Satisfiability Modulo Theories: Theory and Implementation

Mohamed Iguernelala — OCamlPro SAS

slides borrowed from

Sylvain Conchon — LRI, Université Paris-Sud

MPRI 2014-2015

About Me

Who am I ?

- Mohamed Iguernelala
- mohamed.iguernelala@ocamlpro.com (send me an email)
- Senior R&D engineer at OCamlPro SAS
- Research associate in the VALS team, LRI

My Research topics

- Satisfiability Modulo Theories (SMT)
- Combining rewriting and SMT techniques
- Designing decision procedures for SMT
- Combination of decision procedures

Maintainer of the Alt-Ergo SMT solver at OCamlPro

About The Course

Webpage: `https://www.lri.fr/~iguer/mpri`

4×3 hours lectures (including breaks):

- SAT solving
- Theories (Decision procedures)
- Extending a SAT solver with a Theory
- Theories combination
- Handling universally quantified formulas in SMT

Project:

- Solving the Sudoku problem

Part I

Introduction to SMT

What is SMT

SMT

Satisfiability Modulo Theories

=

SAT solver + Decision Procedures

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

SMT With Quantifiers

Satisfiability Modulo Theories

$=$

SAT solver + Decision Procedures + Quantifiers Handler

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

... modulo a set of universally quantified formulas

SMT Solving

An SMT solver's interface:

Input: a first-order formula F

Output: the status of F (sat or unsat),

and optionally :
a model (when sat)
or a proof (when unsat)

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :
  $\forall y$:int.
    $1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \Rightarrow$
    $P(\,f(2y - f(y))\,)$

Is g1 valid modulo linear arithmetic, the theory of uninterpreted function symbols and the axiom my_ax ??

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :
$\forall y$:int.
$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \Rightarrow$
$P(\, f(2y - f(y))\,)$

g1 is valid if and only if $\neg g1$ is unsatisfiable

Example

```
logic P : int → prop
logic f : int → int
axiom my_ax: ∀x:int. 2 ≤ x ≤ 3 ⇒ P(x)
goal g1 :
    ∃y:int.
      1 ≤ 2y ≤ 9 ∧ f(y) = y ∧ y ≠ 4 ∧ P(1) ∧
      ¬P( f(2y − f(y)) )
```

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$\neg P(\, f(2y - f(y))\,)$$

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$\neg P(\, f(2y - y)\,)$$

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge \neg P(\, f(y)\,)$$

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$\neg P(\, y\,)$$

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$\neg P(\, y \,)$$

$$y \in \{1, 2, 3\}$$

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$(\neg P(\,1\,) \vee \neg P(\,2\,) \vee \neg P(\,3\,))$$

Case analysis on y

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$(\neg P(1) \vee \neg P(2) \vee \neg P(3))$$

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$(\neg P(2) \vee \neg P(3))$$

Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow \mathrm{P}(x)$
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$(\neg P(2) \vee \neg P(3))$$

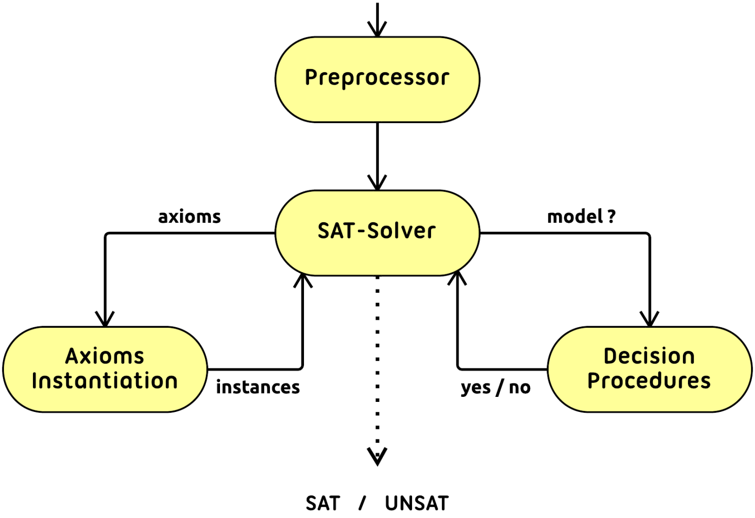
Example

logic P : int $\rightarrow$ prop
logic f : int $\rightarrow$ int
axiom my_ax: $\forall x$:int. $2 \leq x \leq 3 \Rightarrow$ P(x)
goal g1 :

$$1 \leq 2y \leq 9 \wedge f(y) = y \wedge y \neq 4 \wedge \mathrm{P}(1) \wedge$$
$$\bot$$

$\neg g1$ is Unsatisfiable

Components of an SMT Solver



SMT Challenges

- Size of formulas
- Complex Boolean structure
- Combination of theories
- Efficient decision procedures pour certain theories
- Efficient quantifiers handling
- Models generation
- Proofs generation & validation

SMT in the World

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-Lib Input Language

A variant of many-sorted first-order logic with:

- a limited form of polymorphism
- no distinction between Booleans and Propositions
- some high-level constructs (let-in, ite, ...)

SMT-Lib Benchmarks

Organized into sub-logics ...

- quantifier-free categories

  QF_UF, QF_BV, QF_LIA, QF_LRA, QF_NRA, QF_NIA, QF_IDL, QF_AX, etc.

- categories involving quantified formulas with arithmetic and/or (limited forms of) arrays

  AUFLIA, AUFLIRA, AUFNIRA, LRA, UFLRA, UFNIA

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

Applications

Main applications:

- Test case generator
- Program verifier
- Model checking

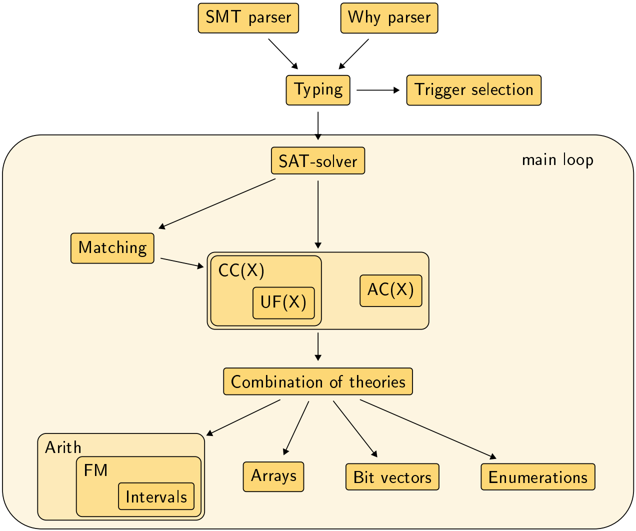
Other applications:

- Type checking
- Termination
- Invariant Generation
- Scheduling
- etc.

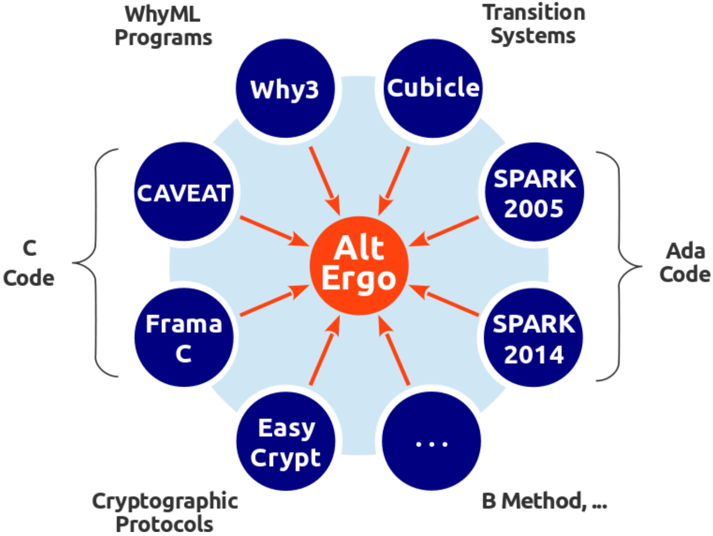
The Alt-Ergo SMT Solver

Architecture

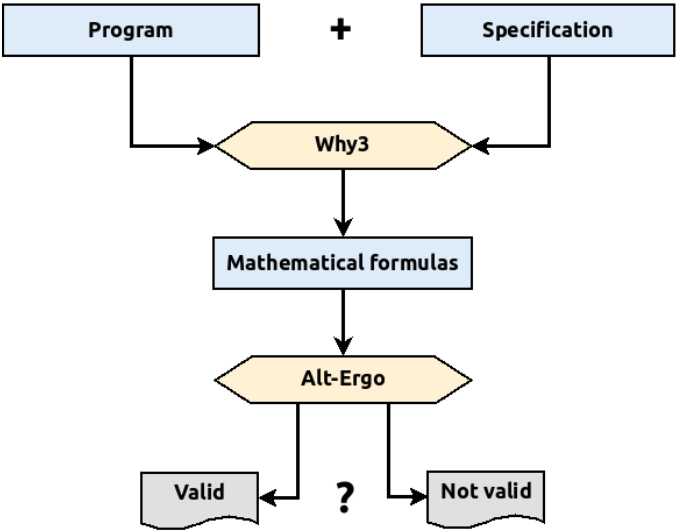
An OCaml SMT solver dedicated to programs verification ...



