

# Formal Methods in Software Development

## SMT Solving

Mădălina Eraşcu

West University of Timișoara  
Faculty of Mathematics and Informatics

Based on slides of the lecture Satisfiability Checking (Erika Ábrahám), RTWH Aachen

December 7, 2018

- We want to extend propositional logic with theories.

- We want to extend propositional logic with theories.
- For satisfiability checking, SAT-solving will be extended to SAT-modulo-theories (SMT) solving.

- We want to extend propositional logic with theories.
- For satisfiability checking, SAT-solving will be extended to SAT-modulo-theories (SMT) solving.
- SMT-LIB: language, benchmarks, tutorials, ...
- SMT-COMP: performance and capabilities of tools
- SMT Workshop: held annually

- How can such an extension to SMT solving look like?

- How can such an extension to SMT solving look like?
- There are basically two different approaches:
  - **Eager SMT solving transforms** logical formulas over some theories into satisfiability-equivalent propositional logic formulas and applies **SAT solving**. (“Eager” means theory first)
  - **Lazy SMT solving** uses a **SAT** solver to find solutions for the Boolean skeleton of the formula, and a **theory solver** to check satisfiability in the underlying theory. (“Lazy” means theory later)

- How can such an extension to SMT solving look like?
- There are basically two different approaches:
  - **Eager SMT solving transforms** logical formulas over some theories into satisfiability-equivalent propositional logic formulas and applies **SAT solving**. (“Eager” means theory first)
  - **Lazy SMT solving** uses a **SAT** solver to find solutions for the Boolean skeleton of the formula, and a **theory solver** to check satisfiability in the underlying theory. (“Lazy” means theory later)
- Today we will have a closer look at the **lazy** approach.

# The Xmas problem

There are three types of Xmas presents Santa Claus can make.

- Santa Claus wants to reduce the overhead by making only two types.
- He needs at least 100 presents.
- He needs at least 5 of either type 1 or type 2.
- He needs at least 10 of the third type.
- Each present of type 1, 2, and 3 need 1, 2, resp. 5 minutes to make.
- Santa Claus is late, and he has only 3 hours left.
- Each present of type 1, 2, and 3 costs 3, 2, resp. 1 EUR.
- He has 300 EUR for presents in total.



# The Xmas problem

There are three types of Xmas presents Santa Claus can make.

- Santa Claus wants to reduce the overhead by making only two types.
- He needs at least 100 presents.
- He needs at least 5 of either type 1 or type 2.
- He needs at least 10 of the third type.
- Each present of type 1, 2, and 3 need 1, 2, resp. 5 minutes to make.
- Santa Claus is late, and he has only 3 hours left.
- Each present of type 1, 2, and 3 costs 3, 2, resp. 1 EUR.
- He has 300 EUR for presents in total.

$$\begin{aligned}(p_1 = 0 \vee p_2 = 0 \vee p_3 = 0) \wedge p_1 + p_2 + p_3 \geq 100 \wedge \\(p_1 \geq 5 \vee p_2 \geq 5) \wedge p_3 \geq 10 \wedge p_1 + 2p_2 + 5p_3 \leq 180 \wedge \\3p_1 + 2p_2 + p_3 \leq 300\end{aligned}$$

# The Xmas problem

There are three types of Xmas presents Santa Claus can make.

- Santa Claus wants to reduce the overhead by making only two types.
- He needs at least 100 presents.
- He needs at least 5 of either type 1 or type 2.
- He needs at least 10 of the third type.
- Each present of type 1, 2, and 3 need 1, 2, resp. 5 minutes to make.
- Santa Claus is late, and he has only 3 hours left.
- Each present of type 1, 2, and 3 costs 3, 2, resp. 1 EUR.
- He has 300 EUR for presents in total.

$$\begin{aligned}(p_1 = 0 \vee p_2 = 0 \vee p_3 = 0) \wedge p_1 + p_2 + p_3 \geq 100 \wedge \\ (p_1 \geq 5 \vee p_2 \geq 5) \wedge p_3 \geq 10 \wedge p_1 + 2p_2 + 5p_3 \leq 180 \wedge \\ 3p_1 + 2p_2 + p_3 \leq 300\end{aligned}$$

Logic:

