SAT : À l'assaut des problèmes difficiles

Laurent Simon Labri, Bordeaux, France

common work with

Gilles Audemard CRIL, Lens, France

Why studying SAT ?

A general perspective

SAT, the canonical NP-Complete problem. A one-million dollar question (is NP=P ?)

- The main open problem of Theoretical Computer Science
- The easiest of the hard problems
- We must face it in most of real-world problems

S. Aaronson, MIT : « **If P = NP**, then the world would be a profoundly different place than we usually assume it to be. There would be no special value in creative leaps, no fundamental gap between solving a problem and recognizing the solution once its found. **Everyone who could appreciate a symphony would be Mozart ; everyone who could follow a step-by-step argument would be Gauss.** » [1]

1. from [Vardi, 2015]

Why working on SAT Solvers ?

From an AI perspective

SAT is hidden in many (logical / reasoning) AI problems

A pragmatic AI researcher approach :

"You can't solve this (interesting) problem ? Let's have a look"

A fascinating power of a very simple logic

- A simple language with complex problems
- A logic formalized more than 2000 years ago by **Aristotle** himself
- The simplest of the hardest (interesting ?) problems

Why using SAT Solvers ?

From an industrial perspective

Any NP-Complete problems can be reduced to SAT.

Many NP-Complete problems can be **efficiently** encoded into SAT

SAT solvers are highly efficient **black boxes**, **freely available**

They can even be used as NP Oracles (many calls to SAT per seconds)

The SAT community is partially driven by solvers performances

Why listening to a talk about SAT ?

From an audience perspective

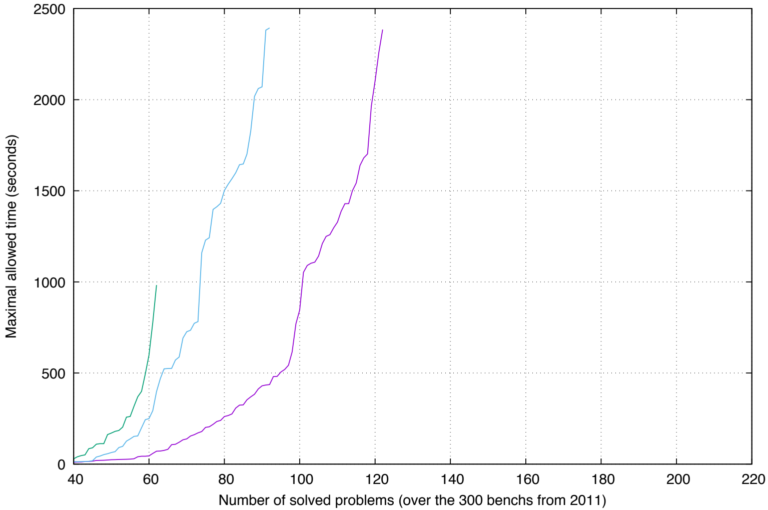
We observed a **major breakthrough** in the practical solving of SAT problems (2001)

Many high-level results from SAT can be applied to other AI fields

- Random Problems ?
- Algorithms Comparisons ?
- AI : To think or to try ?

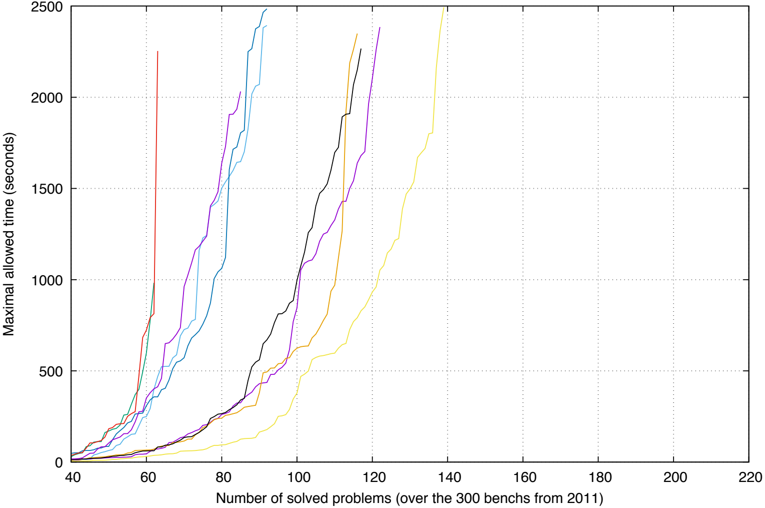
Moshe Vardi talks about **Deep Solving** to advertise the progresses observed in the field.

