Extended resolution as Certificates for Propositional Logic

Chantal Keller

Inria – École Polytechnique - LIX

June, 10th 2013
Motivation

Observations:

- many different automatic theorem provers based on different paradigms
- should be able to explain their results: give proof witness

Claim: no need for hundreds of checkers!

- a standard for proof witnesses
- provers should be able to transform their reasoning into such witnesses
Motivation

Observations:

- many different automatic theorem provers based on different paradigms
- should be able to explain their results: give proof witness

Claim: no need for hundreds of checkers!

- a standard for proof witnesses
- provers should be able to transform their reasoning into such witnesses
Which standard?

For propositional logic: extended resolution

- the base of the standard proposed for SAT and SMT
  [Besson et al. – PxTP’11]
- easily extendable (eg. quantifiers [Deharbe et al. – PxTP’11])
- already related to most existing proof systems
- easy to generate from DPLL with backjumping
- easy to check by a certified tool (eg. SMTCoq, zChaff in Isabelle)
Which provers?

For propositional logic:

- DPLL with backjumping
- clausal BDDs

Contribution:

- tableaux provers
- full BDDs
Outline

1. Boolean unsatisfiability and extended resolution
2. Tableaux
3. BDDs
4. Conclusion
The CNF SAT problem

Decide propositional satisfiability of sets of clauses:

- \( x \lor y \)
- \( x \lor \overline{y} \lor z \)
- \( \overline{x} \lor z \)
- \( \overline{z} \)

Proof witnesses

- If satisfiable: assignment of the variables to \( \top \) or \( \bot \) (gives counter-examples)
- If unsatisfiable: proof by resolution of the empty clause (equivalent to provability)

Resolution rule:

\[
\frac{x \lor C \quad \overline{x} \lor D}{C \lor D}
\]
Example

Unsatisfiability of: \( x \lor y \quad x \lor \bar{y} \lor z \quad \bar{x} \lor z \quad \bar{z} \)

\[
\begin{align*}
\frac{x \lor \bar{y} \lor z}{x \lor y} & \quad \bar{z} \\
\frac{x \lor \bar{y}}{x} & \quad \bar{x} \\
\end{align*}
\]

\[\square\]
The general SAT problem

Replace variables with propositional formulas:

\[ (a \Rightarrow b) \land a \land \bar{b} \]

Proof witness for unsatisfiability

- proof by extended resolution of the empty clause
- nodes are resolutions
- leaves are initial clauses or extension rules

Extension of \( y \triangleq y_1 \Rightarrow y_2 \):

\[
\begin{align*}
\bar{y} \lor \bar{y}_1 \lor y_2 \\
y \lor y_1 \\
y \lor \bar{y}_2
\end{align*}
\]
Example

Unsatisfiability of: \((a \Rightarrow b) \land a \land \overline{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- two initial clauses: \(g\) and \(\overline{b}\)
- proof witness:

\[
\begin{array}{c}
\overline{f} \lor \overline{a} \lor b \\
\overline{f} \lor \overline{a} \lor b \\
\overline{a} \lor b \\
b \\
\overline{b}
\end{array}
\]
Outline

1. Boolean unsatisfiability and extended resolution
2. Tableaux
3. BDDs
4. Conclusion
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \land \overline{b}\):

\[
\downarrow
\]

\[(a \Rightarrow b) \land a \land \overline{b}\]

\[
\downarrow
\]

\[b\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \land \bar{b}:\)

\[
\begin{align*}
& (a \Rightarrow b) \land a \\
\downarrow \\
& (a \Rightarrow b) \land a \\
\downarrow \\
& \bar{b}
\end{align*}
\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \land \overline{b}\):

\[\begin{align*}
(a \Rightarrow b) \land a \\
\downarrow \\
\overline{b} \\
\downarrow \\
a \Rightarrow b
\end{align*}\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \land \bar{b}:

\[
\begin{align*}
&\quad (a \Rightarrow b) \land a \\
\Downarrow &\quad b \\
\Downarrow &\quad a \Rightarrow b
\end{align*}
\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \land \bar{b}\):
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \land \neg b:\)

\[
\begin{align*}
(a \Rightarrow b) & \land a \\
\downarrow \\
\neg b & \\
\downarrow \\
a \Rightarrow b & \\
\downarrow \\
a &
\end{align*}
\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \bar{b}:\)

\[
\begin{align*}
(a \Rightarrow b) & \land a \\
\Rightarrow & \quad \bar{b} \\
\Rightarrow & \\
& \quad a \\
\Rightarrow & \\
& \quad a \\
\Rightarrow & \\
& \quad \bar{a} \quad b
\end{align*}
\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \land \overline{b}:

\[
\begin{array}{c}
(a \Rightarrow b) \land a \\
\overline{b} \\
(a \Rightarrow b) \\
a \\
\overline{a} \\
b
\end{array}
\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \land \bar{b}\):

\[\begin{array}{c}
(a \Rightarrow b) \land a \\
\downarrow \\
b \\
\downarrow \\
a \Rightarrow b \\
\downarrow \\
a \\
\downarrow \\
\bar{a} \land b
\end{array}\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \bar{b}\):

\[
\begin{align*}
(a \Rightarrow b) \land a & \\
\quad \downarrow & \\
\bar{b} & \\
\quad \downarrow & \\
\quad \downarrow & \\
a & \\
\quad \downarrow & \\
\bar{a} \quad b
\end{align*}
\]
The method

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \bar{b}:\)
Transformation into a resolution tree

Unsatisfiability of: \((a \implies b) \land a \land \lnot b\)
Transformation into a resolution tree

Unsatisfiability of: 

\[(a \Rightarrow b) \land a \land \bar{b}\]

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
Transformation into a resolution tree

Unsatisfiability of: \((a \implies b) \land a \land \neg b\)

- let \(f \triangleq a \implies b\) and \(g \triangleq f \land a\)
- build the proof step by step:
Transformation into a resolution tree

\[(a \Rightarrow b) \Lambda a \quad \bar{b}\]

- let \( f \triangleq a \Rightarrow b \) and \( g \triangleq f \Lambda a \)
- build the proof step by step:
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \land \lnot b\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{align*}
(f \land a) \land \lnot b \\
\end{align*}
\]
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \overline{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{align*}
\text{Unsatisfiability of: } & (a \Rightarrow b) \land a \quad \overline{b} \\
\text{let } f & \triangleq a \Rightarrow b \text{ and } g \triangleq f \land a \\
\text{build the proof step by step: } & \quad \overline{b}
\end{align*}
\]
Transformation into a resolution tree

Unsatisfiability of:  \((a \Rightarrow b) \land a \quad \overline{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{array}{c}
\overline{g} \lor f \\
g\\
\hline
f \\
g
\end{array}
\]

\(\overline{b}\)
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \bar{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:
  
  \[
  \frac{\bar{g} \lor f}{\frac{g}{f}}
  \]

  \[
  \frac{g}{a}
  \]

  \[
  \frac{\bar{b}}{a \Rightarrow b}
  \]
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \overline{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{align*}
\overline{g} \lor f &
\quad g \\
\hline
f &
\quad \overline{g} \lor a \\
\hline
a &
\quad \overline{b}
\end{align*}
\]
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \land \bar{b}\)

- Let \(f \equiv a \Rightarrow b\) and \(g \equiv f \land a\)
- Build the proof step by step:

\[
\frac{\bar{g} \lor f}{g} \quad \frac{\bar{g} \lor a}{g}
\]

\[
\frac{f}{a} \quad \frac{a}{\bar{b}}
\]
**Transformation into a resolution tree**

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \overline{b}\)

