Two simulations about DPLL(T)
Mahfuza Farooque, Stéphane Lengrand, Assia Mahboubi

To cite this version:
Mahfuza Farooque, Stéphane Lengrand, Assia Mahboubi. Two simulations about DPLL(T). 2012. <hal-00690044>

HAL Id: hal-00690044
https://hal.archives-ouvertes.fr/hal-00690044
Submitted on 23 Apr 2012
Two simulations about DPLL(T)

Mahfuza Farooque\textsuperscript{1}, Stéphane Lengrand\textsuperscript{1,2} and Assia Mahboubi\textsuperscript{3}

\textsuperscript{1} CNRS
\textsuperscript{2} Ecole Polytechnique
\textsuperscript{3} Microsoft Research - INRIA Joint Centre

Project PSI: “Proof Search control in Interaction with domain-specific methods”
ANR-09-JCJC-0006
23rd April 2012

Abstract

In this paper we relate different formulations of the DPLL(T) procedure. The first formulation is that of [NOT06] based on a system of rewrite rules, which we denote DPLL(T).

The second formulation is an inference system of [Tin02], which we denote LKDPLL(T).

The third formulation is the application of a standard proof-search mechanism in a sequent calculus LKP(T) introduced here.

We formalise an encoding from DPLL(T) to LKDPLL(T) that was, to our knowledge, never explicitly given and, in the case where DPLL(T) is extended with backjumping and Lemma learning, never even implicitly given.

We also formalise an encoding from LKDPLL(T) to LKP(T), building on Ivan Gazeau’s previous work: we extend his work in that we handle the “-modulo-Theory” aspect of SAT-modulo-theory, by extending the sequent calculus to allow calls to a theory solver (seen as a blackbox). We also extend his work in that we handle advanced features of DPLL such as backjumping and Lemma learning, etc.

Finally, we refine the approach by starting to formalise quantitative aspects of the simulations: the complexity is preserved (number of steps to build complete proofs). Other aspects remain to be formalised (non-determinism of the search / width of search space).

Contents

1 Encoding DPLL(T) in LKDPLL(T) .......................... 2
  1.1 Preliminaries: LKDPLL(T) and its properties .............. 2
  1.2 DPLL(T) with backtracking ................................ 5
  1.3 DPLL(T) with backjumping and Lemma learning .......... 8

2 Encoding LKDPLL(T) in LKP(T) ......................... 11
  2.1 Preliminaries: System LKP(T) .............................. 11
  2.2 Simulation .................................................. 12
1 Encoding DPLL(\(T\)) in LK_{DPLL}(\(T\))

In this section we encode DPLL(\(T\)) in LK_{DPLL}(\(T\)).

Note that there exist different variants of DPLL(\(T\)). We first consider the basic version which is equipped with backtracking. This formalises ideas presented in [Tin02].

Then we enhance the encoding to the enhanced version of DPLL(\(T\)) with backjumping, a generalised version of backtracking.

The main gap between DPLL(\(T\)) and an inference system such as LK_{DPLL}(\(T\)) is the fact that a (successful) DPLL(\(T\)) run is a rewrite sequence finishing with the state UNSAT, while a (successful) proof-search run is (/ produces) a proof tree. Roughly speaking, the DPLL(\(T\)) procedure implements the depth-first search of the corresponding tree.

1.1 Preliminaries: LK_{DPLL}(\(T\)) and its properties

**Definition 1 (The system LK_{DPLL}(\(T\)))**

Clauses are finite disjunctions of literals considered up to commutativity and associativity. We will denote them \(C, C_0, C_1\) etc; the empty clause will be denoted by \(\bot\). The cardinality of a clause \(C\) is denoted \(|C|\).

Finite sets of clauses, e.g. \(\{C_1, \ldots, C_n\}\), will be denoted \(\phi, \phi_0, \text{etc.}\), By \(|\phi|\) we denote the sum of the sizes of the clauses in \(\phi\). By \(\text{lit}(\phi)\) we denote the set of literals that appear in \(\phi\) or whose negations appear in \(\phi\).

Given a theory \(\mathcal{T}\) the system LK_{DPLL}(\(\mathcal{T}\)), given in Figure 1, is an inference system on sequences of the form \(\Delta;\phi \vdash_{\mathcal{T}} \top\), where \(\Delta\) is a set of literals (e.g. \(\{l_1, \ldots, l_n\}\)).

![Figure 1: System LK_{DPLL}(\(T\))](image)

The *Assert* rule models the fact that every literal occurring as a unit clause in the current clause set must be satisfied for the whole clause set to be satisfied. The *Split* is mainly used to branch the proof tree from the DPLL rewrite sequence system. This rule corresponds to the decomposition in smaller subproblems of the DPLL method. This rule is the only *don’t know non-deterministic* rule of the calculus. The *Resolve* rule removes from a clause all literals whose complement has been asserted (which corresponds to generating the simplified clause by unit resolution and the discarding the clause by backward subsumption). The *Subsume* rule removes from the clauses that contain an asserted literal (because all of these clause will be satisfied in any model in which the asserted literal is true). To close the branch of a proof tree we use the *empty* rule is in the calculus just for convenience and could be removed with no loss of completeness. It models the fact that a derivation can be terminated as soon as the empty clause is derived. We do not consider that the model is consistent and satisfiable.

**Definition 2 (Semantical entailment)** \(\Delta \models_{\mathcal{T}} C\) is a semantical notion of entailment for a particular theory \(\mathcal{T}\), i.e. every \(\mathcal{T}\)-model of \(\Delta\) is a \(\mathcal{T}\)-model of \(C\). A theory lemma is a clause \(C\) such that \(\emptyset \models_{\mathcal{T}} C\).

**Lemma 1 (Weakening 1)** The following rule is size-preserving admissible in LK_{DPLL}(\(T\))

\[
\Delta; \phi \vdash_{\mathcal{T}} \top \\
\Delta; \phi, C \vdash_{\mathcal{T}}
\]

**Proof:** By induction on \(\Delta; \phi \vdash_{\mathcal{T}} \top\). □
Definition 3 (Consequences) For every set $\Delta$ of literals $l$, let $\text{Sat}(\Delta) = \{l|\Delta \models_T l\}$ and $\text{Sat}_\phi(\Delta) = \text{Sat}(\Delta) \cap \text{lit}(\phi)$.

