Satisfiability Checking

SAT-Modulo-Theories (SMT) Solving

Prof. Dr. Erika Ábrahám

Theory of Hybrid Systems
Informatik 2

WS 10/11

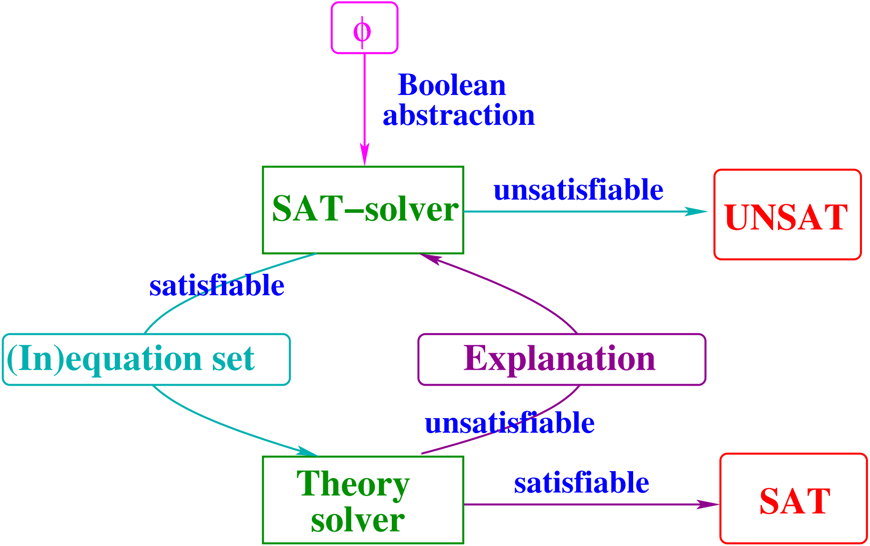
The Xmas Problem

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

- Santa Claus decides to reduce the overhead and make only two types.
- He needs at least 100 presents.
- Hee need 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.

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

Full lazy SMT-solving



Boolean Abstraction

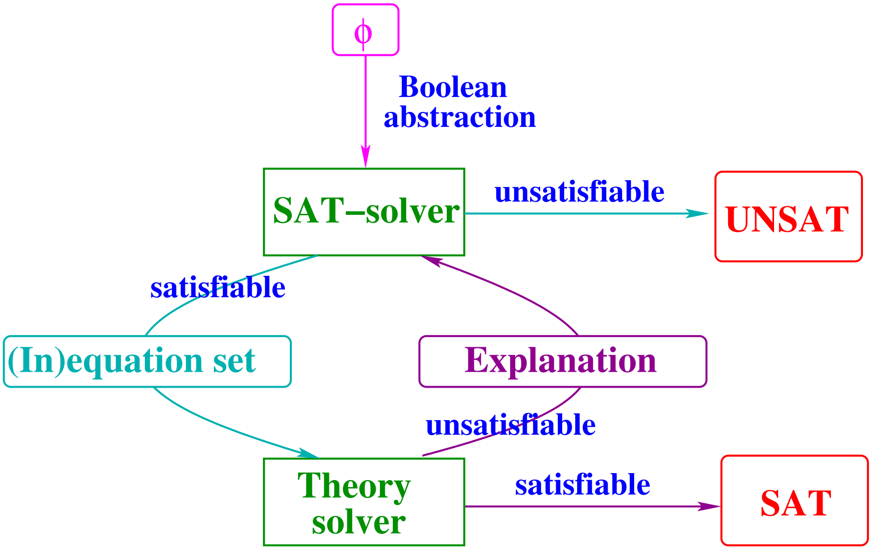
$$(\underbrace{p_1 = 0}_{a_1} \vee \underbrace{p_2 = 0}_{a_2} \vee \underbrace{p_3 = 0}_{a_3}) \wedge \underbrace{p_1 + p_2 + p_3 \geq 100}_{a_4} \wedge$$

