Decision Procedures

~~Jochen Hoenicke~~
Bernd Westphal

Software Engineering
Albert-Ludwigs-University Freiburg

Winter Term 2016/17

DPLL(T)

Suppose we have a $T_{\mathbb{Q}}$-formulae that is not conjunctive:

$$(x \geq 0 \rightarrow y > z) \land (x + y \geq z \rightarrow y \leq z) \land (y \geq 0 \rightarrow x \geq 0) \land x + y \geq z$$

Our approach so far: Converting to DNF.
Yields in 8 conjuncts that have to be checked separately.

Is there a more efficient way to prove unsatisfiability?

CNF and Propositional Core

Suppose we have the following $T_{\mathbb{Q}}$-formulae:

$$(x \geq 0 \rightarrow y > z) \wedge (x + y \geq z \rightarrow y \leq z) \wedge (y \geq 0 \rightarrow x \geq 0) \wedge x + y \geq z$$

Converting to CNF and restricting to $\leq$:

$$(\neg(\underset{P_1}{\boxed{0 \leq x}}) \vee \neg(\overset{P_2}{\boxed{y \leq z}})) \wedge (\neg(\overset{P_3}{\boxed{z \leq x + y}}) \vee (\overset{P_2}{\boxed{y \leq z}}))$$
$$\wedge (\neg(\underset{P_4}{\boxed{0 \leq y}}) \vee (\underset{P_1}{\boxed{0 \leq x}})) \wedge (\underset{P_3}{\boxed{z \leq x + y}})$$

Now, introduce boolean variables for each atom:

$P_1 : 0 \leq x$ $\qquad$ $P_2 : y \leq z$

$P_3 : z \leq x + y$ $\qquad$ $P_4 : 0 \leq y$

Gives a propositional formula:

$$(\neg P_1 \vee \neg P_2) \wedge (\neg P_3 \vee P_2) \wedge (\neg P_4 \vee P_1) \wedge P_3$$

The core feature of the DPLL-algorithm is Unit Propagation.

$$(\neg \underbrace{P_1}_{\text{false}} \lor \underbrace{\neg P_2}_{\text{false}}) \land (\underbrace{\neg P_3}_{\text{false}} \lor \underbrace{P_2}_{\text{true}}) \land (\neg \underbrace{P_4}_{\text{false}} \lor \underbrace{P_1}_{\text{false}}) \land \underbrace{P_3}_{\text{true}}$$

DPLL-Algorithm

The core feature of the DPLL-algorithm is Unit Propagation.

$$(\neg P_1 \lor \neg P_2) \land (\neg P_3 \lor P_2) \land (\neg P_4 \lor P_1) \land P_3$$

The clause P_3 is a unit clause; set P_3 to $\top$.
Then $\neg P_3 \lor P_2$ is a unit clause; set P_2 to $\top$.
Then $\neg P_1 \lor \neg P_2$ is a unit clause; set P_1 to $\bot$.
Then $\neg P_4 \lor P_1$ is a unit clause; set P_4 to $\bot$.

Only solution is $P_3 \land P_2 \land \neg P_1 \land \neg P_4$.

Only solution is $P_3 \wedge P_2 \wedge \neg P_1 \wedge \neg P_4$.

$$P_1 : 0 \leq x \qquad\qquad P_2 : y \leq z$$
$$P_3 : z \leq x + y \qquad\qquad P_4 : 0 \leq y$$

This gives the conjunctive $T_{\mathbb{Q}}$-formula

$$(z \leq x + y) \wedge (y \leq z) \wedge (x < 0) \wedge (y < 0.)$$

DPLL(T) with Learning (CDCL)

We describe DPLL(T) by a set of rules modifying a configuration.
A configuration is a triple

$$\langle M, F, C \rangle,$$

where

- M (model) is a sequence of literals (that are currently set to true) interspersed with backtracking points denoted by $\square$.
- F (formula) is a formula in CNF, i. e., a set of clauses where each clause is a set of literals.
- C (conflict) is either $\top$ or a conflict clause (a set of literals).
  A conflict clause C is a clause with $F \Rightarrow C$ and $M \not\models C$.
  Thus, a conflict clause shows $M \not\models F$.

