Satisfiability Checking

Lazy SAT-Modulo-Theories (SMT) Solving

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 16/17

The Xmas problem

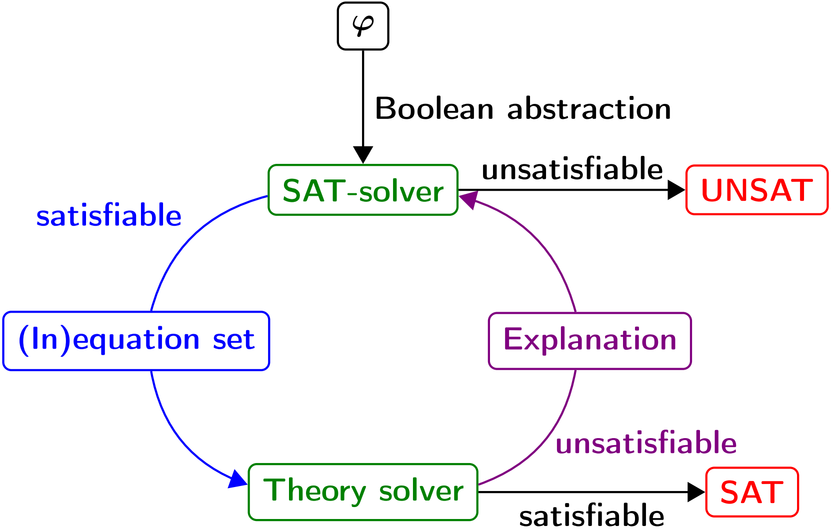
There are three types of Xmas presents Santa Claus can make.

- 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.

Full lazy SMT-solving



Boolean abstraction

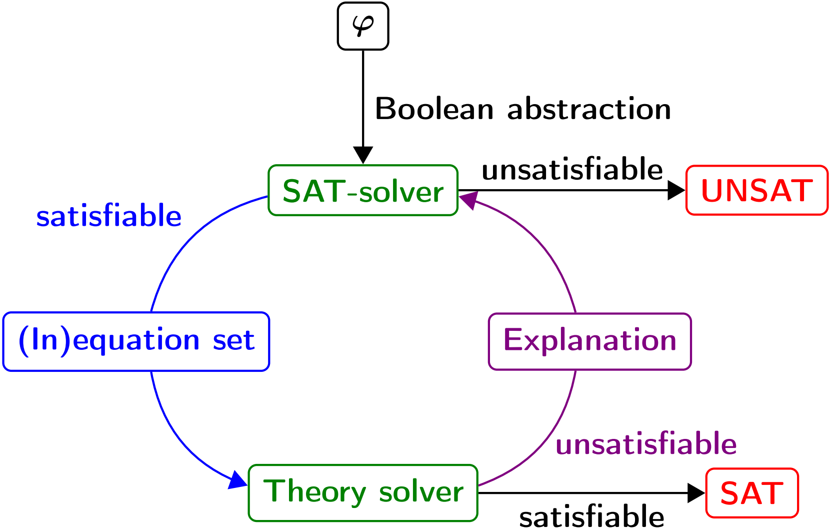
$$(\underbrace{p_1 = 0}_{a_1} \vee \underbrace{p_2 = 0}_{a_2} \vee \underbrace{p_3 = 0}_{a_3}) \wedge \underbrace{p_1 + p_2 + p_3 \geq 100}_{a_4} \wedge$$

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

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

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

Full lazy SMT-solving



SAT-solving

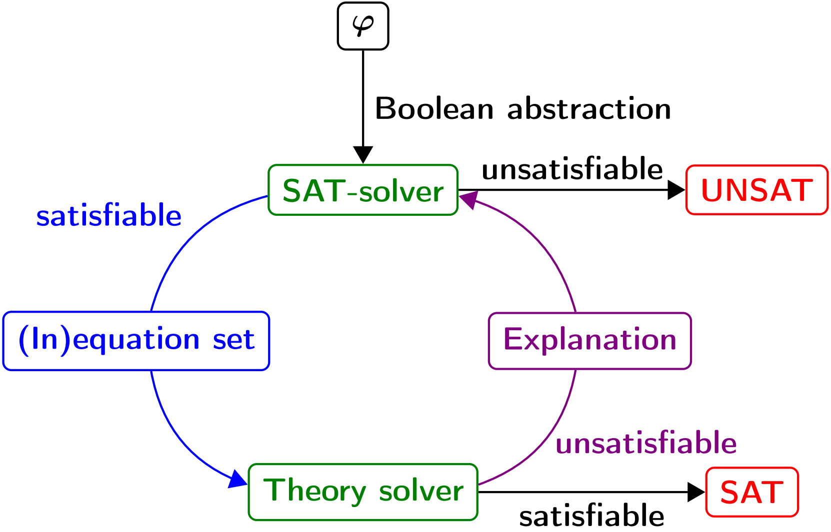
$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

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

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

Solution found for the Boolean abstraction.

