What is the SMT problem?

Satisfiability Modulo Theories (SMT)

The SMT problem
- Modern efficient SAT solvers
- CDCL(T)
- Examples of decision procedures: equality (CC) and difference logic (NCCD)
- Quantifiers

Checking satisfiability of formulas in a decidable combination of first-order theories (e.g. arithmetic, uninterpreted functions, etc.)
SMT Solving

**Input:** a (quantifier-free) **first-order** formula \( F \)

**Output:** the status of \( F \) (**sat** or **unsat**), and optionally a **model** (when sat) or a **proof** (when unsat)

---

**Basic SMT Solving**

Given a quantifier-free formula \( F \)

\[
x + y \geq 0 \land (x = z \Rightarrow y + z = -1) \land z > 3t
\]

satisfiable ?

1. Convert \( F \) to CNF form
2. Replace every literal by a Boolean variable
3. Ask a SAT solver for a Boolean model \( M \)
4. Convert back \( M \) and call a decision procedure for the union of theories

if \( M \) is satisfiable modulo theories, then so is \( F \)
otherwise, add \( \neg M \) to \( F \) and go to step 2

---

**Basic SMT Solving : Example**

\[
x + y \geq 0 \land (x = z \Rightarrow y + z = -1) \land z > 3t
\]

1. CNF conversion
2. Replace arithmetic constraints by Boolean variables
3. Ask the SAT solver for a model
4. Convert the model back to arithmetic
5. Check its consistency with the appropriate decision procedure for arithmetic
6. Add \( \neg M \) to \( F \) and go back to step 2

---

**Basic SMT Solving : Example**

\[
x + y \geq 0 \land (x = z \Rightarrow y + z = -1) \land z > 3t
\]
1. CNF conversion
2. Replace arithmetic constraints by Boolean variables
3. Ask the SAT solver for a model
4. Convert the model back to arithmetic
5. Check its consistency with the appropriate decision procedure for arithmetic
6. Add $\neg M$ to $F$ and go back to step 2

$x + y \geq 0 \land (x \neq z \lor y + z = -1) \land z > 3t$

$p_1 \land (p_2 \lor p_3) \land p_4$

1. CNF conversion
2. Replace arithmetic constraints by Boolean variables
3. Ask the SAT solver for a model

$p_1 \land (p_2 \lor p_3) \land p_4$
Basic SMT Solving: Example

1. CNF conversion
2. Replace arithmetic constraints by Boolean variables
3. Ask the SAT solver for a model
4. Convert the model back to arithmetic
5. Check its consistency with the appropriate decision procedure for arithmetic
6. Add $\neg M$ to $F$ and go back to step 2

$M = \{p_1 = \text{true}, p_2 = \text{false}, p_3 = \text{true}, p_4 = \text{true}\}$

$M = \{x + y \geq 0, x = z, y + z = -1, z > 3t\}$
Basic SMT Solving: Example

1. CNF conversion
2. Replace arithmetic constraints by Boolean variables
3. Ask the SAT solver for a model
4. Convert the model back to arithmetic
5. Check its consistency with the appropriate decision procedure for arithmetic

$x + y \geq 0 \land (x \neq z \lor y + z = -1) \land z > 3t \land 
\neg(x + y \geq 0 \land x = z \land y + z = -1 \land z > 3t)$

1. CNF conversion
2. Replace arithmetic constraints by Boolean variables
3. Ask the SAT solver for a model
4. Convert the model back to arithmetic
5. Check its consistency with the appropriate decision procedure for arithmetic
6. Add $\neg M$ to $F$ and go back to step 2

Main Issues

- Size of formulas
- Complex Boolean structure
- Combination of theories
- Efficient decision procedures
- (Quantifiers)
The Satisfiability Modulo Theory Library
http://www.smtlib.org/

International initiative:
▶ Rigorous description of background theories
▶ Common input and output languages for SMT solvers
▶ Large benchmarks

SMT: Building Blocks

Three main blocks:
▶ SAT Solver
▶ Decision Procedures
▶ Combining Decision Procedures framework (CDP)

The SMT Revolution
70’s: Stanford Pascal Verifier (Nelson-Oppen combination)
1984: Shostak algorithm
1992: Simplify
1995: SVC
2001: ICS
2002: CVC, haRVey
2004: CVC Lite
2005: Barcelogic, MathSAT
2005: Yices
2006: CVC3, Alt-Ergo
2007: Z3, MathSAT4
2008: Boolector, OpenSMT, Beaver,Yices2
2009: STP, VeriT
2010: MathSAT5, SONOLAR
2011: STP2, SMTInterpol
2012: CVC4

Modern SAT solvers
Propositional Logic: Notations

- \( p, q, r, s \) are propositional variables or atoms
- \( l \) is a literal \((p \text{ or } \neg p)\)
- \( \neg l = \begin{cases} 
\neg p & \text{if } l = p \\
 p & \text{if } l = \neg p 
\end{cases} \)

A disjunction of literals \( l_1 \lor \ldots \lor l_n \) is a clause

The empty clause is written \( \bot \)

A conjunction of clauses is a CNF

To improve readability, we sometime
- denote atoms by natural numbers and negation by overlining
- write CNF as sets of clauses

e.g. \((\neg l_1 \lor l_2 \lor \neg l_3) \land (l_4 \lor \neg l_2)\) is simply written \(\{\neg 1 \lor 2 \lor 3, 4 \lor 2\}\)

Propositional Logic: Assignments

- An assignment \( M \) is a set of literals such that if \( l \in M \) then \( \neg l \notin M \)
- A literal \( l \) is true in \( M \) if \( l \in M \), and false if \( \neg l \in M \)
- A literal \( l \) is defined in \( M \) if it is either true or false in \( M \)
- A clause is true in \( M \) if at least one of its literals is true in \( M \), it is false if all its literals are false in \( M \), it is undefined otherwise
- The empty clause \( \bot \) is not satisfiable
- A clause \( C \lor l \) is a unit clause in \( M \) if \( C \) is false in \( M \) and \( l \) is undefined in \( M \)

Propositional Logic: Satisfiability

- A CNF \( F \) is satisfied by \( M \) (or \( M \) is a model of \( F \)), written \( M \models F \), if all clauses of \( F \) are true in \( M \)
- If \( F \) has no model then it is unsatisfiable
- \( F' \) is entailed by \( F \), written \( F \models F' \), if \( F' \) is true in all models of \( F \)
- \( F \) and \( F' \) are equivalent when \( F \models F' \) and \( F' \models F \)
- \( F \) and \( F' \) are equisatisfiable when
  - \( F \) is satisfiable if and only if \( F' \) is satisfiable
  - \( F \) is valid if and only if \( \neg F \) is unsatisfiable
Resolution

- **Proof-finder** procedure
- Works by **saturation** until the empty clause is derived

Exhaustive resolution is not practical:

- exponential amount of memory

The state of the procedure is represented by a variable (imperative style) $F$ containing a set of clauses (CNF)

Resolution : State of the Procedure

Resolution : Algorithm

\[
\begin{align*}
\text{RESOLVE} & \quad C \lor l \in F \quad D \lor \neg l \in F \quad C \lor D \notin F \\
& \quad F := F \cup \{C \lor D\} \\
\text{EMPTY} & \quad l \in F \quad \neg l \in F \\
& \quad F := F \cup \bot \\
\text{TAUTO} & \quad F = F' \cup \{C \lor l \lor \neg l\} \\
& \quad F := F' \\
\text{SUBSUME} & \quad F = F' \cup \{C \lor D\} \\
& \quad C \in F' \\
\text{FAIL} & \quad \bot \in F \\
& \quad \text{return UNSAT}
\end{align*}
\]

Resolution : Example

\[
F = \{\bar{1} \lor \bar{2} \lor 3, \bar{1} \lor 2, 1 \lor 3, 3\}
\]
Resolution: Example

\[ \begin{align*}
\text{Resolve} & \quad 1 \lor 2 \lor 3 \in F \quad 1 \lor 3 \in F \\
\text{Resolution} & \quad F := F \cup \{2 \lor 3\} \\
F & = \{1 \lor 2 \lor 3, 1 \lor 2, 1 \lor 3, 3, 2 \lor 3\}
\end{align*} \]

Resolution: Example

\[ \begin{align*}
\text{Resolve} & \quad 1 \lor 2 \lor 3 \in F \quad 1 \lor 3 \in F \\
\text{Resolution} & \quad F := F \cup \{2 \lor 3\} \\
F & = \{1 \lor 2 \lor 3, 1 \lor 2, 1 \lor 3, 3, 2 \lor 3\}
\end{align*} \]

Resolution: Example

\[ \begin{align*}
\text{Subsume} & \quad F = F' \cup \{1 \lor 2 \lor 3\} \\
\text{Subsume} & \quad 2 \lor 3 \in F' \\
\text{Subsume} & \quad F := F'
\end{align*} \]

