Formal Methods in Software Development

SMT Solving

Mădălina Erașcu

West University of Timișoara
Faculty of Mathematics and Informatics
Department of Computer Science

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

WS 2019/2020

SMT solving

- We want to extend propositional logic with 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 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

SMT solving

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

SMT solving

- 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)

SMT solving

- 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.

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

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.

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

Logic:

The Xmas problem

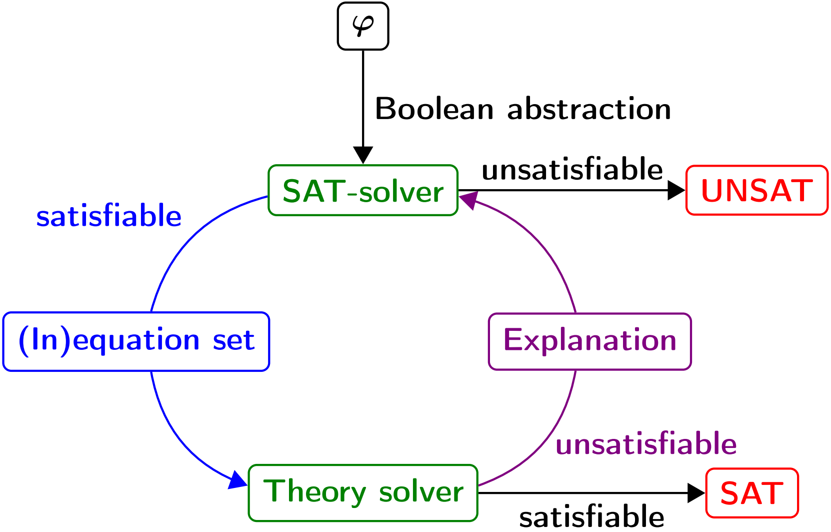
There are three types of Xmas presents Santa Claus can make.

- 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.

Lazy SMT-solving



Boolean abstraction

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

Boolean abstraction

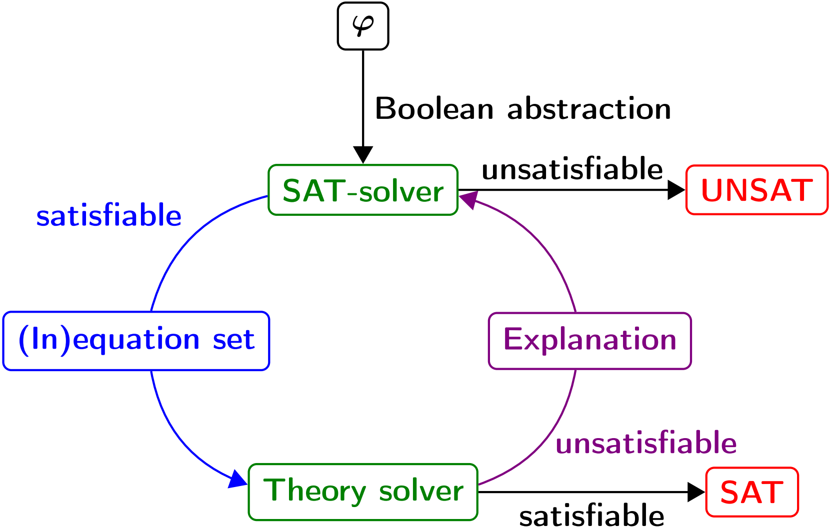
$$(\underbrace{p_1 = 0}_{a_1} \vee \underbrace{p_2 = 0}_{a_2} \vee \underbrace{p_3 = 0}_{a_3}) \wedge \underbrace{p_1 + p_2 + p_3 \geq 100}_{a_4} \wedge$$

$$(\underbrace{p_1 \geq 5}_{a_5} \vee \underbrace{p_2 \geq 5}_{a_6}) \wedge \underbrace{p_3 \geq 10}_{a_7} \wedge \underbrace{p_1 + 2p_2 + 5p_3 \leq 180}_{a_8} \wedge$$

$$\underbrace{3p_1 + 2p_2 + p_3 \leq 300}_{a_9}$$

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

Lazy SMT-solving



SAT-solving

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

Assume a fixed variable order: $a_1, \ldots, a_9$
Assignment to decision variables: false