Applications of Alt-Ergo



Example: Deductive Program Verification



Proving an Euclidean division algorithm
using Why3 + Alt-Ergo

Back to Theoretical Aspects of SMT ...

SMT : Building Blocks

Three main blocks:

- SAT Solver
- Decision Procedures
- Combining Decision Procedures framework (CDP)

+ Quantifiers Handler for some solvers

SAT Solvers

Is $(p \lor q \lor \neg r) \land (r \lor \neg p)$ satisfiable?

- Truth tables
- Resolution
- Tableaux
- DPLL
- CDCL (Modern efficient SAT solvers)

Decision Procedures

Deciding satisfiability of ground conjunctions of literals

- Union-Find

  $$x = y \land y = z \land x \neq z$$

- Congruence closure

  $$g(x, y) = x \land f(x) = x \land g(g(f(x), y), y) \neq x$$

- Fourier-Motzkin, Simplex

  $$x \leq 2y + 4 \land y \leq 2 + x$$

- etc.

Combining Decision Procedures : CDP

- Nelson-Oppen combination
- Shostak algorithm
- Model-based theory propagation
- Delayed Theories combination

Basic SMT Solving

Given a CNF formula F

1. Replace every literal by a Boolean variable
2. Ask SAT for a Boolean model M
3. Convert back M and call the CDP procedure

if M is satisfiable modulo theories, then so is F
otherwise, add $\neg M$ to F and go to step 1.

Basic SMT Solving : Example

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

Basic SMT Solving : Example

$$x + y \geq 0 \wedge (x = z \Rightarrow y + z = -1) \wedge z > 3t$$

1. CNF conversion

Basic SMT Solving : Example

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

1. CNF conversion

Basic SMT Solving : Example

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

1. CNF conversion
2. Replace arithmetic constraints by Boolean variables

Basic SMT Solving : Example

$$p_1 \wedge (p_2 \vee p_3) \wedge p_4$$

1. CNF conversion
2. Replace arithmetic constraints by Boolean variables

Basic SMT Solving : Example

$$p_1 \wedge (p_2 \vee p_3) \wedge p_4$$

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

Basic SMT Solving : Example

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

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

Basic SMT Solving : Example

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

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

Basic SMT Solving : Example

$$M = \{x + y \geq 0,\ x = z,\ y + z = -1,\ z > 3t\}$$

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

Basic SMT Solving : Example

$$M = \{x + y \geq 0,\ x = z,\ y + z = -1,\ z > 3t\}$$

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 a appropriate decision procedure for arithmetic

Basic SMT Solving : Example

M is unsatisfiable modulo arithmetic!

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 a appropriate decision procedure for arithmetic

Basic SMT Solving : Example

M is unsatisfiable modulo arithmetic!

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 a appropriate decision procedure for arithmetic
6. Add $\neg M$ to F and go back to step 2

Basic SMT Solving : Example

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

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 a appropriate decision procedure for arithmetic
6. Add $\neg M$ to F and go back to step 2

Roadmap

Lecture 2 : Modern SAT Solvers, DPLL(T)

Lecture 3 : Theory Combination, EUF, Linear Arithmetic

Lecture 4 : Quantifiers Handling

Part II

Modern SAT Solvers

Propositional Logic : Notations

p, q, r, s are propositional variables or atoms

l is a literal (p or $\neg p$)

$$\neg l = \begin{cases} \neg p & \text{if } l \text{ is } p \\ p & \text{if } l \text{ is } \neg p \end{cases}$$

A disjunction of literals $l_1 \vee \ldots \vee l_n$ is a clause
The empty clause is written $\perp$
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. $(\neg l_1 \vee L_2 \vee \neg l_3) \wedge (l_4 \vee \neg 2)$ is simply written $\{\bar{1} \vee 2 \vee \bar{3}, 4 \vee \bar{2}\}$

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 literal 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 $C \vee l$ 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

CNF Conversion

Convert a formula F into an equivalent CNF

CNF Conversion

Convert a formula F into an equivalent CNF

1. Simple form conversion: eliminate $\Rightarrow$ and $\Leftrightarrow$

$$
\begin{array}{lcl}
(F_1 \Leftrightarrow F_2) & \longrightarrow & (F_1 \Rightarrow F_2) \land (F_2 \Rightarrow F_1) \\
(F_1 \Rightarrow F_2) & \longrightarrow & (\neg F_1 \lor F_2)
\end{array}
$$

CNF Conversion

Convert a formula F into an equivalent CNF

1. Simple form conversion: eliminate $\Rightarrow$ and $\Leftrightarrow$

$$\begin{array}{lcl} (F_1 \Leftrightarrow F_2) & \longrightarrow & (F_1 \Rightarrow F_2) \land (F_2 \Rightarrow F_1) \\ (F_1 \Rightarrow F_2) & \longrightarrow & (\neg F_1 \lor F_2) \end{array}$$

2. NNF conversion: move negations in

$$\begin{array}{lcl} \neg\neg p & \longrightarrow & p \\ \neg(F_1 \lor F_2) & \longrightarrow & (\neg F_1 \land \neg F_2) \\ \neg(F_1 \land F_2) & \longrightarrow & (\neg F_1 \lor \neg F_2) \end{array}$$

CNF Conversion

Convert a formula F into an equivalent CNF

1. Simple form conversion: eliminate $\Rightarrow$ and $\Leftrightarrow$

$$\begin{array}{lcl} (F_1 \Leftrightarrow F_2) & \longrightarrow & (F_1 \Rightarrow F_2) \wedge (F_2 \Rightarrow F_1) \\ (F_1 \Rightarrow F_2) & \longrightarrow & (\neg F_1 \vee F_2) \end{array}$$

2. NNF conversion: move negations in

$$\begin{array}{lcl} \neg\neg p & \longrightarrow & p \\ \neg(F_1 \vee F_2) & \longrightarrow & (\neg F_1 \wedge \neg F_2) \\ \neg(F_1 \wedge F_2) & \longrightarrow & (\neg F_1 \vee \neg F_2) \end{array}$$

3. Distribute disjunctions:

$$\begin{array}{lcl} F_1 \vee (F_2 \wedge F_3) & \longrightarrow & (F_1 \vee F_2) \wedge (F_1 \vee F_3) \\ (F_1 \wedge F_2) \vee F_3 & \longrightarrow & (F_1 \vee F_3) \wedge (F_2 \vee F_3) \end{array}$$

Exponential Explosion in Size

Bad news!