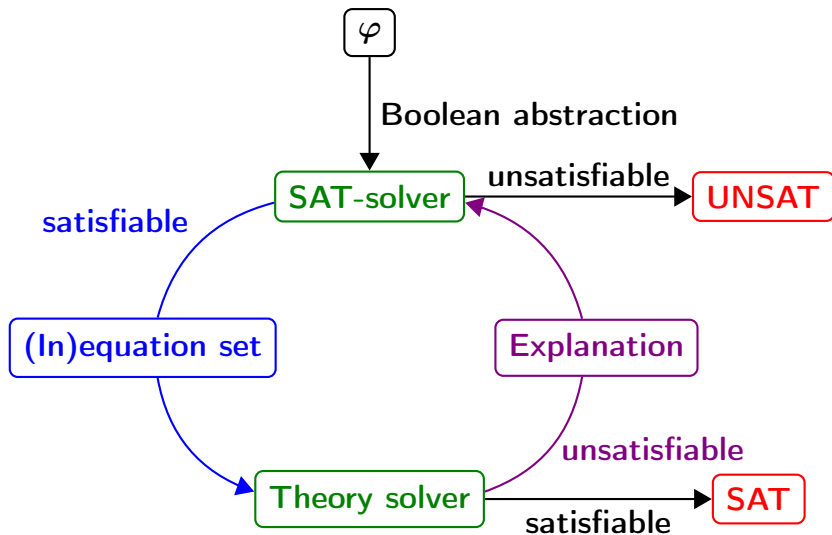
# The Xmas problem

There are three types of Xmas presents Santa Claus can make.

- Santa Claus wants to reduce the overhead by making only two types.
- He needs at least 100 presents.
- He needs at least 5 of either type 1 or type 2.
- He needs at least 10 of the third type.
- Each present of type 1, 2, and 3 need 1, 2, resp. 5 minutes to make.
- Santa Claus is late, and he has only 3 hours left.
- Each present of type 1, 2, and 3 costs 3, 2, resp. 1 EUR.
- He has 300 EUR for presents in total.

$$\begin{aligned}(p_1 = 0 \vee p_2 = 0 \vee p_3 = 0) \wedge p_1 + p_2 + p_3 \geq 100 \wedge \\(p_1 \geq 5 \vee p_2 \geq 5) \wedge p_3 \geq 10 \wedge p_1 + 2p_2 + 5p_3 \leq 180 \wedge \\3p_1 + 2p_2 + p_3 \leq 300\end{aligned}$$

**Logic:** First-order logic over the integers with addition.



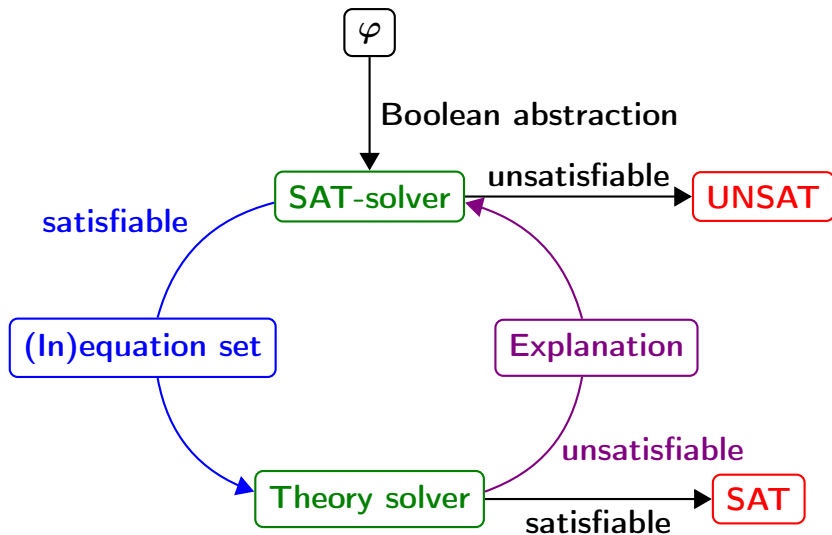
# Boolean abstraction

$$\begin{aligned} & \underbrace{(p_1 = 0)}_{a_1} \vee \underbrace{(p_2 = 0)}_{a_2} \vee \underbrace{(p_3 = 0)}_{a_3} \wedge \underbrace{(p_1 + p_2 + p_3 \geq 100)}_{a_4} \wedge \\ & \underbrace{(p_1 \geq 5)}_{a_5} \vee \underbrace{(p_2 \geq 5)}_{a_6} \wedge \underbrace{(p_3 \geq 10)}_{a_7} \wedge \underbrace{(p_1 + 2p_2 + 5p_3 \leq 180)}_{a_8} \wedge \\ & \underbrace{(3p_1 + 2p_2 + p_3 \leq 300)}_{a_9} \end{aligned}$$