Remark 2 If $\text{Sat}(\Delta) = \text{Sat}(\Delta')$ then $\Delta \models_T l$ iff $\Delta' \models_T l$.

Lemma 3 (Weakening 2) The following rule is size-preserving admissible in LK_{DPLL}(T)

\[
\Delta, \phi \vdash_T \Delta', \phi \vdash_T \text{Sat}_\phi(\Delta) \subseteq \text{Sat}_\phi(\Delta')
\]

Proof: By induction on the derivation of $\Delta, \phi \vdash_T \Delta', l \models_T$

1. **Resolve** \(\Delta, \phi, C \vdash_T \Delta, l \models_T\)
   We assume $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$.
   from which we get $\text{Sat}_\phi(\Delta) \subseteq \text{Sat}_\phi(\Delta')$, so we can apply the induction hypothesis to construct
   \[
   \Delta', \phi, C \vdash_T \Delta', l \models_T
   \]
   The side-condition is a consequence of the assumption $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$.

2. **Subsume** \(\Delta, \phi, l \vdash_T \Delta, l^\bot \models_T\)
   We assume $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$.
   from which we get $\text{Sat}_\phi(\Delta) \subseteq \text{Sat}_\phi(\Delta')$, so we can apply the induction hypothesis to construct
   \[
   \Delta', \phi, l \vdash_T \Delta', l^\bot \models_T
   \]
   The side-condition is a consequence of the assumption $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$.

3. **Assert** \(\Delta, l, \phi, l \vdash_T \Delta, l^\bot \not\models_T\) and $\Delta, l \not\models_T$
   We assume $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$.
   from which we get $\text{Sat}_\phi(\Delta, l) \subseteq \text{Sat}_\phi(\Delta', l)$.
   
   - If $\Delta' \models_T l$, then $\text{Sat}(\Delta', l) = \text{Sat}(\Delta')$, so we have $\text{Sat}_\phi(\Delta, l) \subseteq \text{Sat}_\phi(\Delta')$. The induction hypothesis then gives $\Delta', \phi, l \models_T$.
   
   - If $\Delta' \models_T l^\bot$, then we construct
     \[
     \Delta', \phi, l \vdash_T \text{Empty}
     \]
     \[
     \Delta', \phi, l \vdash_T \text{Resolve}
     \]
     
   - If $\Delta' \not\models_T l$ and $\Delta' \not\models_T l^\bot$: we first apply the induction hypothesis to get $\Delta', l, \phi, l \models_T$ and we conclude by constructing
     \[
     \Delta', l, \phi, l \vdash_T \Delta', l^\bot \not\models_T\) and $\Delta', l \not\models_T$.

4. **Split** \(\Delta, l^\bot, \phi, l \vdash_T \Delta, l, \phi, l \vdash_T \Delta, l^\bot \not\models_T\) and $\Delta, l \not\models_T$
   We assume $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$ from which we get both
   $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$ and $\text{Sat}_\phi(l') \subseteq \text{Sat}_\phi(l)$. The induction hypothesis then gives $\Delta', \phi, l \vdash_T$.
   
   - If $\Delta' \models_T l$, then $\text{Sat}(\Delta') = \text{Sat}(\Delta', l)$, so we have $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$. The induction hypothesis then gives $\Delta', \phi, l \vdash_T$.
   
   - If $\Delta' \models_T l^\bot$, then $\text{Sat}(\Delta') = \text{Sat}(\Delta', l^\bot)$, so we have $\text{Sat}_\phi(l) \subseteq \text{Sat}_\phi(l')$. The induction hypothesis then gives $\Delta', \phi, l \vdash_T$.
- If $\Delta' \not\vdash_T l$ and $\Delta' \not\vdash_T l^+$: the induction hypothesis on both premises gives $\Delta', l; \phi, l \lor C \vdash_T$ and $\Delta', l^+; \phi, l \lor C \vdash_T$, and we can conclude

$$\frac{\Delta', l^+; \phi, l \lor C \vdash_T \Delta', l; \phi, l \lor C \vdash_T}{\Delta' \vdash_T l}$$

Empty Straightforward.

Lemma 4 (Invertibility of Resolve) Resolve is size-preserving invertible in $\text{LK}_{\text{DPLL}}(T)$.

Proof: By induction on the derivation of $\Delta; \phi, C \lor l \vdash_T$ we prove $\Delta; \phi, C \vdash_T$ (with the assumption $\Delta, l \models_T$):

**Resolve** easily permutes with other instances of Resolve and with instances of Subsume.

**Assert** The side-condition of the rule guarantees that the literal added to the model, say $l'$, is different from $l$:

$$\frac{\Delta, l'; \phi', l', C \lor l \vdash_T}{\Delta; \phi', l', C \lor l \vdash_T} \Delta, l^+ \not\vdash_T \text{ and } \Delta, l' \not\vdash_T$$

We can construct

$$\frac{\Delta, l'; \phi', l', C \vdash_T}{\Delta; \phi', l', C \vdash_T} \Delta, l^+ \not\vdash_T \text{ and } \Delta, l' \not\vdash_T$$

whose premise is proved by the induction hypothesis.

**Split** $\frac{\Delta, l^+; \phi, C \lor l \vdash_T}{\Delta; \phi, C \lor l \vdash_T} l' \in \text{lit}(\phi, C \lor l)$ and $\Delta, l^+ \not\vdash_T \text{ and } \Delta, l' \not\vdash_T$

We can construct

$$\frac{\Delta, l'; \phi, C \vdash_T}{\Delta; \phi, C \vdash_T} \Delta, l^+ \not\vdash_T \text{ and } \Delta, l' \not\vdash_T$$

whose branches are closed by using the induction hypothesis. The side-condition $l' \in \text{lit}(\phi, C)$ is satisfied because $l \neq l'$.

Empty Straightforward.

We now introduce a new system $\text{LK}_{\text{DPLL}^+} (T)$ which is an extended version of $\text{LK}_{\text{DPLL}} (T)$ with Weakening1, Weakening2 and the Inverted Resolve. By the previous lemmas, a sequent derivable in $\text{LK}_{\text{DPLL}^+} (T)$ is derivable in $\text{LK}_{\text{DPLL}} (T)$.