Performances of SAT Solvers, after 2001



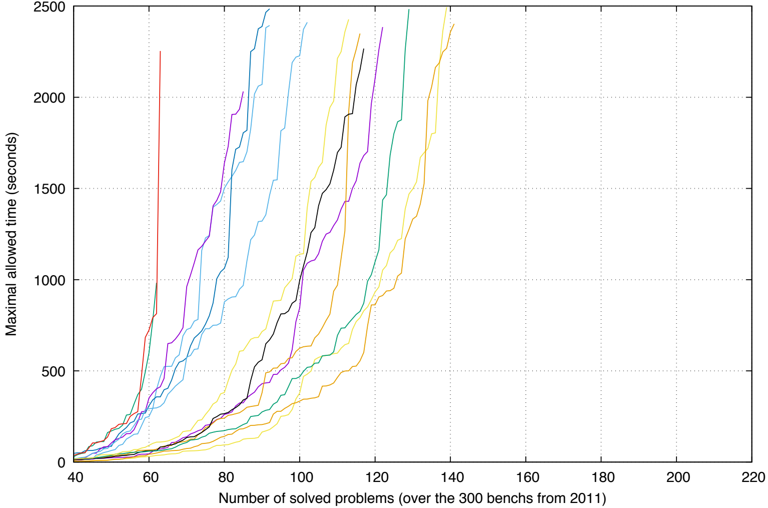
2002

Performances of SAT Solvers, after 2001



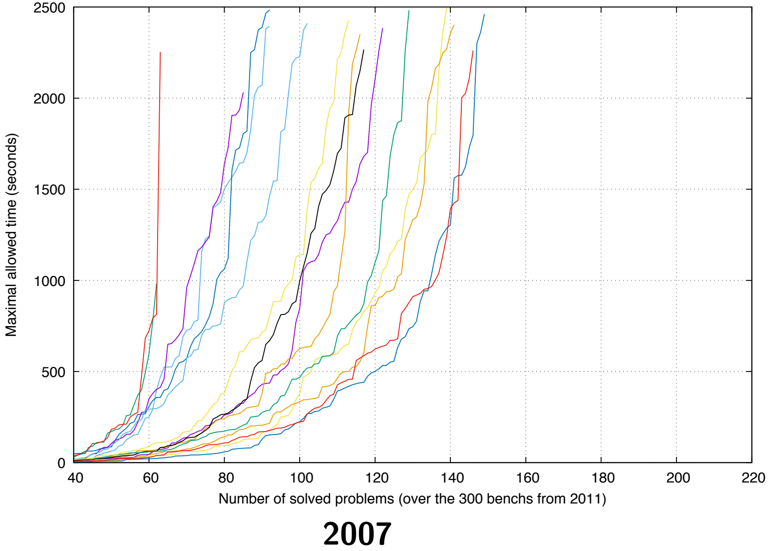
2003

Performances of SAT Solvers, after 2001

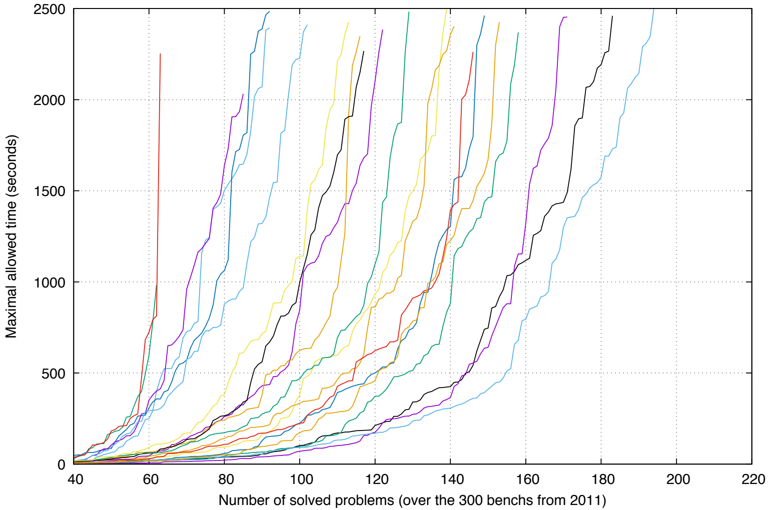


2005

Performances of SAT Solvers, after 2001

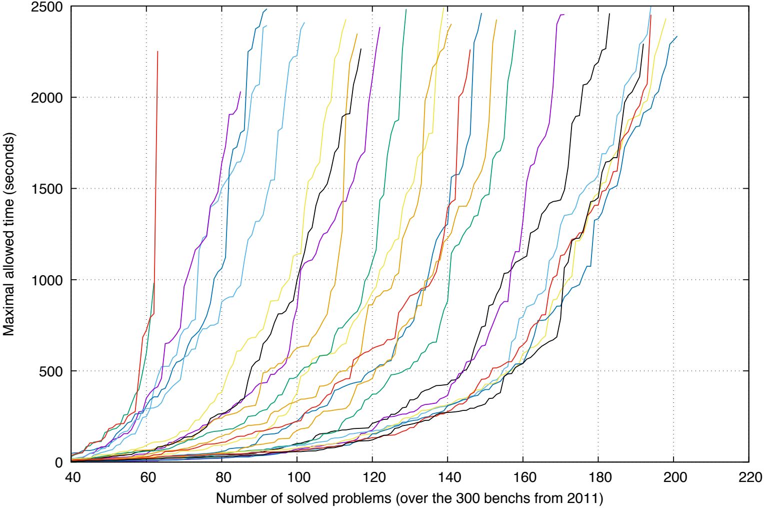


Performances of SAT Solvers, after 2001



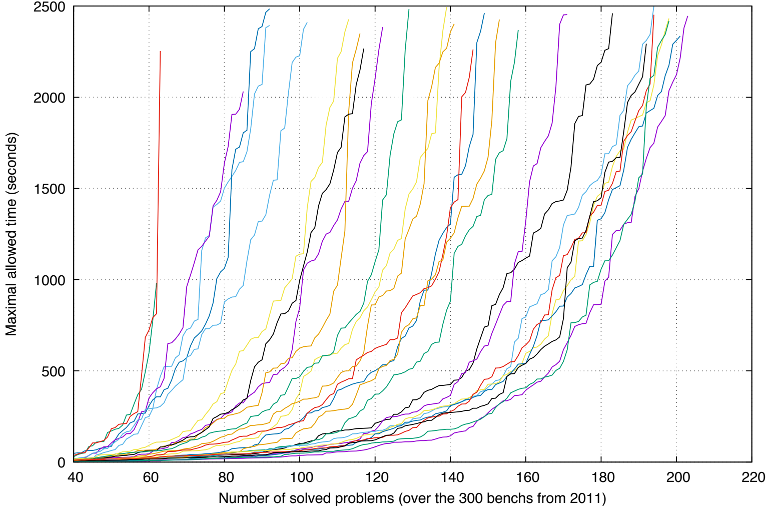
2009

Performances of SAT Solvers, after 2001



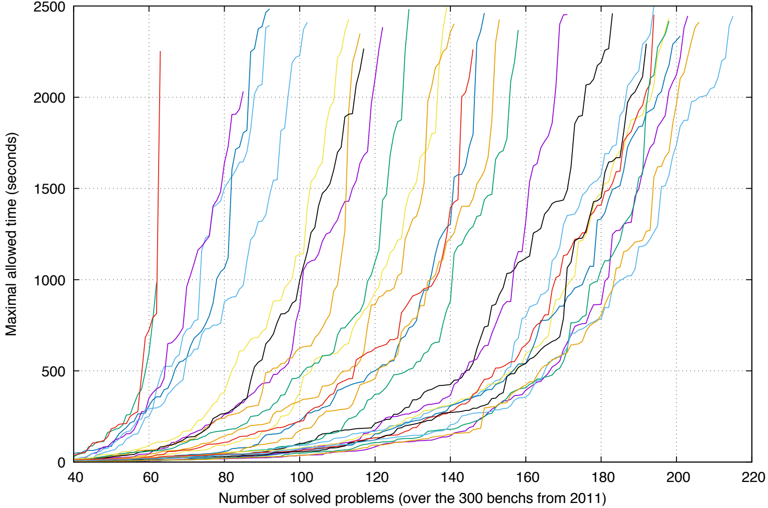
2011

Performances of SAT Solvers, after 2001



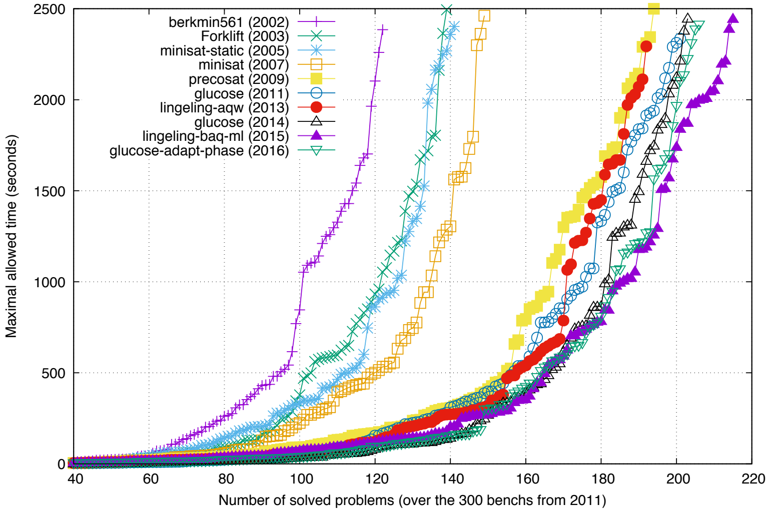
2014

Performances of SAT Solvers, after 2001



2016

Performances of SAT Solvers, after 2001



the winners

The firsts SAT steps

1958 : Hilary Putnam and Martin Davis look for funding their research around propositional logic

« What we're interested in is good algorithms for propositional calculus » (NSA)

Before that, only inefficient methods (truth tables, . . .)

First papers

- *Computational Methods in The Propositional calculus* [Davis Putnam 1958] [2]
- *A Computing Procedure for Quantification Theory* [Davis Putnam 1960]

2. Rapport interne NSA

1960, already a first (kind of) competition !

« *The superiority of the present procedure (i.e. DP) over those previously available is indicated in part by the fact that a formula on which Gilmores routine for the IBM 704 causes* **the machine to compute for 21 minutes** *without obtaining a result was worked successfully by* **hand computation using the present method in 30 minutes** »

[Davis et Putnam 1960], page 202.

What can be done with a so simple logic ?

The facts are propositional variables
The knowledge is a propositional formula