# Boolean abstraction

$$\begin{aligned} & \underbrace{(p_1 = 0)}_{a_1} \vee \underbrace{(p_2 = 0)}_{a_2} \vee \underbrace{(p_3 = 0)}_{a_3} \wedge \underbrace{(p_1 + p_2 + p_3 \geq 100)}_{a_4} \wedge \\ & \underbrace{(p_1 \geq 5)}_{a_5} \vee \underbrace{(p_2 \geq 5)}_{a_6} \wedge \underbrace{(p_3 \geq 10)}_{a_7} \wedge \underbrace{(p_1 + 2p_2 + 5p_3 \leq 180)}_{a_8} \wedge \\ & \underbrace{(3p_1 + 2p_2 + p_3 \leq 300)}_{a_9} \end{aligned}$$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$



$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false



$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4$  : 1

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

*DL2* :



$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

*DL2* :  $a_2 : 0$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

*DL2* :  $a_2 : 0, a_3 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

*DL2* :  $a_2 : 0, a_3 : 1$

*DL3* :

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

*DL2* :  $a_2 : 0, a_3 : 1$

*DL3* :  $a_5 : 0$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

*DL2* :  $a_2 : 0, a_3 : 1$

*DL3* :  $a_5 : 0, a_6 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:  $a_1, \dots, a_9$

Assignment to decision variables: false

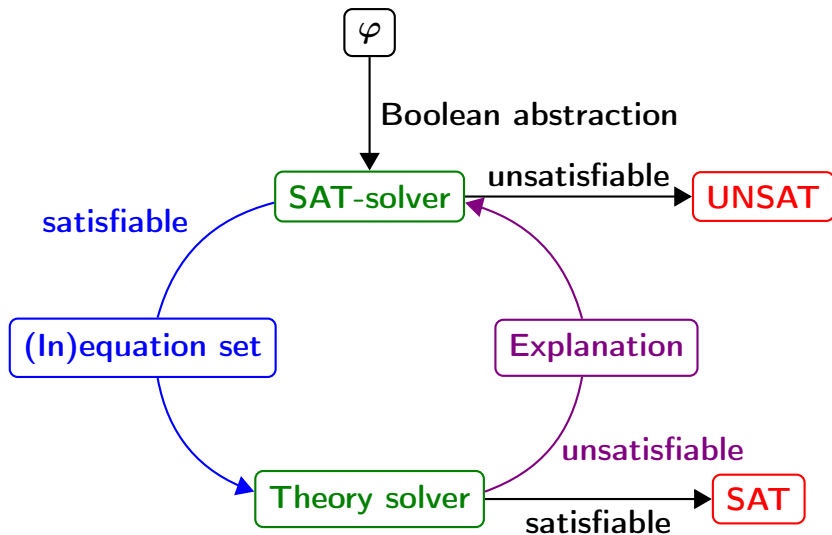
*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

*DL2* :  $a_2 : 0, a_3 : 1$

*DL3* :  $a_5 : 0, a_6 : 1$

Solution found for the Boolean abstraction.



# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$      $DL1 : a_1 : 0$   
 $DL2 : a_2 : 0, a_3 : 1$                        $DL3 : a_5 : 0, a_6 : 1$



# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$      $DL1 : a_1 : 0$

$DL2 : a_2 : 0, a_3 : 1$      $DL3 : a_5 : 0, a_6 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_3, a_6$

# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$      $DL1 : a_1 : 0$

$DL2 : a_2 : 0, a_3 : 1$

$DL3 : a_5 : 0, a_6 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_3, a_6$

$$\begin{aligned} & (\underbrace{p_1 = 0}_{a_1} \vee \underbrace{p_2 = 0}_{a_2} \vee \underbrace{p_3 = 0}_{a_3}) \wedge \underbrace{p_1 + p_2 + p_3 \geq 100}_{a_4} \wedge \\ & (\underbrace{p_1 \geq 5}_{a_5} \vee \underbrace{p_2 \geq 5}_{a_6}) \wedge \underbrace{p_3 \geq 10}_{a_7} \wedge \underbrace{p_1 + 2p_2 + 5p_3 \leq 180}_{a_8} \wedge \\ & \underbrace{3p_1 + 2p_2 + p_3 \leq 300}_{a_9} \end{aligned}$$

# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$      $DL1 : a_1 : 0$

$DL2 : a_2 : 0, a_3 : 1$

$DL3 : a_5 : 0, a_6 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_3, a_6$

$$\begin{aligned} & \underbrace{(p_1 = 0)}_{a_1} \vee \underbrace{(p_2 = 0)}_{a_2} \vee \underbrace{(p_3 = 0)}_{a_3} \wedge \underbrace{(p_1 + p_2 + p_3 \geq 100)}_{a_4} \wedge \\ & \underbrace{(p_1 \geq 5)}_{a_5} \vee \underbrace{(p_2 \geq 5)}_{a_6} \wedge \underbrace{(p_3 \geq 10)}_{a_7} \wedge \underbrace{(p_1 + 2p_2 + 5p_3 \leq 180)}_{a_8} \wedge \\ & \underbrace{(3p_1 + 2p_2 + p_3 \leq 300)}_{a_9} \end{aligned}$$

Encoding:

$$\begin{array}{lll} a_4 : p_1 + p_2 + p_3 \geq 100 & a_7 : p_3 \geq 10 & a_8 : p_1 + 2p_2 + 5p_3 \leq 180 \\ a_9 : 3p_1 + 2p_2 + p_3 \leq 300 & a_3 : p_3 = 0 & a_6 : p_2 \geq 5 \end{array}$$

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_3 : p_3 = 0$$

$$a_6 : p_2 \geq 5$$

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_3 : p_3 = 0$$

$$a_6 : p_2 \geq 5$$

No.

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_3 : p_3 = 0$$

$$a_6 : p_2 \geq 5$$

No.

Reason:

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

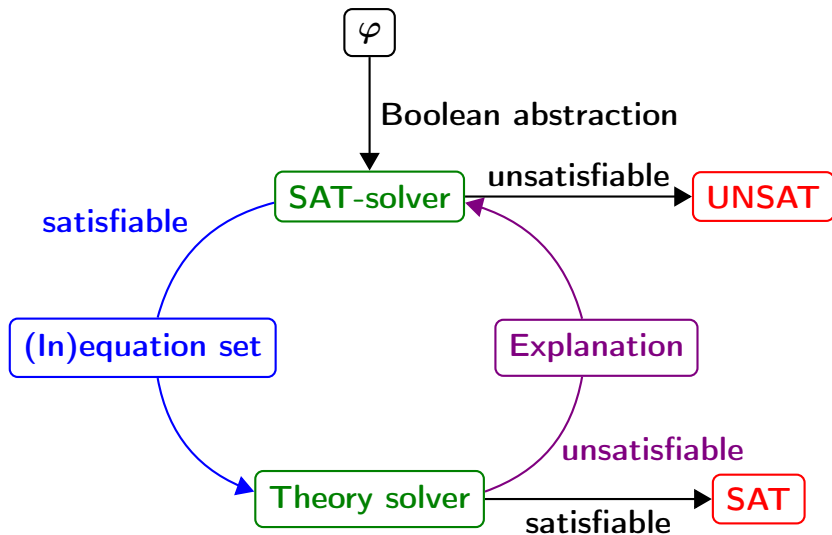
$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_3 : p_3 = 0$$

$$a_6 : p_2 \geq 5$$

No.

Reason:  $\underbrace{p_3 = 0}_{a_3} \wedge \underbrace{p_3 \geq 10}_{a_7}$  are conflicting.





Add clause  $(\neg a_3 \vee \neg a_7)$ .

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$

*DL1* :  $a_1 : 0$

*DL2* :  $a_2 : 0, a_3 : 1$

*DL3* :  $a_5 : 0, a_6 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

$$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1$

*DL2* :