<table>
<thead>
<tr>
<th>$\Delta; \phi \vdash_T$</th>
<th>$\Delta \vdash_T$</th>
<th>$\text{Sat}<em>\phi(\Delta) \subseteq \text{Sat}</em>\phi(\Delta')$</th>
<th>$\Delta; \phi, l \lor C \vdash_T$</th>
<th>$\Delta; C, \phi \vdash_T$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Delta; \phi, C \vdash_T$</td>
<td>$\Delta' \vdash_T$</td>
<td>$\Delta \vdash_T$</td>
<td>$\Delta; \phi, l \lor C \vdash_T$</td>
<td>$\Delta; C, \phi \vdash_T$</td>
</tr>
</tbody>
</table>

Figure 2: System $\text{LK}_{\text{DPLL}^+} (T)$

Definition 4 (Size of proof-trees in $\text{LK}_{\text{DPLL}^+} (T)$) The size of proof-trees in $\text{LK}_{\text{DPLL}^+} (T)$ is defined as the size of trees in the usual sense, but not counting the occurrences of Weakening1, Weakening2 or the Inverted Resolve rules.

Remark 5 The size-preserving admissibility results of those three rules in $\text{LK}_{\text{DPLL}^+} (T)$ entails that a proof-tree in $\text{LK}_{\text{DPLL}^+} (T)$ of size $n$, can be transformed into a proof-tree in $\text{LK}_{\text{DPLL}} (T)$ of size at most $n$.

Lemma 6 If $\Delta \models_T \neg C$ then there is a proof-tree concluding $\Delta, C, \phi \vdash_T$ of size at most $|\phi| + 1$.

For that reason, dashed lines will be used for the occurrences of those inference rules.
**Proof:** Here $\Delta \models T \neg C$ means $C = l_1 \lor \ldots \lor l_n$ and for all $l_i, \forall l_i \; \Delta \models T l_i^+$ where $i=1,\ldots,n$. We can therefore construct

\[
\Delta; l, \phi \vdash_T \frac{\Delta; C, \phi \vdash_T \text{Empty}}{\text{Resolve}}
\]

\[
\hfill \square \hfill
\]

### 1.2 DPLL($T$) with backtracking

In this section we describe the basic DPLL($T$) procedure [NOT06], and its encoding into LK$_{DPLL}(T)$.

**Definition 5 (Basic DPLL($T$))** Models are defined by the following grammar:

\[
\Delta ::= () \mid \Delta, l \mid \Delta, l^d
\]

where $l$ ranges over literals, and $l^d$ is an annotated literal called decision literal.

The basic DPLL($T$) procedure rewrites states of the form $\Delta \parallel \phi, \neg C$ and there is no decision literal in $\Delta$.

- **Fail:**
  \[
  \Delta \parallel \phi, C \Rightarrow \text{UNSAT}, \quad \text{with} \; |\Delta| \models \neg C
  \]

- **Decide:**
  \[
  \Delta \parallel \phi \Rightarrow \Delta, l^d \parallel \phi \quad \text{if} \; |\Delta, l| \models \neg C \quad \text{and} \; l^d \not\in \Delta
  \]

- **Backtrack:**
  \[
  \Delta_1, l, l^d, \Delta_2 \parallel \phi, C \Rightarrow \Delta_1, l^d \parallel \phi, C \quad \text{where} \; |\Delta| \models \neg C \quad \text{and} \; l^d \not\in \Delta
  \]

- **Unit Propagation:**
  \[
  \Delta \parallel \phi \Rightarrow \Delta, l \parallel \phi \quad \text{where} \; |\Delta, l| \models \neg C \quad \text{and} \; l \not\in \Delta
  \]

where $|\Delta|$ denotes the result of erasing the annotations on decision literals, an operation defined in Figure 3.

\[
\begin{array}{c}
|()| := () \\
|\Delta, l| := |\Delta|, l \\
|\Delta, l^d| := |\Delta|, l
\end{array}
\]

**Figure 3:** Erasing annotations

We now proceed with the encoding of the basic DPLL($T$) procedure as the construction of a derivation tree in System LK$_{DPLL}(T)$. The simulation could be be stated as follows:

If $\Delta \parallel \phi \Rightarrow^* \text{UNSAT}$ then there is a LK$_{DPLL}(T)$ proof of $|\Delta| \parallel \phi \vdash_T$ (i.e. there is no $T$-model of $\phi$ extending $\Delta$).

This is true; however, there is more information in $\Delta \parallel \phi \Rightarrow^* \text{UNSAT}$ than in $|\Delta| \parallel \phi \vdash_T$, because the DPLL($T$) sequence leading to UNSAT also backtracks on decision literals. This means that not only there is no $T$-model of $\phi$ extending $|\Delta|$, but no matter how decision literals of $\Delta$ are changed, there is still no $T$-model of $\phi$ that can be constructed. This notion is formalised by collecting the backtrack models as follows:

**Definition 6 (Backtrack models)** In Fig. 4 we define the interpretation of a model as a collection (formally, a multiset) of sets of literals.

**Remark 7** We have $|\Delta| \in [\Delta]$ and $[\Delta] \subseteq |\Delta|$.

We consider a notion of a partial proof-tree to step-by-step simulate DPLL($T$) runs.
Definition 7 (Partial proof-tree) A partial proof-tree in $\text{LK}_{\text{DPLL}^+}(T)$ is a tree labelled with sequents, whose leaves are tagged as either open or closed, and such that every node that is not an open leaf is an instance of the $\text{LK}_{\text{DPLL}^+}(T)$ rules. A complete proof-tree is a partial proof-tree whose leaves are all closed.

A partial proof-tree $\pi'$ is an $n$-extension of $\pi$ if $\pi'$ is $\pi$ or if $\pi'$ is obtained from $\pi$ by replacing one of its open leaves by a partial proof-tree of size at most $n$ and whose conclusion has the same label as that leaf.

Definition 8 (Correspondence between DPLL($T$) states and partial proof-trees) A partial proof-tree $\pi$ corresponds to a DPLL($T$) state $\Delta\|\phi$ if the sequents labelling its open leaves form a sub-set of $\{\Delta'; \phi \vdash \tau \mid \Delta' \in \llbracket \Delta \rrbracket\}$.

A partial proof-tree $\pi$ corresponds to UNSAT if it has no open leaf.