$$\begin{array}{ccccccc} & \neg x_1 & \vee & \neg x_2 & \vee & x_3 \\ \wedge & & & & & \neg x_3 \\ \wedge & x_1 & \vee & x_2 & & \\ \wedge & & & x_2 & \vee & x_3 \end{array}$$

- Variables : $x_1 \ldots x_3$;
- Literals : x_1, $\neg x_1$;
- Clauses : $\neg x_1 \vee \neg x_2 \vee x_3$;
- Formula Σ written in CNF (conjonction of clauses) ;

Big questions

- **SAT** : is there an assignment of variables making the formula true ?
- **UNSAT** : is the theory contradictory ?
- **PI** : deduce all you can from Σ

What can be done with a so simple logic ?

The facts are propositional variables
The knowledge is a propositional formula

$$
\begin{array}{lccccc}
 & \neg x_1 & \vee & \neg x_2 & \vee & x_3 \\
\wedge & & & & & \neg x_3 \\
\wedge & x_1 & \vee & x_2 & & \\
\wedge & & & x_2 & \vee & x_3
\end{array}
$$

x_1	x_2	x_3
$\bot$	$\bot$	$\bot$

- Variables : $x_1 \ldots x_3$;
- Literals : x_1, $\neg x_1$;
- Clauses : $\neg x_1 \vee \neg x_2 \vee x_3$;
- Formula Σ written in CNF (conjonction of clauses) ;

Big questions

- **SAT** : is there an assignment of variables making the formula true ?
- **UNSAT** : is the theory contradictory ?
- **PI** : deduce all you can from Σ

What can be done with a so simple logic ?

The facts are propositional variables
The knowledge is a propositional formula

$$\begin{array}{lccccc} & \neg x_1 & \vee & \neg x_2 & \vee & x_3 \\ \wedge & & & & & \neg x_3 \\ \wedge & x_1 & \vee & x_2 & & \\ \wedge & & & x_2 & \vee & x_3 \end{array}$$

x_1	x_2	x_3
$\bot$	$\bot$	$\bot$

- Variables : $x_1 \dots x_3$;
- Literals : x_1, $\neg x_1$;
- Clauses : $\neg x_1 \vee \neg x_2 \vee x_3$;
- Formula Σ written in CNF (conjonction of clauses) ;

Big questions

- **SAT** : is there an assignment of variables making the formula true ?
- **UNSAT** : is the theory contradictory ?
- **PI** : deduce all you can from Σ

What can be done with a so simple logic ?