Resolution: Example

\[ \begin{align*}
\text{Subsume} & \quad F = F' \cup \{1 \lor 2 \lor 3\} \\
\text{Subsume} & \quad 2 \lor 3 \in F' \\
F & = \{1 \lor 2, 1 \lor 3, 3, 2 \lor 3\}
\end{align*} \]
Resolution : Example

\text{Resolve } \bar{1} \lor 2 \in F, \ 1 \lor 3 \in F

\begin{align*}
F := F \cup \{2 \lor 3\}
\end{align*}

\begin{align*}
F &= \{\bar{1} \lor 2, \ 1 \lor 3, \ \bar{3}, \ 2 \lor 3\}
\end{align*}

\text{Resolve } \bar{1} \lor 2 \in F, \ 1 \lor 3 \in F

\begin{align*}
F := F \cup \{2 \lor 3\}
\end{align*}

\begin{align*}
F &= \{\bar{1} \lor 2, \ 1 \lor 3, \ \bar{3}, \ 2 \lor 3, \ 2 \lor 3\}
\end{align*}

Resolution : Example

\text{Resolve } \bar{2} \lor 3 \in F, \ 2 \lor 3 \in F

\begin{align*}
F := F \cup \{3\}
\end{align*}

\begin{align*}
F &= \{\bar{1} \lor 2, \ 1 \lor 3, \ \bar{3}, \ 2 \lor 3, \ 2 \lor 3\}
\end{align*}

\text{Resolve } \bar{2} \lor 3 \in F, \ 2 \lor 3 \in F

\begin{align*}
F := F \cup \{3\}
\end{align*}

\begin{align*}
F &= \{\bar{1} \lor 2, \ 1 \lor 3, \ \bar{3}, \ 2 \lor 3, \ 2 \lor 3, \ 3\}
\end{align*}
\[
\begin{align*}
\text{Empty} & \quad 3 \in F \quad \bar{3} \in F \\
& \quad F := F \cup \{\bot\}
\end{align*}
\]

\[F = \{\bar{1} \lor 2, 1 \lor 3, \bar{3}, \bar{2} \lor 3, 2 \lor 3, \bot\}\]

Resolution : Example

DPLL is a model-finder procedure that builds incrementally a model \( M \) for a CNF formula \( F \) by

- **deducing** the truth value of a literal \( l \) from \( M \) and \( F \) by Boolean Constraint Propagations (BCP)
  
  \[\text{If } C \lor l \in F \text{ and } M \models \neg C \text{ then } l \text{ must be true}\]

- **guessing** the truth value of an unassigned literal
  
  \[\text{If } M \cup \{l\} \text{ leads to a model for which } F \text{ is unsatisfiable then backtrack and try } M \cup \{\neg l\}\]

\[F = \{\bar{1} \lor 2, 1 \lor 3, \bar{3}, \bar{2} \lor 3, 2 \lor 3, \bot\}\]
The state of the procedure is represented by

- a variable $F$ containing a set of clauses (CNF)
- a variable $M$ containing a list of literals

### DPLL: Algorithm

**Success**

\[ M \models F \]

\[
\text{return SAT}
\]

**Unit**

\[ C \lor l \in F \]

\[ M \models \neg C \]

\[ l \text{ is undefined in } M \]

\[ M := l:: M \]

**Decide**

\[ l \text{ is undefined in } M \]

\[ l \text{ (or } \neg l) \in F \]

\[ M := l^\oplus:: M \]

**Backtrack**

\[ C \in F \]

\[ M \models \neg C \]

\[ M = M_1:: l^\oplus:: M_2 \]

\[ M_1 \text{ contains no decision literals} \]

\[ M := \neg l:: M_2 \]

**Fail**

\[ C \in F \]

\[ M \models \neg C \]

\[ M \text{ contains no decision literals} \]

\[
\text{return SAT}
\]

### DPLL: Example

\[ M = [] \]

\[ F = \{ \overline{1} \lor 2, \overline{3} \lor 4, \overline{5} \lor 6, 6 \lor \overline{5} \lor \overline{2}, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \} \]

**Decide**

\[ 1 \text{ is undefined in } M \]

\[ \overline{1} \in F \]

\[ M := 1^\oplus:: M \]

\[ M = [] \]

\[ F = \{ \overline{1} \lor 2, \overline{3} \lor 4, \overline{5} \lor 6, 6 \lor \overline{5} \lor \overline{2}, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \} \]
DPLL : Example

**Decide** 

1 is undefined in \( M \)  
\( \bar{1} \in F \) 

\[
 M := 1^@ :: M \\
 M = [1^@] \\
 F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}
\]

---

**Unit** 

\( \bar{1} \lor 2 \in F \)  
\( M \models 1 \)  
2 is undefined in \( M \) 

\[
 M := 2 :: M \\
 M = [1^@] \\
 F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}
\]

---

**Decide** 

3 is undefined in \( M \)  
\( \bar{3} \in F \) 

\[
 M := 3^@ :: M \\
 M = [2; 1^@] \\
 F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}
\]

---

**Unit** 

\( \bar{1} \lor 2 \in F \)  
\( M \models 1 \)  
2 is undefined in \( M \) 

\[
 M := 2 :: M \\
 M = [2; 1^@] \\
 F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}
\]
**DPLL: Example**

Decide $3$ is undefined in $M$ \[ \bar{3} \in F \]

$M := 3 :: M$ \[ M = [3; 2; 1] \]

$F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}$

---

**DPLL: Example**

Unit $\bar{3} \lor 4 \in F$ \[ M \models 3 \]

$M := 4 :: M$ \[ M = [3; 2; 1] \]

$F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}$

---

**DPLL: Example**

Unit $\bar{3} \lor 4 \in F$ \[ M \models 3 \]

$M := 4 :: M$ \[ M = [4; 3; 2; 1] \]

$F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}$

---

**DPLL: Example**

Decide $5$ is undefined in $M$ \[ \bar{5} \in F \]

$M := 5 :: M$ \[ M = [4; 3; 2; 1] \]

$F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}$
**DPLL Example**

**Decide**

\[
\begin{align*}
\text{5 is undefined in } & M \quad \bar{5} \in F \\
M := & 5 \oplus :: M
\end{align*}
\]

\[
M = [5^{\oplus}; 4; 3^{\oplus}; 2; 1^{\oplus}]
\]

\[
F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor 6, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}
\]

**Unit**

\[
\begin{align*}
\bar{5} \lor \bar{6} \in F & \quad M \models 5 \quad \bar{6} \text{ is undefined in } M \\
M := & 6 :: M
\end{align*}
\]

\[
M = [6; 5^{\oplus}; 4; 3^{\oplus}; 2; 1^{\oplus}]
\]

\[
F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}
\]

**Backtrack**

\[
\begin{align*}
6 \lor \bar{5} \lor \bar{2} \in F & \quad M = [6] :: 5^{\oplus} :: [4; 3^{\oplus}; 2; 1^{\oplus}] \\
M := & 5 :: [4; 3^{\oplus}; 2; 1^{\oplus}]
\end{align*}
\]

\[
M = [6; 5^{\oplus}; 4; 3^{\oplus}; 2; 1^{\oplus}]
\]

\[
F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}
\]
DPLL : Example

\[ 6 \lor 5 \lor 2 \in F \]
\[ M \models 6 \land 5 \land 2 \]
\[ M = \{6\} :: 5 \]
\[ M := \{6\} :: [4; 3; 2; 1] \]

\[ M = [5; 4] :: \]
\[ F = \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\} \]

DPLL : Example

\[ 5 \lor 7 \in F \]
\[ M \models \overline{5} \]
\[ 7 \text{ is undefined in } M \]
\[ M := 7 :: M \]

\[ M = \{5; 4; 3; 2; 1\} \]
\[ F = \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\} \]

DPLL : Example

\[ 5 \lor 7 \in F \]
\[ M \models \overline{5} \]
\[ 5 \lor 7 \lor 2 \in F \]
\[ M \models \overline{5} \land 7 \land 2 \]
\[ M := \overline{5} :: M \]

\[ M = \{7; 5; 4\} :: 3 \]
\[ M := \overline{7} :: 3 \]
\[ F = \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\} \]

DPLL : Example

\[ 5 \lor 7 \in F \]
\[ M \models \overline{5} \]
\[ 5 \lor 7 \lor 2 \in F \]
\[ M \models \overline{5} \land 7 \land 2 \]
\[ M := \overline{5} :: M \]

\[ M = \{7; 5; 4; 3; 2; 1\} \]
\[ F = \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\} \]
DPLL : Example

Backtrack

\[ 5 \lor \overline{7} \lor \overline{2} \in F \]

\[
M = 5 \land 7 \land 2 \quad M = [7; 5; 4] :: [2; 1^{\circ}] \\
M := 3 :: [2; 1^{\circ}] \\
M = [3; 2; 1^{\circ}] \\
F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor \overline{5} \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \}
\]

Decide

\[ 5 \text{ is undefined in } M \quad \overline{5} \in F \]

\[
M := 5^{\circ} :: M \\
M = [3; 2; 1^{\circ}] \\
F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor \overline{5} \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \}
\]