Converting $(p_1 \wedge q_1) \vee (p_2 \wedge q_2) \vee \ldots \vee (p_n \wedge q_n)$ produces a CNF with 2^n clauses of the form $r_1 \vee \ldots \vee r_n$ where each r_i is either p_i or q_i

Linear transformations exist but the CNF obtained are not equivalent but only equisatisfiable

Linear CNF Conversion

1. Replace each subformula F by a fresh propositional variable r
2. Add the constraint $r \Leftrightarrow F$, that is the clauses

$$\{\neg r \vee F_1, \neg r \vee F_2, r \vee \neg F_1 \vee \neg F_2\} \quad \text{if } F = F_1 \wedge F_2$$

$$\{r \vee \neg F_1, r \vee \neg F_2, \neg r \vee F_1 \vee F_2\} \quad \text{if } F = F_1 \vee F_2$$

Linear CNF Conversion

1. Replace each subformula F by a fresh propositional variable r
2. Add the constraint $r \Leftrightarrow F$, that is the clauses

$$\{\neg r \vee F_1, \neg r \vee F_2, r \vee \neg F_1 \vee \neg F_2\} \quad \text{if } F = F_1 \wedge F_2$$

$$\{r \vee \neg F_1, r \vee \neg F_2, \neg r \vee F_1 \vee F_2\} \quad \text{if } F = F_1 \vee F_2$$

For instance, the linear conversion steps of $\neg(p_1 \wedge (p_2 \vee \neg p_3))$ are

Linear CNF Conversion

1. Replace each subformula F by a fresh propositional variable r
2. Add the constraint $r \Leftrightarrow F$, that is the clauses

$$\{\neg r \vee F_1, \neg r \vee F_2, r \vee \neg F_1 \vee \neg F_2\} \quad \text{if } F = F_1 \wedge F_2$$

$$\{r \vee \neg F_1, r \vee \neg F_2, \neg r \vee F_1 \vee F_2\} \quad \text{if } F = F_1 \vee F_2$$

For instance, the linear conversion steps of $\neg(p_1 \wedge (p_2 \vee \neg p_3))$ are

- $\neg(p_1 \wedge r_1) \wedge r_1 \Leftrightarrow (p_2 \vee \neg p_3)$

Linear CNF Conversion

1. Replace each subformula F by a fresh propositional variable r
2. Add the constraint $r \Leftrightarrow F$, that is the clauses

$$\begin{array}{ll} \{\neg r \vee F_1, \neg r \vee F_2, r \vee \neg F_1 \vee \neg F_2\} & \text{if } F = F_1 \wedge F_2 \\ \{r \vee \neg F_1, r \vee \neg F_2, \neg r \vee F_1 \vee F_2\} & \text{if } F = F_1 \vee F_2 \end{array}$$

For instance, the linear conversion steps of $\neg(p_1 \wedge (p_2 \vee \neg p_3))$ are

- $\neg(p_1 \wedge r_1) \wedge r_1 \Leftrightarrow (p_2 \vee \neg p_3)$
- $\neg r_2 \wedge r_2 \Leftrightarrow (p_1 \wedge r_1) \wedge r_1 \Leftrightarrow (p_2 \vee \neg p_3)$

Linear CNF Conversion

1. Replace each subformula F by a fresh propositional variable r
2. Add the constraint $r \Leftrightarrow F$, that is the clauses

$$\begin{array}{ll} \{\neg r \vee F_1, \neg r \vee F_2, r \vee \neg F_1 \vee \neg F_2\} & \text{if } F = F_1 \wedge F_2 \\ \{r \vee \neg F_1, r \vee \neg F_2, \neg r \vee F_1 \vee F_2\} & \text{if } F = F_1 \vee F_2 \end{array}$$

For instance, the linear conversion steps of $\neg(p_1 \wedge (p_2 \vee \neg p_3))$ are

- $\neg(p_1 \wedge r_1) \wedge r_1 \Leftrightarrow (p_2 \vee \neg p_3)$
- $\neg r_2 \wedge r_2 \Leftrightarrow (p_1 \wedge r_1) \wedge r_1 \Leftrightarrow (p_2 \vee \neg p_3)$
- $\neg r_2 \wedge$
  $(\neg r_2 \vee p_1) \wedge (\neg r_2 \vee r_1) \wedge (\neg p_1 \vee \neg r_1 \vee r_2) \wedge$
  $(\neg r_1 \vee p2 \vee \neg p3) \wedge (\neg p2 \vee r_1) \wedge (p_3 \vee r_1)$

SAT Solvers : History

- Resolution-based procedure (DP [1960])
- Backtracking-based procedure (DPLL [1962])
- 80's - 90's: focus on variable selection heuristics
- Search-pruning techniques: Non-chronological backtracking, Learning clauses (Grasp [1996]) CDCL
- Indexing: two-watched literals (Zchaff, 2001)
- Scoring: deletion of bad learning clauses (Glucose, 2009)

Resolution

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

Exhaustive resolution is not practical:
exponential amount of memory

Resolution : State of the Procedure

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

$$\textsc{Resolve}\ \frac{C \vee l \in F \qquad D \vee \neg l \in F \qquad C \vee D \notin F}{F := F \cup \{C \vee D\}}$$

$$\textsc{Empty}\ \frac{l \in F \qquad \neg l \in F}{F := F \cup \bot}$$

$$\textsc{Tauto}\ \frac{F = F' \uplus \{C \vee l \vee \neg l\}}{F := F'}$$

$$\textsc{Subsume}\ \frac{F = F' \uplus \{C \vee D\} \qquad C \in F'}{F := F'}$$

$$\textsc{Fail}\ \frac{\bot \in F}{\text{return}\textsc{Unsat}}$$

Resolution : Example

$$F = \{\bar{1} \vee \bar{2} \vee 3,\ \bar{1} \vee 2,\ 1 \vee 3,\ \bar{3}\}$$

Resolution : Example

$$\textsc{Resolve}\ \frac{\bar{1} \vee \bar{2} \vee 3 \in F \qquad 1 \vee 3 \in F}{F := F \cup \{\bar{2} \vee 3\}}$$

$$F = \{\bar{1} \vee \bar{2} \vee 3,\ \bar{1} \vee 2,\ 1 \vee 3,\ \bar{3}\}$$

Resolution : Example

$$\textsc{Resolve}\ \frac{\bar{1} \vee \bar{2} \vee 3 \in F \qquad 1 \vee 3 \in F}{F := F \cup \{\bar{2} \vee 3\}}$$

$$F = \{\bar{1} \vee \bar{2} \vee 3,\ \bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3\}$$

Resolution : Example

$$\textsc{Subsume}\ \frac{F = F' \uplus \{\bar{1} \vee \bar{2} \vee 3\} \qquad \bar{2} \vee 3 \in F'}{F := F'}$$

$$F = \{\bar{1} \vee \bar{2} \vee 3,\ \bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3\}$$

Resolution : Example

$$\textsc{Subsume}\ \frac{F = F' \uplus \{\bar{1} \vee \bar{2} \vee 3\} \qquad \bar{2} \vee 3 \in F'}{F := F'}$$

$$F = \{\bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3\}$$

Resolution : Example

$$\textsc{Resolve}\ \frac{\bar{1} \vee 2 \in F \qquad 1 \vee 3 \in F}{F := F \cup \{2 \vee 3\}}$$

$$F = \{\bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3\}$$

Resolution : Example

$$\textsc{Resolve}\ \frac{\bar{1} \vee 2 \in F \qquad 1 \vee 3 \in F}{F := F \cup \{2 \vee 3\}}$$

$$F = \{\bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3,\ 2 \vee 3\}$$

Resolution : Example

$$\textsc{Resolve}\ \frac{\bar{2} \vee 3 \in F \qquad 2 \vee 3 \in F}{F := F \cup \{3\}}$$

$$F = \{\bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3, 2 \vee 3\}$$

Resolution : Example

$$\textsc{Resolve}\ \frac{\bar{2} \vee 3 \in F \qquad 2 \vee 3 \in F}{F := F \cup \{3\}}$$

$$F = \{\bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3, 2 \vee 3, 3\}$$

Resolution : Example

$$\textsc{Empty}\ \frac{3 \in F \qquad \bar{3} \in F}{F := F \cup \{\bot\}}$$

$$F = \{\bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3, 2 \vee 3, 3\}$$

