Lecture 9
Implementing a SAT Solver

Zvonimir Rakamarić
University of Utah

SAT Solver

- Decides Boolean satisfiability
  - Satisfiability of propositional logic formulas

- Usages:
  - Software and hardware verification
  - Automatic test case generation
  - Planning
  - Scheduling
  - …

- Many popular solvers: minisat, picosat,…

Why SAT Solver?

- Well-specified and relatively simple input format
- Many other SAT solvers available
- Many benchmarks available
- Output is easy to check
- Problem people and companies care about
- We should be able to
  - Test, test, test
  - Write assertions
  - Debug, profile, optimize
  - Run other tools (valgrind!)
  - Do code reviews

Homework Assignment

- Implement a SAT solver
- Teams of 4:
  - Testing infrastructure
  - Input processing and error checking
  - Core algorithm (2 people)
- Profiling and optimizations
- Use github for team work (issues, good commit messages)
- Shuffling of teams and team members
- In-class SAT solver competition

Syntax of Propositional Logic (PL)

truth_symbol ::= $\top$ (true), $\bot$ (false)

variable ::= p, q, r, …

atom ::= truth_symbol | variable

literal ::= atom | $\neg$atom

formula ::= literal |
$\neg$formula |
formula $\wedge$ formula |
formula $\vee$ formula |
formula $\rightarrow$ formula |
formula $\leftrightarrow$ formula

Examples of PL Formulae

$F : \top$

$F : \mathrm{p}$

$F : \neg p$

$F : (p \wedge q) \rightarrow (p \vee \neg q)$

$F : (p \vee \neg q \vee r) \wedge (q \vee \neg r)$

$F : (\neg p \vee q) \leftrightarrow (p \rightarrow q)$

$F : p \leftrightarrow (q \rightarrow r)$

Example

$F : (p \wedge q) \rightarrow (p \vee \neg q)$
$I : \{p \mapsto 1, q \mapsto 0\}$
(i.e., $I[p] = 1$, $I[q] = 0$)

p	q	$\neg q$	$p \wedge q$	$p \vee \neg q$	F
1	0	1	0	1	1

F evaluates to *true* under I or $I[F] = \textit{true}$ or $I \models F$...

Interpretation I is a model of F

I satisfies F

Satisfiability and Validity

- F is satisfiable iff (if and only if) there exists I such that $I \models F$
  - Otherwise, F is unsatisfiable
- F is valid iff for all I, $I \models F$
  - Otherwise, F is invalid
- We write $\models F$ if F is valid
- Duality between satisfiablity and validity:

$$F \text{ is valid iff } \neg F \text{ is unsatisfiable}$$

  Note: only holds if logic is closed under negation

Decision Procedure for Satisfiability

- Algorithm that in some finite amount of computation decides if given PL formula *F* is satisfiable
  - NP-complete problem
- Modern decision procedures for PL formulae are called *SAT solvers*
- Naïve approach
  - Enumerate truth table
- Modern SAT solvers
  - DPLL algorithm
    - Davis-Putnam-Logemann-Loveland
  - Operates on Conjunctive Normal Form (CNF)

Normal Forms

- Negation Normal Form (NNF)
  - Only allows $\neg$, $\wedge$, $\vee$
  - Negation only in literals

- Disjunctive Normal Form (DNF)
  - Disjunction of conjunction of literals

- Conjunctive Normal Form (CNF)
  - Conjunction of disjunction of literals

DPLL Algorithm

- Davis–Putnam–Logemann–Loveland
- Introduced in 1962 by Martin Davis, Hilary Putnam, George Logemann, and Donald W. Loveland
- Refinement of earlier Davis–Putnam algorithm

Classical DPLL

- Searching for a model *M* for a given CNF formula *F*
  - Incrementally try to build a model *M*
  - Maintain state during search
- State is a pair $M \mid F$
  - *F* is a set of clauses and it doesn't change during search
  - *M* is a sequence of literals
    - No literals appear twice and no contradiction
    - Order does matter
    - Decision literals marked with l^d