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1$

*DL2* :  $a_5 : 0$



$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1$

*DL2* :  $a_5 : 0, a_6 : 1$

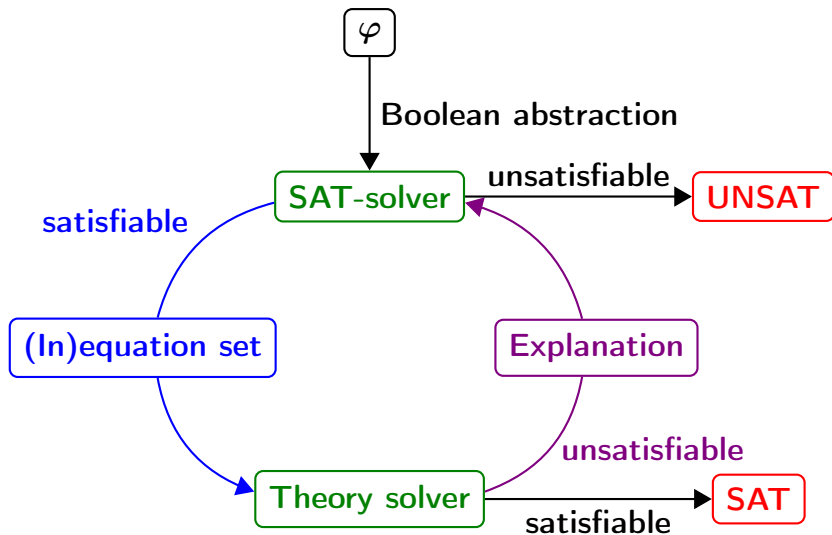
$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1$

*DL2* :  $a_5 : 0, a_6 : 1$

Solution found for the Boolean abstraction.



# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$      $DL1 : a_1 : 0, a_2 : 1$

$DL2 : a_5 : 0, a_6 : 1$

# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$      $DL1 : a_1 : 0, a_2 : 1$

$DL2 : a_5 : 0, a_6 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_2, a_6$

# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$     $DL1 : a_1 : 0, a_2 : 1$

$DL2 : a_5 : 0, a_6 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_2, a_6$

$$\begin{aligned} & (\underbrace{p_1 = 0}_{a_1} \vee \underbrace{p_2 = 0}_{a_2} \vee \underbrace{p_3 = 0}_{a_3}) \wedge \underbrace{p_1 + p_2 + p_3 \geq 100}_{a_4} \wedge \\ & (\underbrace{p_1 \geq 5}_{a_5} \vee \underbrace{p_2 \geq 5}_{a_6}) \wedge \underbrace{p_3 \geq 10}_{a_7} \wedge \underbrace{p_1 + 2p_2 + 5p_3 \leq 180}_{a_8} \wedge \\ & \underbrace{3p_1 + 2p_2 + p_3 \leq 300}_{a_9} \wedge (\neg a_3 \vee \neg a_7) \end{aligned}$$

# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$     $DL1 : a_1 : 0, a_2 : 1$

$DL2 : a_5 : 0, a_6 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_2, a_6$

$$\begin{aligned} & (\underbrace{p_1 = 0}_{a_1} \vee \underbrace{p_2 = 0}_{a_2} \vee \underbrace{p_3 = 0}_{a_3}) \wedge \underbrace{p_1 + p_2 + p_3 \geq 100}_{a_4} \wedge \\ & (\underbrace{p_1 \geq 5}_{a_5} \vee \underbrace{p_2 \geq 5}_{a_6}) \wedge \underbrace{p_3 \geq 10}_{a_7} \wedge \underbrace{p_1 + 2p_2 + 5p_3 \leq 180}_{a_8} \wedge \\ & \underbrace{3p_1 + 2p_2 + p_3 \leq 300}_{a_9} \wedge (\neg a_3 \vee \neg a_7) \end{aligned}$$

Encoding:

$$\begin{array}{lll} a_4 : p_1 + p_2 + p_3 \geq 100 & a_7 : p_3 \geq 10 & a_8 : p_1 + 2p_2 + 5p_3 \leq 180 \\ a_9 : 3p_1 + 2p_2 + p_3 \leq 300 & a_2 : p_2 = 0 & a_6 : p_2 \geq 5 \end{array}$$

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_2 : p_2 = 0$$

$$a_6 : p_2 \geq 5$$



Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_2 : p_2 = 0$$

$$a_6 : p_2 \geq 5$$

No.

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_2 : p_2 = 0$$

$$a_6 : p_2 \geq 5$$

No.

Reason:

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

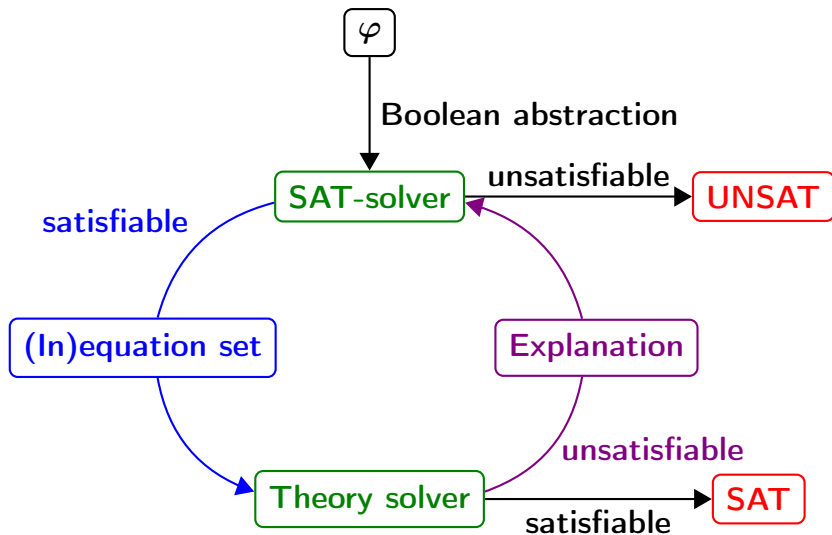
$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_2 : p_2 = 0$$