The facts are propositional variables
The knowledge is a propositional formula

$$\begin{array}{lcccc} & \neg x_1 \vee & \neg x_2 \vee & x_3 \\ \wedge & & & \neg x_3 \\ \wedge & x_1 \vee & x_2 & \\ \wedge & & x_2 \vee & x_3 \end{array}$$

x_1	x_2	x_3
$\bot$	$\top$	$\bot$

- Variables : $x_1 \ldots x_3$;
- Literals : x_1, $\neg x_1$;
- Clauses : $\neg x_1 \vee \neg x_2 \vee x_3$;
- Formula Σ written in CNF (conjonction of clauses) ;

Big questions

- **SAT** : is there an assignment of variables making the formula true ?
- **UNSAT** : is the theory contradictory ?
- **PI** : deduce all you can from Σ

What can be done with a so simple logic ?

The facts are propositional variables
The knowledge is a propositional formula

$$\begin{array}{lccccc} & \neg x_1 & \vee & \neg x_2 & \vee & x_3 \\ \wedge & & & & & \neg x_3 \\ \wedge & x_1 & \vee & x_2 & & \\ \wedge & & & x_2 & \vee & x_3 \end{array}$$

x_1	x_2	x_3
$\bot$	$\top$	$\bot$

- Variables : $x_1 \ldots x_3$;
- Literals : x_1, $\neg x_1$;
- Clauses : $\neg x_1 \vee \neg x_2 \vee x_3$;
- Formula Σ written in CNF (conjonction of clauses) ;

Big questions

- **SAT** : is there an assignment of variables making the formula true ?
- **UNSAT** : is the theory contradictory ?
- **PI** : deduce all you can from Σ

A very simple deduction rule

The Resolution Rule (Cut) [Gentzen 1934, Robinson 1965]

Let $c_1 = (x \vee a_1 \vee \ldots a_n)$ and $c_2 = (\neg x \vee b_1 \vee \ldots b_m)$
$c = (a_1 \vee \ldots a_n \vee b_1 \vee \ldots b_m)$ is obtained by res. on x between c_1 and c_2.

It is a particular case of the following **deduction rule** :

if $a \rightarrow b$ **and** $b \rightarrow c$ **then** $a \rightarrow c$

In general, SAT solvers are only using this rule
(but many, many times per second)

Knowing which resolution to perform is the secret ingredient of SAT solvers

1962-2001 : DPLL rules the world

Systematically explore the space of partial models (backtrack)

- Choose a literal
- Try to find a solution with this literal set to True
- If it is not possible :
  Finds a solution with this literal set to False

Backtrack search on partial models
Systematic (ordered) exploration ensures completeness

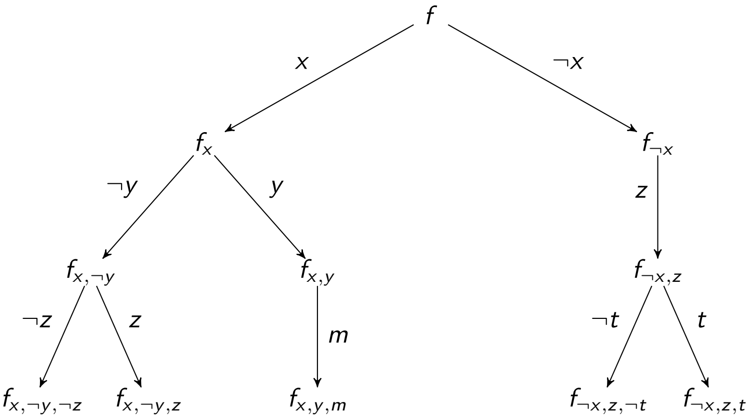
1962-2001 : DPLL rules the world

Systematically explore the space of partial models (backtrack)

- Choose a literal
- Try to find a solution with this literal set to True
- If it is not possible :
  Finds a solution with this literal set to False

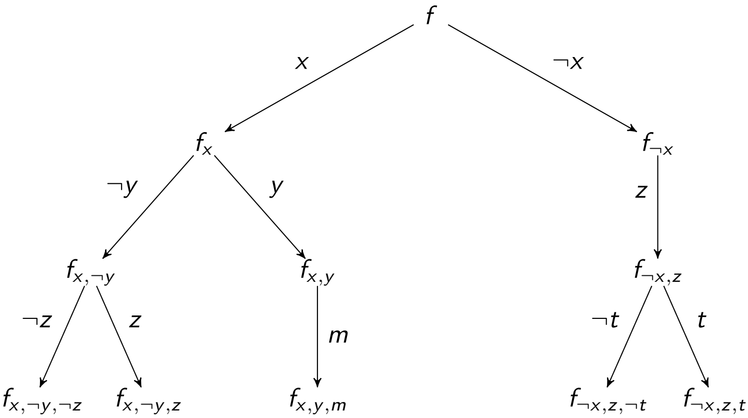
Backtrack search on partial models
Systematic (ordered) exploration ensures completeness

Backtrack search



- How to choose the right literal to branch on ?
- First search for a model or a contradiction ?

Backtrack search



- How to choose the right literal to branch on ?
- First search for a model or a contradiction ?

An example of DPLL

Formule	Simplified Formula
$x_1 \lor x_4$	$x_1 \lor x_4$
$\overline{x_1} \lor x_4 \lor x_{14}$	$\overline{x_1} \lor x_4 \lor x_{14}$
$x_1 \lor \overline{x_3} \lor \overline{x_8}$	$x_1 \lor \overline{x_3} \lor \overline{x_8}$
$x_1 \lor x_8 \lor x_{12}$	$x_1 \lor x_8 \lor x_{12}$
$x_2 \lor x_{12}$	$x_2 \lor x_{12}$
$\overline{x_3} \lor \overline{x_{12}} \lor x_{13}$	$\overline{x_3} \lor \overline{x_{12}} \lor x_{13}$
$\overline{x_3} \lor x_7 \lor \overline{x_{13}}$	$\overline{x_3} \lor x_7 \lor \overline{x_{13}}$
$x_8 \lor \overline{x_7} \lor \overline{x_{12}}$	$x_8 \lor \overline{x_7} \lor \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?