Full lazy SMT-solving



Theory solving

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

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

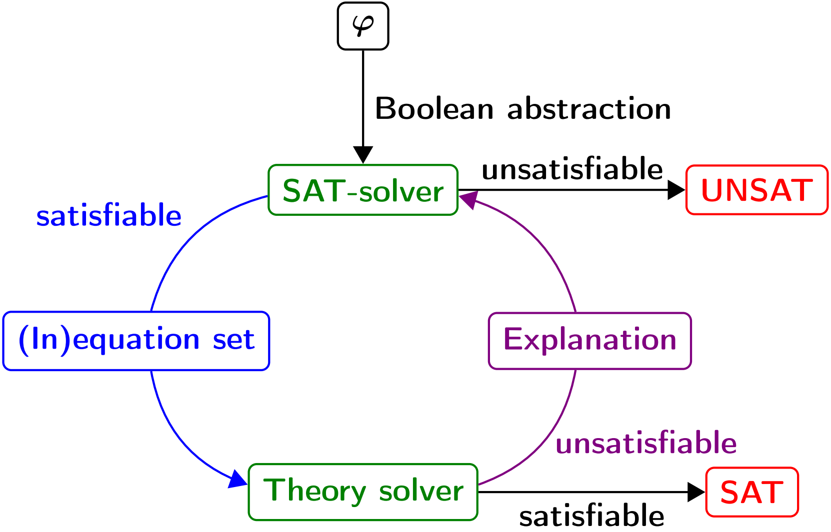
Is the conjunction of the following constraints satisfiable?

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

No.

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

Full lazy SMT-solving



SAT-solving

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

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

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

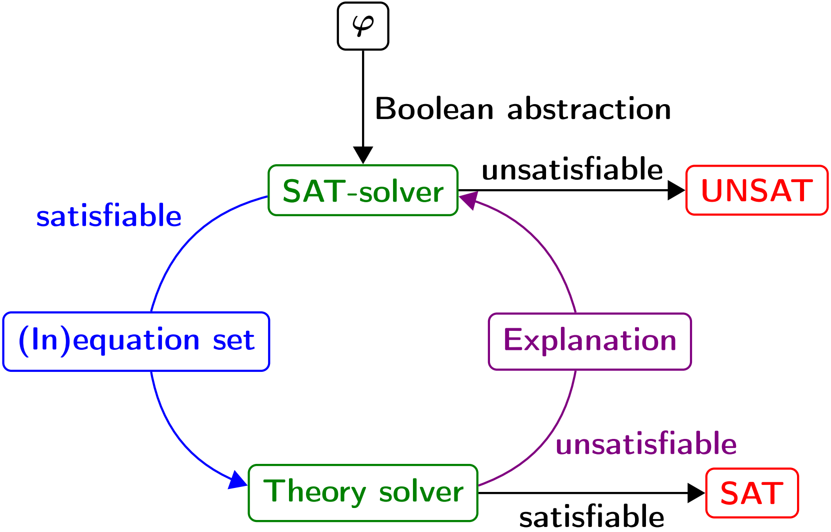
Conflict resolution is simple, since the new clause is already an asserting one.

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

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

Solution found for the Boolean abstraction.

Full lazy SMT-solving



Theory solving

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

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

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

Encoding:

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

Theory solving

Is the conjunction of the following constraints satisfiable?

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

$a_7 : p_3 \geq 10$

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

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

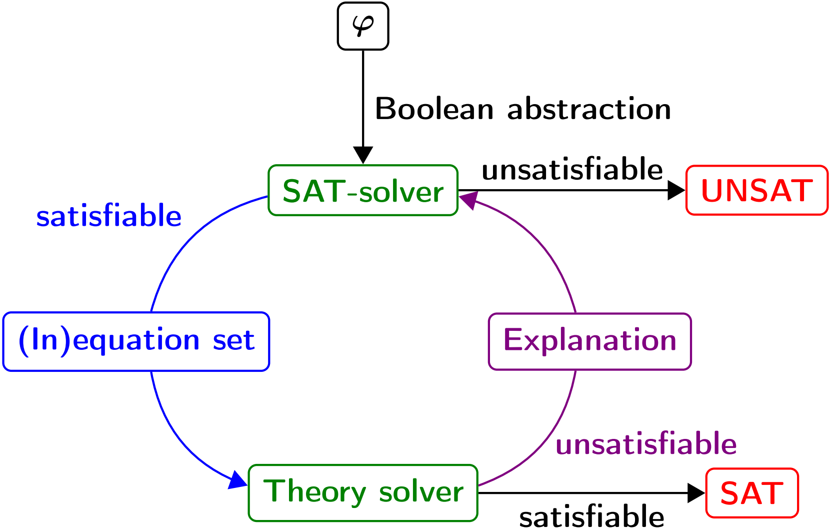
$a_2 : p_2 = 0$

$a_6 : p_2 \geq 5$

No.