SAT-solving

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

Assume a fixed variable order:	$a_1, \ldots, a_9$
Assignment to decision variables:	false

$DL0$:

SAT-solving

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

Assume a fixed variable order: $a_1, \ldots, a_9$
Assignment to decision variables: false

$DL0 : a_4 : 1$

SAT-solving

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

Assume a fixed variable order:	$a_1, \ldots, a_9$
Assignment to decision variables:	false

$DL0 : a_4 : 1, a_7 : 1$

SAT-solving

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

Assume a fixed variable order:	$a_1, \ldots, a_9$
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: $a_1, \ldots, a_9$
Assignment to decision variables: false

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

SAT-solving

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

Assume a fixed variable order: $a_1, \ldots, a_9$
Assignment to decision variables: false

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

SAT-solving

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

Assume a fixed variable order: $a_1, \ldots, a_9$
Assignment to decision variables: false

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

SAT-solving

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

Assume a fixed variable order:	$a_1, \ldots, a_9$
Assignment to decision variables:	false

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$
$DL1 : a_1 : 0$
$DL2 :$

SAT-solving

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

Assume a fixed variable order:	$a_1, \ldots, a_9$
Assignment to decision variables:	false

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$
$DL1 : a_1 : 0$
$DL2 : a_2 : 0$

SAT-solving

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

Assume a fixed variable order: $a_1, \ldots, a_9$
Assignment to decision variables: false

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

SAT-solving

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

Assume a fixed variable order:	$a_1, \ldots, a_9$
Assignment to decision variables:	false

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

SAT-solving

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

Assume a fixed variable order:	$a_1, \ldots, a_9$
Assignment to decision variables:	false

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

SAT-solving

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

Assume a fixed variable order: $a_1, \ldots, a_9$
Assignment to decision variables: false

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

SAT-solving

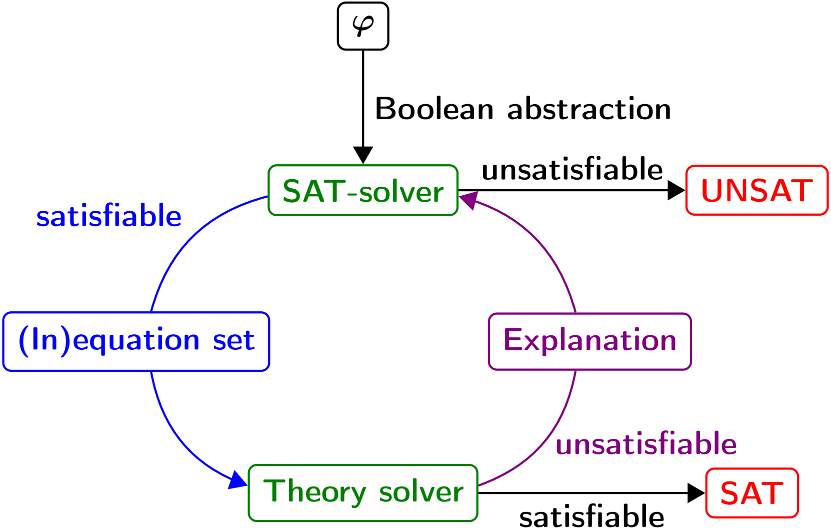
$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

Assume a fixed variable order:	$a_1, \ldots, a_9$
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.

Lazy SMT-solving



Theory solving

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

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

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

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

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

Theory solving

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

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

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

Encoding:

$a_4 : p_1 + p_2 + p_3 \geq 100 \quad a_7 : p_3 \geq 10 \quad a_8 : p_1 + 2p_2 + 5p_3 \leq 180$
$a_9 : 3p_1 + 2p_2 + p_3 \leq 300 \quad a_3 : p_3 = 0 \quad a_6 : p_2 \geq 5$

Theory solving

Is the conjunction of the following constraints satisfiable?

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

$a_7 : p_3 \geq 10$

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

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

$a_3 : p_3 = 0$

$a_6 : p_2 \geq 5$

Theory solving

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.

Theory solving

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:

Theory solving

Is the conjunction of the following constraints satisfiable?