$x1$ appears in 4 clauses and 1 binary clause

An example of DPLL

Formule	Simplified Formula
$x_1 \vee x_4$	$x_1 \vee x_4$
$\overline{x_1} \vee x_4 \vee x_{14}$	$\overline{x_1} \vee x_4 \vee x_{14}$
$x_1 \vee \overline{x_3} \vee \overline{x_8}$	$x_1 \vee \overline{x_3} \vee \overline{x_8}$
$x_1 \vee x_8 \vee x_{12}$	$x_1 \vee x_8 \vee x_{12}$
$x_2 \vee x_{12}$	$x_2 \vee x_{12}$
$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$	$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$
$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$	$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$
$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$	$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?
1	$\overline{x_1}$	(d)

x_4 appears in 1 unary clause

An example of DPLL

Formule	Simplified Formula
$x_1 \vee x_4$	$x_1 \vee x_4$
$\overline{x_1} \vee x_4 \vee x_{14}$	$\overline{x_1} \vee x_4 \vee x_{14}$
$x_1 \vee \overline{x_3} \vee \overline{x_8}$	$x_1 \vee \overline{x_3} \vee \overline{x_8}$
$x_1 \vee x_8 \vee x_{12}$	$x_1 \vee x_8 \vee x_{12}$
$x_2 \vee x_{12}$	$x_2 \vee x_{12}$
$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$	$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$
$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$	$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$
$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$	$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?
1	$\overline{x_1}$	(d)
+	x_4	

x_3 appears in 3 clauses incl. 1 (new) binary clause

An example of DPLL

Formule

$x_1 \vee x_4$
$\overline{x_1} \vee x_4 \vee x_{14}$
$x_1 \vee \overline{x_3} \vee \overline{x_8}$
$x_1 \vee x_8 \vee x_{12}$
$x_2 \vee x_{12}$
$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$
$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$
$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Simplified Formula

$x_1 \vee x_4$
$\overline{x_1} \vee x_4 \vee x_{14}$
$x_1 \vee \overline{x_3} \vee \overline{x_8}$
$x_1 \vee x_8 \vee x_{12}$
$x_2 \vee x_{12}$
$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$
$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$
$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?
1	$\overline{x_1}$	(d)
+	x_4	
2	x_3	(d)

$\overline{x_8}$ appears in one unary clause

An example of DPLL

Formule	Simplified Formula
$x_1 \vee x_4$	$x_1 \vee x_4$
$\overline{x_1} \vee x_4 \vee x_{14}$	$\overline{x_1} \vee x_4 \vee x_{14}$
$x_1 \vee \overline{x_3} \vee \overline{x_8}$	$x_1 \vee \overline{x_3} \vee \overline{x_8}$
$x_1 \vee x_8 \vee x_{12}$	$x_1 \vee x_8 \vee x_{12}$
$x_2 \vee x_{12}$	$x_2 \vee x_{12}$
$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$	$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$
$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$	$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$
$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$	$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?
1	$\overline{x_1}$	(d)
+	x_4	
2	x_3	(d)
+	$\overline{x_8}$	

x_{12} appears in 1 unary clause

An example of DPLL

Formule	Simplified Formula
$x_1 \vee x_4$	$x_1 \vee x_4$
$\overline{x_1} \vee x_4 \vee x_{14}$	$\overline{x_1} \vee x_4 \vee x_{14}$
$x_1 \vee \overline{x_3} \vee \overline{x_8}$	$x_1 \vee \overline{x_3} \vee \overline{x_8}$
$x_1 \vee x_8 \vee x_{12}$	$x_1 \vee x_8 \vee x_{12}$
$x_2 \vee x_{12}$	$x_2 \vee x_{12}$
$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$	$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$
$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$	$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$
$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$	$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?
1	$\overline{x_1}$	(d)
+	x_4	
2	x_3	(d)
+	$\overline{x_8}$	
+	x_{12}	

x_{13}, $\overline{x_7}$ appear in unary clauses

An example of DPLL

Formule	Simplified Formula
$x_1 \vee x_4$	$x_1 \vee x_4$
$\overline{x_1} \vee x_4 \vee x_{14}$	$\overline{x_1} \vee x_4 \vee x_{14}$
$x_1 \vee \overline{x_3} \vee \overline{x_8}$	$x_1 \vee \overline{x_3} \vee \overline{x_8}$
$x_1 \vee x_8 \vee x_{12}$	$x_1 \vee x_8 \vee x_{12}$
$x_2 \vee x_{12}$	$x_2 \vee x_{12}$
$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$	$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$
$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$	$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$
$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$	$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?
1	$\overline{x_1}$	(d)
+	x_4	
2	x_3	(d)
+	$\overline{x_8}$	
+	x_{12}	
+	x_{13}	

x_7, $\overline{x_7}$ appear in unary clauses

An example of DPLL

Formule

$x_1 \vee x_4$

$\overline{x_1} \vee x_4 \vee x_{14}$

$x_1 \vee \overline{x_3} \vee \overline{x_8}$

$x_1 \vee x_8 \vee x_{12}$

$x_2 \vee x_{12}$

$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$

$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$

$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Simplified Formula

$x_1 \vee x_4$

$\overline{x_1} \vee x_4 \vee x_{14}$

$x_1 \vee \overline{x_3} \vee \overline{x_8}$

$x_1 \vee x_8 \vee x_{12}$

$x_2 \vee x_{12}$

$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$

$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$

$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?
1	$\overline{x_1}$	(d)
+	x_4	
2	x_3	(d)
+	$\overline{x_8}$	
+	x_{12}	
+	x_{13}	
+	$\overline{x_7}$	

