equalities and uninterpreted functions
- Bit-vectors
- Bit-blasting
- Interval constraint propagation
- Pseudo-Boolean formulas

Algebraic decision procedures

- Gauß+Fourier-Motzkin
- Simplex [ISSAC'21]
- Gröbner bases [CAI'13]
- MCSAT (FM,VS,CAD) [2xSC^2'19]
- Cylindrical algebraic decomposition [SC^2'21, JLAMP'21, CADE-24, JSC'19, SC^2'17, 3 PhDs]
- Virtual substitution [FCT'11, SC^2'17, 1 PhD]
- Subtropical satisfiability
- Generalized branch-and-bound [CASC'16]
- Cube tests
- Linearization

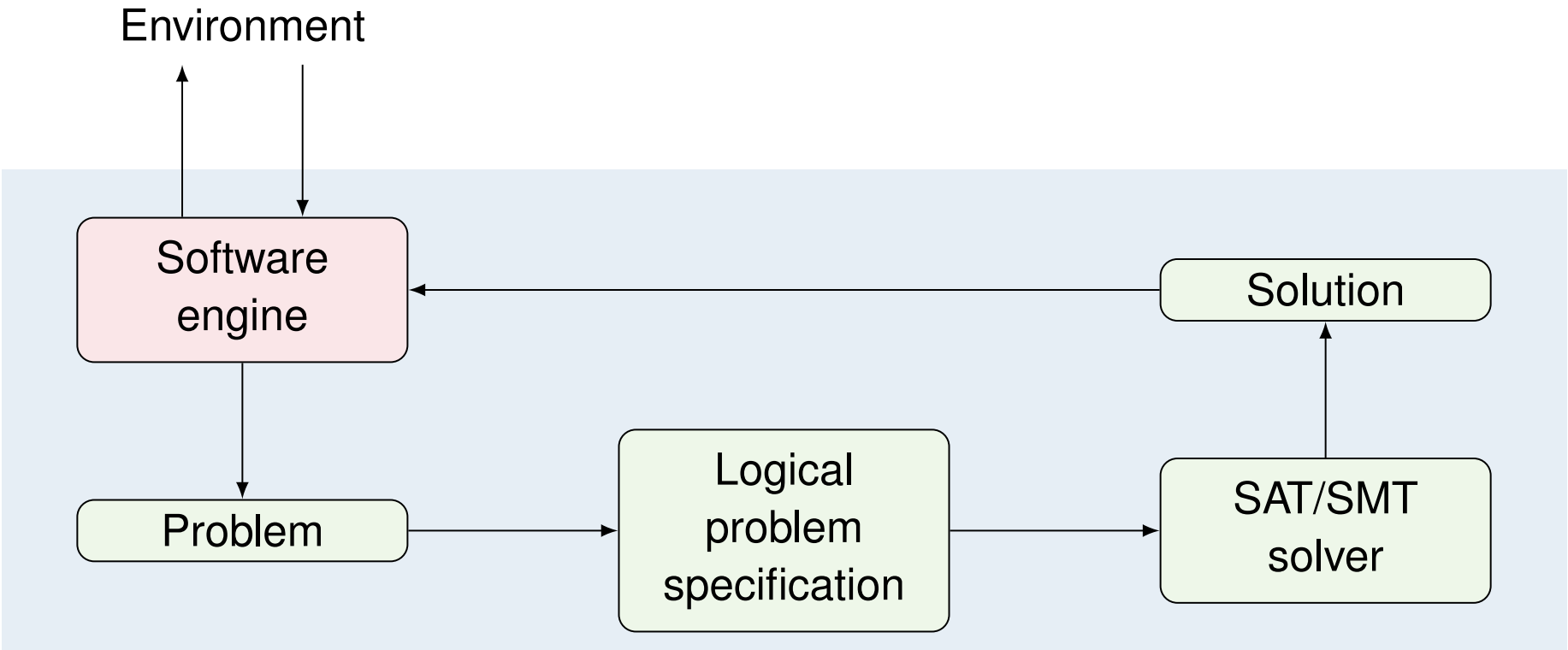
Strategic composition of solver modules in SMT-RAT



