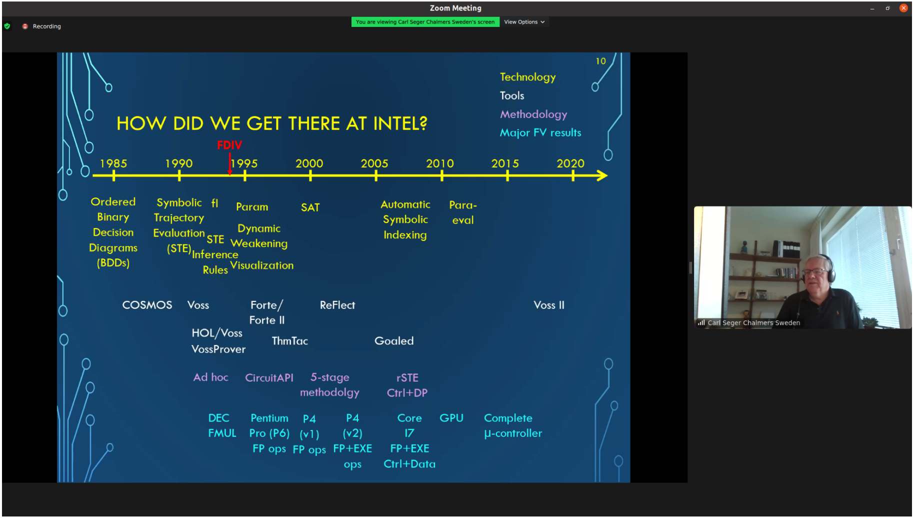
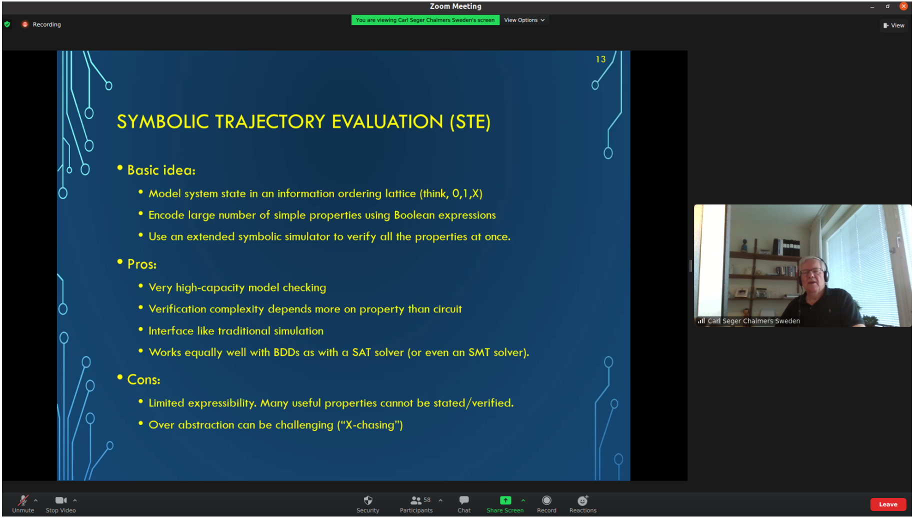

Zoom Meeting
Recording
You are viewing Carl Seger Chalmers Sweden's screen
View Options
10
Technology
Tools
Methodology
Major FV results
HOW DID WE GET THERE AT INTEL?
FDIV
1985
1990
1995
2000
2005
2010
2015
2020
Ordered Binary Decision Diagrams (BDDs)
Symbolic Trajectory Evaluation (STE)
fl
STE Inference Rules
Param
Dynamic Weakening
Visualization
SAT
Automatic Symbolic Indexing
Para-eval
COSMOS
Voss
Forte/ Forte II
ReFlect
Voss II
HOL/Voss
VossProver
ThmTac
Goaled
Ad hoc
CircuitAPI
5-stage methodolgy
rSTE Ctrl+DP
DEC FMUL
Pentium Pro (P6) FP ops
P4 (v1) FP ops
P4 (v2) FP+EXE ops
Core I7 FP+EXE Ctrl+Data
GPU
Complete μ-controller
Carl Seger Chalmers Sweden