Conflict ! Undo everything until last decision

An example of DPLL

Formule

$x_1 \vee x_4$

$\overline{x_1} \vee x_4 \vee x_{14}$

$x_1 \vee \overline{x_3} \vee \overline{x_8}$

$x_1 \vee x_8 \vee x_{12}$

$x_2 \vee x_{12}$

$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$

$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$

$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Simplified Formula

$x_1 \vee x_4$

$\overline{x_1} \vee x_4 \vee x_{14}$

$x_1 \vee \overline{x_3} \vee \overline{x_8}$

$x_1 \vee x_8 \vee x_{12}$

$x_2 \vee x_{12}$

$\overline{x_3} \vee \overline{x_{12}} \vee x_{13}$

$\overline{x_3} \vee x_7 \vee \overline{x_{13}}$

$x_8 \vee \overline{x_7} \vee \overline{x_{12}}$

Partial Model

Lev.	Lit.	Back ?
1	$\overline{x_1}$	(d)
+	x_4	
*	$\overline{x_3}$	

Now, $\overline{x_3}$ is not a decision

1999, on the way to the revolution

Huge problems are coming from the real-world : Planning & Bounded Model Checking

- Planning as Satisfiability. [Kautz and Selman, 92]
- Symbolic Model Checking using SAT procedures instead of BDDs. [Biere & al. 99]
- SAT solvers can't cope with those huge formulas without specialized data structures

DPLL extinction. . .

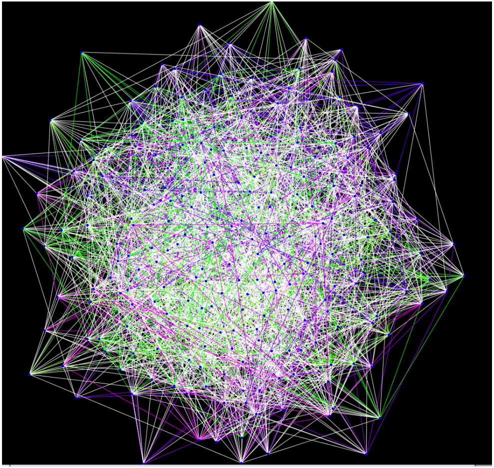
- GRASP : **learning clauses** in SAT solvers
- DLIS : **very simple heuristic**
- SATO : **lazy data structure** to detect unary clauses

Algorithms ingredients for the upcoming revolution
BMC, GRASP, DLIS, SATO

Huge problems ?

Generated by the tool : satgraf `http://satbench.uwaterloo.ca/site/satgraf`

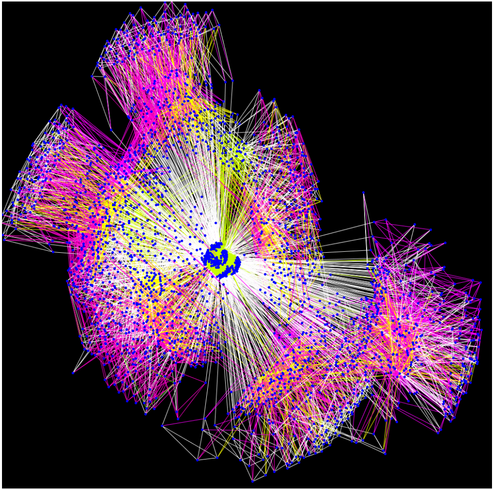
Random formula



Huge problems ?

Generated by the tool : satgraf http://satbench.uwaterloo.ca/site/satgraf

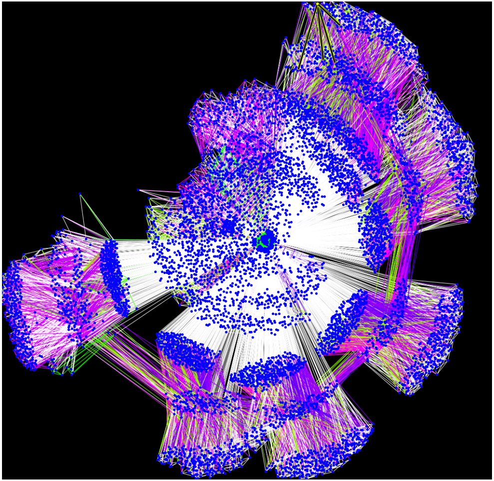
BMC instances



Huge problems ?

Generated by the tool : satgraf http://satbench.uwaterloo.ca/site/satgraf

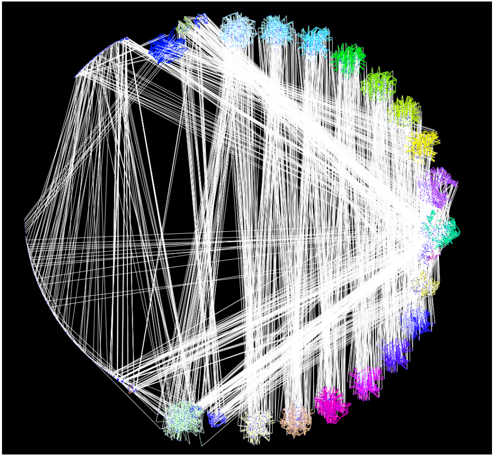
BMC instances



Huge problems ?

Generated by the tool : satgraf `http://satbench.uwaterloo.ca/site/satgraf`

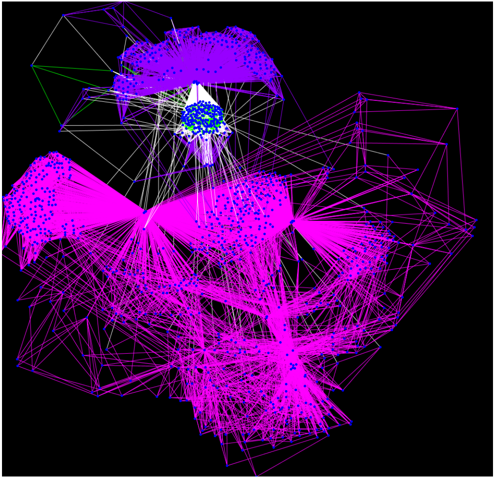
BMC instances



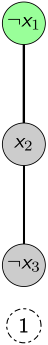
Huge problems ?