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

$a_7 : p_3 \geq 10$

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

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

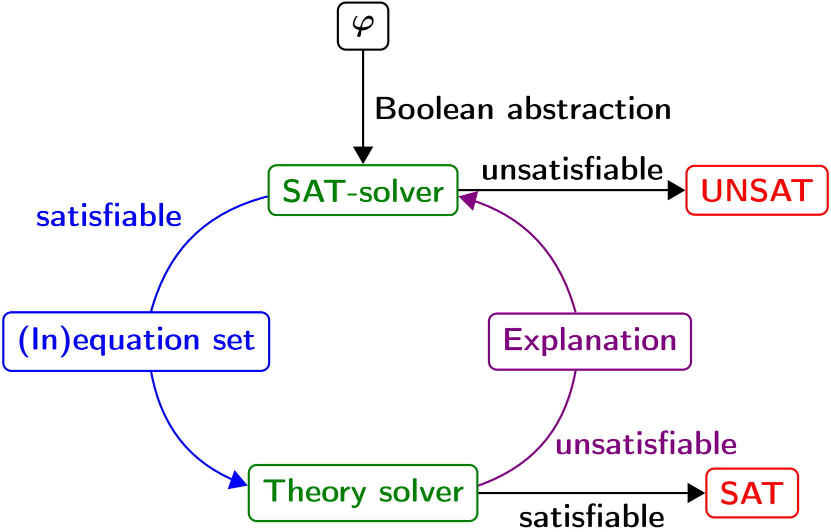
$a_3 : p_3 = 0$

$a_6 : p_2 \geq 5$

No.

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

Lazy SMT-solving



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

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

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

SAT-solving

$$(a_1 \lor a_2 \lor a_3) \land a_4 \land (a_5 \lor a_6) \land a_7 \land a_8 \land a_9 \land \color{red}{(\neg a_3 \lor \neg a_7)}$$

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

SAT-solving

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

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

SAT-solving

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

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

SAT-solving

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

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

SAT-solving

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

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

SAT-solving

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

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

SAT-solving

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

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

SAT-solving

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

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

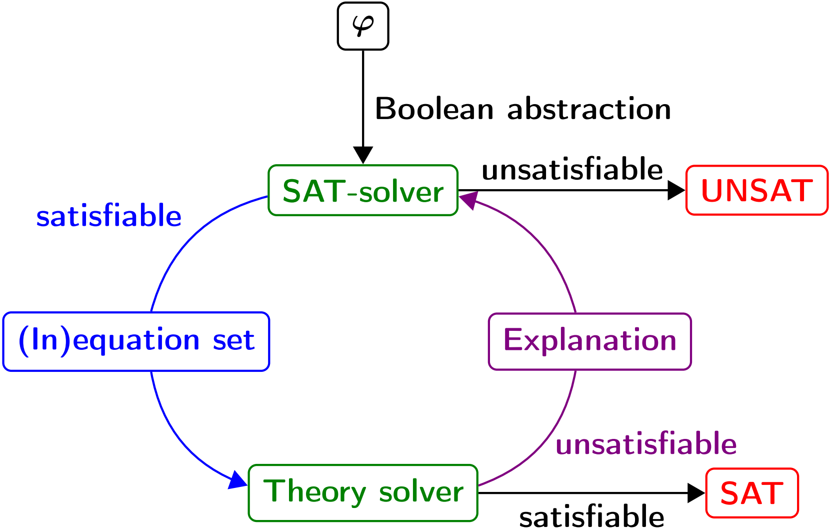
SAT-solving

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

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

Solution found for the Boolean abstraction.

Lazy SMT-solving



Theory solving

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

Theory solving

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

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

Theory solving

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

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

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

Theory solving

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

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

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

Encoding:

$a_4 : p_1 + p_2 + p_3 \geq 100 \quad a_7 : p_3 \geq 10 \quad a_8 : p_1 + 2p_2 + 5p_3 \leq 180$
$a_9 : 3p_1 + 2p_2 + p_3 \leq 300 \quad a_2 : p_2 = 0 \quad a_6 : p_2 \geq 5$

Theory solving

Is the conjunction of the following constraints satisfiable?

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

$a_7 : p_3 \geq 10$

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

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

$a_2 : p_2 = 0$

$a_6 : p_2 \geq 5$

Theory solving

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.