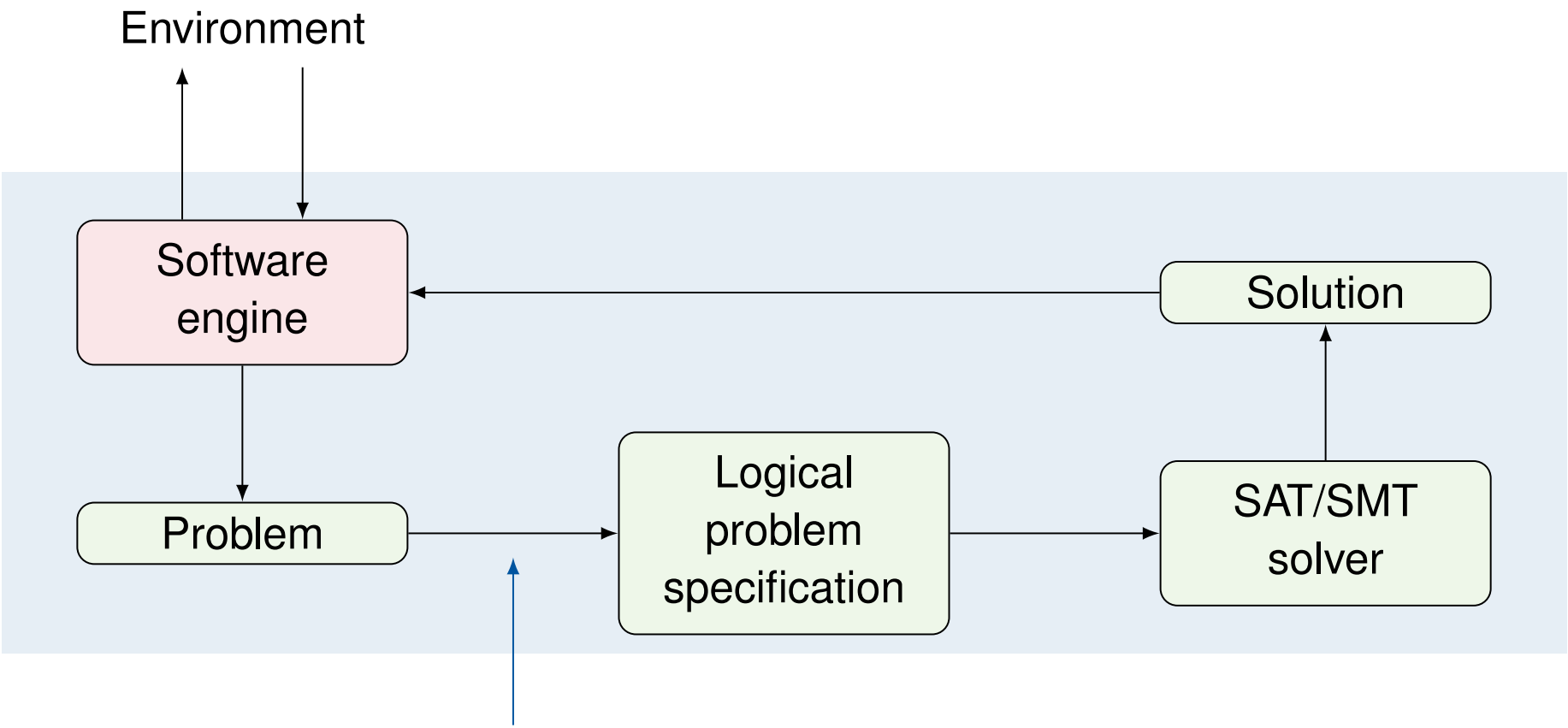
Contents

- SMT solving
- SMT-RAT
- Applications
- Future challenges

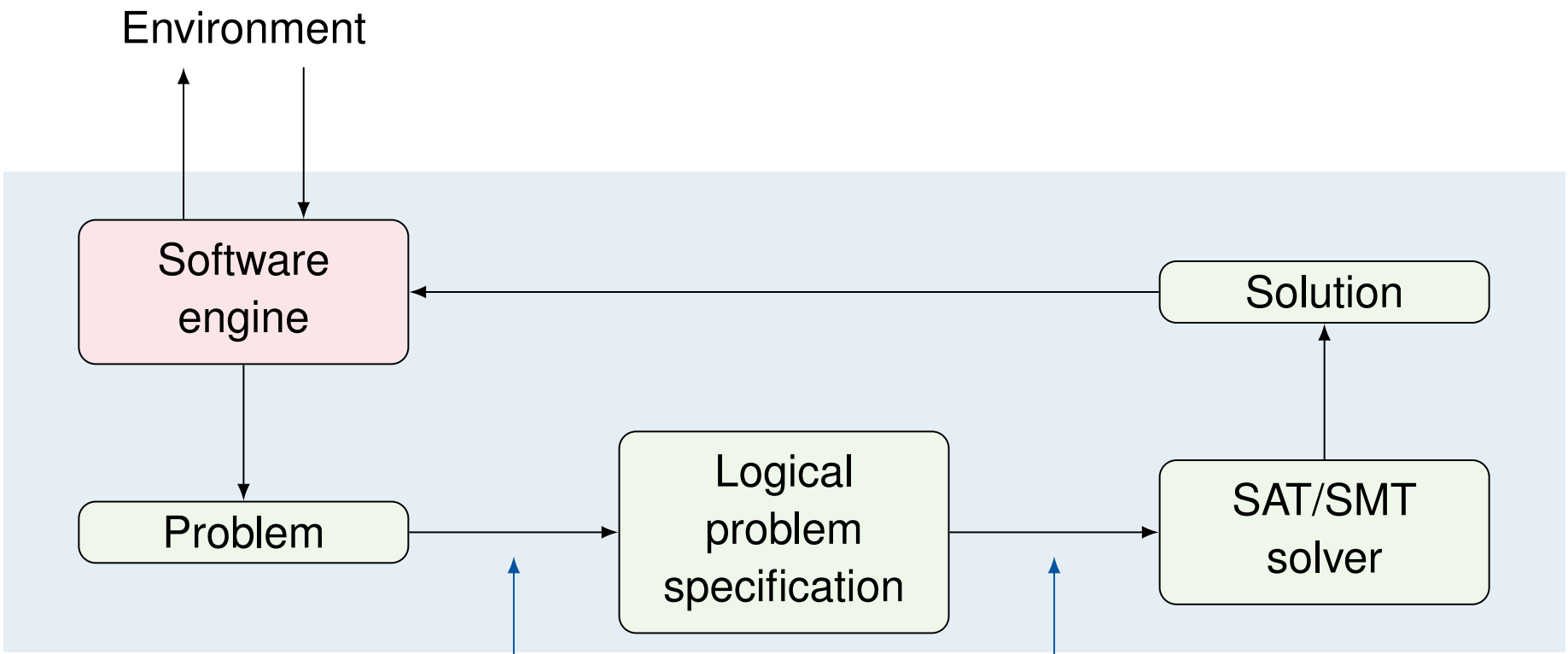
Embedding SAT/SMT solvers



Embedding SAT/SMT solvers



Embedding SAT/SMT solvers

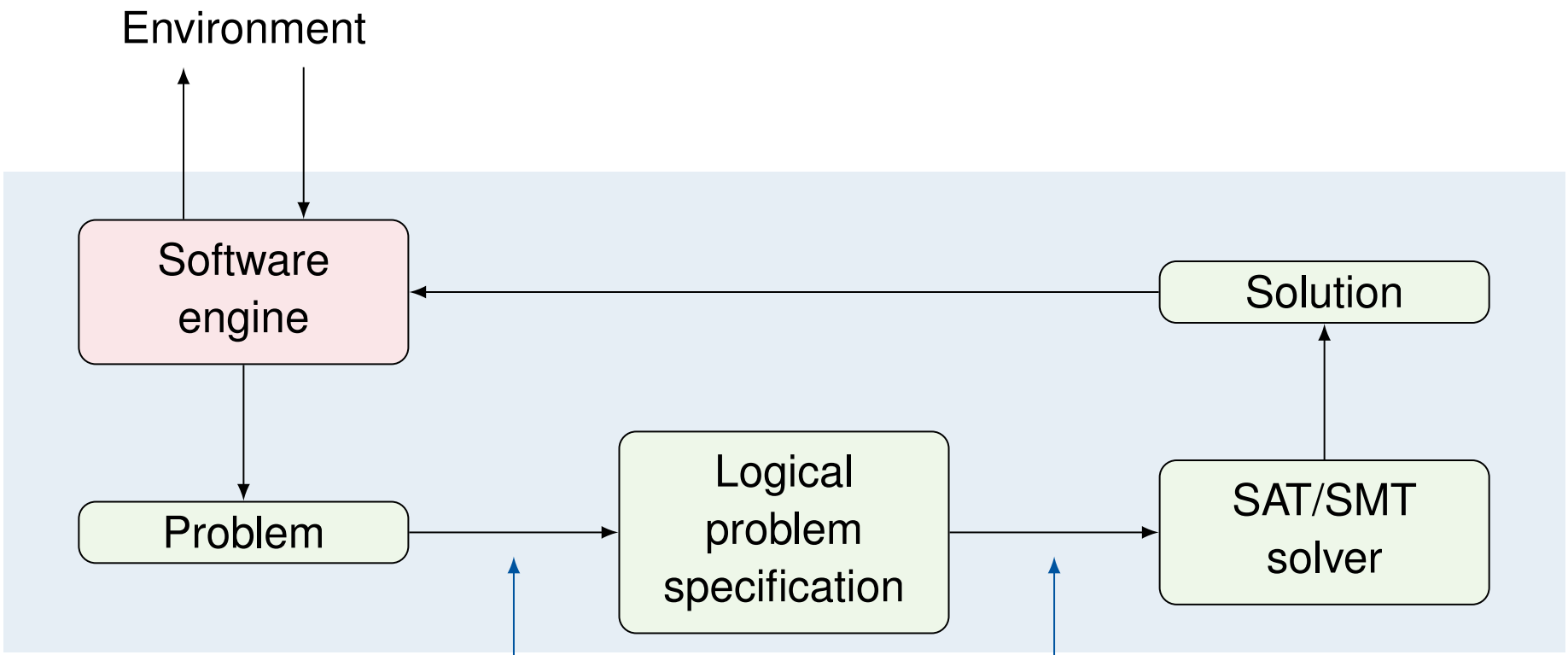


Encoding: SAT/SMT-LIB standard

elaborate encoding is extremely important!