Generated by the tool : satgraf `http://satbench.uwaterloo.ca/site/satgraf`

BMC instances



CDCL rules the world since 2001



$x_1 \vee x_2$
$\neg x_2 \vee \neg x_3$

$\neg x_2 \vee \neg x_4 \vee \neg x_5$
$x_3 \vee x_5 \vee x_6$

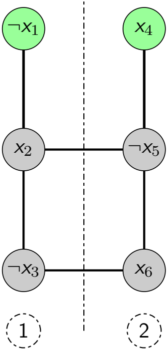
$x_7 \vee \neg x_6 \vee \neg x_8$
$\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$
$\neg x_{11} \vee x_8 \vee \neg x_{12}$
$x_{12} \vee \neg x_{13}$

$\neg x_6 \vee x_{12} \vee x_{15}$
$x_{13} \vee \neg x_{14} \vee \neg x_{16}$
$\neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

CDCL rules the world since 2001



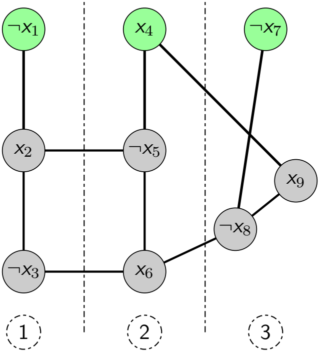
$x_1 \vee x_2$ $\quad \neg x_2 \vee \neg x_4 \vee \neg x_5$ $\quad x_7 \vee \neg x_6 \vee \neg x_8$ $\quad x_{10} \vee \neg x_9 \vee x_{11}$ $\quad \neg x_6 \vee x_{12} \vee x_{15}$

$\neg x_2 \vee \neg x_3$ $\quad x_3 \vee x_5 \vee x_6$ $\quad \neg x_4 \vee x_8 \vee x_9$ $\quad \neg x_{11} \vee x_8 \vee \neg x_{12}$ $\quad x_{13} \vee \neg x_{14} \vee \neg x_{16}$

$x_{12} \vee \neg x_{13}$ $\quad \neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

CDCL rules the world since 2001



$x_1 \vee x_2$

$\neg x_2 \vee \neg x_3$

$\neg x_2 \vee \neg x_4 \vee \neg x_5$

$x_3 \vee x_5 \vee x_6$

$x_7 \vee \neg x_6 \vee \neg x_8$

$\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$

$\neg x_{11} \vee x_8 \vee \neg x_{12}$

$x_{12} \vee \neg x_{13}$

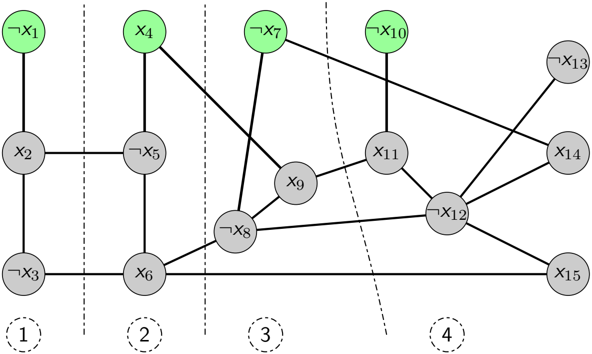
$\neg x_6 \vee x_{12} \vee x_{15}$

$x_{13} \vee \neg x_{14} \vee \neg x_{16}$

$\neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

CDCL rules the world since 2001



$x_1 \vee x_2$
$\neg x_2 \vee \neg x_3$

$\neg x_2 \vee \neg x_4 \vee \neg x_5$
$x_3 \vee x_5 \vee x_6$

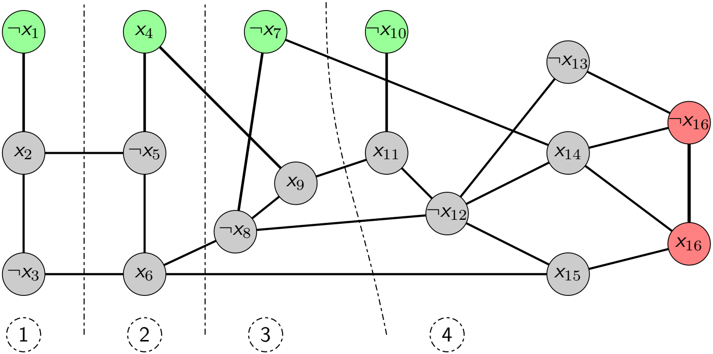
$x_7 \vee \neg x_6 \vee \neg x_8$
$\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$
$\neg x_{11} \vee x_8 \vee \neg x_{12}$
$x_{12} \vee \neg x_{13}$

$\neg x_6 \vee x_{12} \vee x_{15}$
$x_{13} \vee \neg x_{14} \vee \neg x_{16}$
$\neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