The DPLL($T$) procedure starts from an initial state i.e. $\emptyset\|\phi$, to which corresponds the partial proof-tree consisting of one node (both a root and a leaf) labelled with the sequent $\phi \vdash \tau$.

Note that, different partial proof-trees might correspond to the same DPLL($T$) state, as different DPLL($T$) runs can lead to that state from various initial DPLL($T$) states. The simulation theorem below expresses the fact that, when DPLL($T$) rewrites one state to another state, any partial proof-tree corresponding to the formal state can be extended into a partial proof-tree corresponding to the latter state.

Theorem 8 If $\Delta\|\phi \Rightarrow S_2$ is a rewrite step of DPLL($T$) and if $\pi_1$ corresponds to $\Delta\|\phi$ then there is, in $\text{LK}_{\text{DPLL}^+}(T)$, a $|\phi|+1$-extension $\pi_2$ of $\pi_1$ corresponding to $S_2$.

Proof: By case analysis:

- Fail: $\Delta\|\phi, C \Rightarrow^* \text{UNSAT}$ with $|\Delta| \models \neg C$ and there is no decision literal in $\Delta$. Let $\pi_1$ be a partial proof-tree corresponding to $\Delta\|\phi, C$. Since there are no decision literals in $\Delta$, $\pi_1$ can have at most one open leaf, labelled by $|\Delta|\vdash C \vdash \tau$.

We $|\phi, C|$-extend $\pi_1$ into $\pi_2$ by replacing that leaf by a complete tree deriving $|\Delta|\vdash C \vdash \tau$.

We obtain that tree by applying Lemma 6 on the hypothesis $|\Delta| \models \neg C$. The new tree $\pi_2$ is complete and therefore corresponds to the UNSAT state of the DPLL($T$) run.

- Decide: $\Delta\|\phi \Rightarrow \Delta, l^t\|\phi$ where $l \not\in \Delta$, $l^t \not\in \Delta$, $l \in \phi$ or $l^t \in \phi$.

Let $\pi_1$ be a partial proof-tree corresponding to $\Delta\|\phi$. We $1$-extend it into $\pi_2$ by replacing the open leaf labelled with $|\Delta|\vdash C \vdash \tau$ (if there is such a leaf) by one of three proof-trees:

- If $|\Delta|, l \vdash \tau$, we have $\text{Sat}(|\Delta|) = \text{Sat}(|\Delta|, l^t)$ and we take:

  $|\Delta|, l^t\|\phi \vdash \tau$

  $|\Delta;\phi \vdash \tau$ - Weakening2

  The new open leaves form a sub-set of $\{|\Delta|, l^t; \phi \vdash \tau \} \cup \{|\Delta'; \phi \vdash \tau \mid \Delta' \in |\Delta|, l^t\}$ (since $|\Delta|, l^t = |\Delta, l^t| \in |\Delta|, l^t| = |\Delta|, l^t| \subseteq |\Delta|, l^t|$ and therefore $\pi_2$ corresponds to $\Delta, l^t\|\phi$.

- If $|\Delta|, l^t \vdash \tau$, we have $\text{Sat}(|\Delta|) = \text{Sat}(|\Delta|, l)$ and we take:

  $|\Delta|, l^t\|\phi \vdash \tau$

  $|\Delta|, l\|\phi \vdash \tau$ - Weakening2

$2$ A partial proof-tree that has no open leaf is isomorphic to a derivation in $\text{LK}_{\text{DPLL}^+}(T)$. 

---

| $\llbracket \emptyset \rrbracket$ | := $\emptyset$
| $\llbracket \Delta, l \rrbracket$ | := $|\Delta|$ 
| $\llbracket \Delta, l^t \rrbracket$ | := $|\Delta|, l^t$
| $\llbracket \Delta \rrbracket$ | := $|\Delta| \cup \{\llbracket \Delta \rrbracket\}$

Figure 4: Collecting backtrack points
The new open leaves form a sub-set of \( \{\Delta_l, l \vdash \top \} \cup \{\Delta', \phi \vdash \top \mid \Delta' \in [\Delta] \} \subseteq \{\Delta', \phi \vdash \top \mid \Delta' \in \Delta_l \} \) (since \( |\Delta_l|, l = |\Delta, l| \in [\Delta_l, l'] \)) and therefore \( \pi_2 \) corresponds to \( \Delta, l' \parallel \phi \).

- If \( |\Delta_l|, l \not\vdash \top \) and \( |\Delta_l|, l' \not\vdash \top \), we take

\[
|\Delta_l|, l, \phi \vdash \top | |\Delta_l|, l', \phi \vdash \top
\]

\( \text{Split} \)

The new open leaves form a sub-set of \( \{\Delta_l, l \vdash \top \} \cup \{\Delta', \phi \vdash \top \} \cup \{\Delta', \phi \vdash \top \mid \Delta' \in [\Delta] \} \subseteq \{\Delta', \phi \vdash \top \mid \Delta' \in \Delta_l \} \) (since \( |\Delta_l|, l = |\Delta, l| \in [\Delta_l, l'] \)) and therefore \( \pi_2 \) corresponds to \( \Delta, l' \parallel \phi \).

- Backtrack: \( \Delta_l, l, \phi \vdash \top, C \Rightarrow \Delta_l, l' \parallel \phi, C \) if \( |\Delta_l|, l, \Delta, l' \parallel \top \) and no decision literal is in \( \Delta, l' \).

Let \( \pi_1 \) be a partial proof-tree corresponding to \( \Delta_l, l', \Delta, l' \parallel \phi, C \). Since there are no decision literals in \( \Delta, l' \), \( \pi_1 \) can have at most one open leaf, labelled with \( |\Delta_l|, l', \Delta, l' \parallel \phi, C \). We \( |\phi, C \vdash l' \parallel \top \) and replace that leaf by a complete tree deriving \( |\Delta_l|, l', \Delta, l' \parallel \phi, C \). We obtain that partial proof-tree by applying lemma 6 on the assumption \( |\Delta_l|, l', \Delta, l' \parallel \top \).