Theory solving

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:

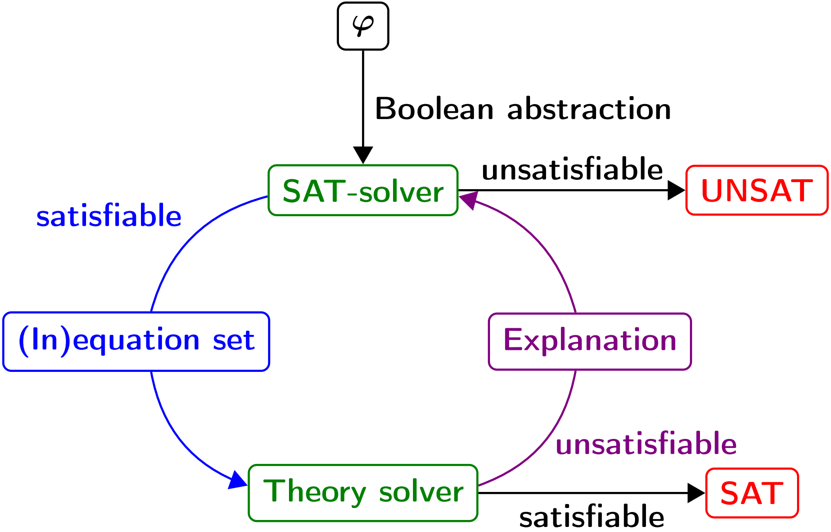
Theory solving

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

Lazy SMT-solving



SAT-solving

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

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

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

SAT-solving

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

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

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

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

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

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

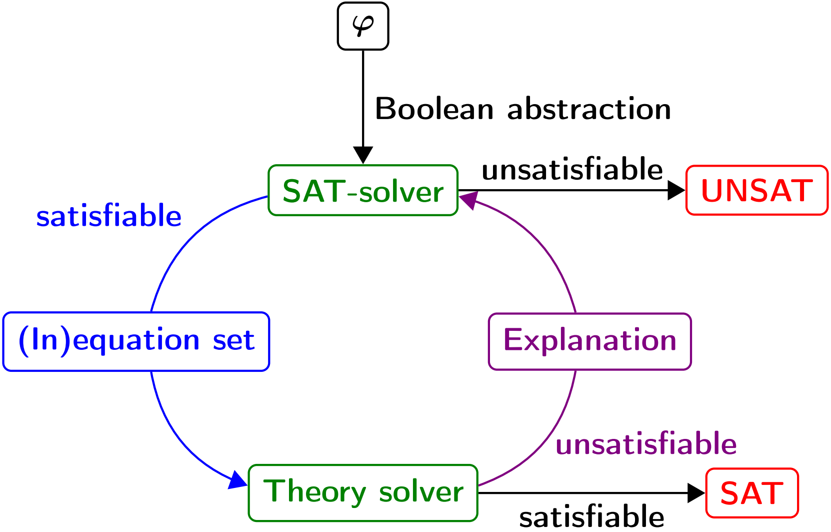
SAT-solving

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

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

Solution found for the Boolean abstraction.

Lazy SMT-solving



Theory solving

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

Theory solving

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

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

Theory solving

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

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

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

Theory solving

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

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

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

Encoding:

$a_4 : p_1 + p_2 + p_3 \geq 100$ $\quad a_7 : p_3 \geq 10$ $\quad a_8 : p_1 + 2p_2 + 5p_3 \leq 180$

$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$ $\quad a_2 : p_2 = 0$ $\quad a_5 : p_1 \geq 5$

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 : $p_1 \geq 5$

Theory solving

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.