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

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

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

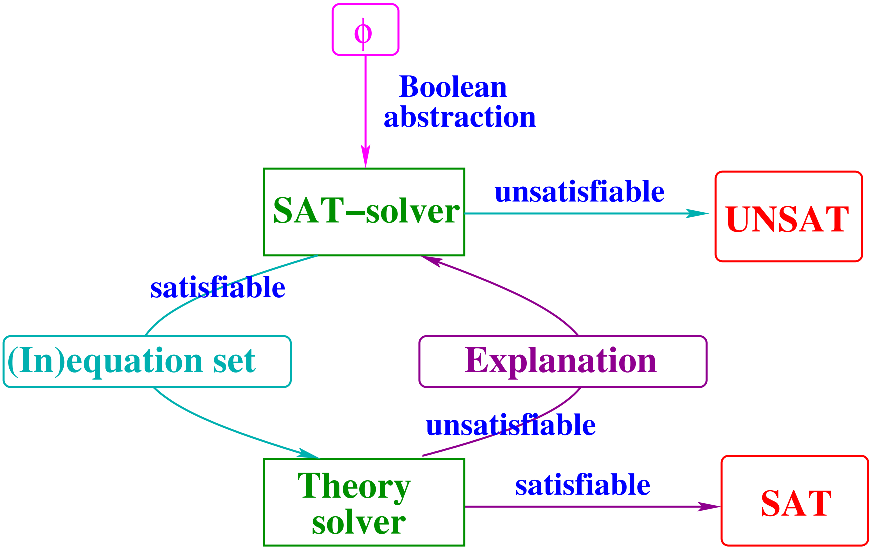
Full lazy SMT-solving



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

Assume a fixed variable order: $a_1, \ldots, a_9$
Assignment to decision variables: false
$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$
$DL1 : a_1 : 0$
$DL2 : a_2 : 0, a_3 : 1$
$DL3 : a_5 : 0, a_6 : 1$

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:
$p_1 + p_2 + p_3 \geq 100,\ p_3 \geq 10,$
$p_1 + 2p_2 + 5p_3 \leq 180,\ 3p_1 + 2p_2 + p_3 \leq 300,\ p_3 = 0,\ p_2 \geq 5$

Theory solving

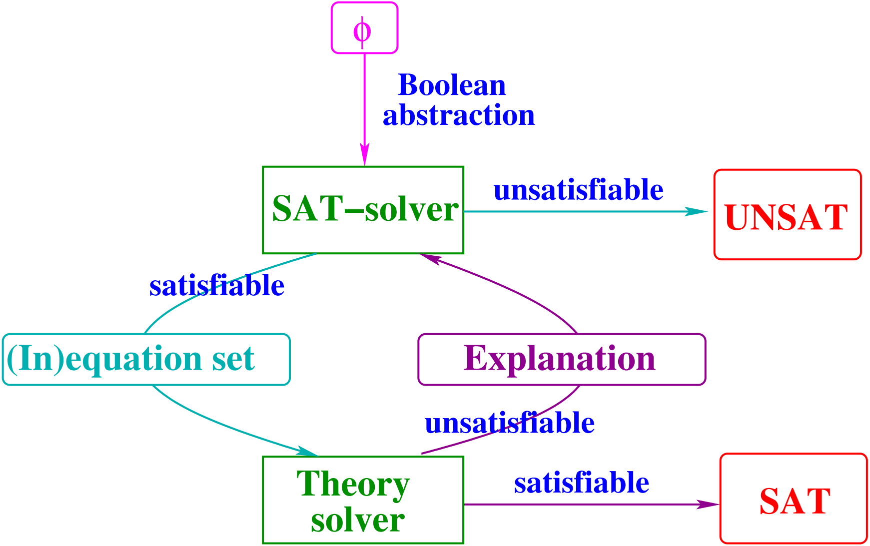
$$
\begin{array}{llll}
p_1 + p_2 + p_3 \geq 100 & \rightarrow & s_1 = p_1 + p_2 + p_3 & s_1 \geq 100 \\
p_3 \geq 10 & \rightarrow & s_2 = p_3 & s_2 \geq 10 \\
p_1 + 2p_2 + 5p_3 \leq 180 & \rightarrow & s_3 = p_1 + 2p_2 + 5p_3 & s_3 \leq 180 \\
3p_1 + 2p_2 + p_3 \leq 300 & \rightarrow & s_4 = 3p_1 + 2p_2 + p_3 & s_4 \leq 300 \\
p_3 = 0 & \rightarrow & s_5 = p_3 & s_5 = 0 \\
p_2 \geq 5 & \rightarrow & s_6 = p_2 & s_6 \geq 5
\end{array}
$$

	p_1	p_2	p_3
s_1	1	1	1
s_2	0	0	1
s_3	1	2	5
s_4	3	2	1
s_5	0	0	1
s_6	0	1	0

Conflict:

$\underbrace{p_3 = 0}_{a_3} \wedge \underbrace{p_3 \geq 10}_{a_7}$

is not satisfiable.