$$a_6 : p_2 \geq 5$$

No.

Reason:  $\underbrace{p_2 = 0}_{a_2} \wedge \underbrace{p_2 \geq 5}_{a_6}$  are conflicting.



Add clause  $(\neg a_2 \vee \neg a_6)$ .

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7) \wedge$$
$$(\neg a_2 \vee \neg a_6)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1$

*DL2* :  $a_5 : 0, a_6 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7) \wedge$$
$$(\neg a_2 \vee \neg a_6)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7) \wedge$$
$$(\neg a_2 \vee \neg a_6)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1, a_6 : 0$

$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7) \wedge$$
$$(\neg a_2 \vee \neg a_6)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1, a_6 : 0, a_5 : 1$

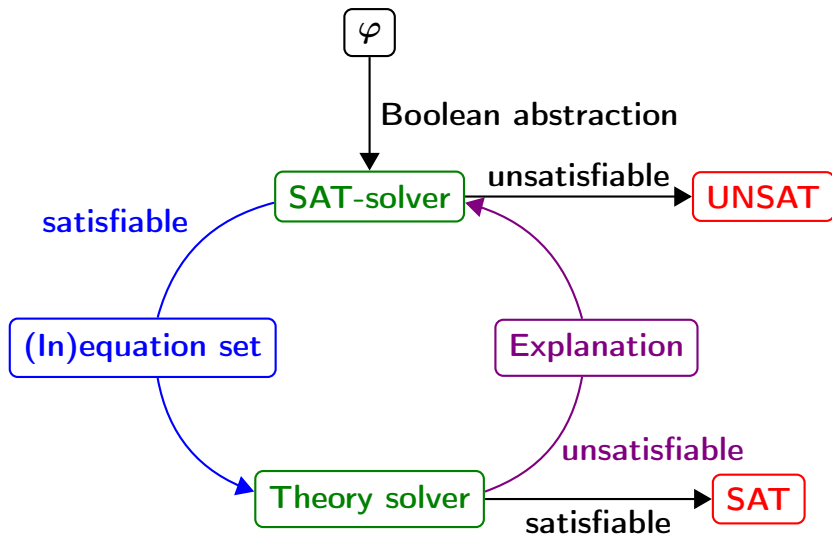


$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7) \wedge$$
$$(\neg a_2 \vee \neg a_6)$$

*DL0* :  $a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$

*DL1* :  $a_1 : 0, a_2 : 1, a_6 : 0, a_5 : 1$

Solution found for the Boolean abstraction.



$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$      $DL1 : a_1 : 0, a_2 : 1, a_6 : 0, a_5 : 1$

# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$     $DL1 : a_1 : 0, a_2 : 1, a_6 : 0, a_5 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_2, a_5$

# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$     $DL1 : a_1 : 0, a_2 : 1, a_6 : 0, a_5 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_2, a_5$

$$\begin{aligned} & (\underbrace{p_1 = 0}_{a_1} \vee \underbrace{p_2 = 0}_{a_2} \vee \underbrace{p_3 = 0}_{a_3}) \wedge \underbrace{p_1 + p_2 + p_3 \geq 100}_{a_4} \wedge \\ & (\underbrace{p_1 \geq 5}_{a_5} \vee \underbrace{p_2 \geq 5}_{a_6}) \wedge \underbrace{p_3 \geq 10}_{a_7} \wedge \underbrace{p_1 + 2p_2 + 5p_3 \leq 180}_{a_8} \wedge \\ & \underbrace{3p_1 + 2p_2 + p_3 \leq 300}_{a_9} \wedge (\neg a_3 \vee \neg a_7) \wedge (\neg a_2 \vee \neg a_6) \end{aligned}$$