Decide

\[ 5 \text{ is undefined in } M \quad \overline{5} \in F \]

\[
M := 5^{\circ} :: M \\
M = [3; 2; 1^{\circ}] \\
F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor \overline{5} \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \}
\]

Unit

\[ \overline{5} \lor \overline{6} \in F \quad M \models 5 \quad \overline{6} \text{ is undefined in } M \]

\[
M := 6^{\circ} :: M \\
M = [5^{\circ}; \overline{3}; 2; 1^{\circ}] \\
F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor \overline{5} \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \}
\]
DPLL: Example

**Unit**

\[
5 \lor 6 \in F \\
M \models 5 \\
6 \text{ is undefined in } M
\]

\[
M := 6 :: M
\]

\[
M = [6; 5^{\oplus}; 3; 2; 1^{\oplus}]
\]

\[
F = \{\overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor 7 \lor 2\}
\]

---

**Backtrack**

\[
6 \lor 5 \lor 2 \in F \\
M \models 6 \land 5 \land 2 \\
M = [6] :: 5^{\oplus} :: [3; 2; 1^{\oplus}]
\]

\[
M := 5 :: [3; 2; 1^{\oplus}]
\]

\[
M = [6; 5^{\oplus}; 3; 2; 1^{\oplus}]
\]

\[
F = \{\overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\}
\]

---

**Unit**

\[
5 \lor 7 \in F \\
M \models 5 \\
7 \text{ is undefined in } M
\]

\[
M := 7 :: M
\]

\[
M = [5; \overline{3}; 2; 1^{\oplus}]
\]

\[
F = \{\overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor 7 \lor 2\}
\]

---
DPLL : Example

\[ \begin{align*}
\text{UNIT} & \quad 5 \lor 7 \in F \quad M \models \overline{5} \quad 7 \text{ is undefined in } M \\
& \quad M := 7 :: M
\end{align*} \]

\[ M = [7; 5; \overline{3}; 2; 1] \]

\[ F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \} \]

DPLL : Example

\[ \begin{align*}
\text{BACKTRACK} & \quad 5 \lor \overline{7} \lor \overline{2} \in F \\
& \quad M = [7; 5; \overline{3}; 2] :: 1@ :: [] \\
& \quad M := \overline{1} :: []
\end{align*} \]

\[ M = [7; 5; \overline{3}; 2] \]

\[ F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \} \]

DPLL : Example

\[ \begin{align*}
\text{DECIDE} & \quad \overline{3} \text{ is undefined in } M \\
& \quad \overline{3} \in F \\
& \quad M := \overline{3}@ :: M
\end{align*} \]

\[ M = [\overline{1}] \]

\[ F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \} \]
DPLL: Example

Decide \( \bar{3} \) is undefined in \( M \) \( \bar{3} \in F \)

\[
M := \bar{3}^\triangledown :: M
\]

\[
M = [\bar{3}^\triangledown; \bar{1}]
\]

\[
F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}
\]

---

Decide \( \bar{5} \) is undefined in \( M \) \( \bar{5} \in F \)

\[
M := \bar{5}^\triangledown :: M
\]

\[
M = [\bar{5}^\triangledown; \bar{1}]
\]

\[
F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}
\]

---

Decide \( \bar{5} \) is undefined in \( M \) \( \bar{5} \in F \)

\[
M := \bar{5}^\triangledown :: M
\]

\[
M = [\bar{5}^\triangledown; \bar{1}]
\]

\[
F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}
\]

---

Decide \( \bar{5} \) is undefined in \( M \) \( \bar{5} \in F \)

\[
M := \bar{5}^\triangledown :: M
\]

\[
M = [\bar{5}^\triangledown; \bar{1}]
\]

\[
F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}
\]
DPLL : Example

Unit

5 ∨ 7 ∈ F  \quad M |= 5 \quad 7 is undefined in M  

\[ M := 7 :: M \]

\[ M = [7; \bar{5}@; \bar{3}@; \bar{1}] \]

\[ F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor 6, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor \bar{7} \lor \bar{2}\} \]

Success

\[ M |= F \]

\text{return SAT}

\[ M = [\bar{2}; 7; \bar{5}@; \bar{3}@; \bar{1}] \]

\[ F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor 6, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor \bar{7} \lor \bar{2}\} \]
Backjumping

The clause \( 6 \lor \overline{5} \lor \overline{2} \) is false in \([\overline{6}; 5@; 4; 3@; 2; 1@]\)

It is also false in \([\overline{6}; 5@; ; 2; 1@]\)

Instead of backtracking to \( M = [\overline{5}; 4; 3@; 2; 1@] \), we would prefer to backjump directly to \( M = [\overline{5}; 2; 1@] \)

Conflict are reflected by backjump clauses

For instance, we have the following backjump clauses in the previous example:

\[
F \models \overline{1} \lor \overline{5} \\
F \models \overline{2} \lor \overline{5}
\]

Given a backjump clause \( C \lor l \), backjumping can undo several decisions at once: it goes back to the assignment \( M \) where \( M \models \neg C \) and add \( l \) to \( M \)

DPLL + Backjumping

We just replace Backtrack by

\[
\frac{\begin{align*}
C \in F & \quad M \models \neg C & \quad M = M_1 :: l^{@} :: M_2 \\
F \models C' \lor l' & \quad M_2 \models \neg C' \\
l' \text{ is undefined in } M_2 & \quad l' \text{ (or } \neg l') \in F
\end{align*}}{\text{BACKJUMP}} \quad M := l' :: M_2
\]

where \( C' \lor l' \) is a backjump clause

Backjumping : Example

\[ F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor 6, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor 7 \lor \overline{2} \} \]
Backjumping : Example

**Decide**

1 is undefined in $M$

$M := 1 \oplus :: M$

$M = []$

$F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}$

---

**Unit**

$\bar{1} \lor 2 \in F$

$M |= 1$

2 is undefined in $M$

$M := 2 :: M$

$M = [1]$ 

$F = \{ \bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor \bar{5} \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2} \}$
**Backjumping : Example**

**Decide**

3 is undefined in $M \bar{3} \in F$

$M := 3^{\alpha} :: M$

$F = \{\bar{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}$

$M = [3^{\alpha}; 2; 1^{\alpha}]$

$F = \{\bar{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}$

---

**Backjumping : Example**

**Unit**

$\bar{3} \lor 4 \in F\quad M \models 3\quad 4$ is undefined in $M$

$M := 4 :: M$

$F = \{\bar{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}$

$M = [4; 3^{\alpha}; 2; 1^{\alpha}]$

$F = \{\bar{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}$
**Backjumping : Example**

**Decide** 5 is undefined in $M$

$\bar{5} \in F$

$M := 5^i :: M$

$M = [4; 3^\@; 2; 1^\@]$

$F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}$

**Backjumping : Example**

**Unit** $\bar{5} \lor \bar{6} \in F$

$M \models 5 \quad \bar{6}$ is undefined in $M$

$M := 6 :: M$

$M = [5^\@; 4; 3^\@; 2; 1^\@]$

$F = \{\bar{1} \lor 2, \bar{3} \lor 4, 5 \lor \bar{6}, 6 \lor 5 \lor \bar{2}, 5 \lor 7, 5 \lor 7 \lor \bar{2}\}$
Backjumping : Example

**Backjump**

\[ 6 \lor 5 \lor 2 \in F \quad M \models 6 \land 5 \land 2 \]
\[ M = [6; 5^\alpha; 4] :: 3^\alpha :: [2; 1^\alpha] \quad F \models 2 \lor 5 \]
\[ [2; 1^\alpha] \models 2 \quad \bar{5} \text{ is undefined in } [2; 1^\alpha] \]
\[ M := \bar{5} :: [2; 1^\alpha] \]

\[ M = [\bar{6}; 5^\alpha; 4; 3^\alpha; 2; 1^\alpha] \]
\[ F = \{ \bar{1} \lor 2, 3 \lor 4, 5 \lor \bar{6}, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \bar{7} \lor 2 \} \]

**Backjump**

\[ 6 \lor 5 \lor 2 \in F \quad M \models 6 \land 5 \land 2 \]
\[ M = [\bar{6}; 5^\alpha; 4] :: 3^\alpha :: [2; 1^\alpha] \quad F \models 2 \lor 5 \]
\[ [2; 1^\alpha] \models 2 \quad \bar{5} \text{ is undefined in } [2; 1^\alpha] \]
\[ M := \bar{5} :: [2; 1^\alpha] \]

\[ M = [\bar{5}; 2; 1^\alpha] \]
\[ F = \{ \bar{1} \lor 2, 3 \lor 4, 5 \lor \bar{6}, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \bar{7} \lor 2 \} \]

**Backjumping : Example**

**Unit**

\[ 5 \lor 7 \in F \quad M \models \bar{5} \quad 7 \text{ is undefined in } M \]
\[ M := 7 :: M \]

\[ M = [\bar{5}; 2; 1^\alpha] \]
\[ F = \{ \bar{1} \lor 2, 3 \lor 4, 5 \lor \bar{6}, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \bar{7} \lor 2 \} \]