Theory solving

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.,

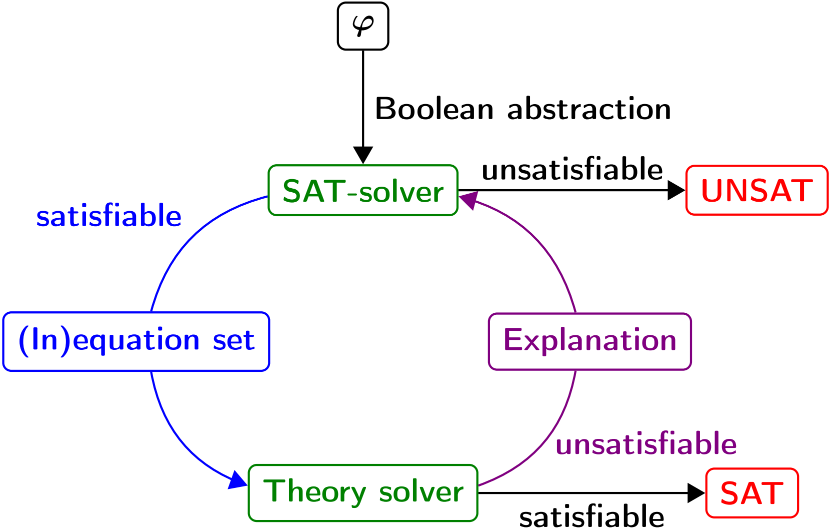
Theory solving

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.

Lazy SMT-solving



Lazy SMT-solving

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

Output: Is φ SAT (+model) or UNSAT?

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

Lazy SMT-solving

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

Ouput: Is φ SAT (+model) or UNSAT?

1. Build the Boolean skeleton (also called Boolean abstraction) φ_{abs} of the input formula φ by replacing each theory constraint $c \in C$ in φ by $\mu(c)$
2. Search for a solution for φ_{abs} (using SAT solving)
3. If there is no solution for φ_{abs} then the input formula φ is unsatisfiable
4. Otherwise, given a solution $\alpha : P \rightarrow \{0, 1\}$ for φ_{abs}, check the set of all true theory constraints $C_\mu := \{c \in C | \alpha(\mu(c)) = 1\}$ 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_μ 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

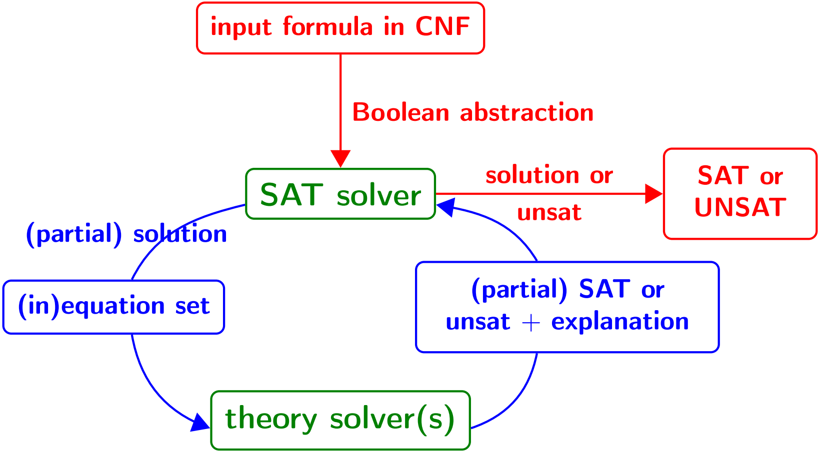
Lazy SMT-solving

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

Ouput: Is φ SAT (+model) or UNSAT?

1. Build the Boolean skeleton (also called Boolean abstraction) φ_{abs} of the input formula φ by replacing each theory constraint $c \in C$ in φ by $\mu(c)$
2. Search for a solution for φ_{abs} (using SAT solving)
3. If there is no solution for φ_{abs} then the input formula φ is unsatisfiable
4. Otherwise, given a solution $\alpha : P \to \{0, 1\}$ for φ_{abs}, check the set of all true theory constraints $C_\mu := \{c \in C | \alpha(\mu(c)) = 1\}$ 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_μ 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.

More involved SMT-structures

- 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.

Exercise

Decide if the following formula is SAT or UNSAT:

- $(x_1 > 0 \vee x_4 > 0) \wedge (x_1 > 0 \vee \neg x_3 > 0 \vee \neg x_8 > 0) \wedge (x_1 > 0 \vee x_8 > 0 \vee x_{12} > 0) \wedge (x_2 > 0 \vee x_{11} > 0) \wedge (\neg x_7 > 0 \vee \neg x_3 > 0 \vee x_9 > 0) \wedge (\neg x_7 > 0 \vee x_8 \vee \neg x_9 > 0) \wedge (x_7 > 0 \vee x_8 > 0 \vee \neg x_{10} > 0) \wedge (x_7 > 0 \vee x_{10} > 0 \vee \neg x_{12} > 0)$