Zoom Meeting
Recording
You are viewing Carl Seger Chalmers Sweden's screen
View Options
View
13
SYMBOLIC TRAJECTORY EVALUATION (STE)
• Basic idea:
• Model system state in an information ordering lattice (think, 0,1,X)
• Encode large number of simple properties using Boolean expressions
• Use an extended symbolic simulator to verify all the properties at once.
• Pros:
• Very high-capacity model checking
• Verification complexity depends more on property than circuit
• Interface like traditional simulation
• Works equally well with BDDs as with a SAT solver (or even an SMT solver).
• Cons:
• Limited expressibility. Many useful properties cannot be stated/verified.
• Over abstraction can be challenging ("X-chasing")
Carl Seger Chalmers Sweden
Unmute
Stop Video
Security
58
Participants
Chat
Share Screen
Record
Reactions
Leave

Satisfiability Checking
11 Lazy SAT-Modulo-Theories (SMT) solving

Prof. Dr. Erika Ábrahám

RWTH Aachen University
Informatik 2
LuFG Theory of Hybrid Systems

WS 22/23

The Xmas problem

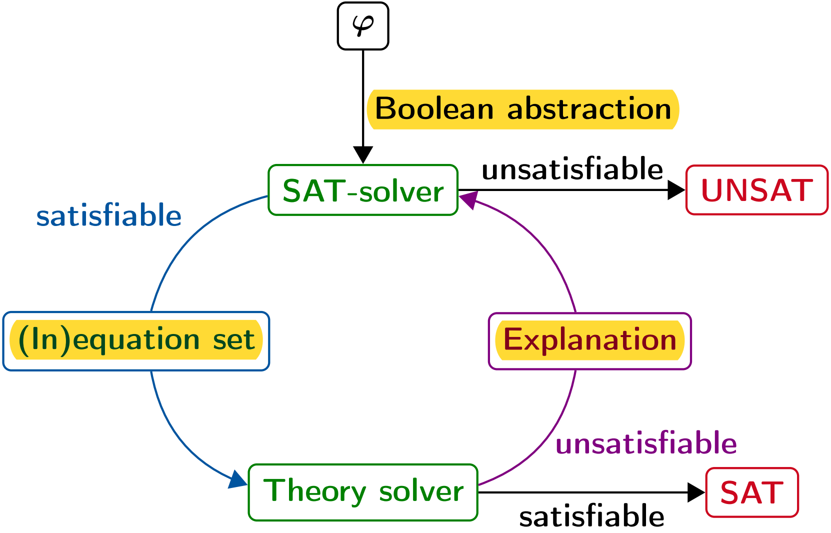
There are three types of Xmas presents Santa Claus can make.

- 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.