Resolution : Example

$$\textsc{Empty}\ \frac{3 \in F \qquad \bar{3} \in F}{F := F \cup \{\bot\}}$$

$$F = \{\bar{1} \vee 2,\ 1 \vee 3,\ \bar{3},\ \bar{2} \vee 3, 2 \vee 3, 3, \bot\}$$

$$\textsc{Fail}\ \frac{\bot \in F}{\text{return } \textsc{Unsat}}$$

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

DPLL

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)

  $$\text{If } C \vee l \in F \text{ and } M \models \neg C \text{ then } l \text{ must be true}$$

- guessing the truth value of an unassigned literal

  If $M \cup \{l\}$ leads to a model for which F is unsatisfiable then backtrack and try $M \cup \{\neg l\}$

DPLL : State of the Procedure

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

$$\textsc{Success}\ \frac{M \models F}{\text{return}\ \ \textsc{Sat}}$$

$$\textsc{Unit}\ \frac{C \vee l \in F \qquad M \models \neg C \qquad l \text{ is undefined in } M}{M := l :: M}$$

$$\textsc{Decide}\ \frac{l \text{ is undefined in } M \qquad l \text{ (or } \neg l) \in F}{M := l^{@} :: M}$$

$$\textsc{Backtrack}\ \frac{\begin{array}{c} C \in F \quad M \models \neg C \quad M = M_1 :: l^{@} :: M_2 \\ M_1 \text{ contains no decision literals} \end{array}}{M := \neg l :: M_2}$$

$$\textsc{Fail}\ \frac{C \in F \qquad M \models \neg C \qquad M \text{ contains no decision literals}}{\text{return}\ \ \textsc{Unsat}}$$

DPLL : Example

$$M = []$$

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

DPLL : Example

$$\textsc{Decide}\ \frac{1 \text{ is undefined in } M \qquad \bar{1} \in F}{M := 1^{@} :: M}$$

$M = []$

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

DPLL : Example

$$\textsc{Decide}\ \frac{1 \text{ is undefined in } M \qquad \bar{1} \in F}{M := 1^{@} :: M}$$

$M = [1^{@}]$

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

DPLL : Example

$$\textsc{Unit}\ \frac{\bar{1} \vee 2 \in F \qquad M \models 1 \qquad 2 \text{ is undefined in } M}{M := 2 :: M}$$

$M = [1^{@}]$

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

DPLL : Example

$$\textsc{Unit}\ \frac{\bar{1} \vee 2 \in F \qquad M \models 1 \qquad 2 \text{ is undefined in } M}{M := 2 :: M}$$

$M = [2; 1^{@}]$

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

DPLL : Example

$$\textsc{Decide}\ \frac{3 \text{ is undefined in } M \qquad \bar{3} \in F}{M := 3^{@} :: M}$$

$M = [2; 1^{@}]$

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

DPLL : Example

$$\textsc{Decide}\ \frac{3 \text{ is undefined in } M \qquad \bar{3} \in F}{M := 3^{@} :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{\bar{3} \vee 4 \in F \qquad M \models 3 \qquad 4 \text{ is undefined in } M}{M := 4 :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{\bar{3} \vee 4 \in F \qquad M \models 3 \qquad 4 \text{ is undefined in } M}{M := 4 :: M}$$

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

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

DPLL : Example

$$\textsc{Decide}\ \frac{5 \text{ is undefined in } M \qquad \bar{5} \in F}{M := 5^{@} :: M}$$

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

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

DPLL : Example

$$\textsc{Decide}\ \frac{5 \text{ is undefined in } M \qquad \bar{5} \in F}{M := 5^{@} :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{\bar{5} \vee \bar{6} \in F \qquad M \models 5 \qquad \bar{6} \text{ is undefined in } M}{M := \bar{6} :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{\bar{5} \vee \bar{6} \in F \qquad M \models 5 \qquad \bar{6} \text{ is undefined in } M}{M := \bar{6} :: M}$$

$M = [\bar{6}; 5^{@}; 4; 3^{@}; 2; 1^{@}]$

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

DPLL : Example

$$\textsc{Backtrack}\ \frac{6 \vee \bar{5} \vee \bar{2} \in F \qquad M \models \bar{6} \wedge 5 \wedge 2 \qquad M = [6] :: 5^{@} :: [4; 3^{@}; 2; 1^{@}]}{M := \bar{5} :: [4; 3^{@}; 2; 1^{@}]}$$

$$M = [\bar{6}; 5^{@}; 4; 3^{@}; 2; 1^{@}]$$

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

DPLL : Example

$$\textsc{Backtrack}\ \frac{6 \lor \bar{5} \lor \bar{2} \in F \qquad M \models \bar{6} \land 5 \land 2 \qquad M = [6] :: 5^{@} :: [4; 3^{@}; 2; 1^{@}]}{M := \bar{5} :: [4; 3^{@}; 2; 1^{@}]}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

$$M = [7; \bar{5}; 4; 3^{@}; 2; 1^{@}]$$

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

DPLL : Example

$$\textsc{Backtrack}\ \frac{M \models \bar{5} \wedge 7 \wedge 2 \qquad \begin{array}{c} 5 \vee \bar{7} \vee \bar{2} \in F \\ M = [7; \bar{5}; 4] :: 3^{@} :: [2; 1^{@}] \end{array}}{M := \bar{3} :: [2; 1^{@}]}$$

$$M = [7; \bar{5}; 4; 3^{@}; 2; 1^{@}]$$

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

DPLL : Example

$$\textsc{Backtrack}\ \frac{M \models \bar{5} \wedge 7 \wedge 2 \qquad \begin{array}{c} 5 \vee \bar{7} \vee \bar{2} \in F \\ M = [7; \bar{5}; 4] :: 3^{@} :: [2; 1^{@}] \end{array}}{M := \bar{3} :: [2; 1^{@}]}$$

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

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

DPLL : Example

$$\textsc{Decide}\ \frac{5 \text{ is undefined in } M \qquad \bar{5} \in F}{M := 5^{@} :: M}$$

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

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

DPLL : Example

$$\textsc{Decide}\ \frac{5 \text{ is undefined in } M \qquad \bar{5} \in F}{M := 5^{@} :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{\bar{5} \vee \bar{6} \in F \qquad M \models 5 \qquad \bar{6} \text{ is undefined in } M}{M := \bar{6} :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{\bar{5} \vee \bar{6} \in F \qquad M \models 5 \qquad \bar{6} \text{ is undefined in } M}{M := \bar{6} :: M}$$

$M = [\bar{6}; 5^{@}; \bar{3}; 2; 1^{@}]$

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

DPLL : Example

$$\textsc{Backtrack}\ \frac{M \models \bar{6} \wedge 5 \wedge 2 \qquad 6 \vee \bar{5} \vee \bar{2} \in F \qquad M = [\bar{6}] :: 5^{@} :: [\bar{3}; 2; 1^{@}]}{M := \bar{5} :: [\bar{3}; 2; 1^{@}]}$$

$M = [\bar{6}; 5^{@}; \bar{3}; 2; 1^{@}]$

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

DPLL : Example

$$\textsc{Backtrack}\ \frac{\begin{array}{c} 6 \vee \bar{5} \vee \bar{2} \in F \\ M \models \bar{6} \wedge 5 \wedge 2 \qquad M = [\bar{6}] :: 5^{@} :: [\bar{3}; 2; 1^{@}] \end{array}}{M := \bar{5} :: [\bar{3}; 2; 1^{@}]}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

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

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

DPLL : Example

$$\textsc{Backtrack}\ \frac{M \models \bar{5} \wedge 7 \wedge 2 \qquad \overset{5 \vee \bar{7} \vee \bar{2} \in F}{M = [7; 5; \bar{3}; 2] :: 1@ :: []}}{M := \bar{1} :: []}$$

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

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

DPLL : Example

$$\textsc{Backtrack}\ \frac{5 \vee \bar{7} \vee \bar{2} \in F \qquad M \models \bar{5} \wedge 7 \wedge 2 \qquad M = [7; 5; \bar{3}; 2] :: 1@ :: []}{M := \bar{1} :: []}$$

$M = [\bar{1}]$

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

DPLL : Example

$$\textsc{Decide}\ \frac{\bar{3} \text{ is undefined in } M \qquad \bar{3} \in F}{M := \bar{3}^{@} :: M}$$