We describe the algorithm by a set of rules, which each describe a set of transitions between configurations, e. g.,

Explain $\quad \dfrac{\langle M, F, C \cup \{\ell\}\rangle}{\langle M, F, C \cup \{\ell_1, \dots, \ell_k\}\rangle}$ where $\ell \notin C$, $\{\ell_1, \dots, \ell_k, \bar{\ell}\} \in F$, and $\bar{\ell}_1, \dots, \bar{\ell}_k \prec \bar{\ell}$ in M.

name

Here, $\bar{\ell}_1, \dots, \bar{\ell}_k \prec \ell$ in M means the literals $\bar{\ell}_1, \dots, \bar{\ell}_k$ occur in the sequence M before the literal ℓ (and all literals appear in M).

Example: for $M = P_1 \bar{P}_3 \bar{P}_2 \bar{P}_4$, $F = \{\{P_1\}, \{P_3, \bar{P}_4\}\}$, and $C = \{P_2\}$ the transition

$C \cup \{\ell\}$

$$\langle M, F, \{P_2, P_4\}\rangle \xrightarrow[\text{Explain}]{} \langle M, F, \{P_2, P_3\}\rangle$$

is possible.

sequence concatenation

$R_1 < R_2$ iff R_1 better than R_2 (Heur.)

Decide	$\dfrac{\langle M, F, \top\rangle}{\langle M \cdot \Box \cdot \ell, F, \top\rangle}$	where $\ell \in lit(F)$, $\ell, \bar{\ell} \not\in M$
Propagate	$\dfrac{\langle M, F, \top\rangle}{\langle M \cdot \ell, F, \top\rangle}$	where $\{\ell_1, \ldots, \ell_k, \ell\} \in F$ and $\bar{\ell_1}, \ldots, \bar{\ell_k}$ in M, $\ell, \bar{\ell} \not\in M$.
Conflict	$\dfrac{\langle M, F, \top\rangle}{\langle M, F, \{\ell_1, \ldots, \ell_k\}\rangle}$	where $\{\ell_1, \ldots, \ell_k\} \in F$ and $\bar{\ell_1}, \ldots, \bar{\ell_k}$ in M.
Explain (Heur: go backwards in M)	$\dfrac{\langle M, F, C \cup \{\ell\}\rangle}{\langle M, F, C \cup \{\ell_1, \ldots, \ell_k\}\rangle}$	where $\ell \notin C$, $\{\ell_1, \ldots, \ell_k, \bar{\ell}\} \in F$, and $\bar{\ell_1}, \ldots, \bar{\ell_k} \prec \bar{\ell}$ in M.
Learn (Heur.: apply Learn right before Back)	$\dfrac{\langle M, F, C\rangle}{\langle M, F \cup \{C\}, C\rangle}$	where $C \neq \top$, $C \notin F$.
Back	$\dfrac{\langle M, F, \{\ell_1, \ldots, \ell_k, \ell\}\rangle}{\langle M' \cdot \underbrace{\ell}_{\text{backtrack exactly once}}, F, \top\rangle}$	Heur: choose M' small. where $\{\ell_1, \ldots, \ell_k, \ell\} \in F$, $M = M' \cdot \Box \cdots \bar{\ell} \cdots$, (conflict already learned) and $\bar{\ell_1}, \ldots, \bar{\ell_k}$ in M'.

Example: DPLL with Learning

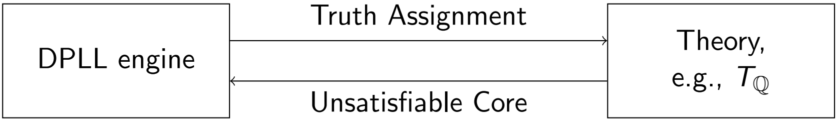
$$\underset{1}{P_1} \land (\neg P_2 \underset{2}{\lor} P_3) \land (\neg P_4 \underset{3}{\lor} P_3) \land (P_2 \underset{4}{\lor} P_4) \land (\neg P_1 \underset{5}{\lor} \neg P_4 \lor \neg P_3) \land (P_4 \underset{6}{\lor} \neg P_3)$$

The algorithm starts with $M = \epsilon$, $C = \top$ and
$F = \{\{P_1\}, \{\bar{P}_2, P_3\}, \{\bar{P}_4, P_3\}, \{P_2, P_4\}, \{\bar{P}_1, \bar{P}_4, \bar{P}_3\}, \{P_4, \bar{P}_3\}\}$.