ϕ
Boolean abstraction
SAT–solver
unsatisfiable
UNSAT
satisfiable
(In)equation set
Explanation
unsatisfiable
Theory solver
satisfiable
SAT

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

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

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

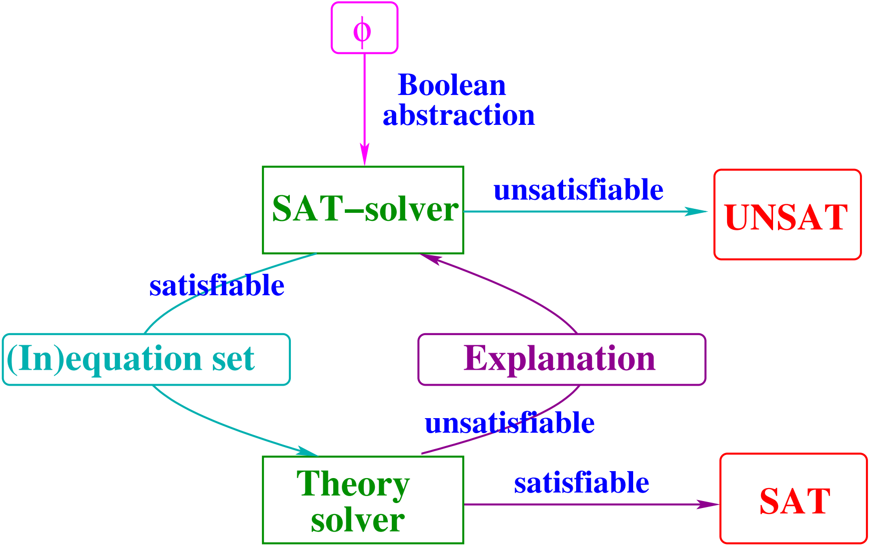
Conflict resolution is simple, since the new clause is already an asserting one.

SAT-solving

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

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

Full lazy SMT-solving



Theory solving

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

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:
$p_1 + p_2 + p_3 \geq 100,\ p_3 \geq 10,$
$p_1 + 2p_2 + 5p_3 \leq 180,\ 3p_1 + 2p_2 + p_3 \leq 300,\ p_2 = 0,\ p_2 \geq 5$

Theory solving

$$\begin{array}{lclr}
p_1 + p_2 + p_3 \geq 100 & \to & s_1 = p_1 + p_2 + p_3 & s_1 \geq 100 \\
p_3 \geq 10 & \to & s_2 = p_3 & s_2 \geq 10 \\
p_1 + 2p_2 + 5p_3 \leq 180 & \to & s_3 = p_1 + 2p_2 + 5p_3 & s_3 \leq 180 \\
3p_1 + 2p_2 + p_3 \leq 300 & \to & s_4 = 3p_1 + 2p_2 + p_3 & s_4 \leq 300 \\
p_2 = 0 & \to & s_5 = p_2 & s_5 = 0 \\
p_2 \geq 5 & \to & s_6 = p_2 & s_6 \geq 5
\end{array}$$