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

Full lazy SMT-solving



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

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

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

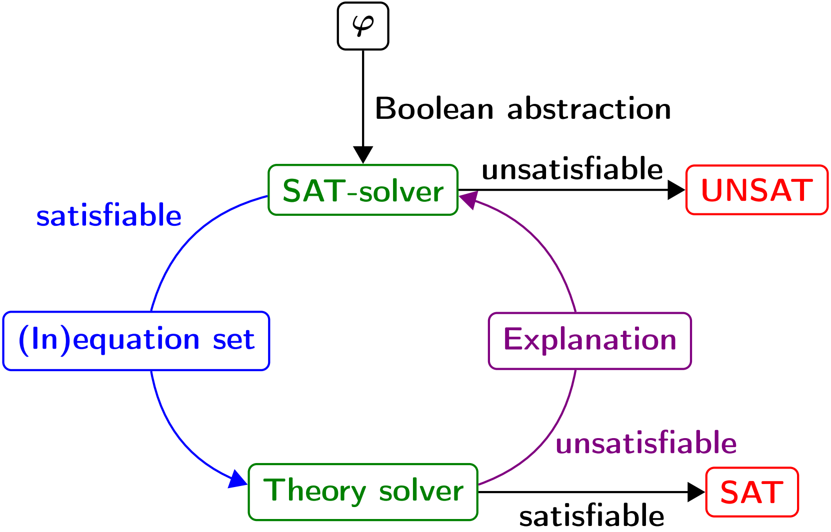
Conflict resolution is simple, since the new clause is already an asserting one.

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

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

Solution found for the Boolean abstraction.

Full lazy SMT-solving



Theory solving

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

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:

$a_4 : p_1 + p_2 + p_3 \geq 100 \quad a_7 : p_3 \geq 10 \quad a_8 : p_1 + 2p_2 + 5p_3 \leq 180$
$a_9 : 3p_1 + 2p_2 + p_3 \leq 300 \quad a_2 : p_2 = 0 \quad a_5 : p_1 \geq 5$

Theory solving

Is the conjunction of the following constraints satisfiable?

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

$a_7 : p_3 \geq 10$

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

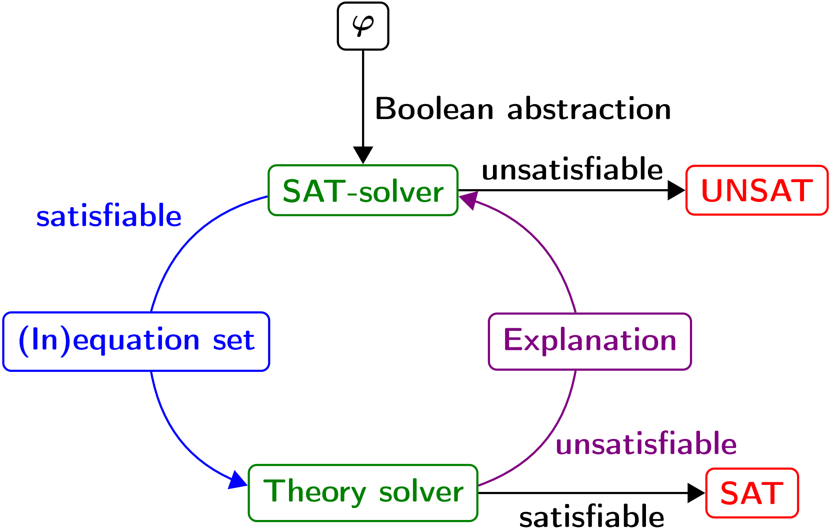
$a_9 : 3p_1 + 2p_2 + p_3 \leq 300$

$a_2 : p_2 = 0$

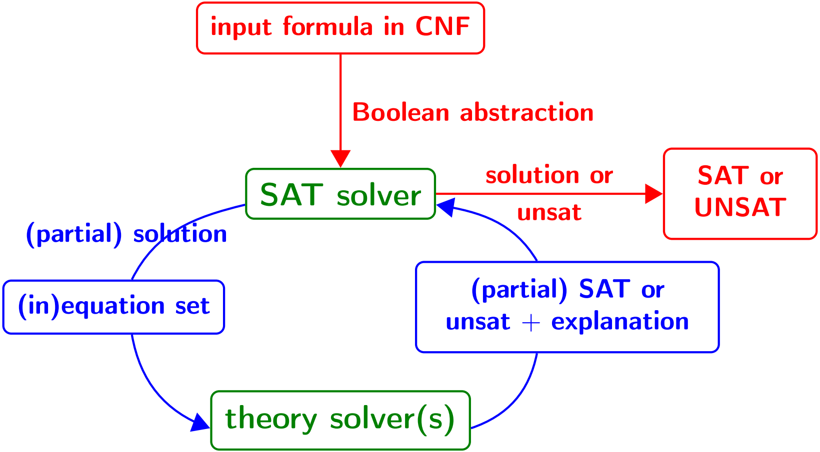
$a_5 : p_1 \geq 5$

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

Full lazy SMT-solving



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.