**Unit**

\[ 5 \lor 7 \in F \quad M \models \bar{5} \quad 7 \text{ is undefined in } M \]
\[ M := 7 :: M \]

\[ M = [\bar{7}; 5; 2; 1^\alpha] \]
\[ F = \{ \bar{1} \lor 2, 3 \lor 4, 5 \lor \bar{6}, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \bar{7} \lor 2 \} \]
Backjumping : Example

\[
5 \lor \overline{7} \lor \overline{2} \in F
\]
\[
M \models 5 \land 7 \land 2 \quad M = [7; 5; 2] :: 1^\oplus :: []
\]
\[
F \models \overline{1} \quad [] \models true \quad \overline{1} \text{ is undefined in } []
\]
\[
M := \overline{1} :: []
\]
\[
M = [\overline{1}]
\]
\[
F = \{\overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\}
\]

Backjumping : Example

Decide \[\overline{3} \text{ is undefined in } M\] \[\overline{3} \in F\]
\[
M := \overline{3}^\oplus :: M
\]
\[
M = [\overline{3}^\oplus; \overline{1}]
\]
\[
F = \{\overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\}
\]
Backjumping : Example

**Decide** \( \overline{5} \) is undefined in \( M \)
\( M := \overline{5} :: M \)

\[
M = [\overline{3}^0; 1]
F = \{1 \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\}
\]

---

Backjumping : Example

**Unit** \( 5 \lor 7 \in F \)
\( M \models \overline{5} \)
\( 7 \) is undefined in \( M \)
\( M := 7 :: M \)

\[
M = [\overline{5}^0; \overline{3}^0; 1]
F = \{1 \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\}
\]
Backjumping : Example

\[ 5 \lor \overline{7} \lor \overline{2} \in F \quad M \models 5 \land \overline{7} \lor \overline{2} \text{ is undefined in } M \]
\[ M := 2 :: M \]

\[ M = [7; 5 \hat{v}; 3 \hat{v}; 1] \]
\[ F = \{ \overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \} \]

Backjumping : Example

\[ 5 \lor \overline{7} \lor \overline{2} \in F \quad M \models 5 \land \overline{7} \lor \overline{2} \text{ is undefined in } M \]
\[ M := 2 :: M \]

\[ M = [2; 7; 5 \hat{v}; 3 \hat{v}; 1] \]
\[ F = \{ \overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2} \} \]

CDCL

Conflict-Driven Clause Learning SAT solvers (CDCL) add backjump clauses to \( M \) as learned clauses (or lemmas) to prevent future similar conflicts.

\[ \text{LEARN } F \models C \quad \text{each atom of } C \text{ occurs in } F \text{ or } M \]
\[ F := F \cup \{ C \} \]

Lemmas can also be removed from \( M \)

\[ \text{FORGET } F = F' \lor C \quad F' \models C \]
\[ F := F' \]
How to Find Backjump Clauses?

1. Build an implication graph that captures the way propagation literals have been derived from decision literals
2. Use the implication graph to explain a conflict (by a specific cutting technique) and extract backjump clauses

Implication Graph

An implication graph $G$ is a DAG that can be built during the run of DPLL as follows:

1. Create a node for each decision literal
2. For each clause $l_1 \lor \ldots \lor l_n \lor l$ such that $\neg l_1, \ldots, \neg l_n$ are nodes in $G$, add a node for $l$ (if not already present in the graph), and add edges $\neg l_i \rightarrow l$, for $1 \leq i \leq n$ (if not already present)

Implication Graph : Example

(Partial) implication graph for the following state of DPLL

$F = \{\neg 9 \lor \neg 6 \lor 7 \lor 8 \lor 7 \lor 5, \neg 6 \lor 8 \lor 4, \neg 4 \lor 5 \lor 2, 5 \lor 7 \lor 3, 1 \lor 2 \lor 3\}$

$M = [\neg 3; 2; \neg 1; 4; \neg 5; \neg 8; 9@; \ldots; \neg 7; \ldots; 6; \ldots]$
Cutting the Implication Graph: Example

\[ F = \{\neg 9 \lor \neg 6 \lor 7 \lor \neg 8, 8 \lor 7 \lor \neg 5, \neg 6 \lor 8 \lor 4, \neg 4 \lor \neg 1, \neg 4 \lor 5 \lor 2, 5 \lor 7 \lor 3, 1 \lor 2 \lor 3\} \]

\[ M = [\neg 3; 2; \neg 1; 4; 5; 8; 9^@; \ldots; 7; \ldots; 6; \ldots] \]
In the first example, **Backjump** is applied for the first time when

\[ F = \{ \neg 1 \lor 2, \neg 3 \lor 4, \neg 5 \lor \neg 6, 6 \lor \neg 5 \lor \neg 2, 5 \lor 7, 5 \lor \neg 7 \lor \neg 2 \} \]

\[ M = [\neg 6; 5 \circ; 4; 3 \circ; 2; 1 \circ] \]

When **Backjump** is applied for the second time, we have

\[ F = \{ \neg 1 \lor 2, \neg 3 \lor 4, \neg 5 \lor \neg 6, 6 \lor \neg 5 \lor \neg 2, 5 \lor 7, 5 \lor \neg 7 \lor \neg 2 \} \]

\[ M = [7; \neg 5; 2; 1 \circ] \]
When **Backjump** is applied for the second time, we have

\[ F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor 6, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor 7 \lor \overline{2} \} \]

\[ M = [7; 5; 2; 1^@] \]

---

**Backward Conflict Resolution**

Backjump clauses can also be obtained by successive application of **resolution steps**

Starting from the **conflict clause**, the (negation of) propagation literals are resolved away in the **reverse order** with the respective clauses that caused their propagations

We stop when the **resolvent** contains **only one** literal in the current decision level

\[ F = \{ \overline{9} \lor 6 \lor 7 \lor 8, 8 \lor 7 \lor 5, 6 \lor 8 \lor 4, 4 \lor \overline{1}, 4 \lor 5 \lor 2, 5 \lor 7 \lor 3, 1 \lor \overline{2} \lor 3 \} \]

\[ M = [3; 2; \overline{1}; 4; \overline{5}; \overline{8}; 9^@; \ldots; 7; \ldots; 6; \ldots] \]

\[ R = 1 \lor \overline{2} \lor 3 \]
Backward Conflict Resolution: Example

\[ F = \{9 \lor 6 \lor 7 \lor 8, 8 \lor 7 \lor 5, 6 \lor 8 \lor 4, 4 \lor 1, 4 \lor 5 \lor 2, 5 \lor 7 \lor 3, 1 \lor 2 \lor 3\} \]
\[ M = [3; 2; 1; 4; 5; 8; 9^{\ominus}; \ldots; 7; \ldots; 6; \ldots] \]

\[
\text{Resolve} \quad R = \begin{array}{c}
1 \lor \bar{2} \lor 3 \\
5 \lor 7 \lor \bar{3}
\end{array} \in F
\]

\[
R := 5 \lor 7 \lor 1 \lor 2
\]

\[ R = 1 \lor \bar{2} \lor 3 \]

R = 5 \lor 7 \lor 1 \lor 2
Backward Conflict Resolution: Example

\[ F = \{ 9 \lor 6 \lor 7 \lor 8, 8 \lor 7 \lor 5, 6 \lor 8 \lor 4, 4 \lor 1, 4 \lor 5 \lor 2, 5 \lor 7 \lor 3, 1 \lor 2 \lor 3 \} \]

\[ M = [3; 2; 1; 4; 5; 8; 9; \ldots; 7; \ldots; 6; \ldots] \]

\[ R = \overline{4} \lor 5 \lor 7 \lor 1 \]

\[ R = 5 \lor 7 \lor \overline{4} \quad \overline{4} \lor \overline{1} \in F \]

\[ R := 5 \lor 7 \lor 4 \]

\[ R = 5 \lor 7 \lor 4 \]

\[ F = \{ 9 \lor 6 \lor 7 \lor 8, 8 \lor 7 \lor 5, 6 \lor 8 \lor 4, 4 \lor 1, 4 \lor 5 \lor 2, 5 \lor 7 \lor 3, 1 \lor 2 \lor 3 \} \]

\[ M = [3; 2; 1; 4; 5; 8; 9; \ldots; 7; \ldots; 6; \ldots] \]

\[ R = \overline{4} \lor 5 \lor 7 \lor 1 \quad \overline{4} \lor \overline{1} \in F \]

\[ R := 5 \lor 7 \lor 4 \]

\[ R = \overline{6} \lor 8 \lor 4 \in F \]

\[ R := 6 \lor 8 \lor 7 \lor 5 \]

\[ R = 6 \lor 8 \lor 7 \lor 5 \]
Backward Conflict Resolution: Example

\[ F = \{ \neg 9 \lor \neg 6 \lor 7 \lor \neg 8, 8 \lor 7 \lor \neg 5, \neg 6 \lor 8 \lor 4, \neg 4 \lor \neg 1, \neg 4 \lor 5 \lor 2, 5 \lor 7 \lor \neg 3, 1 \lor \neg 2 \lor 3 \} \]

\[ M = [3; 2; 1; 4; 5; 8; \ldots ; 7; \ldots ; 6; \ldots ] \]