standard input syntax → free solver choice

Embedding SAT/SMT solvers



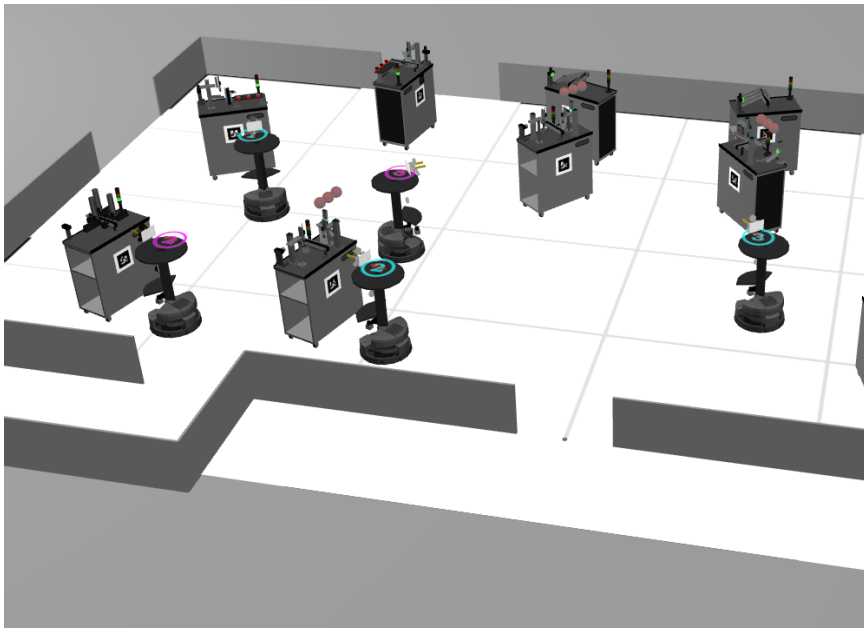
Encoding: SAT/SMT-LIB standard

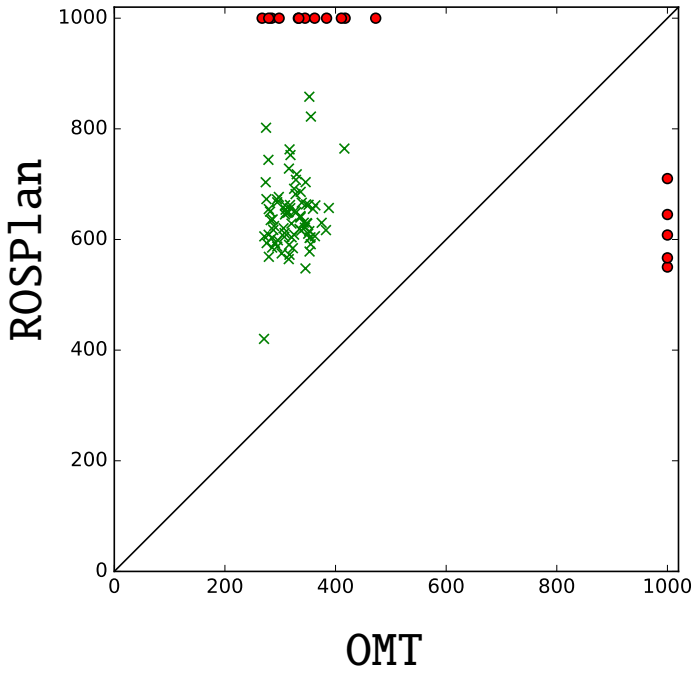
elaborate encoding is extremely important!

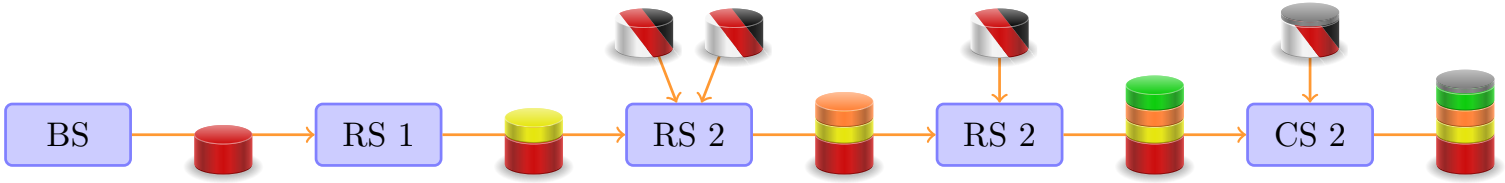
standard input syntax → free solver choice

Next: 4 own applications

Planning with Optimization Modulo Theories



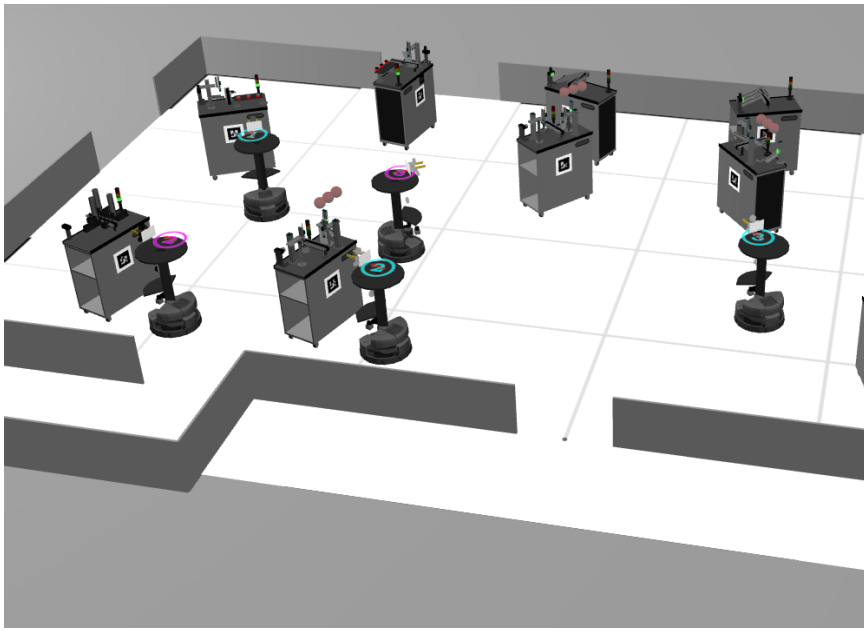


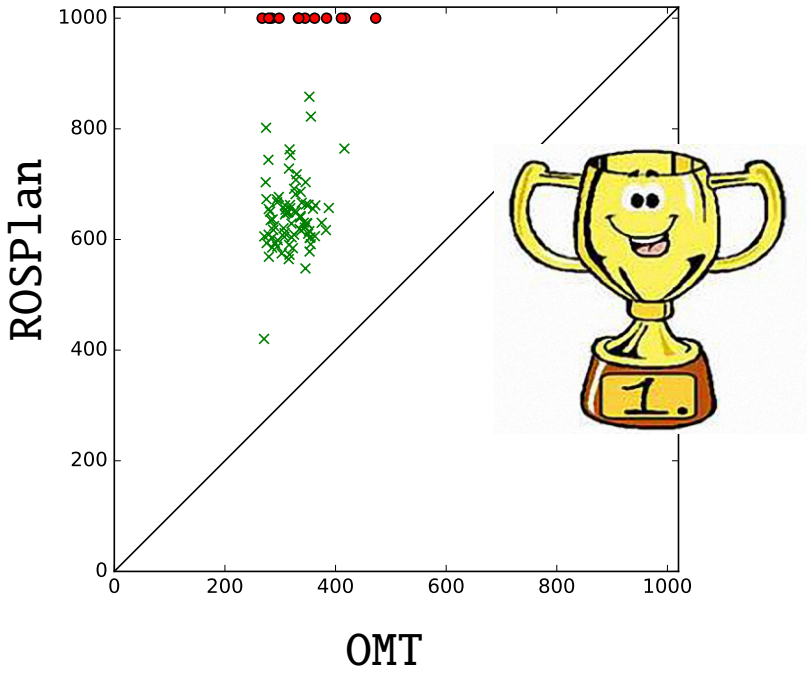


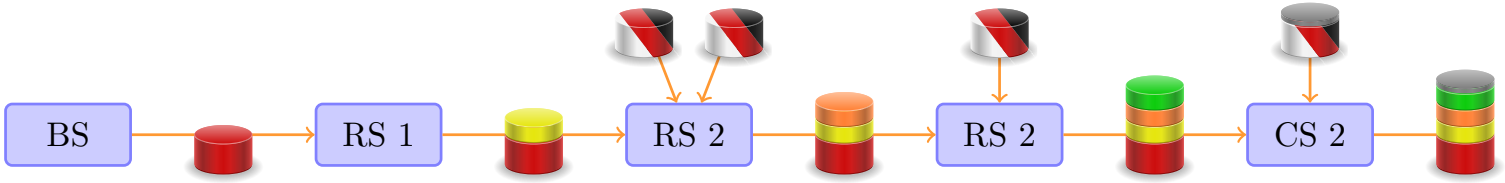
E. Ábrahám, G. Lakemeyer, F. Leofante, T. D. Niemüller, A. Tacchella.