$M = [\bar{1}]$

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

DPLL : Example

$$\textsc{Decide}\ \frac{\bar{3} \text{ is undefined in } M \qquad \bar{3} \in F}{M := \bar{3}^{@} :: M}$$

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

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

DPLL : Example

$$\textsc{Decide}\ \frac{\bar{5} \text{ is undefined in } M \qquad \bar{5} \in F}{M := \bar{5}^{@} :: M}$$

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

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

DPLL : Example

$$\textsc{Decide}\ \frac{\bar{5} \text{ is undefined in } M \qquad \bar{5} \in F}{M := \bar{5}^{@} :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{5 \vee \bar{7} \vee \bar{2} \in F \qquad M \models \bar{5} \wedge 7 \qquad \bar{2} \text{ is undefined in } M}{M := \bar{2} :: M}$$

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

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

DPLL : Example

$$\textsc{Unit}\ \frac{5 \vee \bar{7} \vee \bar{2} \in F \qquad M \models \bar{5} \wedge 7 \qquad \bar{2} \text{ is undefined in } M}{M := \bar{2} :: M}$$

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

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

DPLL : Example

$$\textsc{Success}\ \frac{M \models F}{\text{return } \textsc{Sat}}$$

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

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

Backjumping

- The clause $6 \vee \bar{5} \vee \bar{2}$ is false in $[\bar{6}; 5^{@}; 4; 3^{@}; 2; 1^{@}]$
- It is also false in $[\bar{6}; 5^{@}; \quad ; 2; 1^{@}]$
- Instead of backtracking to $M = [\bar{5}; 4; 3^{@}; 2; 1^{@}]$, we would prefer to backjump directly to $M = [\bar{5}; 2; 1^{@}]$

Backjump Clauses

Conflict are reflected by backjump clauses

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

$$F \models \bar{1} \vee \bar{5}$$
$$F \models \bar{2} \vee \bar{5}$$

Given a backjump clause $C \vee l$, 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

$$\textsc{Backjump}\ \frac{C \in F \quad M \models \neg C \quad M = M_1 :: l^{@} :: M_2 \\ F \models C' \vee l' \quad M_2 \models \neg C' \\ l' \text{ is undefined in } M_2 \quad l' \text{ (or } \neg l') \in F}{M := l' :: M_2}$$

where $C' \vee l'$ is a backjump clause

Backjumping : Example

$M = []$

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

Backjumping : Example

$$\textsc{Decide}\ \frac{1 \text{ is undefined in } M \qquad \bar{1} \in F}{M := 1^{@} :: M}$$

$M = []$

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

Backjumping : Example

$$\textsc{Decide}\ \frac{1 \text{ is undefined in } M \qquad \bar{1} \in F}{M := 1^{@} :: M}$$

$M = [1^{@}]$

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

Backjumping : Example

$$\textsc{Unit}\ \frac{\bar{1} \vee 2 \in F \qquad M \models 1 \qquad 2 \text{ is undefined in } M}{M := 2 :: M}$$

$M = [1^{@}]$

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

Backjumping : Example

$$\textsc{Unit}\ \frac{\bar{1} \lor 2 \in F \qquad M \models 1 \qquad 2 \text{ is undefined in } M}{M := 2 :: M}$$

$M = [2; 1^{@}]$

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

Backjumping : Example

$$\textsc{Decide}\ \frac{3 \text{ is undefined in } M \qquad \bar{3} \in F}{M := 3^{@} :: M}$$

$M = [2; 1^{@}]$

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

Backjumping : Example

$$\textsc{Decide}\ \frac{3 \text{ is undefined in } M \qquad \bar{3} \in F}{M := 3^{@} :: M}$$

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

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

Backjumping : Example

$$\textsc{Unit}\ \frac{\bar{3} \vee 4 \in F \qquad M \models 3 \qquad 4 \text{ is undefined in } M}{M := 4 :: M}$$

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

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

Backjumping : Example

$$\textsc{Unit}\ \frac{\bar{3} \vee 4 \in F \qquad M \models 3 \qquad 4 \text{ is undefined in } M}{M := 4 :: M}$$

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

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

Backjumping : Example

$$\textsc{Decide}\ \frac{5 \text{ is undefined in } M \qquad \bar{5} \in F}{M := 5^{@} :: M}$$

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

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

Backjumping : Example

$$\textsc{Decide}\ \frac{5 \text{ is undefined in } M \qquad \bar{5} \in F}{M := 5^{@} :: M}$$

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

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

Backjumping : Example

$$\textsc{Unit}\ \frac{\bar{5} \vee \bar{6} \in F \qquad M \models 5 \qquad \bar{6} \text{ is undefined in } M}{M := \bar{6} :: M}$$

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

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

Backjumping : Example

$$\textsc{Unit}\ \frac{\bar{5} \vee \bar{6} \in F \qquad M \models 5 \qquad \bar{6} \text{ is undefined in } M}{M := \bar{6} :: M}$$

$$M = [\bar{6}; 5^{@}; 4; 3^{@}; 2; 1^{@}]$$

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

Backjumping : Example

$$\textsc{Backjump}\ \frac{\begin{array}{c} 6 \vee \bar{5} \vee \bar{2} \in F \\ M \models \bar{6} \wedge 5 \wedge 2 \qquad M = [6; 5^{@}; 4] :: 3^{@} :: [2; 1^{@}] \\ F \models \bar{2} \vee \bar{5} \qquad [2; 1^{@}] \models 2 \qquad \bar{5} \text{ is undefined in } [2; 1^{@}] \end{array}}{M := \bar{5} :: [2; 1^{@}]}$$

$$M = [\bar{6}; 5^{@}; 4; 3^{@}; 2; 1^{@}]$$

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

Backjumping : Example

$$\text{BACKJUMP}\ \frac{\begin{array}{c} 6 \vee \bar{5} \vee \bar{2} \in F \\ M \models \bar{6} \wedge 5 \wedge 2 \qquad M = [6; 5^{@}; 4] :: 3^{@} :: [2; 1^{@}] \\ F \models \bar{2} \vee \bar{5} \qquad [2; 1^{@}] \models 2 \qquad \bar{5} \text{ is undefined in } [2; 1^{@}] \end{array}}{M := \bar{5} :: [2; 1^{@}]}$$

$M = [\bar{5}; 2; 1^{@}]$

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

Backjumping : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

$M = [\bar{5}; 2; 1^{@}]$

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

Backjumping : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

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

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

Backjumping : Example

$$\textsc{Backjump}\ \frac{\begin{array}{c} 5 \vee \bar{7} \vee \bar{2} \in F \\ M \models \bar{5} \wedge 7 \wedge 2 \qquad M = [7; \bar{5}; 2] :: 1^{@} :: [] \\ F \models \bar{1} \qquad [] \models \mathit{true} \qquad \bar{1} \text{ is undefined in } [] \end{array}}{M := \bar{1} :: []}$$

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

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

Backjumping : Example

$$\textsc{Backjump}\ \frac{\begin{array}{c} 5 \vee \bar{7} \vee \bar{2} \in F \\ M \models \bar{5} \wedge 7 \wedge 2 \qquad M = [7; \bar{5}; 2] :: 1^{@} :: [] \\ F \models \bar{1} \qquad [] \models \mathit{true} \qquad \bar{1} \text{ is undefined in } [] \end{array}}{M := \bar{1} :: []}$$

$M = [\bar{1}]$

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

Backjumping : Example

$$\textsc{Decide}\ \frac{\bar{3} \text{ is undefined in } M \qquad \bar{3} \in F}{M := \bar{3}^{@} :: M}$$

$M = [\bar{1}]$

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

Backjumping : Example

$$\textsc{Decide}\ \frac{\bar{3} \text{ is undefined in } M \qquad \bar{3} \in F}{M := \bar{3}^{@} :: M}$$

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

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

Backjumping : Example

$$\textsc{Decide}\ \frac{\bar{5} \text{ is undefined in } M \qquad \bar{5} \in F}{M := \bar{5}^{@} :: M}$$

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

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

Backjumping : Example

$$\textsc{Decide}\ \frac{\bar{5} \text{ is undefined in } M \qquad \bar{5} \in F}{M := \bar{5}^{@} :: M}$$