Weakening\( _2 \) if there is such a leaf)

- If \( |\Delta_l|, l' \vdash \top \), we have \( \text{Sat}(|\Delta_l|) = \text{Sat}(|\Delta_l|, l) \) and we take:

\[
|\Delta_l|, l, \phi \vdash \top | |\Delta_l|, l', \phi \vdash \top
\]

\( \text{Weakening}_2 \)

The new open leaves form a sub-set of \( \{\Delta_l, l \vdash \top \} \cup \{\Delta', \phi \vdash \top \mid \Delta' \in [\Delta] \} \subseteq \{\Delta', \phi \vdash \top \mid \Delta' \in \Delta_l \} \) (since \( |\Delta_l|, l = |\Delta, l| \in [\Delta_l, l'] \)) and therefore \( \pi_2 \) corresponds to \( \Delta, l' \parallel \phi \).

- If \( |\Delta_l|, l \not\vdash \top \) then lemma 6 directly provides a partial proof-tree of \( |\Delta_l|, \phi \vdash \top \).

- If \( |\Delta_l|, l \not\vdash \top \), we can construct the following tree:

\[
|\Delta_l|, l, \phi \vdash \top | |\Delta_l|, l', \phi \vdash \top
\]

\( \text{Inverted Resolve} \)

\[
|\Delta_l|, l', \phi, C \parallel \top
\]

\( \text{Assert} \)

\[
|\Delta_l|, l', \phi, C \parallel \top
\]

\( \text{Resolve} \)

where the side-conditions of \( \text{Resolve} \) are provided by the hypothesis \( \Delta' \vdash \top \).

The new open leaves form a sub-set of \( \{\Delta_l, l \vdash \top \} \cup \{\Delta', \phi \vdash \top \mid \Delta' \in [\Delta] \} \subseteq \{\Delta', \phi \vdash \top \mid \Delta' \in \Delta_l \} \) and therefore \( \pi_2 \) corresponds to \( \Delta, l' \parallel \phi \).

- Theory Propagate: \( \Delta, \phi \Rightarrow \Delta, \top \) where \( |\Delta| \vdash \top, l \in \text{litr}(\phi) \) and \( l \not\in \Delta, l' \not\in \Delta \).

Let \( \pi_1 \) be a partial proof-tree corresponding to \( \Delta, \phi \). We \( 1 \)-extend it into \( \pi_2 \) by replacing the open leaf labelled with \( |\Delta|, l \vdash \top \) by the following proof-tree:

\[
|\Delta|, l, \phi \vdash \top
\]

\( \text{Weakening}_2 \)

The new open leaves form a sub-set of \( \{\Delta_l, l \vdash \top \} \cup \{\Delta', \phi \vdash \top \mid \Delta' \in [\Delta] \} \subseteq \{\Delta', \phi \vdash \top \mid \Delta' \in \Delta_l \} \) (since \( |\Delta_l|, l = |\Delta, l| \in [\Delta_l, l'] \)) and therefore \( \pi_2 \) corresponds to \( \Delta, l' \parallel \phi \).
Corollary 9 \( LK_{DPLL}(T) \) is complete, i.e. if \( \phi \models \tau \) then \( \phi \vdash \tau \).

Proof: By completeness of basic DPLL(\( T \)) and Theorem 8. \( \square \)

1.3 DPLL(\( T \)) with backjumping and Lemma learning

We now consider a more advanced version of DPLL(\( T \)), which involves backjumping and lemma learning features, and which we denote DPLL\(_b\)(\( T \)). DPLL\(_b\)(\( T \)) extends basic DPLL(\( T \)) with the rules known as \( T \)-Backjump, \( T \)-Learn, \( T \)-Forget, and Restart [NOT06]. Those rules drastically increase the efficiency of SMT-solvers.

\( T \)-Backjump: \( \Delta_1, l^1, \Delta_2 \parallel \phi, C \Rightarrow \Delta_1, b_j \parallel \phi, C \) with
1. \(|\Delta_1, l^1, \Delta_2| \models \neg C\).
2. \(|\Delta_1| \models \neg C'\).
3. \( \phi, C \models \tau \) \( C' \lor b_j \).
4. \( l_{h_j} \notin \Delta_1, l_{h_j} \notin \Delta_1 \) and \( b_j \in \text{lit}(\phi, \Delta_1, l^1, \Delta_2)\).

for some clause \( C' \) such that \( \text{lit}(C') \subseteq \text{lit}(\phi, C)\).

\( T \)-Learn: \( \Delta \parallel \phi \Rightarrow \Delta \parallel \phi, C \) if \( \text{lit}(C) \subseteq \text{lit}(\phi, \Delta) \) and \( \phi \models \tau \) \( C \).

\( T \)-Forget: \( \Delta \parallel \phi, C \Rightarrow \Delta \parallel \phi \) if \( \phi \models \tau \) \( C \).

Restart: \( \Delta \parallel \phi \Rightarrow \emptyset \parallel \phi \).

In order to simulate those extra rules in \( LK_{DPLL}(T) \), we need to extend \( LK_{DPLL}(T) \) with a cut rule as follows:

Definition 9 (\( LK_{DPLL}(T) \) with cut) System \( LK_{DPLL}(T) \) is obtained by extending system \( LK_{DPLL+}(T) \) with the following cut-rule:

\[
\Delta \parallel \phi, l_1, \ldots, l_n \vdash \Delta \parallel \phi \vdash \tau \\
\Delta \parallel \phi \vdash \tau
\]

Cut where \( C = l_1^1, \ldots, l_n^1 \)

We define the size of proof-trees in \( LK_{DPLL}(T) \) as we did for \( LK_{DPLL+}(T) \) (ignoring Weakening1, Weakening2 or the Inverted Resolve), but also ignoring the left-branch of the cut-rules.\(^3\)

Definition 10 (\( n, \phi, S \)-sync action) \( \pi_\phi \) is a \( n, \phi, S \)-sync action if it is a function that maps every model \( \Delta \in S \) to a partial proof-tree of size at most \( n \) and concluding \( \Delta \parallel \phi \vdash \tau \).

Definition 11 (Parallel \( n \)-extension of partial proof-trees) \( \pi_2 \) is a parallel \( n \)-extension of \( \pi_1 \) according to \( \pi_\phi \) if \( \pi_\phi \) is a \( n, \phi, S \)-sync action and if \( \pi_2 \) is obtained from \( \pi_1 \) by replacing all the open leaves of \( \pi_1 \) labelled by sequents of the form \( \Delta \parallel \phi \vdash \tau \) (where \( \Delta \in S \)) by \( \pi_\phi(\Delta) \).