PhD Leofante, publications in IJCAI'20, Information Systems Frontiers 2019, ECMS'19, AAAI'18, iFM'18, ICAPS'17, PlanRob'17, IRI'17.

Planning with Optimization Modulo Theories



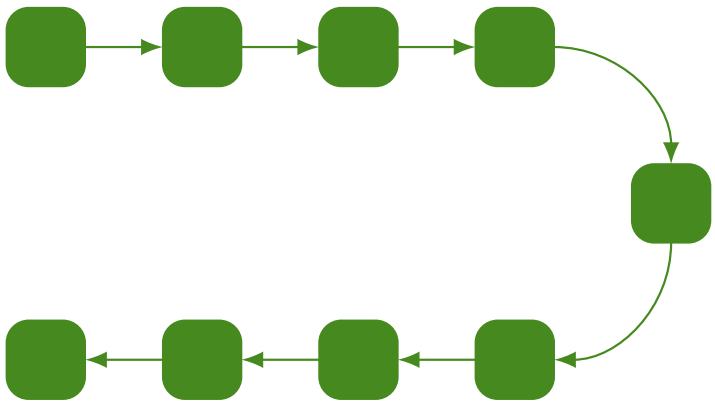




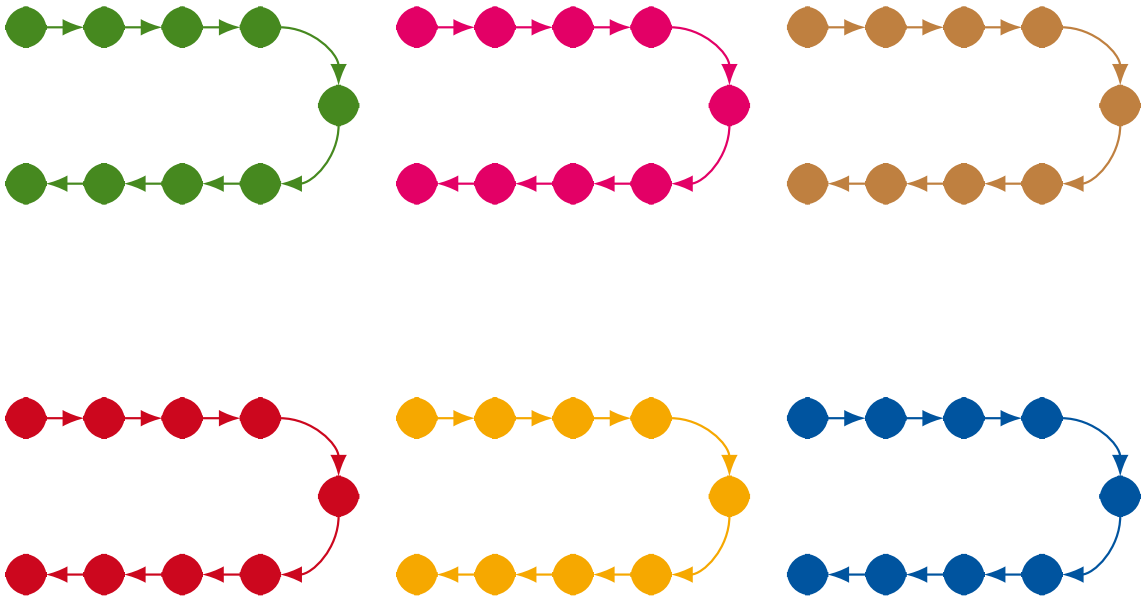
E. Ábrahám, G. Lakemeyer, F. Leofante, T. D. Niemüller, A. Tacchella.

PhD Leofante, publications in IJCAI'20, Information Systems Frontiers 2019, ECMS'19, AAAI'18, iFM'18, ICAPS'17, PlanRob'17, IRI'17.

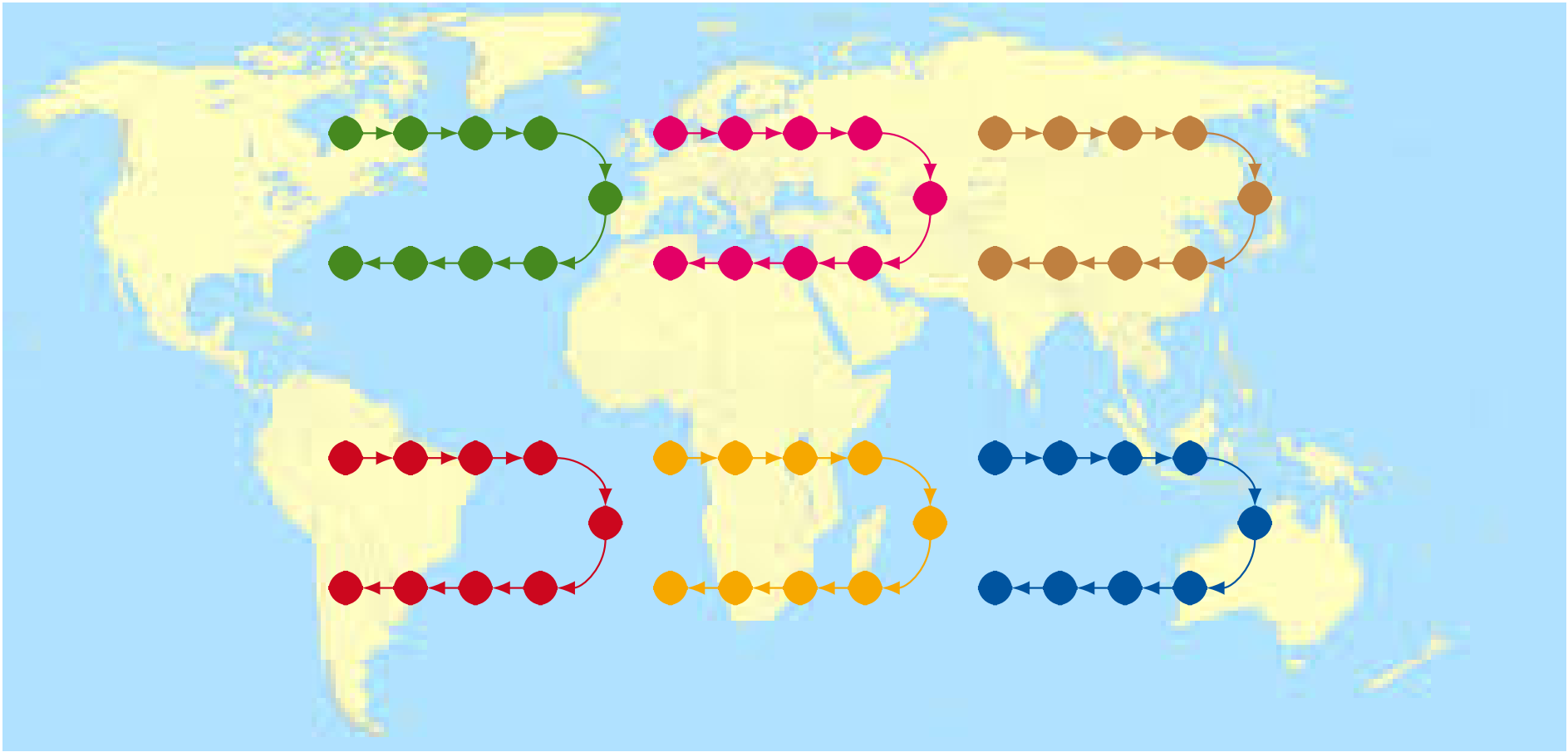
Product line construction and scheduling (Bosch)