Abstract Transition System

- Contains a set of rules of the form

$$M \mid F \Longrightarrow M' \mid F'$$

  denoting that search can move from state $M \mid F$ to state $M' \mid F'$

DPLL Rules – Extending *M*

- Propagate

$$M \mid G, C \vee l \;\Rightarrow\; M, l \mid G, C \vee l$$

if $M \models \neg C$ and l not in M

- Decide

$$M \mid F \;\Rightarrow\; M, l^d \mid F$$

if l or $\neg l$ in F and l not in M

DPLL Rules – Adjusting *M*

- Fail

$M \mid G, C \implies \mathit{fail}$
  if $M \models \neg C$ and M contains no decision literals

- Backtrack

$M, l^d, N \mid G, C \implies M, \neg l \mid G, C$
  if $M, l^d, N \models \neg C$ and N contains no decision literals

- Propagate

$M \mid G, C \vee l \;\Rightarrow\; M, l \mid G, C \vee l$
if $M \models \neg C$ and l not in M

- Decide

$M \mid F \;\Rightarrow\; M, l^d \mid F$
if l or $\neg l$ in F and l not in M

- Fail

$M \mid G, C \;\Rightarrow\; \mathit{fail}$
if $M \models \neg C$ and M contains no decision literals

- Backtrack

$M, l^d, N \mid G, C \;\Rightarrow\; M, \neg l \mid G, C$
if $M, l^d, N \models \neg C$ and N contains no decision literals

DPLL Example 1

$\emptyset \quad \| \quad \neg p \vee q \vee r,\ p,\ \neg q \vee r,\ \neg q \vee \neg r,\ q \vee r,\ q \vee \neg r$

DPLL Example 2

$\emptyset \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$

DPLL Example 2

$\emptyset \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \quad \Rightarrow$ (Decide p)

DPLL Example 2

$\emptyset \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \quad \Rightarrow$ (Decide p)

$p^d \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$

DPLL Example 2

$\emptyset \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \quad \Longrightarrow$ (Decide p)

$p^d \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \quad \Longrightarrow$ (Propagate q)

DPLL Example 2

$\emptyset \;\|\; \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Decide p)

$p^d \;\|\; \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Propagate q)

$p^d, q \;\|\; \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$

DPLL Example 2

$\emptyset$	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide p)
p^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate q)
p^d, q	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide r)

DPLL Example 2

$\emptyset$	$\Vert\ \neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Decide p)
p^d	$\Vert\ \neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Propagate q)
p^d, q	$\Vert\ \neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Decide r)
p^d, q, r^d	$\Vert\ \neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	

DPLL Example 2

$\emptyset \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \quad \Rightarrow$ (Decide p)

$p^d \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \quad \Rightarrow$ (Propagate q)

$p^d, q \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \quad \Rightarrow$ (Decide r)

$p^d, q, r^d \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \quad \Rightarrow$ (Propagate s)

DPLL Example 2

$\emptyset$	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide p)
p^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate q)
p^d, q	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide r)
p^d, q, r^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate s)
p^d, q, r^d, s	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	

DPLL Example 2

$\emptyset$	$\Vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Decide p)
p^d	$\Vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Propagate q)
p^d, q	$\Vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Decide r)
p^d, q, r^d	$\Vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Propagate s)
p^d, q, r^d, s	$\Vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Decide t)

DPLL Example 2

$\emptyset$	$\|$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Decide p)
p^d	$\|$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Propagate q)
p^d, q	$\|$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Decide r)
p^d, q, r^d	$\|$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Propagate s)
p^d, q, r^d, s	$\|$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Decide t)
p^d, q, r^d, s, t^d	$\|$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	

DPLL Example 2

$\emptyset$	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide p)
p^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate q)
p^d, q	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide r)
p^d, q, r^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate s)
p^d, q, r^d, s	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide t)
p^d, q, r^d, s, t^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate $\neg u$)