**Resolve**

\[ R = \neg 6 \lor 8 \lor 7 \lor 5 \]

\[ R := 8 \lor 7 \lor \neg 6 \]

\[ R = 8 \lor 7 \lor \neg 6 \]

**CDCL + Resolution + Learning + Restart**

When \( \text{Mode} = \text{search} \)

**SUCCESS**

\[ M \models F \]

return \text{SAT}

**UNIT**

\[ C \lor l \in F \]

\[ M \models \neg C \]

\[ l \text{ is undefined in } M \]

\[ M := l_{C \lor l} :: M \]

**DECIDE**

\[ l \text{ is undefined in } M \]

\[ l \text{ (or } \neg l) \in F \]

\[ M := l :: M \]

**CONFLICT**

\[ C \in F \]

\[ M \models \neg C \]

\[ R := C; \ Mode := \text{resolution} \]

When \( \text{Mode} = \text{resolution} \)

**FAIL**

\[ R = \bot \]

return \text{UNSAT}

**RESOLVE**

\[ R = C \lor \neg l \]

\[ l_{D \lor l} \in M \]

\[ R := C \lor D \]

**BACKJUMP**

\[ R = C \lor l \]

\[ M = M_1 :: l' :: M_2 \]

\[ M_2 \models \neg C \]

\[ l \text{ is undefined in } M_2 \]

\[ M := l_{C \lor l} :: M_2; \ Mode := \text{search} \]
When \( \text{Mode} = \text{resolution} \)

\[
\text{LEARN} \quad R \notin F \\
F := F \cup \{R\}
\]

When \( \text{Mode} = \text{search} \)

\[
\text{FORGET} \quad C \text{ is a learned clause} \\
F := F \setminus \{C\}
\]

\[
\text{RESTART} \\
M := \emptyset
\]

\[
\text{MODE} = \text{search} \\
M = []
\]

\[
F = \{\overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2}\}
\]

\[
R =
\]

\[
\text{DECIDE} \quad 1 \text{ is undefined in } M \\
\overline{1} \in F \\
M := 1 :: M
\]

\[
\text{MODE} = \text{search} \\
M = [1]
\]

\[
F = \{\overline{1} \lor 2, \overline{3} \lor 4, 5 \lor \overline{6}, 6 \lor 5 \lor \overline{2}, 5 \lor 7, 5 \lor \overline{7} \lor \overline{2}\}
\]

\[
R =
\]
CDCL + Resolution: Example

**Unit**

\[
\begin{align*}
\text{Unit} & \quad \bar{1} \vee 2 \in F \\
M \models 1 & \quad 2 \text{ is undefined in } M \\
M := 2_{\bar{1} \vee 2} :: M
\end{align*}
\]

*Mode = search*

\(M = [1]\)

\(F = \{\bar{1} \vee 2, \bar{3} \vee 4, 5 \vee 6, 6 \vee 5 \vee \bar{2}, 5 \vee 7, 5 \vee \bar{7} \vee 2\}\)

\(R =\)

---

**Decide**

\[
\begin{align*}
\text{Decide} & \quad \bar{3} \text{ is undefined in } M \\
\bar{3} \in F & \quad M := \bar{3} :: M
\end{align*}
\]

*Mode = search*

\(M = [2_{\bar{1} \vee 2}; 1]\)

\(F = \{\bar{1} \vee 2, \bar{3} \vee 4, 5 \vee 6, 6 \vee 5 \vee \bar{2}, 5 \vee 7, 5 \vee \bar{7} \vee 2\}\)

\(R =\)

---

**Unit**

\[
\begin{align*}
\text{Unit} & \quad \bar{1} \vee 2 \in F \\
M \models 1 & \quad 2 \text{ is undefined in } M \\
M := 2_{\bar{1} \vee 2} :: M
\end{align*}
\]

*Mode = search*

\(M = [2_{\bar{1} \vee 2}; 1]\)

\(F = \{\bar{1} \vee 2, \bar{3} \vee 4, 5 \vee 6, 6 \vee 5 \vee \bar{2}, 5 \vee 7, 5 \vee \bar{7} \vee 2\}\)

\(R =\)

---

**Decide**

\[
\begin{align*}
\text{Decide} & \quad \bar{3} \text{ is undefined in } M \\
\bar{3} \in F & \quad M := \bar{3} :: M
\end{align*}
\]

*Mode = search*

\(M = [3; 2_{\bar{1} \vee 2}; 1]\)

\(F = \{\bar{1} \vee 2, \bar{3} \vee 4, 5 \vee 6, 6 \vee 5 \vee \bar{2}, 5 \vee 7, 5 \vee \bar{7} \vee 2\}\)

\(R =\)
CDCL + Resolution : Example

\text{UNIT} \quad \frac{3 \lor 4 \in F}{M := 4_{3 \lor 4} :: M} \quad 3 \lor 4 \text{ is undefined in } M

\text{Mode} = \text{search}
\begin{align*}
M &= [3; 2_{1 \lor 2}; 1] \\
F &= \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\} \\
R &=
\end{align*}

CDCL + Resolution : Example

\text{UNIT} \quad \frac{3 \lor 4 \in F}{M := 4_{3 \lor 4} :: M} \quad 3 \lor 4 \text{ is undefined in } M

\text{Mode} = \text{search}
\begin{align*}
M &= [4_{3 \lor 4}; 3; 2_{1 \lor 2}; 1] \\
F &= \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\} \\
R &=
\end{align*}

CDCL + Resolution : Example

\text{DETERM} \quad \frac{5 \text{ is undefined in } M}{M := 5 :: M} \quad 5 \in F

\text{Mode} = \text{search}
\begin{align*}
M &= [4_{3 \lor 4}; 3; 2_{1 \lor 2}; 1] \\
F &= \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\} \\
R &=
\end{align*}

CDCL + Resolution : Example

\text{DETERM} \quad \frac{5 \text{ is undefined in } M}{M := 5 :: M} \quad 5 \in F

\text{Mode} = \text{search}
\begin{align*}
M &= [5; 4_{3 \lor 4}; 3; 2_{1 \lor 2}; 1] \\
F &= \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2\} \\
R &=
\end{align*}
Unit $5 \lor 6 \in F$ \[ M \models 5 \quad 6 \text{ is undefined in } M \]
\[ M := \neg 6 \lor \neg 5 \lor \neg 6 :: M \]

Mode = search
\[ M = [5; 4_3 \lor 4; 3; 2_1 \lor 2; 1] \]
\[ F = \{ \bar{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2 \} \]
\[ R = \]

Conflict $6 \lor 5 \lor 2 \in F$ \[ M \models 6 \land 5 \land 2 \]
\[ R := 6 \lor 5 \lor 2; Mode := \text{resolution} \]

Mode = search
\[ M = [6_5 \lor 6; 5; 4_3 \lor 4; 3; 2_1 \lor 2; 1] \]
\[ F = \{ \bar{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2 \} \]
\[ R = \]

Conflict $6 \lor 5 \lor 2 \in F$ \[ M \models 6 \land 5 \land 2 \]
\[ R := 6 \lor 5 \lor 2; Mode := \text{resolution} \]

Mode = resolution
\[ M = [6_5 \lor 6; 5; 4_3 \lor 4; 3; 2_1 \lor 2; 1] \]
\[ F = \{ \bar{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor 7 \lor 2 \} \]
\[ R = 6 \lor 5 \lor 2 \]
\[ \text{Resolve} \quad R = 6 \lor \overline{5} \lor \overline{2} \quad \overline{6} \lor \overline{5} \lor \overline{6} \in M \]

\[
R := \overline{2} \lor \overline{5}
\]

Mode = \textit{resolution}

\[
M = [6 \overline{5} \lor \overline{6}; 5; 4_3 \lor 4; 3; 2_{1v2}; 1]
\]

\[
F = \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor 2\}
\]

\[
R = 6 \lor \overline{5} \lor \overline{2}
\]

\[
\text{Backjump} \quad R = \overline{2} \lor \overline{5}
\]

\[
M = [6 \overline{5} \lor \overline{6}; 5; 4_3 \lor 4; 3; 2_{1v2}; 1]
\]

\[
F = \{\overline{1} \lor 2, 3 \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor 2\}
\]

\[
R = \overline{2} \lor \overline{5}
\]
CDCL + Resolution : Example

etc.