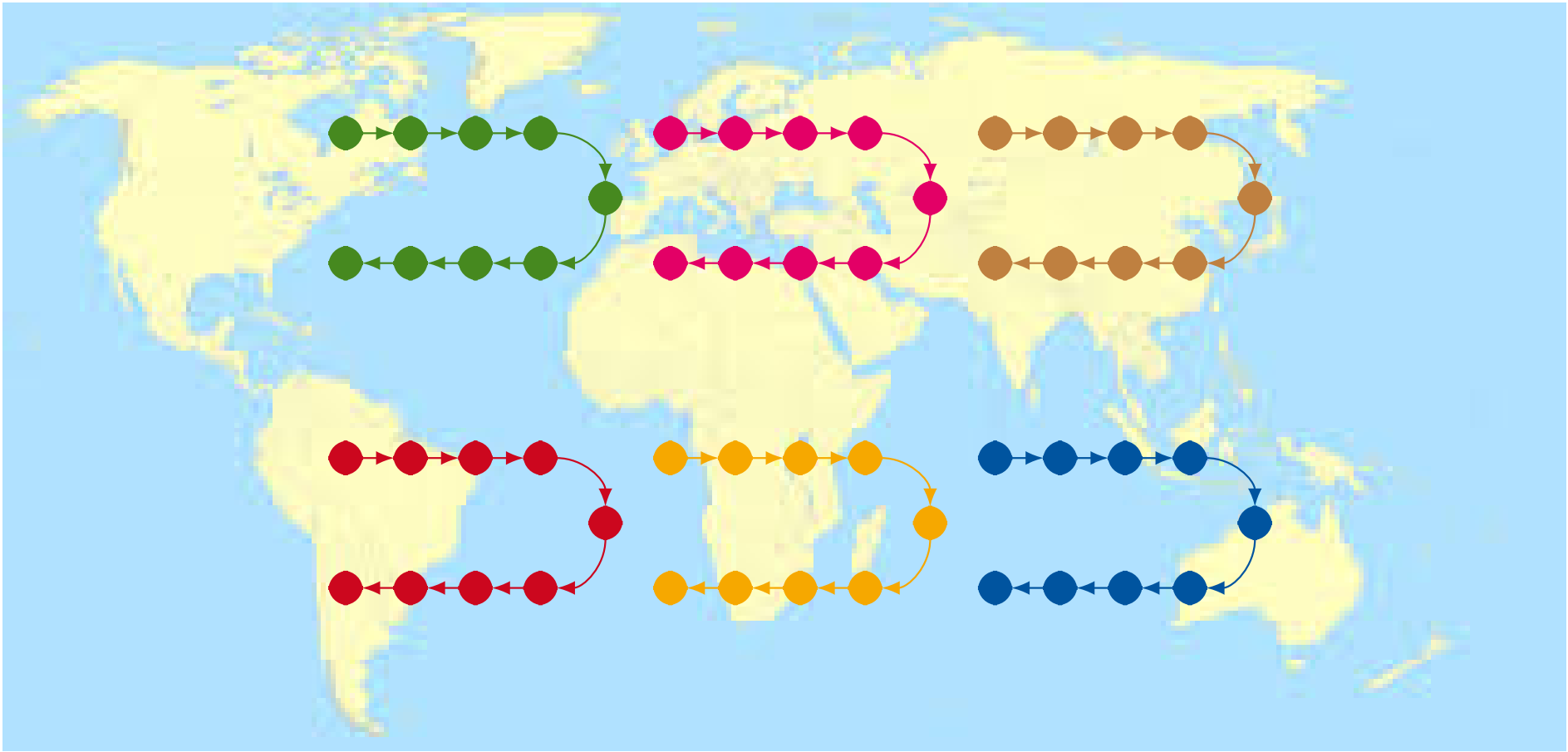
Product line construction and scheduling (Bosch)



Product line construction and scheduling (Bosch)



Product line construction and scheduling (Bosch)



product line functionalities — delivery distance

product line capacities (target: either 0% or ∼80% occupation)

long-time scheduling — customer preferences

forecast-based product line (de-)construction

Parameter synthesis

Parametric system model

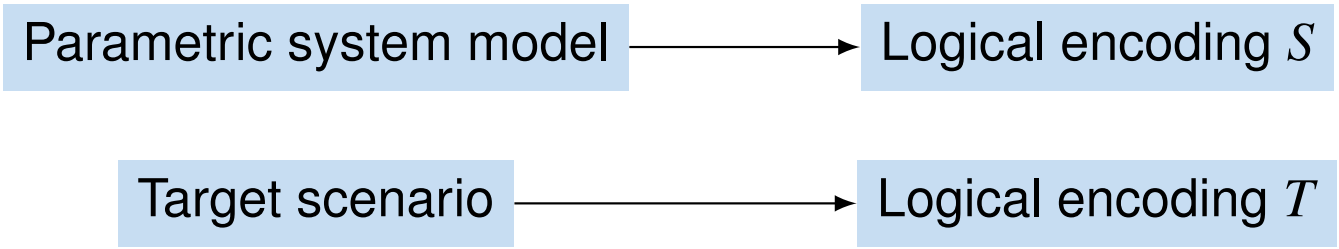
Target scenario

C. Dehnert, S. Junges, N. Jansen, F. Corzilius, M. Volk, H. Bruintjes, J.-P. Katoen, E. Ábrahám.

PROPhESY: A probabilistic parameter synthesis tool.

In Proc. of CAV'15.

Parameter synthesis



C. Dehnert, S. Junges, N. Jansen, F. Corzilius, M. Volk, H. Bruintjes, J.-P. Katoen, E. Ábrahám.

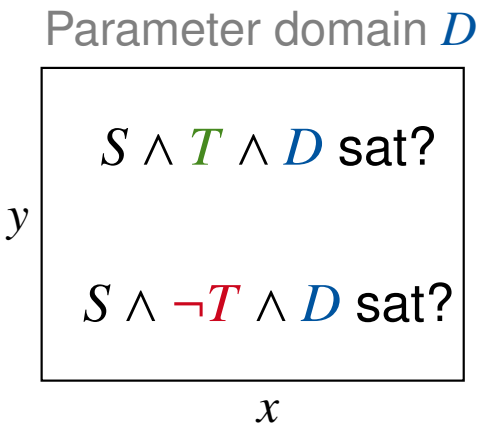
PROPhESY: A probabilistic parameter synthesis tool.

In Proc. of CAV'15.

Parameter synthesis

Parametric system model → Logical encoding S

Target scenario → Logical encoding T

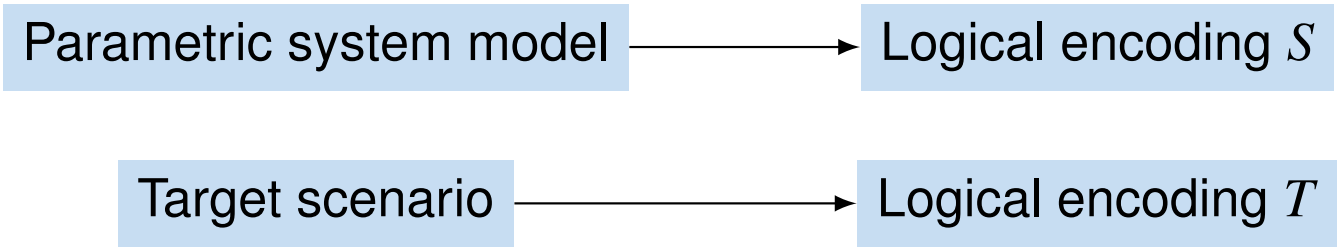


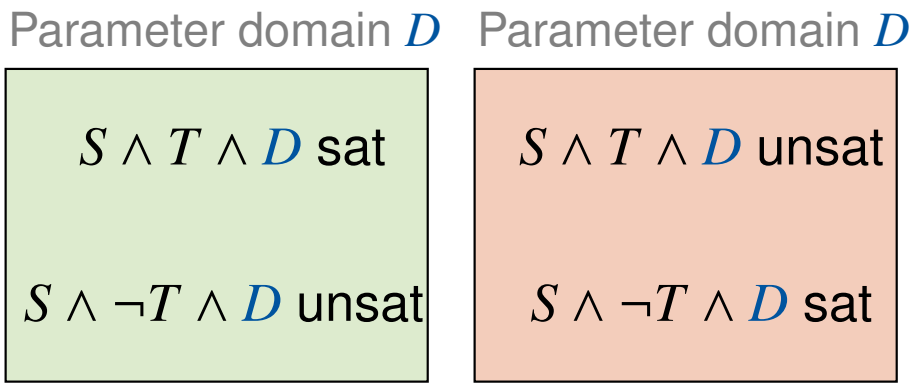
C. Dehnert, S. Junges, N. Jansen, F. Corzilius, M. Volk, H. Bruintjes, J.-P. Katoen, E. Ábrahám.