Theorem 10 If \( \Delta \parallel \phi \Rightarrow DPLL_b(T) \) \( S_2 \) and \( \pi_1 \) corresponds to \( \Delta \parallel \phi \), there is parallel \( \phi \parallel 3 \)-extension \( \pi_2 \) of \( \pi_1 \) (according to some \( \pi_\phi \)) such that \( \pi_2 \) corresponds to \( S_2 \).

Proof: Since \( LK_{DPLL}(T) \) is a sub-system of \( LK_{DPLL}(T) \), we only need to simulate (in \( LK_{DPLL}(T) \)) the new rules.

\( T \)-Backjump: \( \Delta_1, l^1, \Delta_2 \parallel \phi, C \Rightarrow \Delta_1, b_j \parallel \phi, C \) with
1. \(|\Delta_1, l^1, \Delta_2| \models \neg C\).
2. \(|\Delta_1| \models \neg C'\).
3. \( \phi, C \models \tau \) \( C' \lor b_j \).
4. \( l_{h_j} \notin \Delta_1, l_{h_j} \notin \Delta_1 \) and \( b_j \in \text{lit}(\phi, \Delta_1, l^1, \Delta_2)\).

\(^3\)As we shall see in the simulation theorem, this definition mimics the fact that the length of DPLL(\( T \)) sequences is a complexity measure that ignores the cost of checking the side-conditions.
Let $\pi_1$ be a partial proof-tree corresponding to $\Delta_1, l_{b_j} \parallel \phi, C$. We have to build a $\pi_2$ that corresponds to $\Delta_1, l_{b_j} \parallel \phi, C$ in the DPLL$_{b_j}(T)$ run. This means that the open leaves of $\pi_2$ should be labelled with sequents of the form $\Delta': \phi, C \vdash \tau$ where $\Delta' \in [\Delta_1, l_{b_j}]$.

Let $S = [\Delta_1, l_{b_j}] \parallel [\Delta_1]$ and $\pi_\phi$ be the $|\phi, C| + 3, \phi, C, S$-sync action that maps every $\Delta \in S$ to

\[
\Delta; \phi, C, C' \vdash \tau \rightarrow Weakening2 \quad \Delta; \phi, \neg C' \vdash \tau \rightarrow Weakening2 \quad \Delta; \phi, C \vdash \tau \rightarrow \text{Resolve} \quad [\Delta_1]; \phi, C \vdash \tau \rightarrow \text{Subsume} \quad [\Delta_1]; l_{b_j} \phi, C \vdash \tau \rightarrow \text{Assert} \quad [\Delta_1]; l_{b_j} \phi, C \vdash \tau \rightarrow \text{Cut}
\]

It is a valid partial proof-tree because $\Delta \in S$ entails $[\Delta_1] \subseteq \Delta$ and therefore $\text{Sat}_o([\Delta_1]) \subseteq \text{Sat}_o(\Delta)$. The left branch is closed by assumption (3) and the completeness of $\text{LK}_{\text{DPLL}}(T)$ on $\phi, C, \neg C', l_{b_j} \vdash \tau$ (Corollary 9). We cannot anticipate the size of the proof-tree closing that branch, and we therefore ignore that proof-tree to compute the size of the whole tree, just as the length of the DPLL(T) run ignores the cost of checking $C' \parallel l_{b_j}$.

Let $\pi_2$ be the parallel $|\phi, C| + 3$-extension of $\pi_1$ according to $\pi_\phi$. The new open leaves form a sub-set of $\{[\Delta_1, l_{b_j} \phi, C \vdash \tau] \cup \{\Delta': \phi \vdash \tau \mid \Delta' \in [\Delta_1] \} \subseteq \{\Delta': \phi \vdash \tau \mid \Delta' \in [\Delta_1, l_{b_j}]\}$ (since $[\Delta_1], l_{b_j} = [\Delta_1, l_{b_j}] = [\Delta_1, l_{b_j}] = [\Delta_1]$) and therefore $\pi_2$ corresponds to $[\Delta_1, l_{b_j}] \parallel \phi, C$.

**T-Forget:** $\Delta; \phi \Rightarrow [\Delta]; \phi$ if $\phi \vdash \tau \parallel C$.

Let $\pi_1$ be a partial proof-tree corresponding to $[\Delta]; \phi$. We have to build a $\pi_2$ that corresponds to $[\Delta]; \phi$ in the DPLL$_{b_j}(T)$ run. This means that the open leaves of $\pi_2$ should be labelled with sequents of the form $\Delta': \phi \vdash \tau$ where $\Delta' \in [\Delta]$. Let $S = [\Delta]$ and $\pi_\phi$ be the $1, \phi, C, S$-sync action that maps every $\Delta' \in S$ to

$\Delta'; \phi \vdash \tau \rightarrow \text{Cut}$

The left branch of the cut is closed by assumption and completeness of $\text{LK}_{\text{DPLL}}(T)$ on $\phi, \neg C \vdash \tau$ (Corollary 9). We cannot anticipate the size of the proof-tree closing that branch, and we therefore ignore that proof-tree to compute the size of the whole tree, just as the length of the DPLL(T) run ignores the cost of checking $\phi \vdash \tau \parallel C$.

Let $\pi_2$ be the parallel $|\phi| + 3$-extension of $\pi_1$ according to $\pi_\phi$. The new open leaves form a sub-set of $\{\Delta': \phi, C \vdash \tau \mid \Delta' \in [\Delta]\}$ and therefore $\pi_2$ corresponds to $[\Delta]; \phi, C$.

**T-Learn:** $\Delta; \phi \Rightarrow [\Delta]; \phi$ if $\phi \vdash \tau \parallel C$.

Let $\pi_1$ be a partial proof-tree corresponding to $\Delta; \phi, C$. We have to build a $\pi_2$ that corresponds to $\Delta; \phi, C$ in the DPLL$_{b_j}(T)$ run. This means that the open leaves of $\pi_2$ should be labelled with sequents of the form $\Delta': \phi, C \vdash \tau$ where $\Delta' \in [\Delta]$.