- Let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- Build the proof step by step:

\[
\begin{align*}
&\overline{f} \lor \overline{a} \lor b &\overline{g} \lor f & g \\
&\overline{a} \lor b & f & \overline{g} \lor a & g \\
&\overline{a} \lor b & a & \overline{b}
\end{align*}
\]
Unsatisfiability of: \((a \Rightarrow b) \land a \quad \bar{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{array}{c}
\overline{f} \lor \overline{a} \lor b \\
\hline
\begin{array}{cc}
\bar{g} \lor f & g \\
\hline
f & a \\
\bar{g} \lor a & g \\
\hline
\overline{a} \lor b & a
\end{array}
\end{array}
\]

\(\bar{b}\)
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \bar{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{align*}
\bar{f} \lor \bar{a} \lor b & \quad \bar{g} \lor f \\
\bar{a} \lor b & \quad f \\
\bar{a} \lor b & \quad \bar{g} \lor a \\
\bar{b} & \quad a
\end{align*}
\]
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \bar{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{align*}
\neg f \lor \neg a \lor b & \quad \bar{g} \lor f \quad g \\
\bar{f} \lor a \lor b & \quad a \quad \bar{g} \lor a \quad g \\
\neg a \lor b & \quad a \\
& \quad b \\
& \quad \bar{b}
\end{align*}
\]
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \land \overline{b}\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{align*}
\overline{f} \lor \overline{a} \lor b & \quad \overline{g} \lor f & \quad g \\
\hline
\overline{f} \lor \overline{a} \lor b & \quad f & \quad \overline{g} \lor a \\
\hline
\overline{a} \lor b & \quad a & \quad \overline{b}
\end{align*}
\]
Transformation into a resolution tree

Unsatisfiability of: \((a \Rightarrow b) \land a \quad \neg b\)

- let \(f \triangleq a \Rightarrow b\) and \(g \triangleq f \land a\)
- build the proof step by step:

\[
\begin{align*}
\frown & \quad \neg g \lor f \\
\frown & \quad g \\
\frown & \quad f \\
\frown & \quad \neg a \lor b \\
\frown & \quad \neg a \lor b \\
\frown & \quad b \\
\frown & \quad \neg b \\
\frown & \quad \square \\
\end{align*}
\]

\(\rightarrow\) linear transformation
## Outline

1. Boolean unsatisfiability and extended resolution
2. Tableaux
3. BDDs
4. Conclusion
BDDs

Canonical representation of a Boolean formula:

- choose an order for the variables
- nodes are successive Shannon expansions of the variables
- $F \iff \text{if } a \text{ then } F\{a \leftarrow \top\} \text{ else } F\{a \leftarrow \bot\}$
- merge isomorphic subtrees and eliminate some variables

BDD of $(a \Rightarrow (b \lor c)) \land (a \lor b \lor c)$ with $a > b > c$:

```
    b
   / \c
  /   \
0    1
```

BDD of an unsatisfiable formula: 0
Build the BDD little by little and simplify at the same time

Example of implication:

\[
\begin{align*}
\Gamma_1 & \Rightarrow \Delta_1 & a & \Rightarrow \Delta_1 & \Delta_2 & \Rightarrow \Delta_2 \\
\Gamma_2 & \Rightarrow \Delta_1 & \Delta_1 & \Rightarrow \Delta_1 & \Gamma_1 & \Rightarrow \Delta_1 \\
\Gamma_2 & \Rightarrow \Delta_1 & \Delta_1 & \Rightarrow \Delta_1 & \Gamma_2 & \Rightarrow \Delta_1 \\
0 & \Rightarrow \Delta & 1 & \Rightarrow \Delta & \Gamma & \Rightarrow 0 \\
1 & \Rightarrow \Delta & \Delta & \Rightarrow \Delta & \Gamma & \Rightarrow 1 \\
\end{align*}
\]
Example

Unsatisfiability of \((a \Rightarrow b) \land a \land \overline{b}\):

\[
\begin{align*}
\text{a} & \quad \text{0} \quad \text{1} \\
\text{b} & \quad 0 \quad 1 \\
\text{neg} & \quad \text{1} \quad 0 \\
\end{align*}
\]

\[
\begin{align*}
\text{imp} & \\
\text{and} & \\
\text{neg} & \\
\end{align*}
\]

\[
\begin{align*}
\text{elim} & \\
\text{elim} & 0 \\
\end{align*}
\]
Set of clauses representing a BDD