DPLL Example 2

$\emptyset \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \ \Rightarrow$ (Decide p)

$p^d \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \ \Rightarrow$ (Propagate q)

$p^d, q \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \ \Rightarrow$ (Decide r)

$p^d, q, r^d \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \ \Rightarrow$ (Propagate s)

$p^d, q, r^d, s \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \ \Rightarrow$ (Decide t)

$p^d, q, r^d, s, t^d \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \ \Rightarrow$ (Propagate $\neg u$)

$p^d, q, r^d, s, t^d, \neg u \quad \| \quad \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$

DPLL Example 2

$\emptyset$	$\parallel$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Decide p)
p^d	$\parallel$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Propagate q)
p^d, q	$\parallel$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Decide r)
p^d, q, r^d	$\parallel$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Propagate s)
p^d, q, r^d, s	$\parallel$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Decide t)
p^d, q, r^d, s, t^d	$\parallel$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Propagate $\neg u$)
$p^d, q, r^d, s, t^d, \neg u$	$\parallel$	$\neg p \lor q,\ \neg r \lor s,\ \neg t \lor \neg u,\ u \lor \neg t \lor \neg q$	$\Rightarrow$ (Backtrack)

DPLL Example 2

$\emptyset$	$\vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Decide p)
p^d	$\vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Propagate q)
p^d, q	$\vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Decide r)
p^d, q, r^d	$\vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Propagate s)
p^d, q, r^d, s	$\vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Decide t)
p^d, q, r^d, s, t^d	$\vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Propagate $\neg u$)
$p^d, q, r^d, s, t^d, \neg u$	$\vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Longrightarrow$ (Backtrack)
$p^d, q, r^d, s, \neg t$	$\vert$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	

DPLL Example 2

$\emptyset$	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide p)
p^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate q)
p^d, q	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide r)
p^d, q, r^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate s)
p^d, q, r^d, s	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide t)
p^d, q, r^d, s, t^d	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Propagate $\neg u$)
$p^d, q, r^d, s, t^d, \neg u$	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Backtrack)
$p^d, q, r^d, s, \neg t$	$\parallel$	$\neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$	$\Rightarrow$ (Decide u)

DPLL Example 2

$\emptyset \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Decide p)

$p^d \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Propagate q)

$p^d, q \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Decide r)

$p^d, q, r^d \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Propagate s)

$p^d, q, r^d, s \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Decide t)

$p^d, q, r^d, s, t^d \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Propagate $\neg u$)

$p^d, q, r^d, s, t^d, \neg u \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Backtrack)

$p^d, q, r^d, s, \neg t \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q \;\Rightarrow$ (Decide u)

$p^d, q, r^d, s, \neg t, u^d \mid \neg p \vee q,\ \neg r \vee s,\ \neg t \vee \neg u,\ u \vee \neg t \vee \neg q$

Modern SAT Solvers: DPLL+more

- Backjumping
- Dynamic variable ordering
- Learning conflict clauses
- Random restarts
- Parallel SAT solver
  - Hard to beat sequential version
- …

Input Format

```
c
c start with comments
c
p cnf 5 3
1 -5 4 0
-1 5 3 4 0
-3 -4 0
```

Useful Links

- http://baldur.iti.kit.edu/sat-race-2015/
- http://www.satcompetition.org/2014/
- http://www.cs.cornell.edu/gomes/papers/satsolvers-kr-handbook.pdf
- https://en.wikipedia.org/wiki/Boolean_satisfiability_problem
- https://en.wikipedia.org/wiki/DPLL_algorithm
- http://people.mpi-inf.mpg.de/~sofronie/lecture-ar-09/slides/lecture-14-may.pdf
- http://people.mpi-inf.mpg.de/~sofronie/lecture-ar-09/slides/lecture-14-may.pdf
- http://webcourse.cs.technion.ac.il/236342/Winter2011-2012/ho/WCFiles/Tut14.pdf