Let $S = [\Delta]$ and $\pi_\phi$ be the $1, \phi, C, S$-sync action that maps every $\Delta' \in S$ to

$\Delta'; \phi \vdash \tau \rightarrow \text{Cut}$

Let $\pi_2$ be the parallel $1$-extension of $\pi_1$ according to $\pi_\phi$. The new open leaves form a sub-set of $\{\Delta': \phi \vdash \tau \mid \Delta' \in [\Delta]\}$ and therefore $\pi_2$ corresponds to $\Delta; \phi$. Restarts: $\Delta; \phi \Rightarrow [\emptyset]; \phi$.

Let $\pi_1$ be a partial proof-tree corresponding to $\Delta; \phi$. We have to build a $\pi_2$ that corresponds to $\emptyset; \phi$ in the DPLL$_{b_j}(T)$ run. This means that the open leaves of $\pi_2$ should be labelled with sequents of the form $\emptyset; \phi \vdash \tau$.
Let $S = [\Delta]$ and $\pi_\phi$ be the $1, \phi, S$-sync action that maps every $\Delta' \in S$ to:

\[
;\phi \vdash \tau \\
\Delta', \phi \vdash \tau \quad \text{Weakening}2
\]

Let $\pi_2$ be the parallel 1-extension of $\pi_1$ according to $\pi_\phi$. The new open leaves form a sub-set of $\{;\phi \vdash \tau\}$ and therefore $\pi_2$ corresponds to $\emptyset || \phi$.

□
2 Encoding \( \text{LK}_{\text{DPLL}}(T) \) in \( \text{LK}^p(T) \)

2.1 Preliminaries: System \( \text{LK}^p(T) \)

In this section we introduce (the propositional fragment of) system \( \text{LK}^p(T) \).

**Definition 12 (Formulae, negation)** The formulae of \( \text{LK}^p(T) \) are given by the following grammar:

\[
\text{Formulae } A, B, \ldots \quad ::= \quad l \mid A \wedge B \mid A \vee B \mid A \wedge \neg B \mid A \vee \neg B
\]

where \( l \) ranges over literals.

Let \( \mathcal{P} \) be a set of literals declared to be *positive*, while their negations, required to not be in \( \mathcal{P} \), are declared to be *negative*. Given such a set \( \mathcal{P} \), we define positive formulae and negative formulae as the formulae generated by the following grammars:

**positive formulae**

\[
P, \ldots ::= p \mid A \wedge B \mid A \vee B
\]

where \( p \) ranges over \( \mathcal{P} \).

**negative formulae**

\[
N, \ldots ::= p \bot \mid A \wedge \neg B \mid A \vee \neg B
\]

Negation is recursively extended into an involutive map from formulae to formulae as follows:

\[
\begin{align*}
(A \wedge B)^\bot &= A \vee \neg B \wedge\wedge \\
(A \vee B)^\bot &= A \wedge \neg B \vee\vee
\end{align*}
\]

**Definition 13 (System \( \text{LK}^p(T) \))** The sequent calculus \( \text{LK}^p(T) \) has two kinds of sequents:

\[
\Gamma \vdash_T [P] \quad \text{where } P \text{ is in the focus of the sequent}
\]

\[
\Gamma, p \vdash_T P, p
\]

\[
\Gamma \vdash_T A, \Delta \quad \Gamma, l \vdash_T l
\]

\[
\text{with the condition that } l \text{ appears in } \Gamma.
\]

The general cut:

\[
\Gamma, l \vdash_T \Gamma, l^\bot \Gamma
\]
\[ \Gamma, l_1, \ldots, l_n \vdash^P \Gamma, (l_1 \lor \cdots \lor l_n) \vdash^P \Gamma \vdash^P \]

### 2.2 Simulation

We now encode \( \text{LK}_{DPLL}(T) \) in \( \text{LK}^o(T) \).

The main gap between \( \text{LK}_{DPLL}(T) \) (or even \( \text{DPLL}(T) \)) and a sequent calculus such as \( \text{LK}^o(T) \) is the fact that the structures handled by the former are very flexible (e.g. clauses are multisets of literals), while sequent calculus implements a root-first decomposition of formulae trees.

Clauses in \( \text{DPLL}(T) \) (and in \( \text{LK}_{DPLL}(T) \)) are disjunctions considered modulo associativity and commutativity. The way we encode them as formulae of sequent calculus is as follows: a clause \( C \) will be represented by a formula \( C' \) which is a disjunctive tree whose leaves contain at least all the literals of \( C \) but also other literals that we can consider as garbage.

Of course, one could fear that the presence of garbage parts within \( C' \) degrades the efficiency of proof-search when simulating \( \text{DPLL}(T) \). This garbage comes from the original clauses at the start of the \( \text{DPLL}(T) \) rewriting sequence, which might have been simplified in later steps of \( \text{DPLL}(T) \) but which remain unchanged in sequent calculus. The size of the garbage is therefore smaller than the size of the original problem. We ensure that the inspection, by the proof-search process, of the garbage in \( C' \), takes no more inference steps than the size of the garbage itself (the waste of time is linear in the size of the garbage). In order to ensure this, we use polarities and the focusing properties of \( \text{LK}^o(T) \): the garbage literals in \( C' \) must be negative atoms that are negated in the model/context.

**Definition 14 \((\mathcal{P}-\text{correspondence})\)** Let \( \mathcal{P} \) be a multiset of literals.

- A formula \( C' \) \( \mathcal{P} \)-corresponds to a clause \( C \) (in system \( \text{LK}_{DPLL}(T) \)), where \( C = l_1 \lor \cdots \lor l_p \), if \( C' = l_1' \lor \cdots \lor l_p' \) with \( \{l_j \}_{j=1}^p \subseteq \{l_j' \}_{j=1}^{p'} \) and for any \( l \in \{l_j \}_{j=1}^p \setminus \{l_j' \}_{j=1}^{p'} \).

- A \( \text{LK}^o(T) \) sequent \( \Delta, C_1, \ldots, C_m \vdash^P \) corresponds to a \( \text{LK}_{DPLL}(T) \) sequent \( \Delta; C_1, \ldots, C_m \vdash_T \), if \( C'_i \mathcal{P} \)-corresponds to \( C_i \) and for all \( l \in \mathcal{P}, \Delta \vdash_T l \).

**Lemma 11** If \( C' \mathcal{P} \)-corresponds to \( C \), then \( C' \) also \((\mathcal{P}, l)\)-corresponds to \( C \).