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

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

Full lazy SMT solving

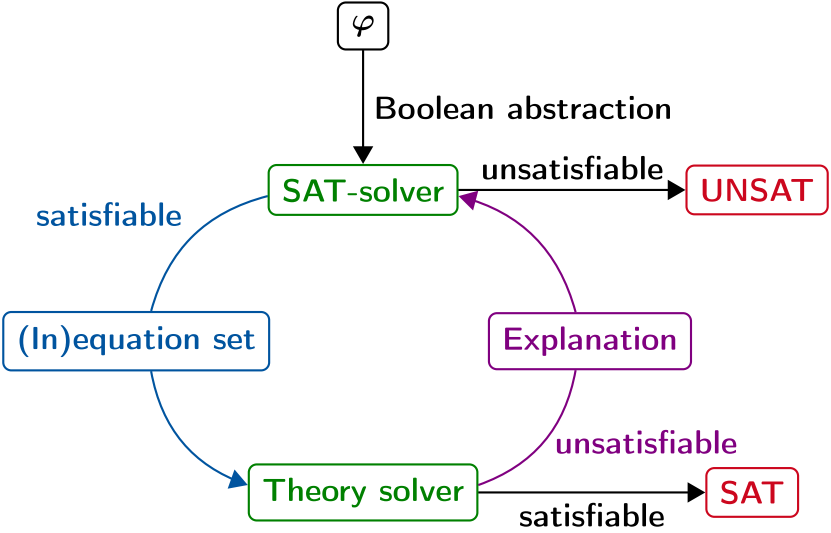


Boolean abstraction

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

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

Full lazy SMT solving



SAT solving

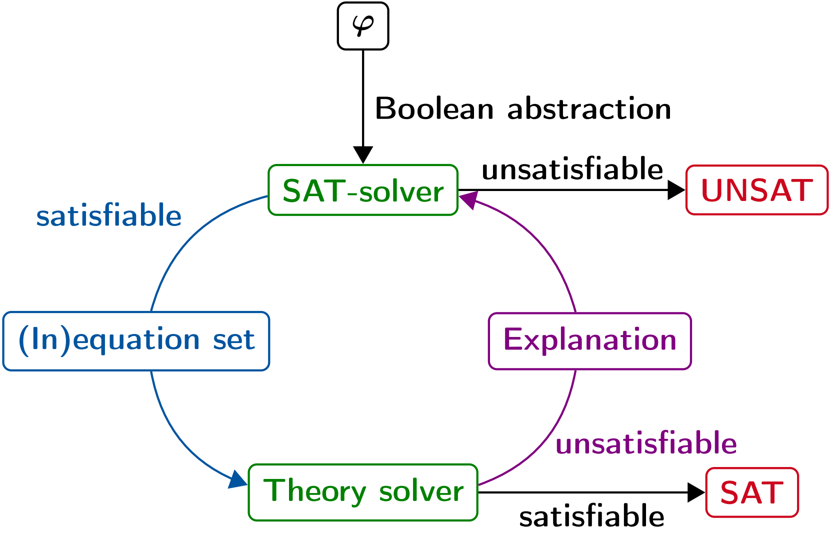
$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9$$

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

$DL0 : a_4 : 1, a_7 : 1, a_8 : 1, a_9 : 1$ 所有的 unit clause 都在 DL0 赋值
$DL1 : a_1 : 0$
$DL2 : a_2 : 0, a_3 : 1$
$DL3 : a_5 : 0, a_6 : 1$

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: $a_4, a_7, a_8, a_9, a_3, a_6$

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

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

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

标红的为取值为1的variable

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?

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

$a_7 : p_3 \geq 10$

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

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

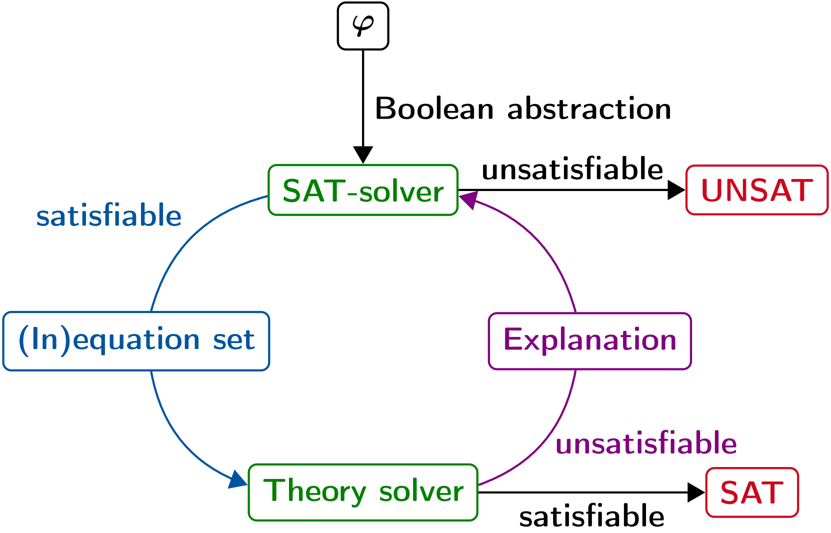
$a_3 : p_3 = 0$

$a_6 : p_2 \geq 5$

No.

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

Full lazy SMT solving



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

加入学习到的冲突
¬(a3∧ a7)=(¬a3∨ ¬a7)

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

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

回到学习的子句的上一决策层

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

SAT solving

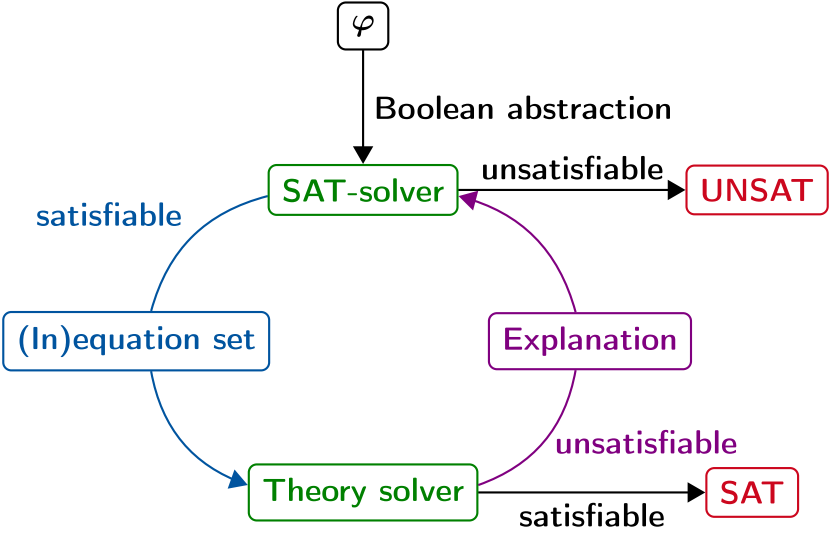
$$(a_1 \vee a_2 \vee a_3) \wedge a_4 \wedge (a_5 \vee a_6) \wedge a_7 \wedge a_8 \wedge a_9 \wedge (\neg a_3 \vee \neg a_7)$$