$\langle \epsilon, F, \top\rangle \xrightarrow[1]{\text{Propagate}} \langle P_1, F, \top\rangle \xrightarrow{\text{Decide}} \langle P_1 \Box \bar{P}_2, F, \top\rangle \xrightarrow[4]{\text{Propagate}}$
$\langle P_1 \Box \bar{P}_2 P_4, F, \top\rangle \xrightarrow[3]{\text{Propagate}} \langle P_1 \Box \bar{P}_2 P_4 P_3, F, \top\rangle \xrightarrow[5]{\text{Conflict}}$
$\langle P_1 \Box \bar{P}_2 P_4 P_3, F, \{\bar{P}_1, \bar{P}_4, \bar{P}_3\}\rangle \xrightarrow[3]{\text{Explain}} \langle P_1 \Box \bar{P}_2 P_4 P_3, F, \{\bar{P}_1, \bar{P}_4\}\rangle \xrightarrow{\text{Learn}}$
$\langle P_1 \Box \bar{P}_2 P_4 P_3, F', \{\bar{P}_1, \bar{P}_4\}\rangle \xrightarrow{\text{Back}} \langle P_1 \bar{P}_4, F', \top\rangle \xrightarrow[4,\ 2]{\text{Propagate}}$
$\langle P_1 \bar{P}_4 P_2 P_3, F', \top\rangle \xrightarrow[6]{\text{Conflict}} \langle P_1 \bar{P}_4 P_2 P_3, F', \{P_4, \bar{P}_3\}\rangle \xrightarrow[2]{\text{Explain}}$
$\langle P_1 \bar{P}_4 P_2 P_3, F', \{P_4, \bar{P}_2\}\rangle \xrightarrow[4]{\text{Explain}} \langle P_1 \bar{P}_4 P_2 P_3, F', \{P_4\}\rangle \xrightarrow[7]{\text{Explain}}$
$\langle P_1 \bar{P}_4 P_2 P_3, F', \{\bar{P}_1\}\rangle \xrightarrow[1]{\text{Explain}} \langle P_1 \bar{P}_4 P_2 P_3, F', \emptyset\rangle \xrightarrow{\text{Learn}}$
$\langle P_1 \bar{P}_4 P_2 P_3, F' \cup \{\emptyset\}, \emptyset\rangle$

where $F' = F \cup \{\{\bar{P}_1, \overset{7}{\bar{P}_4}\}\}$.

The DPLL/CDCL algorithm is combined with a Decision Procedures for a Theory



DPLL takes the propositional core of a formula,
assigns truth-values to atoms.

Theory takes a conjunctive formula (conjunction of literals),
returns a (minimal) unsatisfiable core.

Minimal Unsatisfiable Core

Suppose we have a decision procedure for a conjunctive theory, e.g., Simplex Algorithm for $T_{\mathbb{Q}}$.

Given an unsatisfiable conjunction of literals $\ell_1 \land \cdots \land \ell_n$.
Find a subset UnsatCore $= \{\ell_{i_1}, \ldots, \ell_{i_m}\}$, such that $1 \leq i_1, \ldots, i_m \leq n$

- $\ell_{i_1} \land \ldots \land \ell_{i_m}$ is unsatisfiable.
- For each subset of UnsatCore the conjunction is satisfiable. } minimal

Possible approach: check for each literal whether it can be omitted.
$\longrightarrow$ n calls to decision procedure.