Mode = search

\[ M = [\overline{5} \lor \overline{2}; 2 \lor 1; 1] \]

\[ F = \{ \overline{1} \lor 2, \overline{3} \lor 4, 5 \lor 6, 6 \lor 5 \lor 2, 5 \lor 7, 5 \lor \overline{7} \lor 2 \} \]

\[ R = \]

Strategies

The inference rules given for DPLL and CDCL are flexible

Basic strategy :
   ▶ apply Decide only if Unit or Fail cannot be applied

Conflict resolution :
   ▶ Learn only one clause per conflict (the clause used in Backjump)
   ▶ Use Backjump as soon as possible (FUIP)
   ▶ When applying Resolve, use the literals in \( M \) in the reverse order they have been added

Decision heuristic : VSIDS

The Variable State Independent Decaying Sum (VSIDS) heuristic associates a score to each literal in order to select the literal with the highest score when Decide is used

▶ Each literal has a counter, initialized to 0
▶ Increase the counters of
   ▶ the literal \( l \) when Resolve is used
   ▶ the literals of the clause in \( R \) when Backjump is used
▶ Counters are divided by a constant, periodically

Scoring Learned Clauses

CDCL performances are tightly related to their learning clause management

▶ Keeping too many clauses decrease the BCP efficiency
▶ Cleaning out too many clauses break the overall learning benefit

Quality measures for learning clauses are based on scores associated with learned clauses

▶ VSIDS (dynamic): increase the score of clauses involved in Resolve
▶ LBD (static): number of different decision levels in a learned clause
BCP = 80% of SAT-solver runtime

How to implement efficiently $M \models C$ (in Unit and Conflict)?

Two watched literals technique:

- assign two non-false watched literals per clause
- only if one of the two watched literal becomes false, the clause is inspected:
  - if the other watched literal is assigned to true, then do nothing
  - otherwise, try to find another watched literal
  - if no such literal exists, then apply Backjump
  - if the only possible literal is the other watched literal of the clause, then apply Unit

Main advantages:

- clauses are inspected only when watched literal are assigned
- no updating when backjumping

First-Order Logic: Signature and Terms

- A signature $\Sigma$ is a finite set of function and predicate symbols with an arity
- Constants are just function symbols of arity 0
- We assume that $\Sigma$ contains the binary predicate $=$
- We assume a set $\mathcal{V}$ of variables, distinct from $\Sigma$
- $T(\Sigma, \mathcal{V})$ is the set of terms, i.e. the smallest set which contains $\mathcal{V}$ and such that $f(t_1, \ldots, t_n) \in T(\Sigma, \mathcal{V})$ whenever $t_1, \ldots, t_n \in T(\Sigma, \mathcal{V})$ and $f \in \Sigma$
- $T(\Sigma, \emptyset)$ is the set of ground terms
- Terms are just trees. Given a term $t$ and a position $\pi$ in a tree, we write $t_\pi$ for the sub-term of $t$ at position $\pi$. We also write $t[\pi \mapsto t']$ for the replacement of the sub-term of $t$ at position $\pi$ by the term $t'$

First-Order Logic: Formulas

- An atomic formula is $P(t_1, \ldots, t_n)$, where $t_1, \ldots, t_n$ are terms in $T(\Sigma, \mathcal{V})$ and $P$ is a predicate symbol of $\Sigma$
- Literals are atomic formulas or their negation
- Formulas are inductively constructed from atomic formulas with the help of Boolean connectives and quantifiers $\forall$ and $\exists$
- Ground formulas contain only ground terms
- A variable is free if it is not bound by a quantifier
- A sentence is a formula with no free variables
A model $\mathcal{M}$ for a signature $\Sigma$ is defined by

- a domain $D_{\mathcal{M}}$
- an interpretation $f^\mathcal{M}$ for each function symbol $f \in \Sigma$
- a subset $P^\mathcal{M}$ of $D_{\mathcal{M}}^n$ for each predicate $P \in \Sigma$ of arity $n$
- an assignment $\mathcal{M}(x)$ for each variable $x \in V$

The cardinality of model $\mathcal{M}$ is the the cardinality of $D_{\mathcal{M}}$

**First-Order Logic : Semantics**

Interpretation of terms:

- $\mathcal{M}[x] = \mathcal{M}(x)$
- $\mathcal{M}[f(t_1,\ldots,t_n)] = f^\mathcal{M}(\mathcal{M}[t_1],\ldots,\mathcal{M}[t_n])$

Interpretation of formulas:

- $\mathcal{M} = t_1 = t_2 = \mathcal{M}[t_1] = \mathcal{M}[t_2]$
- $\mathcal{M} = P(t_1,\ldots,t_n) = (\mathcal{M}[t_1],\ldots,\mathcal{M}[t_n]) \in P^\mathcal{M}$
- $\mathcal{M} = \neg F = \mathcal{M} \not\models F$
- $\mathcal{M} = F_1 \land F_2 = \mathcal{M} \models F_1$ and $\mathcal{M} \models F_2$
- $\mathcal{M} = F_1 \lor F_2 = \mathcal{M} \models F_1$ or $\mathcal{M} \models F_2$
- $\mathcal{M} = \forall x.F = \mathcal{M}\{x \mapsto v\} \models F$ for all $v \in D_{\mathcal{M}}$
- $\mathcal{M} = \exists x.F = \mathcal{M}\{x \mapsto v\} \models F$ for some $v \in D_{\mathcal{M}}$

**First-Order Logic : Validity**

- A formula $F$ is satisfiable if there a model $\mathcal{M}$ such that $\mathcal{M} \models F$, otherwise $F$ is unsatisfiable
- A formula $F$ is valid if $\neg F$ is unsatisfiable

**First-Order Logic : Theories**

A first-order theory $T$ over a signature $\Sigma$ is a set of sentences

- A theory is consistent if it has (at least) a model
- A formula $F$ is satisfiable in $T$ (or $T$-satisfiable) if there exists a model $\mathcal{M}$ for $T \land F$, written $\mathcal{M} \models_T F$
- A formula $F$ is $T$-validity, denoted $\models_T F$, if $\neg F$ is $T$-unsatisfiable
A decision procedure is an algorithm used to determine whether a formula $F$ in a theory $T$ is satisfiable.

Many decision procedures work on conjunctions of (ground) literals.

CDCL(T) has the same rules than CDCL, augmented with

**T-CONFLICT**

- Mode = search
  - $l_1, \ldots, l_n \in M$ 
  - $l_1, \ldots, l_n \models_T \bot$
  - $R := \neg l_1 \lor \ldots \lor \neg l_n$; Mode = resolution

**T-PROPAGATE**

- Mode = search
  - $l$ (or $\neg l$) $\in F$ 
  - $l$ is undefined in $M$
  - $l_1, \ldots, l_n \in M$ 
  - $l_1, \ldots, l_n \models_T l$
  - $M := \bot \lor l_1 \lor \ldots \lor l_n$ :: $M$

We assume a fix theory $T$.

The state of the procedure is similar to CDCL:

- $F$ contains quantifier-free clauses in $T$
- $M$ is a list of literals in $T$
CDCL(T) : Example

\[ \text{UNIT } \frac{3 < x \in F}{M := 3 < x \text{ undefined in } M} \]

Mode = \textit{search}

\[ M = [] \]

\[ F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\} \]

\[ R = \]

\[ x < 0 \in F \text{ is undefined in } M \]

\[ \frac{3 < x \in M}{M := x \geq 0} \]

\[ \text{T-PROPAGATE } \frac{3 < x \in M}{M := x \geq 0; 3 < x \text{ undefined in } M} \]

Mode = \textit{search}

\[ M = [3 < x_{<x}] \]

\[ F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\} \]

\[ R = \]

CDCL(T) : Example

\[ \text{UNIT } \frac{3 < x \in F}{M := 3 < x \text{ undefined in } M} \]

Mode = \textit{search}

\[ M = [3 < x_{<x}] \]

\[ F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\} \]

\[ R = \]

\[ x < 0 \in F \text{ is undefined in } M \]

\[ \frac{3 < x \in M}{M := x \geq 0} \]

\[ \text{T-PROPAGATE } \frac{3 < x \in M}{M := x \geq 0; 3 < x \text{ undefined in } M} \]

Mode = \textit{search}

\[ M = [x \geq 0; 3 < x_{<x}] \]

\[ F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\} \]

\[ R = \]
\[ x < 0 \lor x < y \in F \]
\[ M \models_T x \geq 0 \quad x < y \text{ is undefined in } M \]
\[ M := x < y_{(x<0 \lor x<y)} :: M \]

**Mode = search**
\[ M = [x \geq 0_{(3 \geq x \lor x \geq 0)}; 3 < x_{3<x}] \]
\[ F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\} \]
\[ R = \]

\[ y < 0 \lor x \geq y \in F \]
\[ M \models_T x < y \quad y < 0 \text{ is undefined in } M \]
\[ M := y < 0_{(y<0 \lor x \geq y)} :: M \]

**Mode = search**
\[ M = [x < y_{(x<0 \lor x<y)}; x \geq 0_{(3 \geq x \lor x \geq 0)}; 3 < x_{3<x}] \]
\[ F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\} \]
\[ R = \]
CDCL(T) : Example

\[ 3 < x, x < y, y < 0 \in M \]
\[ 3 < x, x < y, y < 0 \models_T \bot \]
\[ R := 3 \geq x \lor x \geq y \lor y \geq 0; \text{Mode} := \text{resolution} \]