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

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

Backjumping : Example

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

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

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

$$\textsc{Unit}\ \frac{5 \vee 7 \in F \qquad M \models \bar{5} \qquad 7 \text{ is undefined in } M}{M := 7 :: M}$$

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

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

Backjumping : Example

$$\textsc{Unit}\ \frac{5 \vee \bar{7} \vee \bar{2} \in F \qquad M \models \bar{5} \wedge 7 \qquad \bar{2} \text{ is undefined in } M}{M := \bar{2} :: M}$$

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

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

Backjumping : Example

$$\textsc{Unit}\ \frac{5 \vee \bar{7} \vee \bar{2} \in F \qquad M \models \bar{5} \wedge 7 \qquad \bar{2} \text{ is undefined in } M}{M := \bar{2} :: M}$$

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

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

Backjumping : Example

$$\textsc{Success}\ \frac{M \models F}{\text{return } \textsc{Sat}}$$

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

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

CDCL

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

$$\textsc{Learn}\ \frac{F \models C \quad \text{each atom of } C \text{ occurs in } F \text{ or } M}{F := F \cup \{C\}}$$

Lemmas can also be removed from M

$$\textsc{Forget}\ \frac{F = F' \uplus C \qquad F' \models C}{F := F'}$$

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

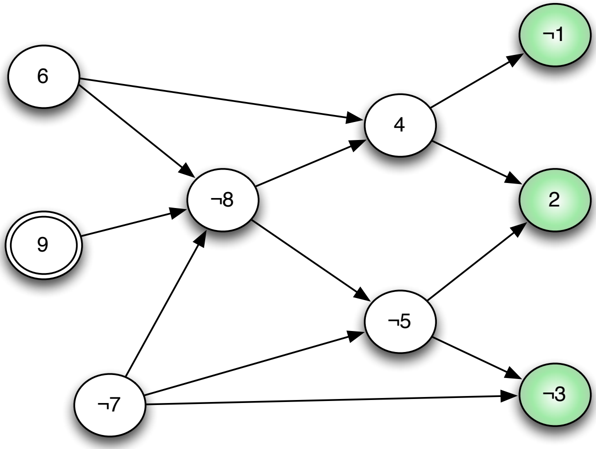
Implication Graph

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 $l_1 \vee \ldots \vee l_n \vee l$ 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 $\neg l_i \to l$, for $1 \leq i \leq n$ (if not already present)

(Partial) implication graph for the following state of DPLL

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$



Cutting the Implication Graph

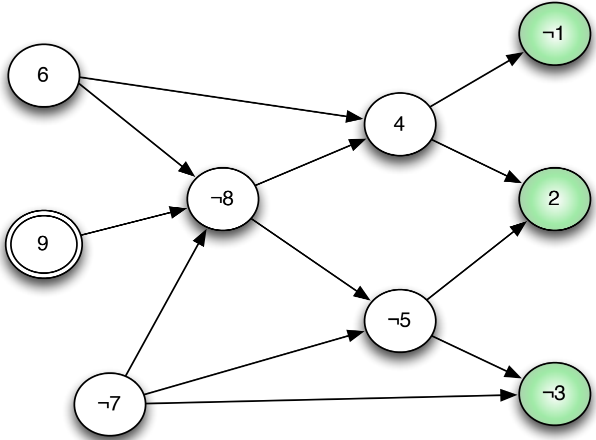
To extract backjump clauses, we first cut the implication graph in two parts:

- the first part must contains (at least) all the nodes with no incoming arrows
- the second part must contains (at least) all the nodes with no outgoing arrows

The literals whose outgoing edges are cut form a backjump clause provided that exactly one of these literals belongs to the current decision level.

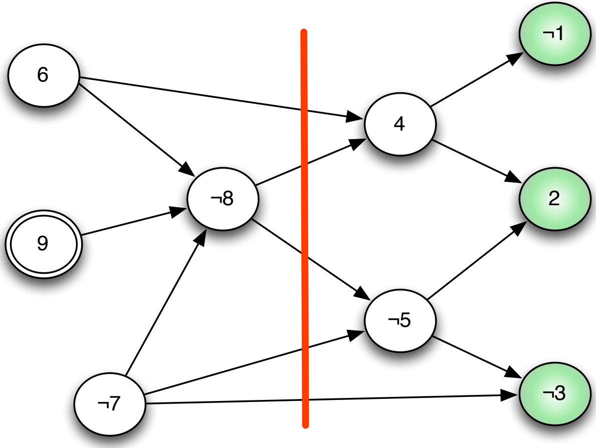
Cutting the Implication Graph: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$



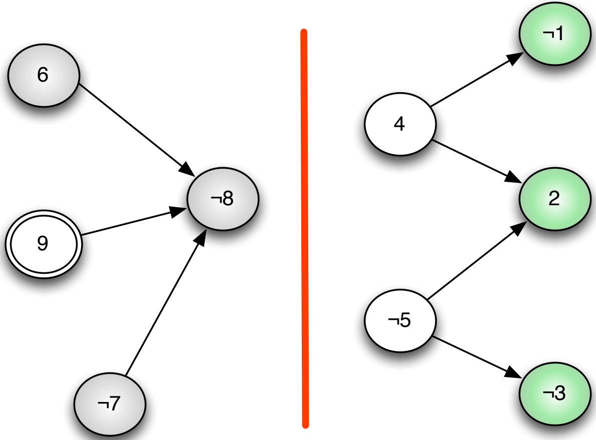
Cutting the Implication Graph: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$



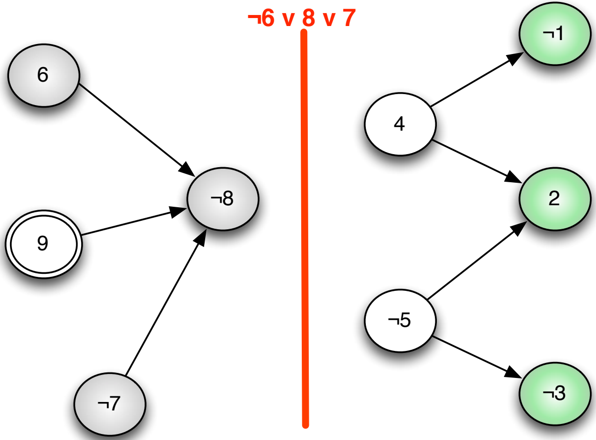
Cutting the Implication Graph: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$



Cutting the Implication Graph: Example

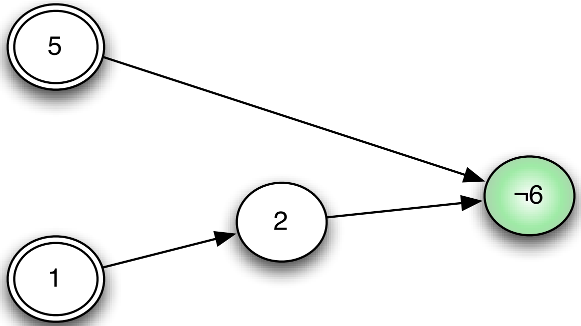
$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$



Cutting the Implication Graph : Other Example

In the first example, Backjump is applied for the first time when

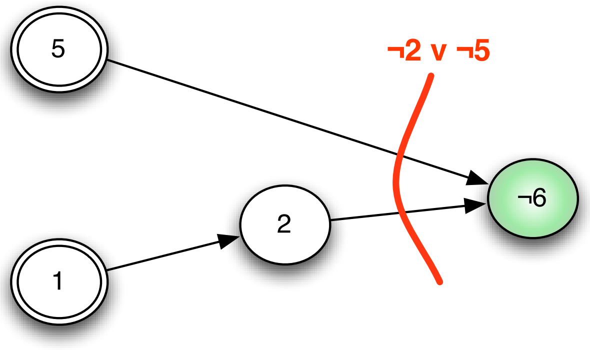
$F = \{\bar{1} \vee 2, \bar{3} \vee 4, \bar{5} \vee \bar{6}, 6 \vee \bar{5} \vee \bar{2}, 5 \vee 7, 5 \vee \bar{7} \vee \bar{2}\}$
$M = [\bar{6}; 5^{@}; 4; 3^{@}; 2; 1^{@}]$