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

BCP

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:

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

Is the conjunction of the following constraints satisfiable?

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

$a_7: p_3 \geq 10$

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

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

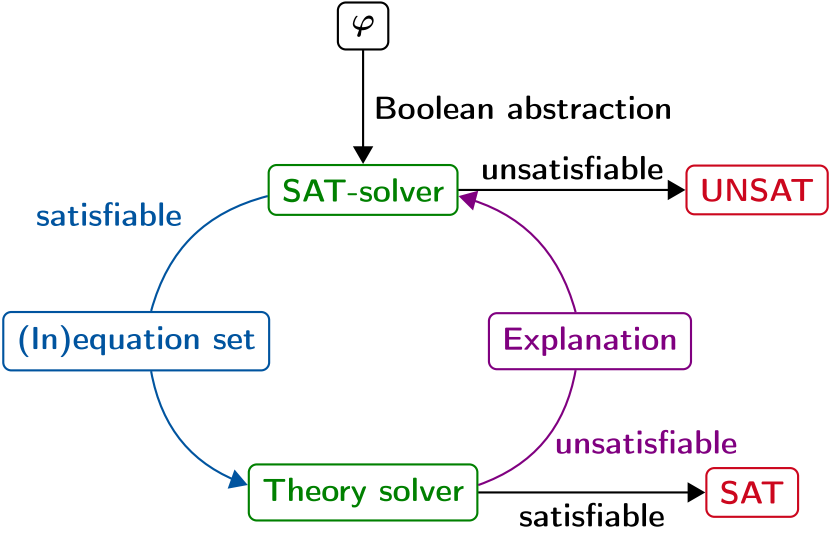
$a_2: p_2 = 0$

$a_6: p_2 \geq 5$

No.

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

Full lazy SMT solving



SAT solving

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

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

$$(\neg a_2 \vee \neg a_6)$$

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

第2高决策层

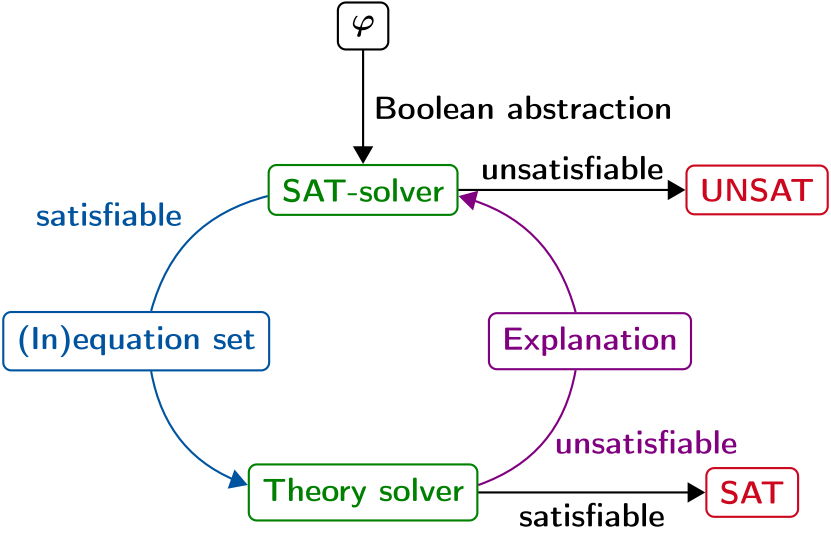
Conflict resolution is simple, since the new clause is already an asserting one.