PROPhESY: A probabilistic parameter synthesis tool.

In Proc. of CAV'15.

Parameter synthesis



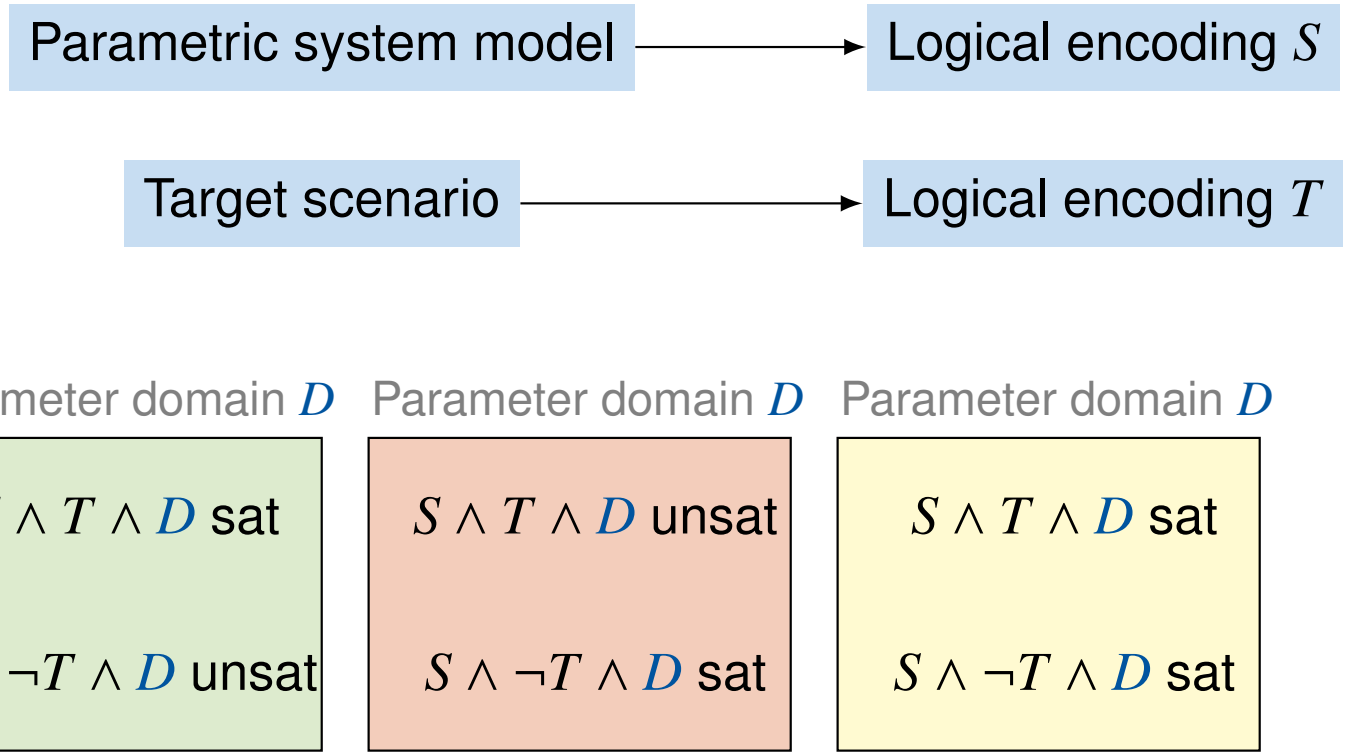


C. Dehnert, S. Junges, N. Jansen, F. Corzilius, M. Volk, H. Bruintjes, J.-P. Katoen, E. Ábrahám.

PROPhESY: A probabilistic parameter synthesis tool.

In Proc. of CAV'15.

Parameter synthesis



C. Dehnert, S. Junges, N. Jansen, F. Corzilius, M. Volk, H. Bruintjes, J.-P. Katoen, E. Ábrahám.

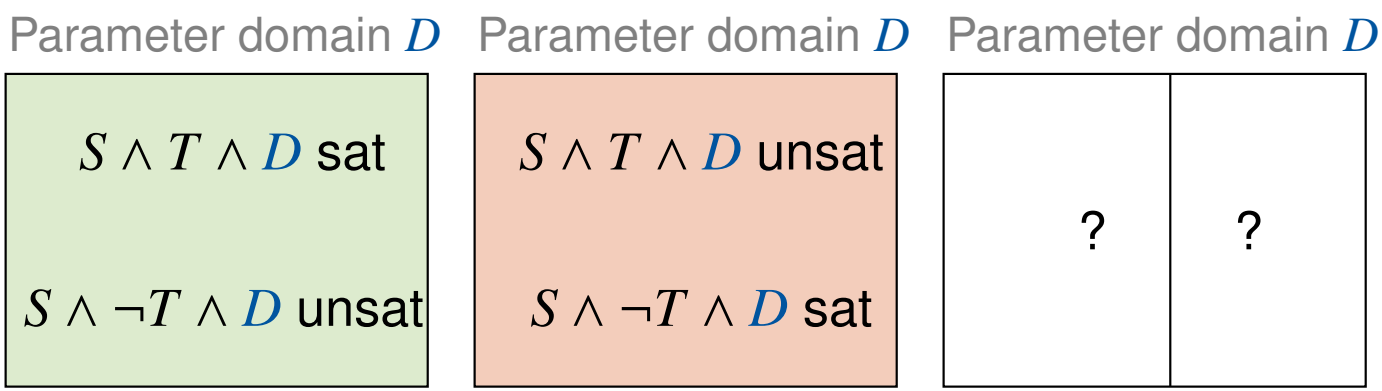
PROPhESY: A probabilistic parameter synthesis tool.

In Proc. of CAV'15.

Parameter synthesis

Parametric system model → Logical encoding S

Target scenario → Logical encoding T



C. Dehnert, S. Junges, N. Jansen, F. Corzilius, M. Volk, H. Bruintjes, J.-P. Katoen, E. Ábrahám.

PROPhESY: A probabilistic parameter synthesis tool.

In Proc. of CAV'15.

Parameter synthesis

Parametric system model → Logical encoding S

Target scenario → Logical encoding T

Parameter domain D | Parameter domain D | Parameter domain D

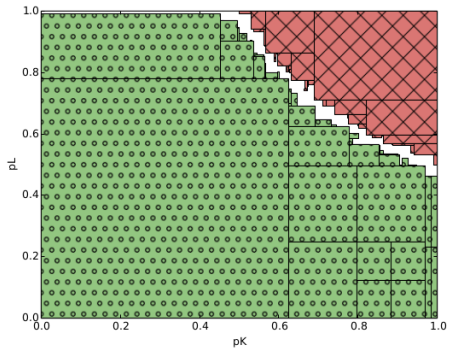
$S \wedge T \wedge D$ sat

$S \wedge \neg T \wedge D$ unsat

$S \wedge T \wedge D$ unsat

$S \wedge \neg T \wedge D$ sat

? ?