Cutting the Implication Graph : Other Example

In the first example, Backjump is applied for the first time when

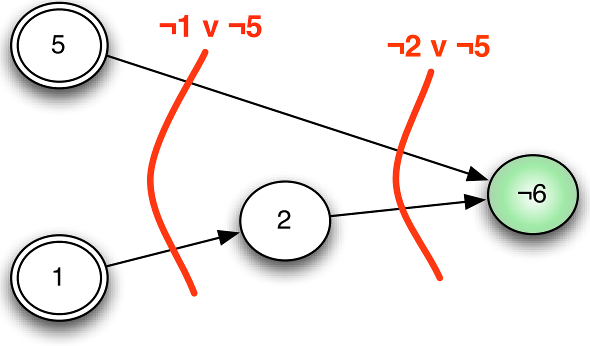
$F = \{\bar{1} \vee 2, \bar{3} \vee 4, \bar{5} \vee \bar{6}, 6 \vee \bar{5} \vee \bar{2}, 5 \vee 7, 5 \vee \bar{7} \vee \bar{2}\}$
$M = [\bar{6}; 5^{@}; 4; 3^{@}; 2; 1^{@}]$



Cutting the Implication Graph : Other Example

In the first example, Backjump is applied for the first time when

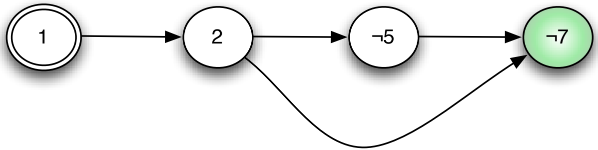
$F = \{\bar{1} \vee 2, \bar{3} \vee 4, \bar{5} \vee \bar{6}, 6 \vee \bar{5} \vee \bar{2}, 5 \vee 7, 5 \vee \bar{7} \vee \bar{2}\}$
$M = [\bar{6}; 5^{@}; 4; 3^{@}; 2; 1^{@}]$



Cutting the Implication Graph : Other Example

When Backjump is applied for the second time, we have

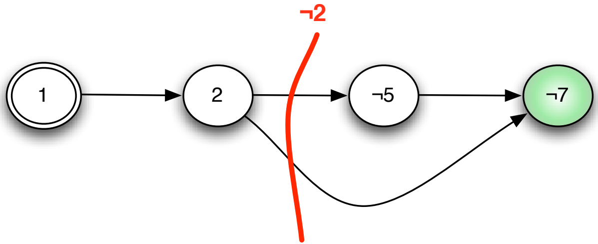
$F = \{\bar{1} \vee 2, \bar{3} \vee 4, \bar{5} \vee \bar{6}, 6 \vee \bar{5} \vee \bar{2}, 5 \vee 7, 5 \vee \bar{7} \vee \bar{2}\}$
$M = [7; \bar{5}; 2; 1^{@}]$



Cutting the Implication Graph : Other Example

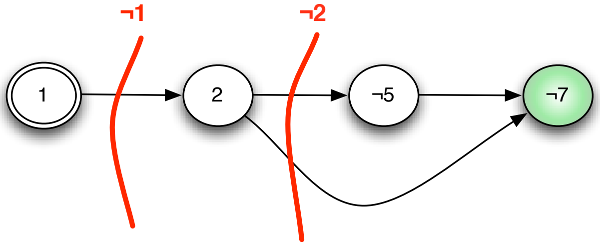
When Backjump is applied for the second time, we have

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



When Backjump is applied for the second time, we have

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



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

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$R = 1 \vee \bar{2} \vee 3$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = 1 \vee \bar{2} \vee 3 \qquad 5 \vee 7 \vee \bar{3} \in F}{R := 5 \vee 7 \vee 1 \vee \bar{2}}$$

$$R = 1 \vee \bar{2} \vee 3$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = 1 \vee \bar{2} \vee 3 \qquad 5 \vee 7 \vee \bar{3} \in F}{R := 5 \vee 7 \vee 1 \vee \bar{2}}$$

$$R = 5 \vee 7 \vee 1 \vee \bar{2}$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = 5 \vee 7 \vee 1 \vee \bar{2} \qquad \bar{4} \vee 5 \vee 2 \in F}{R := \bar{4} \vee 5 \vee 7 \vee 1}$$

$$R = 5 \vee 7 \vee 1 \vee \bar{2}$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = 5 \vee 7 \vee 1 \vee \bar{2} \qquad \bar{4} \vee 5 \vee 2 \in F}{R := \bar{4} \vee 5 \vee 7 \vee 1}$$

$$R = \bar{4} \vee 5 \vee 7 \vee 1$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = \bar{4} \vee 5 \vee 7 \vee 1 \qquad \bar{4} \vee \bar{1} \in F}{R := 5 \vee 7 \vee \bar{4}}$$

$$R = \bar{4} \vee 5 \vee 7 \vee 1$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = \bar{4} \vee 5 \vee 7 \vee 1 \qquad \bar{4} \vee \bar{1} \in F}{R := 5 \vee 7 \vee \bar{4}}$$

$$R = 5 \vee 7 \vee \bar{4}$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = 5 \vee 7 \vee \bar{4} \qquad \bar{6} \vee 8 \vee 4 \in F}{R := \bar{6} \vee 8 \vee 7 \vee 5}$$

$$R = 5 \vee 7 \vee \bar{4}$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = 5 \vee 7 \vee \bar{4} \qquad \bar{6} \vee 8 \vee 4 \in F}{R := \bar{6} \vee 8 \vee 7 \vee 5}$$

$$R = \bar{6} \vee 8 \vee 7 \vee 5$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\textsc{Resolve}\ \frac{R = \bar{6} \vee 8 \vee 7 \vee 5 \qquad 8 \vee 7 \vee \bar{5} \in F}{R := 8 \vee 7 \vee \bar{6}}$$

$$R = \bar{6} \vee 8 \vee 7 \vee 5$$

Backward Conflict Resolution: Example

$F = \{\bar{9} \vee \bar{6} \vee 7 \vee \bar{8}, 8 \vee 7 \vee \bar{5}, \bar{6} \vee 8 \vee 4, \bar{4} \vee \bar{1}, \bar{4} \vee 5 \vee 2, 5 \vee 7 \vee \bar{3}, 1 \vee \bar{2} \vee 3\}$
$M = [\bar{3}; 2; \bar{1}; 4; \bar{5}; \bar{8}; 9^{@}; \ldots; \bar{7}; \ldots; 6; \ldots]$

$$\text{RESOLVE}\ \frac{R = \bar{6} \vee 8 \vee 7 \vee 5 \qquad 8 \vee 7 \vee \bar{5} \in F}{R := 8 \vee 7 \vee \bar{6}}$$

$$R = 8 \vee 7 \vee \bar{6}$$

CDCL + Resolution + Learning + Restart

When $\mathit{Mode} = \text{search}$

$$\textsc{Success}\ \frac{M \models F}{\text{return}\quad \textsc{Sat}}$$

$$\textsc{Unit}\ \frac{C \vee l \in F \qquad M \models \neg C \qquad l \text{ is undefined in } M}{M := l_{C \vee l} :: M}$$

$$\textsc{Decide}\ \frac{l \text{ is undefined in } M \qquad l \text{ (or } \neg l) \in F}{M := l :: M}$$

$$\textsc{Conflict}\ \frac{C \in F \qquad M \models \neg C}{R := C;\ \mathit{Mode} := \text{resolution}}$$

When $\mathit{Mode} = \text{resolution}$

$$\textsc{Fail}\ \frac{R = \bot}{\text{return}\ \ \textsc{Unsat}}$$

$$\textsc{Resolve}\ \frac{R = C \vee \neg l \qquad l_{D \vee l} \in M}{R := C \vee D}$$

$$\textsc{Backjump}\ \frac{\begin{array}{ll} R = C \vee l & M = M_1 :: l' :: M_2 \\ M_2 \models \neg C & l \text{ is undefined in } M_2 \end{array}}{M := l_{C \vee l} :: M_2;\ \ \mathit{Mode} := \text{search}}$$