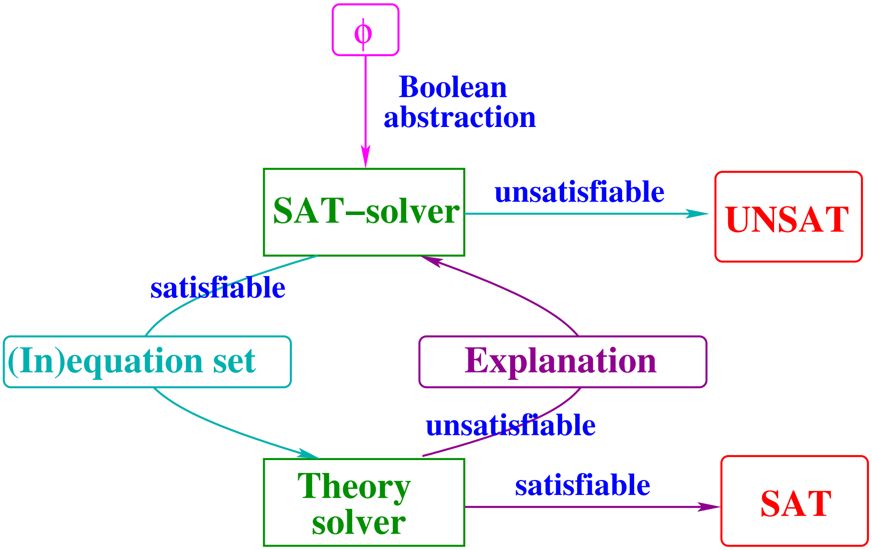
	p_1	p_2	p_3
s_1	1	1	1
s_2	0	0	1
s_3	1	2	5
s_4	3	2	1
s_5	0	1	0
s_6	0	1	0

Conflict:

$$\underbrace{p_2 = 0}_{a_2} \wedge \underbrace{p_2 \geq 5}_{a_6}$$

is not satisfiable.

Full lazy SMT-solving



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

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

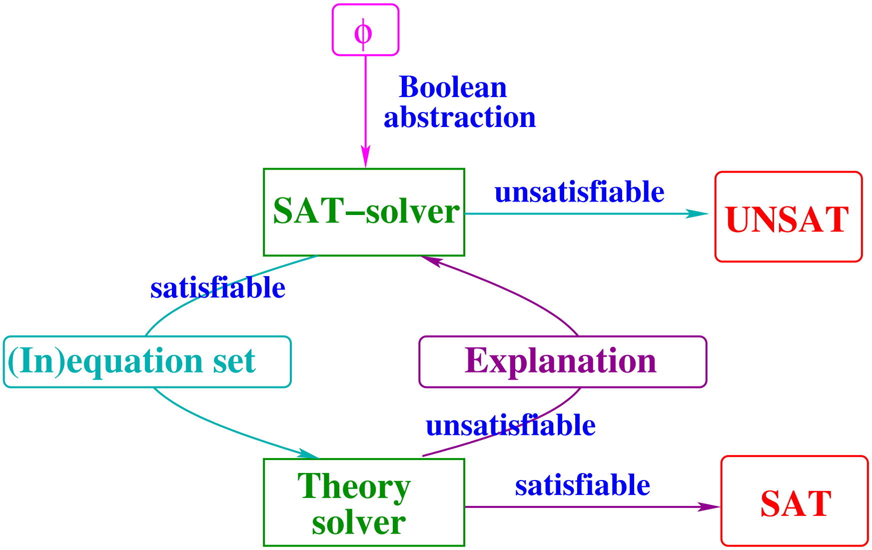
$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1, a_3 : 0$
$DL1 : a_1 : 0, a_2 : 1$
$DL3 : a_5 : 0, a_6 : 1$

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

SAT-solving

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

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



ϕ
Boolean abstraction
SAT–solver
unsatisfiable
UNSAT
satisfiable
(In)equation set
Explanation
unsatisfiable
Theory solver
satisfiable
SAT

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:

$p_1 + p_2 + p_3 \geq 100,\ p_3 \geq 10,$
$p_1 + 2p_2 + 5p_3 \leq 180,\ 3p_1 + 2p_2 + p_3 \leq 300,\ p_2 = 0,\ p_1 \geq 5$