# Theory solving

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$     $DL1 : a_1 : 0, a_2 : 1, a_6 : 0, a_5 : 1$

True theory constraints:  $a_4, a_7, a_8, a_9, a_2, a_5$

$$\begin{aligned} & \underbrace{(p_1 = 0 \vee p_2 = 0 \vee p_3 = 0)}_{a_1} \wedge \underbrace{p_1 + p_2 + p_3 \geq 100}_{a_4} \wedge \\ & \underbrace{(p_1 \geq 5 \vee p_2 \geq 5)}_{a_5} \wedge \underbrace{p_3 \geq 10}_{a_7} \wedge \underbrace{p_1 + 2p_2 + 5p_3 \leq 180}_{a_8} \wedge \\ & \underbrace{3p_1 + 2p_2 + p_3 \leq 300}_{a_9} \wedge (\neg a_3 \vee \neg a_7) \wedge (\neg a_2 \vee \neg a_6) \end{aligned}$$

Encoding:

$$\begin{array}{lll} a_4 : p_1 + p_2 + p_3 \geq 100 & a_7 : p_3 \geq 10 & a_8 : p_1 + 2p_2 + 5p_3 \leq 180 \\ a_9 : 3p_1 + 2p_2 + p_3 \leq 300 & a_2 : p_2 = 0 & a_5 : p_1 \geq 5 \end{array}$$

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_2 : p_2 = 0$$

$$a_5 : p_1 \geq 5$$

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_2 : p_2 = 0$$

$$a_5 : p_1 \geq 5$$

Yes.



Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_2 : p_2 = 0$$

$$a_5 : p_1 \geq 5$$

Yes. E.g.,

Is the conjunction of the following constraints satisfiable?

$$a_4 : p_1 + p_2 + p_3 \geq 100$$

$$a_7 : p_3 \geq 10$$

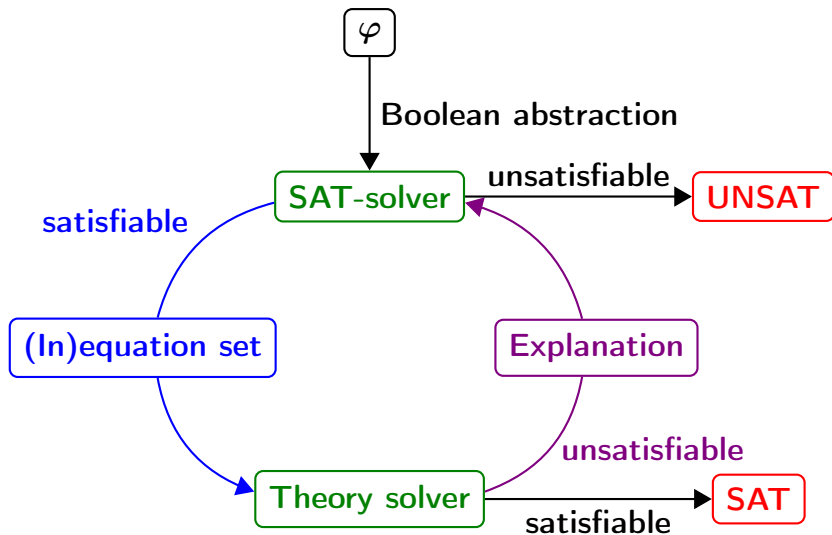
$$a_8 : p_1 + 2p_2 + 5p_3 \leq 180$$

$$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$$

$$a_2 : p_2 = 0$$

$$a_5 : p_1 \geq 5$$

Yes. E.g.,  $p_1 = 90$ ,  $p_2 = 0$ ,  $p_3 = 10$  is a solution.



Input: Quantifier-free FO logic formula  $\varphi$  over some theories in CNF without any negation

Output: Satisfiability of the input formula

- Let  $C$  be the set of all theory constraints in  $\varphi$
- Let  $P = \{p_c | c \in C\}$  be a set of fresh atomic propositions (fresh means not appearing in  $\varphi$ )
- Let  $\mu : C \rightarrow P$  be the bijective function with  $\mu(c) = p_c$  and  $\mu^{-1}(p_c) = c$
- For each formula  $\varphi'$  with constraints from  $C$  we define the Boolean abstraction (or Boolean skeleton)  $\mu(\varphi')$  of  $\varphi'$  under  $\mu$  to be the propositional logic formula we get by replacing each theory constraint  $c$  in  $\varphi'$  by  $\mu(c)$