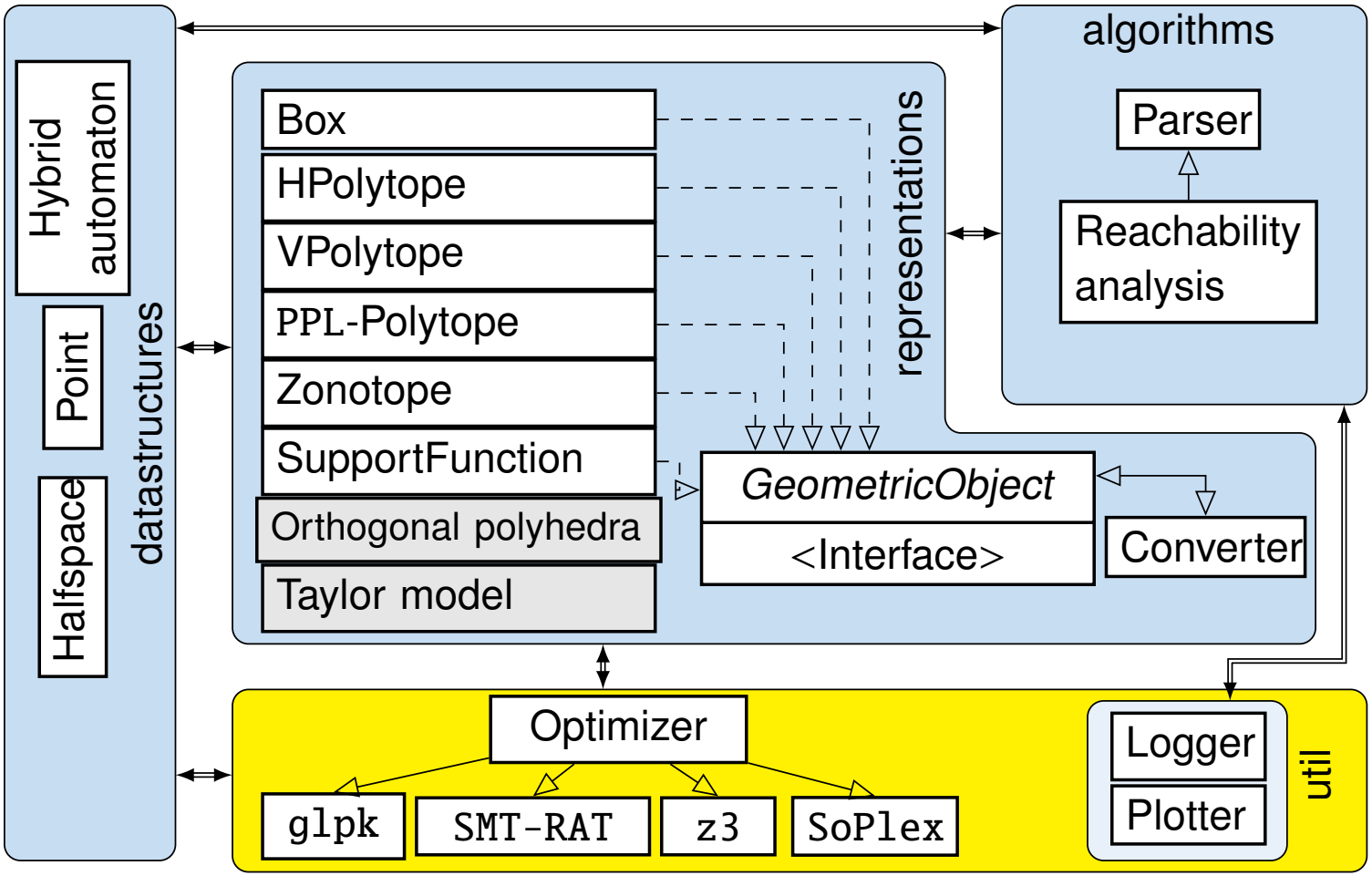


C. Dehnert, S. Junges, N. Jansen, F. Corzilius, M. Volk, H. Bruintjes, J.-P. Katoen, E. Ábrahám.

PROPhESY: A probabilistic parameter synthesis tool.

In Proc. of CAV'15.

Reachability analysis for hybrid systems with HyPro



S. Schupp, E. Ábrahám, I. Ben Makhlouf, S. Kowalewski.

HyPro: A C++ library of state set representations for hybrid systems reachability analysis.

In Proc. of NFM'17.

Contents

- SMT solving
- SMT-RAT
- Applications
- Future challenges

Usage of SMT solvers

- Standard input language, benchmarks
- Online usage, command-line, programming interfaces
- Black-box usage possible, but specific knowledge is advantageous
  - for efficient usage and
  - selection of the best fitting tool (e.g. fast vs complete).

Algorithmic as well as practical complexity

Beautiful but complex topics.

Algorithmic as well as practical complexity

Beautiful but complex topics.

Solvers in SMT-COMP'21, category QF_NRA:

Algorithmic as well as practical complexity

Beautiful but complex topics.

Solvers in SMT-COMP'21, category QF_NRA:

Mostly academic tools, not in the central focus of funding agencies.
More ideas than resources!

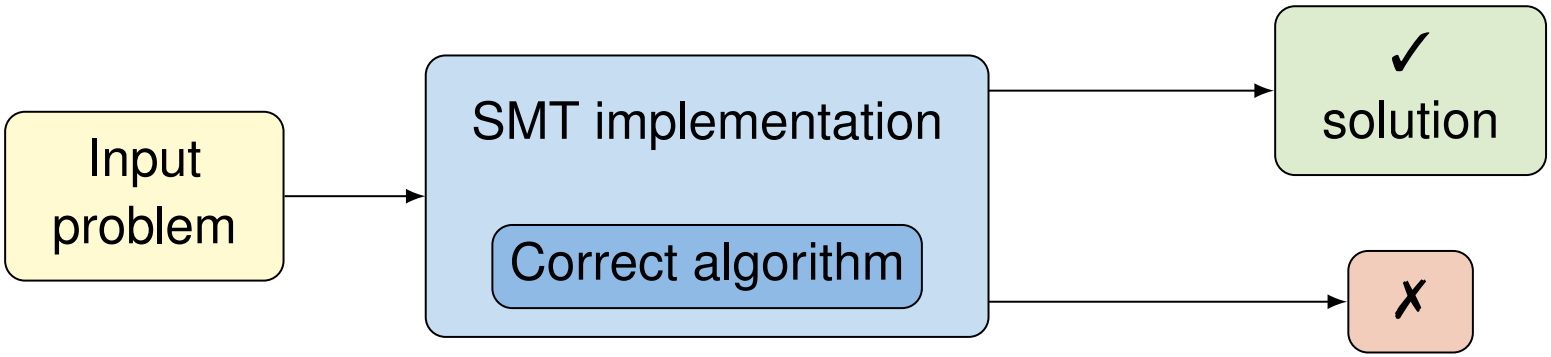
Proof generation

- Theoretical basics: algorithms with correctness proofs.