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

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

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: $a_4, a_7, a_8, a_9, a_2, a_5$

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

Encoding:

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

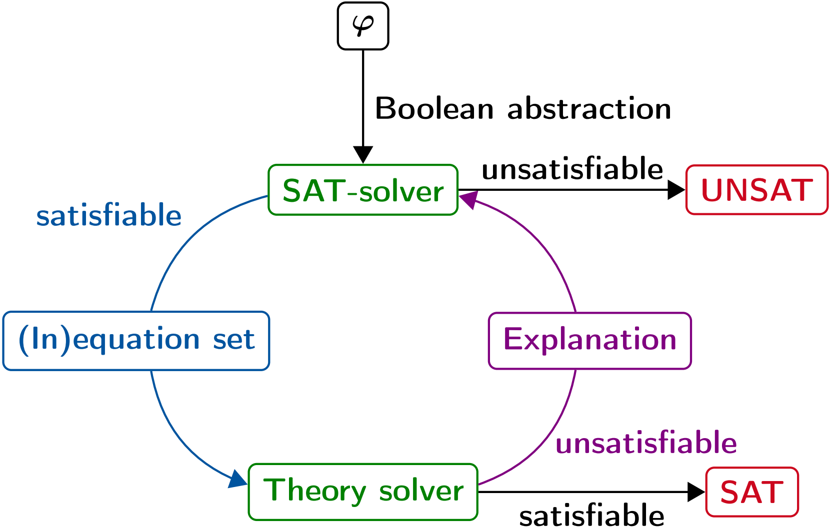
$a_9 : 3p_1 + 2p_2 + p_3 \leq 300 \quad a_2 : p_2 = 0 \quad a_5 : p_1 \geq 5$

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 : $p_1 \geq 5$

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

Full lazy SMT solving



Full lazy SMT solving

Input: Quantifier-free FO logic formula φ over some theories in CNF
without any negation
Output: Satisfiability of the input formula

Some notations we use:

- 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 $\mu^{-1}(p_c) = c$.
- 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 $\mu(c)$.

$$\mu(\varphi_1 \vee \varphi_2) = \mu(\varphi_1) \vee \mu(\varphi_2)$$

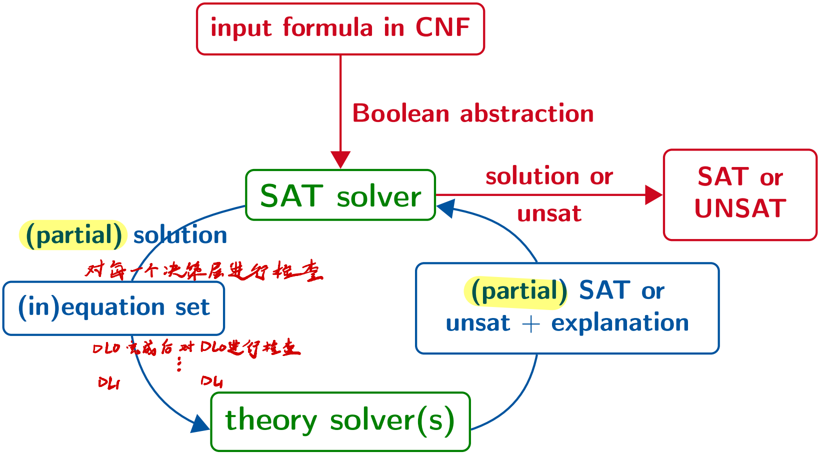
$$\mu(\varphi_1 \wedge \varphi_2) = \mu(\varphi_1) \wedge \mu(\varphi_2)$$

Full lazy SMT solving

Input: Quantifier-free FO logic formula φ over some theories in CNF
without any negation
Output: Satisfiability of the input formula

1. Build the Boolean skeleton $\varphi_{abs} := \mu(\varphi)$ (see previous page).
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 the input formula φ is satisfiable.
6. Otherwise, compute an explanation for the inconsistency in form of a CNF formula with constraints from C implying that the constraints in C_μ cannot be all satisfied by the same assignment.
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.

Bonus exercise 16

Assume the following set of constraints over real-valued variables:

$$C = \{x - y \geq 0,\ x \cdot y > 0,\ x^2 + 1 = 0, x + y > 0, x \cdot y < 0\}$$

Which of the following are (not necessarily minimal) infeasible subsets of C?

Multiple choice: please select all true cases!

1. $\{x \cdot y > 0\}$
2. $\{x \cdot y > 0, x + y > 0\}$
3. $\{x \cdot y > 0, x + y > 0, x \cdot y < 0\}$
4. $\{x^2 + 1 = 0\}$
5. $\{x \cdot y > 0, x^2 + 1 = 0\}$

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.

Learning target

- How does lazy SMT solving work?
- What are incrementality, explanations and backtracking in the context of lazy SMT solving?