Shannon expansion at each node:

\[ \begin{align*}
\Gamma &\implies P_\Gamma \\
\Gamma_1 &\implies \neg P_\Gamma \\
\Gamma_2 &\implies \neg P_\Gamma \\
a &\implies P_\Gamma \\
\end{align*} \]

\[ \begin{align*}
\neg P_\Gamma \lor a \lor P_{\Gamma_1} &
\neg P_\Gamma \lor \neg a \lor P_{\Gamma_2} \\
\neg P_\Gamma \lor a \lor \neg P_{\Gamma_1} &
\neg P_\Gamma \lor \neg a \lor \neg P_{\Gamma_2} \\
\end{align*} \]

Leaves:

- \(0_{P_0} \implies \neg P_0\)
- \(1_{P_1} \implies P_1\)
Example

BDD and set of clauses for a variable:

\[
\begin{aligned}
\neg P_a \lor a \lor P_0 \\
 P_a \lor a \lor \neg P_0 \\
\neg P_a \lor \neg a \lor P_1 \\
 P_a \lor \neg a \lor \neg P_1 \\
\neg P_0 \\
P_1
\end{aligned}
\]

For an unsatisfiable formula:

\[0 P_0 \leadsto \neg P_0\]
Transformation into a resolution tree

Idea of the algorithm:

- start with the BDDs of the variables and the corresponding sets of clauses
- at each application of a connective $f \star g$, transform the sets of clauses representing $f$ and $g$ into the set of clauses representing $f \star g$ using extended resolution
- these transformations correspond to pieces of certificates
- put together, they prove the negation of the initial formula, and it only remains to resolve with it
Example

Negation of a variable:

\[
\begin{align*}
\overline{P}_a \lor a \lor P_0 & \quad P_a \lor a \lor \overline{P}_0 \\
\overline{P}_a \lor \overline{a} \lor P_1 & \quad P_a \lor \overline{a} \lor \overline{P}_1 \\
\overline{P}_0 & \quad P_1 \\
\overline{P}'_0 & \quad P'_1
\end{align*}
\]

- pose \( P'_a \triangleq \neg P_a, \quad P'_0 \triangleq \neg P_1, \quad P'_1 \triangleq \neg P_0 \)
- by extension \( P'_a \lor P_a \) and \( \overline{P}'_a \lor \overline{P}_a \) (idem for \( P'_0 \) and \( P'_1 \))
- the 6 new clauses are obtained by resolution
Example

Negation of a variable:

\[
\begin{align*}
\overline{P}_a \lor a \lor P_0 & \quad P_a \lor a \lor \overline{P}_0 \\
\overline{P}_a \lor \overline{a} \lor P_1 & \quad P_a \lor \overline{a} \lor \overline{P}_1 \\
\overline{P}_0 & \quad P_1 \\
\end{align*}
\]

- pose \( \overline{P}_a \triangleq \neg P_a, \overline{P}_0 \triangleq \neg P_0, \overline{P}_1 \triangleq \neg P_1 \)
- by extension \( P_a' \lor P_a \) and \( \overline{P}_a' \lor \overline{P}_a \) (idem for \( P_0' \) and \( P_1' \))
- the 6 new clauses are obtained by resolution

\[\rightarrow\] polynomial transformation
Outline

1. Boolean unsatisfiability and extended resolution
2. Tableaux
3. BDDs
4. Conclusion
Conclusion and perspectives

Extended resolution is theoretically suited for certificates:

- three major paradigms can return such certificates in polynomial time: DPLL with backjumping, tableaux and BDDs
- remind: efficient certified checking

Validation

- instrument existing provers with these algorithms
- evaluate the efficiency

Perspectives

- cope with enhancements implemented by these provers
- extensions to more expressive logics and other provers