Correct algorithm

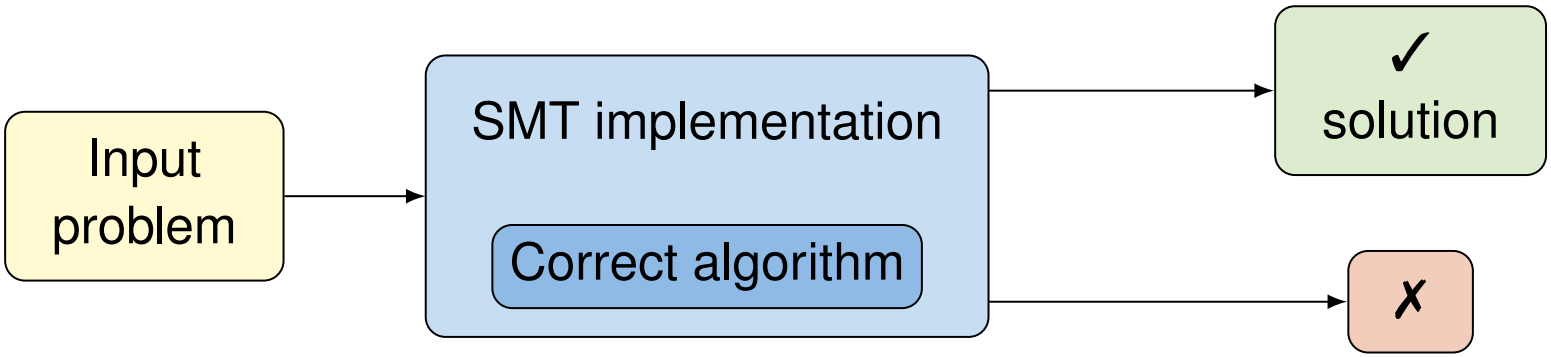
Proof generation

- Theoretical basics: algorithms with correctness proofs.
- Reliable tools: in QF_NRA for SMT-COMP'21, no bugs discovered on large benchmark sets.



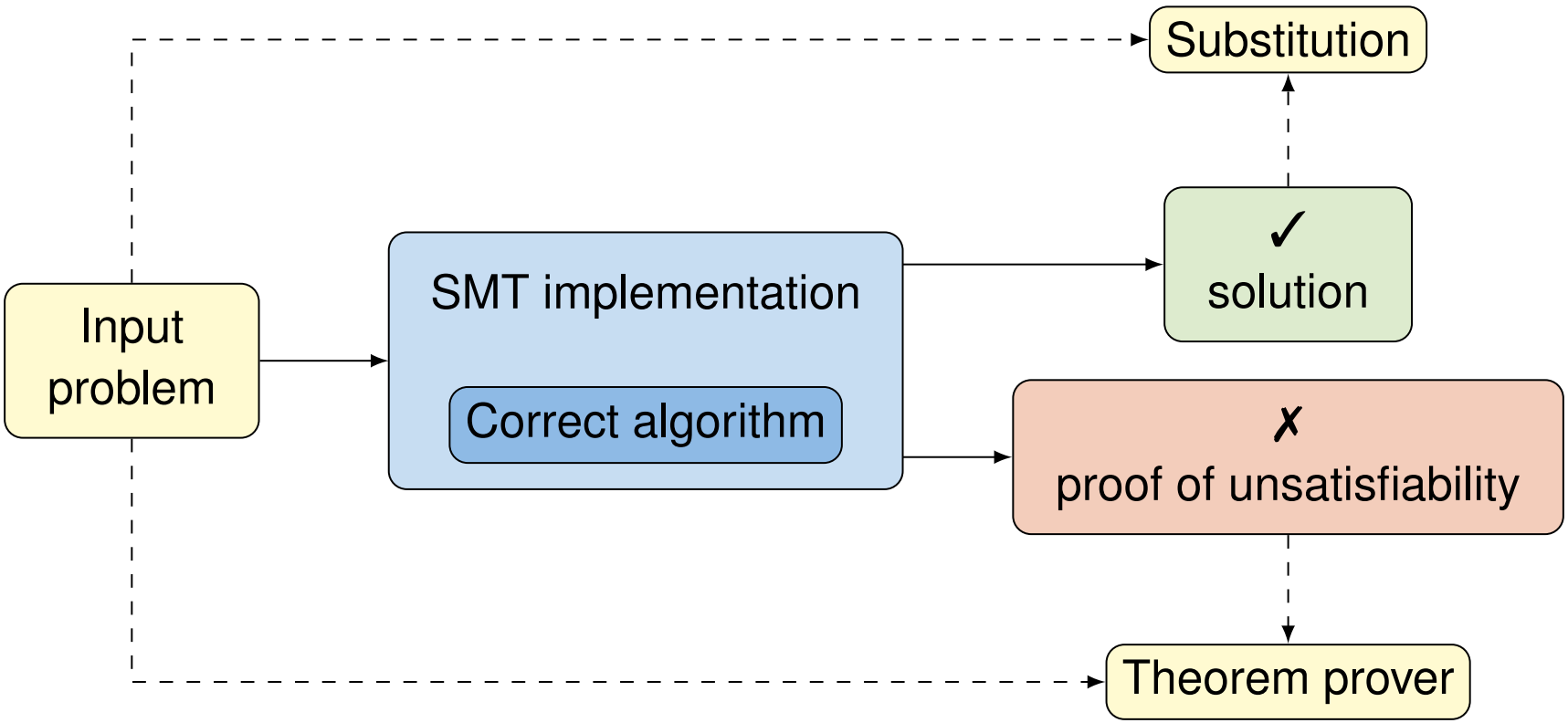
Proof generation

- Theoretical basics: algorithms with correctness proofs.
- Reliable tools: in QF_NRA for SMT-COMP'21, no bugs discovered on large benchmark sets.
- But still: bugs can remain undetected for a long time.



Proof generation

- Theoretical basics: algorithms with correctness proofs.
- Reliable tools: in QF_NRA for SMT-COMP'21, no bugs discovered on large benchmark sets.
- But still: bugs can remain undetected for a long time.
- Solution: automatically checkable proof certificates.



Further functionalities

- Model generation
- Explanations of unsatisfiability (unsat cores, interpolants)
- Optimization

- Satisfiability for quantified formulas
- Quantifier elimination (get all solutions symbolically)

- Scalability
  - Preprocessing
  - Heuristics, especially variable ordering
  - Machine learning
  - Closer integration of decision procedures
  - Parallelization

Education

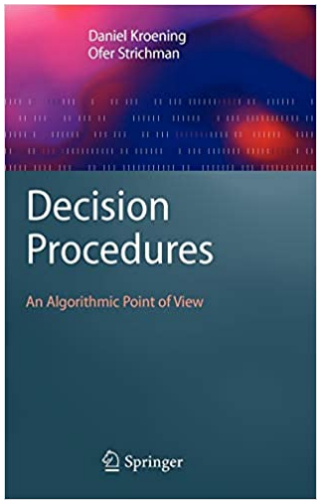
- We need more enthusiastic young researchers for academia as well as well-educated experts who go for an industrial career.
- High requirements, combined skills

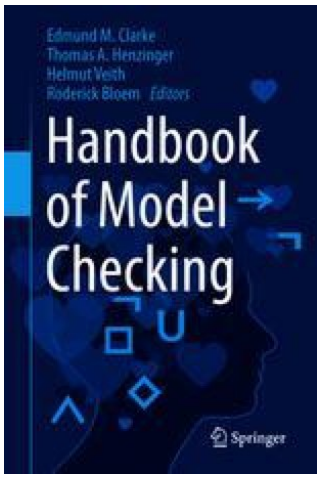
Education

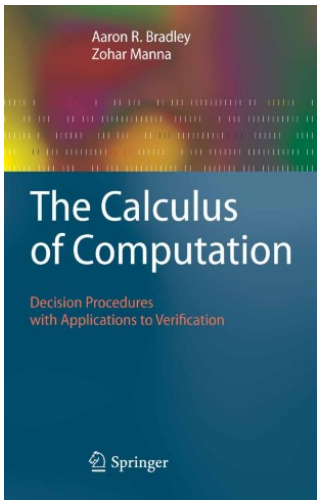
- We need more enthusiastic young researchers for academia as well as well-educated experts who go for an industrial career.
- High requirements, combined skills
- Girls, where are you?!

Education

- We need more enthusiastic young researchers for academia as well as well-educated experts who go for an industrial career.
- High requirements, combined skills
- Girls, where are you?!
- Very popular but challenging to teach:
  - Complex topic for students with diverse background.
  - Hard to combine theory and practice in limited time.
  - Restricted availability of teaching material.







You are wanted

Got interested? Wanna contribute to

- SMT solver development,
- benchmarks or
- applications?

Be part of it!