Theory solving

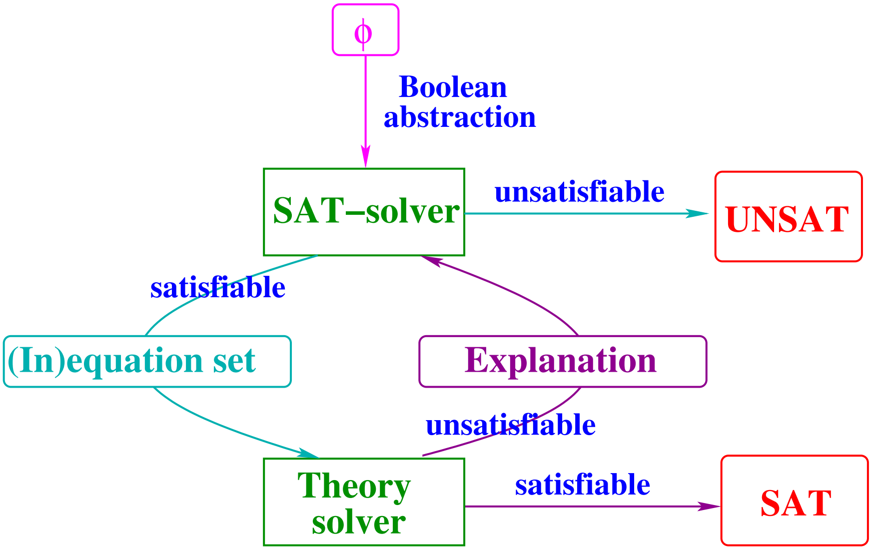
$$
\begin{array}{llll}
p_1 + p_2 + p_3 \geq 100 & \rightarrow & s_1 = p_1 + p_2 + p_3 & s_1 \geq 100 \\
p_3 \geq 10 & \rightarrow & s_2 = p_3 & s_2 \geq 10 \\
p_1 + 2p_2 + 5p_3 \leq 180 & \rightarrow & s_3 = p_1 + 2p_2 + 5p_3 & s_3 \leq 180 \\
3p_1 + 2p_2 + p_3 \leq 300 & \rightarrow & s_4 = 3p_1 + 2p_2 + p_3 & s_4 \leq 300 \\
p_2 = 0 & \rightarrow & s_5 = p_2 & s_5 = 0 \\
p_1 \geq 5 & \rightarrow & s_6 = p_1 & s_6 \geq 5
\end{array}
$$

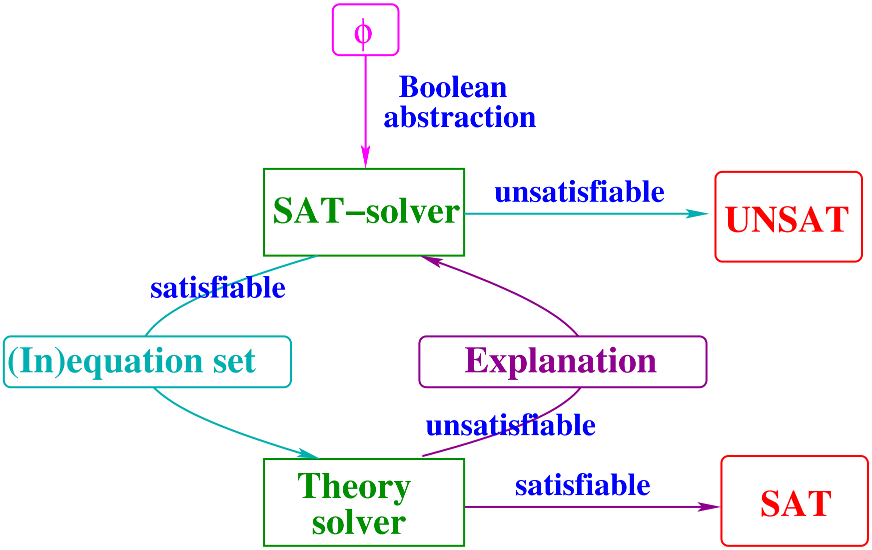
	p_1	p_2	p_3
s_1	1	1	1
s_2	0	0	1
s_3	1	2	5
s_4	3	2	1
s_5	0	1	0
s_6	1	0	0

Solution:

$p_1 = 90, \quad p_2 = 0, \quad p_3 = 10.$

Full lazy SMT-solving




ϕ
Boolean abstraction
SAT–solver
unsatisfiable
UNSAT
satisfiable
(In)equation set
Explanation
unsatisfiable
Theory solver
satisfiable
SAT

Requirement: Incrementality of the theory solver

Incrementality in Simplex is straightforward:

- Add all constraints but without bounds on non-active constraints.
- If a constraint becomes true, activate its bound.

More involved SMT-structures

- What we got known to is called the DPLL(T)-solving approach.
- There are other approaches, which do not divide Boolean and theory solving so strictly.
- Main idea: Propagate in the SAT-solver bounds on theory variables.