**Mode = search**

\[ M = [y < 0(y < 0 \lor x \geq y); x < y(x < 0 \lor x < y); x \geq 0(3 \geq x \lor x \geq 0); 3 < x < x] \]
\[ F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\} \]
\[ R = 3 \geq x \lor x \geq y \lor y \geq 0 \]

---

CDCL(T) : Example

**Resolved**

\[ R = 3 \geq x \lor x \geq y \lor y \geq 0 \]
\[ y < 0(y < 0 \lor x \geq y) \in M \]
\[ R := 3 \geq x \lor x \geq y \]

**Mode = resolution**

\[ M = [y < 0(y < 0 \lor x \geq y); x < y(x < 0 \lor x < y); x \geq 0(3 \geq x \lor x \geq 0); 3 < x < x] \]
\[ F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\} \]
\[ R = 3 \geq x \lor x \geq y \lor y \geq 0 \]
\[
\text{Resolve} \quad R = 3 \geq x \vee x \geq y \quad x < y(x \leq 0 \vee y < x) \in M
\]
\[
R := 3 \geq x
\]

*Mode = resolution*

\[
M = [y < 0(y < 0 \vee y \geq x); x < y(x \leq 0 \vee y < x); x \geq 0(3 \geq x \vee x \geq y); 3 < x \leq y]
\]

\[
F = \{3 < x, x < 0 \vee x < y, y < 0 \vee x \geq y\}
\]

\[
R = 3 \geq x \vee x \geq y
\]
Resolution

\[
\text{RESOLVE} \quad R = \perp \\
\text{return} \text{ UNSAT}
\]

Mode = \textit{resolution}

\[
M = [y < 0 (y < 0 \lor x \geq y); x < y (x < 0 \lor x < y); x \geq 0 (3 \geq x \lor x \geq 0); 3 < x 3 < x]
\]

\[
F = \{3 < x, x < 0 \lor x < y, y < 0 \lor x \geq y\}
\]

\[
R = \perp
\]

How to find efficiently \( l_1, \ldots, l_n \in M \) such that \( l_1, \ldots, l_n \models \perp \) ?

- In practice, we check for \( M \models \perp \) and, if that's true, then we ask the theory solver to produce an \textit{explanation}, that is, a set of literals \( \{l_1, \ldots, l_n\} \subseteq M \) such that \( \{l_1, \ldots, l_n\} \models \perp \)

- There may be \textit{several} explanations and some of them may contain \textit{irrelevant} literals

- Decision procedures try to produce \textit{minimal} explanations

Theory Propagation

- Similarly to rule \textit{Unit}, rule \textit{T-propagate} is optional

- Contrary to rule \textit{Unit}, the implementation of rule \textit{T-propagate} can be very costly

How to find efficiently \( l \) and \( l_1, \ldots, l_n \in M \) s.t \( l_1, \ldots, l_n \models l \) ?

- Theory solver are instrumented to find a literal \( l \) implied by \( M \) and to return an explanation of the \textit{unsatisfiability} of \( M \land \neg l \)

- The explanation is also expected to be \textit{minimal}

- In practice, decision procedures find \textit{some} implied literals, not all as this can be very costly

Decision Procedures for SMT

Decision procedures found in articles or textbooks need usually to be adapted for being used in SMT solvers

- \textit{Incrementally} : decision procedures are called successively on set of literals \( M_0 \subset M_1 \subset \ldots \subset M_k \)

  To gain for efficiency, we don’t want to restart from scratch for each \( M_i \) but try to reuse work done for \( M_i \) when processing \( M_{i+1} \)

- \textit{Backtracking} : operations for going back to a previous state of the decision procedure should be very efficient

- \textit{Propagation} : find the good tradeoff between precision and performance

- \textit{Explanations} : find an efficient generation mechanism that removes irrelevant literals (decidability issues)
Examples of decision procedures

The Free Theory of Equality with Uninterpreted Symbols

Axioms:

- **Reflexivity** \( \forall x.x = x \)
- **Symmetry** \( \forall x,y. x = y \Rightarrow y = x \)
- **Transitivity** \( \forall x,y,z. x = y \land y = z \Rightarrow x = z \)
- **Congruence**

\[
\forall x_1, \ldots, x_n, y_1, \ldots, y_n.
\quad x_1 = y_1 \land \cdots \land x_n = y_n \Rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)
\]

Examples:

\[
g(y, x) = y \land g(g(y, x), x) \neq y
\]

\[
f(f(f(a))) = a \land f(f(f(f(f(a))))) = a \land f(a) \neq a
\]

**Congruence Closure**

Let \( \mathcal{R} \) an equivalence relation on terms. The domain of \( \mathcal{R} \), denoted by \( \text{dom}(\mathcal{R}) \), is the set of all terms and subterms of \( \mathcal{R} \)

- **Congruence**
  Two terms \( t \) and \( u \) are congruent by \( \mathcal{R} \) if they are respectively of the form \( f(t_1, \ldots, t_n) \) and \( f(u_1, \ldots, u_n) \) and \( (t_i, u_i) \in \mathcal{R} \) for all \( i \)

\( \mathcal{R} \) is closed by congruence if for all terms \( t, u \in \text{dom}(\mathcal{R}) \) congruent par \( \mathcal{R} \) we have \( (t, u) \in \mathcal{R} \)

- **Congruence Closure**
  The congruence closure of \( \mathcal{R} \) is the smallest relation containing \( \mathcal{R} \) and which is closed by congruence

**Representation of Terms and Equality Relation**

1. Terms are represented by **DAG** (directed acyclic graphs)

   For instance, \( f(f(a), b) \) is represented by the following graph

   ![DAG Diagram](attachment:image.png)
1. Terms are represented by **DAG** (directed acyclic graphs)
   For instance, \( f(f(a, b), b) \) is represented by the following graph

   ![DAG example](image)

2. \( R \) is represented by dotted lines
   For instance, \( f(f(a, b), b) = a \) is represented by a dotted line between \( f \) and \( a \)

3. DAG associated with an equivalence relation are called **E-DAG** (equality DAG)

---

**Naive Congruence Closure**

The equivalent relation \( R \) (the dotted lines) is implemented as a union-find data structure on the nodes of the DAG

- `find(n)` returns the representative of the node \( n \)
- `union(n, m)` merges the equivalence classes of \( n \) and \( m \)

Naive congruence closure algorithm:

For every nodes \( n \) and \( m \) such that `find(n) ≠ find(m)`,

- if \( n \) and \( m \) are labeled with the same symbol and they have the same number of children and `find(n_i) = find(m_i)` for every children \( n_i \) and \( m_i \) of \( n \) and \( m \)
- then, merge the classes of \( n \) and \( m \) by `union(n, m)`

---

**Example**

\( g(g(g(a))) = a \land g(g(g(g(g(a)))))) = a \land g(a) \neq a \) satisfiable?

\( g(g(a)) = a \land g(g(g(g(a)))) \neq a \)

---
Example

\[ g(g(g(a))) = a \land g(g(g(g(a)))) = a \land g(a) \neq a \text{ satisfiable?} \]

Example

\[ g(g(g(a))) = a \land g(g(g(g(a)))) = a \land g(a) \neq a \text{ satisfiable?} \]
\[
g(g(a)) = a \land g(g(g(g(a)))) = a \land g(a) \neq a \text{ satisfiable?}
\]

\[
g(g(a)) = a \land g(g(g(g(g(a))))) = a \land g(a) \neq a \text{ satisfiable?}
\]
Example

\[ g(g(g(a))) = a \land g(g(g(g(a)))) = a \land g(a) \neq a \text{ satisfiable?} \]

Difference logic

\[ g(a) = a \text{ is implied by the E-DAG} \]

Difference Logic (DL)

\[ x - y \leq c \quad \text{where } x, y, c \in (\mathbb{Q} \text{ or } \mathbb{Z}) \]

Strict inequalities

- in \( \mathbb{Z} \), \( x - y < c \) is replaced \( x - y \leq c - 1 \)
- in \( \mathbb{Q} \), \( x - y < c \) is replaced \( x - y \leq c - \delta \) where \( \delta \) is a symbolic sufficiently small parameter

Equalities

- \( x = y \) is the same as \( x - y \leq c \land y - x \leq -c \)

One variable constraints

- \( x \leq c \) is replaced by \( x - x_{\text{zero}} \leq c \), where \( x_{\text{zero}} \) is a fresh variable whose value must be 0 in any solution

Given a set of difference constraints \( M \), we construct a weighted directed graph \( G_M(V, E) \) as follows:

- the set of vertices \( V \) contains the variables of the problem plus an extra variable \( s \)
- the set of weighted edges \( E \) contains an edge \( y \xrightarrow{c} x \) for each constraint \( x - y \leq c \), plus an edge \( s \xrightarrow{0} x \) for each variable \( x \) of the problem
A negative cycle in $G_M(V, E)$ is a path

$$x_0 \xrightarrow{c_0} x_1 \xrightarrow{c_1} \ldots \xrightarrow{c_{n-1}} x_n \xrightarrow{c_n} x_0$$

such that $c_0 + c_1 + \cdots + c_{n-1} + c_n < 0$

**Theorem**

If $G_M(V, E)$ has a negative cycle then $M$ is unsatisfiable, otherwise a solution is

$$x_1 = \delta(s, x_1), \ldots, x_n = \delta(s, x_n)$$

where $\delta(s, x_i)$ is the shortest-path weight from $s$ to $x_i$
Negative Cycle Detection

Negative cycle can be detected with shortest path algorithms

Most algorithms are based on the technique of relaxation

- For each vertex $x$, we maintain an upper bound $d[x]$ on the weight of a shortest path from $s$ to $x$
- Relaxing an edge $x \rightarrow y$ consists in testing whether we can improve the shortest path to $y$ found so far by going through $x$
- Additionally, shortest paths are saved in an array $\pi$ that gives the predecessor of each vertex

\[
\text{if } d[y] > d[x] + c \text{ then} \\
d[y] := d[x] + c \\
\pi[y] := x
\]

Bellman-Ford Algorithm

\[
\text{for each } x_i \in V \text{ do } d[x_i] := \infty \text{ done} \\
d[s] := 0 \\
\text{for } i := 1 \text{ to } |V| - 1 \text{ do} \\
\text{for each } x_i \rightarrow x_j \in E \text{ do} \\
\quad \text{if } d[x_j] > d[x_i] + c \text{ then} \\
\quad \quad d[x_j] := d[x_i] + c \\
\quad \quad \pi[x_j] := u \\
\text{done} \\
\text{done} \\
\text{for each } x_i \rightarrow x_j \in E \text{ do} \\
\quad \text{if } d[x_j] > d[x_i] + c \text{ then} \\
\quad \quad \text{return Negative Cycle Detected} \\
\quad \quad \text{Follow } \pi \text{ to reconstruct the cycle} \\
\text{done}
\]
Bellman-Ford Algorithm: Correctness

Proof.

Suppose that $G_M(V,E)$ contains a negative cycle $x_0 \xrightarrow{c_0} x_1 \xrightarrow{c_1} \cdots \xrightarrow{c_{k-1}} x_k$ with $x_0 = x_k$. Assume Bellman-Ford does not find the cycle. Thus, $d[x_i] \leq d[x_{i-1}] + c_{i-1}$ for all $i = 1, 2, \ldots, k$. Summing these inequalities, we get

$$\sum_{i=1}^{k} d[x_i] \leq \sum_{i=1}^{k} d[x_{i-1}] + \sum_{i=1}^{k} c_{i-1}$$

but, since $x_0 = x_k$, we have

$$\sum_{i=1}^{k} d[x_i] = \sum_{i=1}^{k} d[x_{i-1}]$$

which is impossible since the cycle is negative.

Bellman-Ford Algorithm: Correctness

Proof.

Suppose that $G_M(V,E)$ contains a negative cycle $x_0 \xrightarrow{c_0} x_1 \xrightarrow{c_1} \cdots \xrightarrow{c_{k-1}} x_k$ with $x_0 = x_k$. Assume Bellman-Ford does not find the cycle. Thus, $d[x_i] \leq d[x_{i-1}] + c_{i-1}$ for all $i = 1, 2, \ldots, k$. Summing these inequalities, we get

$$\sum_{i=1}^{k} d[x_i] - \sum_{i=1}^{k} d[x_{i-1}] \leq \sum_{i=1}^{k} c_{i-1}$$

but, since $x_0 = x_k$, we have

$$\sum_{i=1}^{k} d[x_i] = \sum_{i=1}^{k} d[x_{i-1}]$$

which is impossible since the cycle is negative.
Bellman-Ford Algorithm (cont)

- Checking satisfiability can be performed in time $O(|V|.|E|)$
- Inconsistency explanations are negative cycles (irredundant but not minimal explanations)
- Incremental and backtrackable extensions exist

Quantifiers

Consider the following axiomatization (in Alt-Ergo’s syntax) for an ordering relation $le$

```plaintext
logic le: int,int -> prop
axiom refl: forall x:int. le(x,x)
axiom trans:
    forall x,y,z:int. le(x,y) and le(y,z) -> le(x,z)
axiom antisym:
    forall x,y:int. le(x,y) and le(y,x) -> x = y
```

and some goals we want to prove:

```plaintext
goal g1:  le(2,5) and le(5,10) -> le(2,10)
goal g2:
    forall a:int.
        le(a,5) and le(5,8) and le(8,a) -> a=5
```
Many SMT solvers handle universal formulas through an instantiation mechanism.

Questions:

▶ How to find good instances to prove a goal?
▶ How to limit the (prohibitive) number of instances?

A possible answer: find good heuristics!

In practice, heuristics for choosing new instances are based on triggers: lists of patterns (terms with variables) that guide (or restrict) instantiations to known ground terms that have a given form.
If \( P(x) \) is used as trigger in the following axiom \( \text{ax1} \)

\[
\text{logic } P,Q,R: \text{int} \rightarrow \text{prop} \\
\text{axiom } \text{ax1}: \forall x: \text{int}. (P(x) \lor Q(x)) \rightarrow R(x) \\
\text{goal } g3: P(1) \rightarrow R(1) \\
\text{goal } g4: Q(2) \rightarrow R(2)
\]

then, among the set of known terms \{P(1), R(1), P(2), R(2)\}, only \( P(1) \) can be used to create the following instance of \( \text{ax1} \)

\[
(P(1) \lor Q(1)) \rightarrow R(1)
\]

which implies that only goal \( g3 \) is proved.

---

**Triggers: Example**

---

**Explicit Triggers**

SMT solvers’ input syntax provides the possibility for a user to specify its own triggers.

For instance, in Alt-Ergo, the list of terms \([f(x), Q(y)]\) is an explicit trigger for the following axiom \( \text{ax2} \)

\[
\text{logic } P,Q,R: \text{int} \rightarrow \text{prop} \\
\text{logic } f: \text{int} \rightarrow \text{int} \\
\text{axiom } \text{ax2}: \forall x,y: \text{int}. [f(x), Q(y)]. P(f(x)) \land Q(y) \rightarrow R(x)
\]

---

**Matching**

We use a **matching** algorithm to create new instances of universal formulas.

Given a **ground term** \( t \) and a **pattern** \( p \), the matching algorithm returns a set \( S \) of substitutions over the variables of \( p \) such that

\[
t = \sigma(p) \text{ for all } \sigma \in S
\]

---

**Limitation of Matching**

Purely syntactic matching is very limited!

Consider for instance the following formulas:

\[
\text{logic } P,R : \text{int} \rightarrow \text{prop} \\
\text{logic } f : \text{int} \rightarrow \text{int} \\
\text{axiom } \text{ax} : \forall x: \text{int}. [P(f(x))]. P(f(x)) \rightarrow R(x) \\
\text{goal } g1 : \forall a: \text{int}. P(a) \rightarrow a = f(2) \rightarrow R(2)
\]

The trigger \( P(f(x)) \) prevents the creation of instances of axiom \( \text{ax} \) since there is no ground term of the form \( P(f(\_)) \) in the problem.

To prove such goals, we need to extend the matching algorithm to find substitutions modulo (ground) equalities.
E-Matching

Given a set of ground equations $E$, a ground term $t$ and a pattern $p$, the e-matching algorithm returns a set $S$ of substitutions over the variables of $p$ such that

$$E \models t = \sigma(p) \text{ for all } \sigma \in S$$

In the previous example

logic $P,R : \text{int} \rightarrow \text{prop}$
logic $f : \text{int} \rightarrow \text{int}$
axiom $ax : \forall x : \text{int}. [P(f(x))]. P(f(x)) \rightarrow R(x)$
goal $g1 : \forall a : \text{int}. P(a) \rightarrow a = f(2) \rightarrow R(2)$

E-matching takes advantage of ground equality $a = f(2)$ and returns the substitution $\sigma = \{ x \mapsto 2 \}$ which is used to create the instance $P(f(2)) \rightarrow R(2)$ of axiom $ax$

Ground Terms

Known ground terms are extracted from literals assumed or implied by the SAT solver

Instantiation based mechanisms are strongly impacted by the number and the relevance of known ground terms:

- more ground terms, more instances of lemmas
- irrelevant ground terms, irrelevant instances

Ground Terms and Linear CNF

The shape of formulas to be proved, and in particular the conversion process used to produce a CNF, has a strong impact on the number of known ground terms

Consider for instance the following formula

$$A \lor (B \land C)$$

When $A$ is assumed to be true, terms of $A$ become known and the rest of the formula $(B \land C)$ can be ignored

However, because of the shape of the CNF conversion

$$(A \lor X) \land (X \leftrightarrow (B \land C))$$

the SMT solver will assign a value to $X$ (even when $A$ is true) and terms from $B$ and $C$ will be considered has known terms. :-(