Most decision procedures can give small unsatisfiable cores for free.

yields <u>an</u> min. unsat. core (not necessarily the smallest)

$(x>0) \wedge (x<0)$

$\ell_1 \wedge \dots \wedge \ell_n$ unsat.

Theory returns an unsatisfiable core:

- a conjunction of literals from current truth assignment
- that is unsatisfible.

DPLL learns conflict clauses, a disjunction of literals

- that are implied by the formula
- and in conflict to current truth assignment.

Thus the negation of an unsatisfiable core is a conflict clause.

i.e. valid

$\bar{\ell}_1 \vee \dots \vee \bar{\ell}_n$

The DPLL part only needs one new rule:

TConflict $\dfrac{\langle M, F, \top \rangle}{\langle M, F, C \rangle}$ where M is unsatisfiable in the theory and $\neg C$ an unsatisfiable core of M.

$$F \;:\; \boxed{y \geq 1}_{P_1} \wedge (x \geq 0 \rightarrow y \leq 0) \wedge (x \leq 1 \rightarrow y \leq 0)$$

Atomic propositions:

$$P_1 : y \geq 1 \qquad\qquad P_2 : x \geq 0$$
$$P_3 : y \leq 0 \qquad\qquad P_4 : x \leq 1$$

Propositional core of F in CNF:

$$F_0 \;:\; (P_1) \wedge (\neg P_2 \vee P_3) \wedge (\neg P_4 \vee P_3)$$

$$F_0 : \{\overset{1}{\{P_1\}}, \overset{2}{\{\bar{P}_2, P_3\}}, \overset{3}{\{\bar{P}_4, P_3\}}\}$$

$$P_1 : \underbrace{y \geq 1} \quad P_2 : \underbrace{x \geq 0} \quad P_3 : \underbrace{y \leq 0} \quad P_4 : \underbrace{x \leq 1}$$

$$\langle \epsilon, F_0, \top \rangle \xrightarrow{\text{Propagate}}_{1} \langle P_1, F_0, \top \rangle \xrightarrow{\text{Decide}} \langle P_1 \Box P_3, F_0, \top \rangle \xrightarrow{\text{TConflict}}$$
$$\langle P_1 \Box P_3, F_0, \{\bar{P}_1, \bar{P}_3\} \rangle \xrightarrow{\text{Learn}} \langle P_1 \Box P_3, F_1, \{\bar{P}_1, \bar{P}_3\} \rangle \xrightarrow{\text{Back}}$$
$$\langle P_1 \bar{P}_3, F_1, \top \rangle \xrightarrow{\text{Propagate}}_{2} \langle P_1 \bar{P}_3 \bar{P}_2, F_1, \top \rangle \xrightarrow{\text{Propagate}}_{3}$$
$$\langle P_1 \bar{P}_3 \bar{P}_2 \bar{P}_4, F_1, \top \rangle \xrightarrow{\text{TConflict}} \langle P_1 \bar{P}_3 \bar{P}_2 \bar{P}_4, F_1, \{P_2, P_4\} \rangle \xrightarrow{\text{Explain}}_{3}$$
$$\langle P_1 \bar{P}_3 \bar{P}_2 \bar{P}_4, F_1, \{P_2, P_3\} \rangle \xrightarrow{\text{Explain}}_{2} \langle P_1 \bar{P}_3 \bar{P}_2 \bar{P}_4, F_1, \{P_3\} \rangle \xrightarrow{\text{Explain}}_{4}$$
$$\langle P_1 \bar{P}_3 \bar{P}_2 \bar{P}_4, F_1, \{\bar{P}_1\} \rangle \xrightarrow{\text{Explain}}_{1} \langle P_1 \bar{P}_3 \bar{P}_2 \bar{P}_4, F_1, \emptyset \rangle \xrightarrow{\text{Learn}}$$
$$\langle P_1 \bar{P}_3 \bar{P}_2 \bar{P}_4, F_1 \cup \{\emptyset\}, \emptyset \rangle$$

where $F_1 := F_0 \cup \{\underset{4}{\{\bar{P}_1, \bar{P}_3\}}\}$

No further step is possible; the formula F is unsatisfiable.