# Lazy SMT-solving

Input: Quantifier-free FO logic formula  $\varphi$  over some theories in CNF without any negation

Output: Satisfiability of the input formula

- 1 Build the Boolean skeleton (also called Boolean abstraction)  $\varphi_{abs}$  of the input formula  $\varphi$  by replacing each theory constraint  $c \in C$  in  $\varphi$  by  $\mu(c)$
- 2 Search for a solution for  $\varphi_{abs}$  (using SAT solving)
- 3 If there is no solution for  $\varphi_{abs}$  then the input formula  $\varphi$  is unsatisfiable
- 4 Otherwise, given a solution  $\alpha : P \rightarrow \{0, 1\}$  for  $\varphi_{abs}$ , check the set of all true theory constraints  $C_\mu := \{c \in C \mid \alpha(\mu(c)) = 1\}$  for consistency
- 5 If they are consistent then input formula is satisfiable
- 6 Otherwise, compute an explanation for the inconsistency in form of CNF formula with constraints from  $C$  implying that the constraints in  $C_\mu$  cannot be all true
- 7 Learn the Boolean abstraction  $E$  of the theory lemma by setting  $\varphi_{abs} := \varphi_{abs} \wedge E$
- 8 Apply conflict resolution if the learnt clause is not asserting
- 9 Goto 2

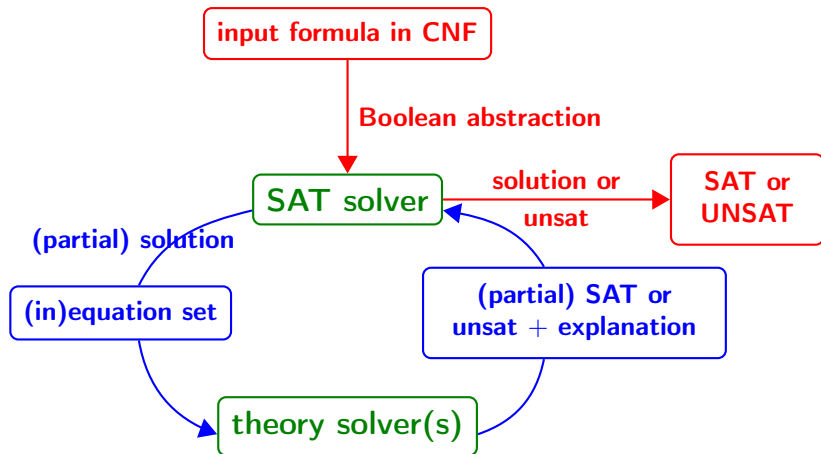
# Lazy SMT-solving

Input: Quantifier-free FO logic formula  $\varphi$  over some theories in CNF **without any negation**

Output: Satisfiability of the input formula

- 1 Build the Boolean skeleton (also called Boolean abstraction)  $\varphi_{abs}$  of the input formula  $\varphi$  by replacing each theory constraint  $c \in C$  in  $\varphi$  by  $\mu(c)$
- 2 Search for a solution for  $\varphi_{abs}$  (using SAT solving)
- 3 If there is no solution for  $\varphi_{abs}$  then the input formula  $\varphi$  is unsatisfiable
- 4 Otherwise, given a solution  $\alpha : P \rightarrow \{0, 1\}$  for  $\varphi_{abs}$ , check the **set of all true theory constraints**  $C_\mu := \{c \in C \mid \alpha(\mu(c)) = 1\}$  for consistency
- 5 If they are consistent then input formula is satisfiable
- 6 Otherwise, compute an explanation for the inconsistency in form of CNF formula with constraints from  $C$  implying that the constraints in  $C_\mu$  cannot be all true
- 7 Learn the Boolean abstraction  $E$  of the theory lemma by setting  $\varphi_{abs} := \varphi_{abs} \wedge E$
- 8 Apply conflict resolution if the learnt clause is not asserting
- 9 Goto 2

# Less lazy SMT-solving



# Requirements on the theory solver

- 1 **Incrementality**: In less lazy solving we extend the set of constraints. The solver should make use of the previous satisfiability check for the check of the extended set.
- 2 **(Preferably minimal) infeasible subsets**: Compute a reason for unsatisfaction
- 3 **Backtracking**: The theory solver should be able to remove constraints in inverse chronological order.



- This approach strictly divides between logical (Boolean) structure and theory constraints.
- There are other approaches, which do not divide Boolean and theory solving so strictly.
- One idea: Propagate in the SAT-solver **bounds** on theory variables.