When Mode = resolution

$$\textsc{Learn}\ \frac{R \notin F}{F := F \cup \{R\}}$$

When Mode = search

$$\textsc{Forget}\ \frac{C \text{ is a learned clause}}{F := F \setminus \{C\}}$$

$$\textsc{Restart}\ \frac{}{M := \emptyset}$$

CDCL + Resolution : Example

$Mode = \textit{search}$

$M = []$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Decide}\ \frac{1 \text{ is undefined in } M \qquad \bar{1} \in F}{M := 1 :: M}$$

$Mode = \textit{search}$

$M = []$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Decide}\ \frac{1 \text{ is undefined in } M \qquad \bar{1} \in F}{M := 1 :: M}$$

$Mode = \textit{search}$

$M = [1]$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Unit}\ \frac{\bar{1} \vee 2 \in F \qquad M \models 1 \qquad 2 \text{ is undefined in } M}{M := 2_{\bar{1}\vee 2} :: M}$$

$Mode = \textcolor{blue}{search}$

$M = [1]$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Unit}\ \frac{\bar{1} \vee 2 \in F \qquad M \models 1 \qquad 2 \text{ is undefined in } M}{M := 2_{\bar{1}\vee 2} :: M}$$

$Mode = \textcolor{blue}{search}$

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

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

$R =$

CDCL + Resolution : Example

$$\textsc{Decide}\ \frac{3 \text{ is undefined in } M \qquad \bar{3} \in F}{M := 3 :: M}$$

$Mode = \textit{search}$

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

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

$R =$

CDCL + Resolution : Example

$$\textsc{Decide}\ \frac{3 \text{ is undefined in } M \qquad \bar{3} \in F}{M := 3 :: M}$$

$Mode = \textcolor{blue}{search}$

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

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

$R =$

CDCL + Resolution : Example

$$\textsc{Unit}\ \frac{\bar{3} \vee 4 \in F \qquad M \models 3 \qquad 4 \text{ is undefined in } M}{M := 4_{\bar{3} \vee 4} :: M}$$

$Mode = \textit{search}$

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

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

$R =$

CDCL + Resolution : Example

$$\textsc{Unit}\ \frac{\bar{3} \vee 4 \in F \qquad M \models 3 \qquad 4 \text{ is undefined in } M}{M := 4_{\bar{3} \vee 4} :: M}$$

$Mode = \textit{search}$

$M = [4_{\bar{3}\vee 4}; 3; 2_{\bar{1}\vee 2}; 1]$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Decide}\ \frac{5 \text{ is undefined in } M \qquad \bar{5} \in F}{M := 5 :: M}$$

$Mode = \mathit{search}$

$M = [4_{\bar{3} \vee 4}; 3; 2_{\bar{1} \vee 2}; 1]$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Decide}\ \frac{5 \text{ is undefined in } M \qquad \bar{5} \in F}{M := 5 :: M}$$

$Mode = \textit{search}$

$M = [5; 4_{\bar{3}\vee 4}; 3; 2_{\bar{1}\vee 2}; 1]$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Unit}\ \frac{\bar{5} \vee \bar{6} \in F \qquad M \models 5 \qquad \bar{6} \text{ is undefined in } M}{M := \bar{6}_{\bar{5} \vee \bar{6}} :: M}$$

$Mode = search$

$M = [5; 4_{\bar{3} \vee 4}; 3; 2_{\bar{1} \vee 2}; 1]$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Unit}\ \frac{\bar{5} \vee \bar{6} \in F \qquad M \models 5 \qquad \bar{6} \text{ is undefined in } M}{M := \bar{6}_{\bar{5}\vee\bar{6}} :: M}$$

$Mode = $ *search*

$M = [6_{\bar{5}\vee\bar{6}}; 5; 4_{\bar{3}\vee 4}; 3; 2_{\bar{1}\vee 2}; 1]$

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

CDCL + Resolution : Example

$$\textsc{Conflict}\ \frac{6 \vee \bar{5} \vee \bar{2} \in F \qquad M \models \bar{6} \wedge 5 \wedge 2}{R := 6 \vee \bar{5} \vee \bar{2};\ Mode := \text{resolution}}$$

$Mode = \textit{search}$

$M = [6_{\bar{5}\vee\bar{6}}; 5; 4_{\bar{3}\vee 4}; 3; 2_{\bar{1}\vee 2}; 1]$

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

$R =$

CDCL + Resolution : Example

$$\textsc{Conflict}\ \frac{6 \vee \bar{5} \vee \bar{2} \in F \qquad M \models \bar{6} \wedge 5 \wedge 2}{R := 6 \vee \bar{5} \vee \bar{2};\ \mathit{Mode} := \text{resolution}}$$

$\mathit{Mode} = \mathit{resolution}$

$M = [6_{\bar{5}\vee\bar{6}}; 5; 4_{\bar{3}\vee 4}; 3; 2_{\bar{1}\vee 2}; 1]$

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

$R = 6 \vee \bar{5} \vee \bar{2}$

CDCL + Resolution : Example

$$\textsc{Resolve}\ \frac{R = 6 \vee \bar{5} \vee \bar{2} \qquad 6_{\bar{5}\vee\bar{6}} \in M}{R := \bar{2} \vee \bar{5}}$$

$Mode = \mathit{resolution}$

$M = [6_{\bar{5}\vee\bar{6}}; 5; 4_{\bar{3}\vee 4}; 3; 2_{\bar{1}\vee 2}; 1]$

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

$R = 6 \vee \bar{5} \vee \bar{2}$

CDCL + Resolution : Example

$$\textsc{Resolve}\ \frac{R = 6 \vee \bar{5} \vee \bar{2} \qquad 6_{\bar{5}\vee\bar{6}} \in M}{R := \bar{2} \vee \bar{5}}$$

$Mode = \textit{resolution}$

$M = [6_{\bar{5}\vee\bar{6}}; 5; 4_{\bar{3}\vee 4}; 3; 2_{\bar{1}\vee 2}; 1]$

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

$R = \bar{2} \vee \bar{5}$

CDCL + Resolution : Example

$$\textsc{Backjump}\ \frac{\begin{array}{c} R = \bar{2} \vee \bar{5} \\ M = [6_{\bar{5}\vee\bar{6}}; 5; 4_{\bar{3}\vee 4}] :: 3 :: [2_{\bar{1}\vee 2}; 1] \\ [2_{\bar{1}\vee 2}; 1] \models 2 \\ \bar{5} \text{ undefined in } [2_{\bar{1}\vee 2}; 1] \end{array}}{M := \bar{5}_{\bar{2}\vee\bar{5}} :: [2_{\bar{1}\vee 2}; 1]; \mathit{Mode} := \text{search}}$$

$\mathit{Mode} = \mathit{resolution}$

$M = [6_{\bar{5}\vee\bar{6}}; 5; 4_{\bar{3}\vee 4}; 3; 2_{\bar{1}\vee 2}; 1]$

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

$R = \bar{2} \vee \bar{5}$

CDCL + Resolution : Example

$$\textsc{Backjump}\ \frac{\begin{array}{c} R = \bar{2} \vee \bar{5} \\ M = [6_{\bar{5}\vee\bar{6}}; 5; 4_{\bar{3}\vee 4}] :: 3 :: [2_{\bar{1}\vee 2}; 1] \\ [2_{\bar{1}\vee 2}; 1] \models 2 \\ \bar{5} \text{ undefined in } [2_{\bar{1}\vee 2}; 1] \end{array}}{M := \bar{5}_{\bar{2}\vee\bar{5}} :: [2_{\bar{1}\vee 2}; 1]; \mathit{Mode} := \text{search}}$$

$\mathit{Mode} = \mathit{search}$

$M = [\bar{5}_{\bar{2}\vee\bar{5}}; 2_{\bar{1}\vee 2}; 1]$

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

$R =$

etc.

$$Mode = \mathit{search}$$

$$M = [\bar{5}_{\bar{2} \vee \bar{5}}; 2_{\bar{1} \vee 2}; 1]$$

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

$$R =$$

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

Indexing

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