**Proof:** Straightforward.

**Theorem 12** Assume \( S_i \) is a rule of \( \text{LK}_{DPLL}(T) \). For every \( \text{LK}^o(T) \) sequent \( S' \) that corresponds to \( S_i \), there exist a partial proof-tree in \( \text{LK}^o(T) \)

- whose open leaves \( (S_i') \) are such that \( \forall i, S'_i \) corresponds to \( S_i \), and

- whose size is smaller than size \((S') + 4\).

**Proof:** By case analysis:

- Split:

  \[ \Delta, l \vdash^T \Delta, l' \vdash^T \]

  where \( l \in \text{lit}(\phi) \), \( \Delta, l \vdash_T \phi \) and \( \Delta, l \not\vdash_T \phi \)

Assume that \( \Delta, \phi' \vdash^P \) corresponds to \( \Delta; \phi \vdash_T \) (i.e. \( \phi' = C'_1, \ldots, C'_{n} \) and \( \phi = C_1, \ldots, C_n \) with \( C'_i \mathcal{P} \)-corresponding to \( C_i \) for \( i = 1 \ldots n \)).

We build in \( \text{LK}^o(T) \) the following derivation that uses an analytic cut:

\[ \Delta, l \vdash^T \phi' \Delta, l, \phi' \vdash^T \phi \]

and \( \Delta, l \vdash^T \phi' \mathcal{P} \)-corresponds to \( \Delta, l \vdash^T \phi \) and \( \Delta, l \vdash^T \phi' \mathcal{P} \)-corresponds to \( \Delta, l \vdash^T \phi' \).

12
- Assert:

\[ \Delta, l \phi, l \vdash_T \Delta, l \vdash_T \] and \( \Delta, l \not\vdash_T \)

Assume that \( \Delta, \phi', C' \vdash^P_T \) corresponds to \( \Delta; \phi, l \vdash_T \). (i.e. \( \phi' = C'_1, \ldots, C'_n \) and \( \phi = C_1, \ldots, C_n \) with \( C'_i \) \( T \)-corresponding to \( C_i \) for \( i = 1 \ldots n \), and \( C' \) \( T \)-corresponds to \( l \), that is to say \( C' = \bigvee_{i=1}^n C_i \) where \( l = l_{i_0} \) for some \( i_0 \in 1 \ldots n \))

We build in \( \text{LK}^P \) the following derivation:

\[
\begin{array}{c}
T(\Delta, \phi', C', l_i) \\
\Delta, \phi', C' \vdash^P_T [l_i^+] \\
\end{array}
\]

For \( i \neq i_0 \), \( l_i^+ \in \Delta_0 \), so it is positive and we can use an axiom (remember that \( \Delta \models l_i^+ \)).

- Empty:

\[ \Delta; \phi, \bot \vdash_T \]

Assume that \( \Delta, \phi', C' \vdash^P_T \) corresponds to \( \Delta; \phi, \bot \vdash_T \) (i.e. \( C' \) \( T \)-corresponds to \( \bot \), \( \phi' = C'_1, \ldots, C'_n \) and \( \phi = C_1, \ldots, C_n \) with \( C'_i \) \( T \)-corresponding to \( C_i \) for \( i = 1 \ldots n \)).

We build in \( \text{LK}^P \) the following derivation:

\[
\begin{array}{c}
T(\Delta, \phi', C', l_i) \\
\Delta, \phi', C' \vdash^P_T [l_i^+] \\
\end{array}
\]

Again, \( l_i^+ \in \Delta_0 \), so it is positive and we can use an axiom (remember that \( \Delta \models l_i^+ \)).

- Resolve:

\[ \Delta; \phi, C \vdash_T \]

Assume that \( \Delta, \phi', C' \vdash^P_T \) corresponds to \( \Delta; \phi, C' \vdash_T \) (i.e. \( C' \) \( T \)-corresponds to \( l \lor C \), \( \phi' = C'_1, \ldots, C'_n \) and \( \phi = C_1, \ldots, C_n \) with \( C'_i \) \( T \)-corresponding to \( C_i \) for \( i = 1 \ldots n \)). We build in \( \text{LK}^P(T) \) the following derivation

\[ \frac{\Delta; \phi', C' \vdash^P_{T, l^+}}{\Delta; \phi, C' \vdash^P_{T, \text{pol}}} \]

It suffices to notice that \( \Delta, \phi', C' \vdash^P_{\text{pol}} \) corresponds to \( \Delta; \phi, C \vdash_T \).

- Subsume:

\[ \Delta; \phi \vdash_T \]

Assume that \( \Delta, \phi', C' \vdash^P_T \) corresponds to \( \Delta; \phi, C' \vdash_T \) (i.e. \( C' \) \( T \)-corresponds to \( l \lor C \), \( \phi' = C'_1, \ldots, C'_n \) and \( \phi = C_1, \ldots, C_n \) with \( C'_i \) \( T \)-corresponding to \( C_i \) for \( i = 1 \ldots n \)).

- Cut: If we want to simulate \( \text{DPLL}(T) \) with backjump, we need to encode the cut rule of \( \text{LK}_{\text{DPLL}} \).
Assume that $\Delta, \phi' \vdash_{\mathcal{T}}$ corresponds to $\Delta; \phi \vdash_{\mathcal{T}}$ (i.e. $\phi' = C'_1, \ldots, C'_n$ and $\phi = C_1, \ldots, C_n$ with $C'_i$ $\mathcal{P}$-corresponding to $C_i$ for $i = 1 \ldots n$).

We build in $\text{LK}^\emptyset(\mathcal{T})$ the following derivation that uses a general cut:

$$
\Delta, \phi', l_1, \ldots, l_n \vdash_{\mathcal{P}} \Delta, \phi', (l_1^+ \vee \ldots \vee l_n^+) \vdash_{\mathcal{P}} \quad \text{cut}
$$

Clearly, $\Delta, \phi', l_1, \ldots, l_n \vdash_{\mathcal{T}}$ corresponds to $\Delta; \phi, l_1, \ldots, l_n \vdash_{\mathcal{T}}$ and $\Delta, \phi', (l_1^+ \vee \ldots \vee l_n^+) \vdash_{\mathcal{T}}$ corresponds to $\Delta; \phi, C \vdash_{\mathcal{T}}$.

\[\square\]

References