CDCL rules the world since 2001



$x_1 \vee x_2$

$\neg x_2 \vee \neg x_3$

$\neg x_2 \vee \neg x_4 \vee \neg x_5$

$x_3 \vee x_5 \vee x_6$

$x_7 \vee \neg x_6 \vee \neg x_8$

$\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$

$\neg x_{11} \vee x_8 \vee \neg x_{12}$

$x_{12} \vee \neg x_{13}$

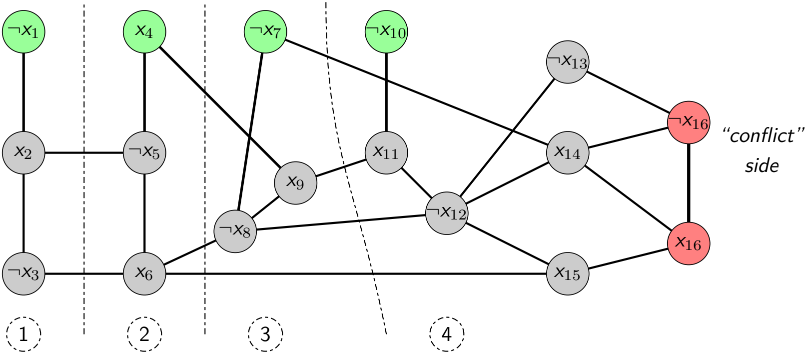
$\neg x_6 \vee x_{12} \vee x_{15}$

$x_{13} \vee \neg x_{14} \vee \neg x_{16}$

$\neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

CDCL rules the world since 2001



$x_1 \vee x_2$
$\neg x_2 \vee \neg x_3$

$\neg x_2 \vee \neg x_4 \vee \neg x_5$
$x_3 \vee x_5 \vee x_6$

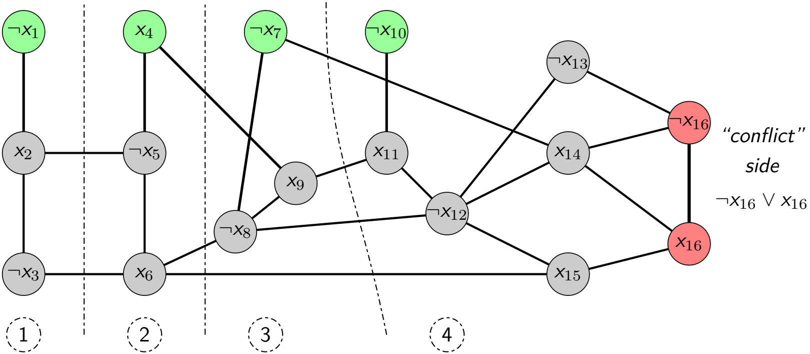
$x_7 \vee \neg x_6 \vee \neg x_8$
$\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$
$\neg x_{11} \vee x_8 \vee \neg x_{12}$
$x_{12} \vee \neg x_{13}$

$\neg x_6 \vee x_{12} \vee x_{15}$
$x_{13} \vee \neg x_{14} \vee \neg x_{16}$
$\neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

CDCL rules the world since 2001



$x_1 \lor x_2$

$\neg x_2 \lor \neg x_3$

$\neg x_2 \lor \neg x_4 \lor \neg x_5$

$x_3 \lor x_5 \lor x_6$

$x_7 \lor \neg x_6 \lor \neg x_8$

$\neg x_4 \lor x_8 \lor x_9$

$x_{10} \lor \neg x_9 \lor x_{11}$

$\neg x_{11} \lor x_8 \lor \neg x_{12}$

$x_{12} \lor \neg x_{13}$

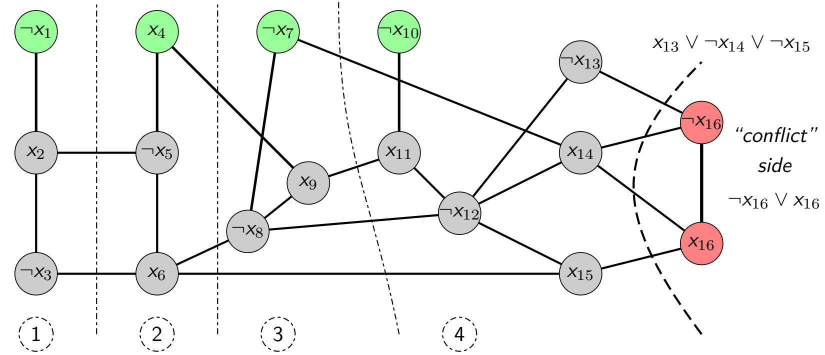
$\neg x_6 \lor x_{12} \lor x_{15}$

$x_{13} \lor \neg x_{14} \lor \neg x_{16}$

$\neg x_{15} \lor \neg x_{14} \lor x_{16}$

$x_7 \lor x_{12} \lor x_{14}$

CDCL rules the world since 2001



$x_1 \vee x_2$

$\neg x_2 \vee \neg x_3$

$\neg x_2 \vee \neg x_4 \vee \neg x_5$

$x_3 \vee x_5 \vee x_6$

$x_7 \vee \neg x_6 \vee \neg x_8$

$\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$

$\neg x_{11} \vee x_8 \vee \neg x_{12}$

$x_{12} \vee \neg x_{13}$

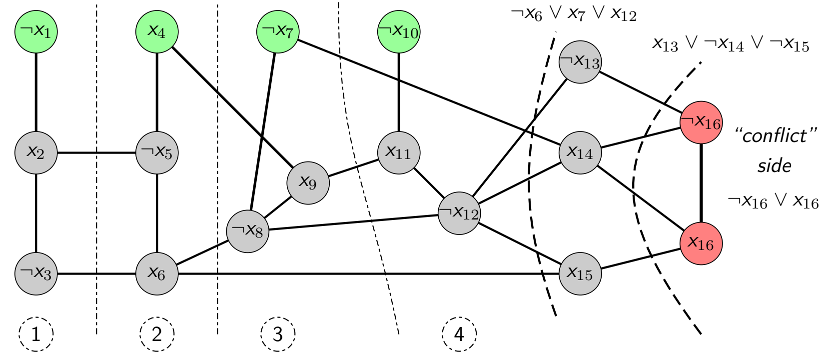
$\neg x_6 \vee x_{12} \vee x_{15}$

$x_{13} \vee \neg x_{14} \vee \neg x_{16}$

$\neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

CDCL rules the world since 2001



$x_1 \vee x_2$

$\neg x_2 \vee \neg x_3$

$\neg x_2 \vee \neg x_4 \vee \neg x_5$

$x_3 \vee x_5 \vee x_6$

$x_7 \vee \neg x_6 \vee \neg x_8$

$\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$

$\neg x_{11} \vee x_8 \vee \neg x_{12}$

$x_{12} \vee \neg x_{13}$

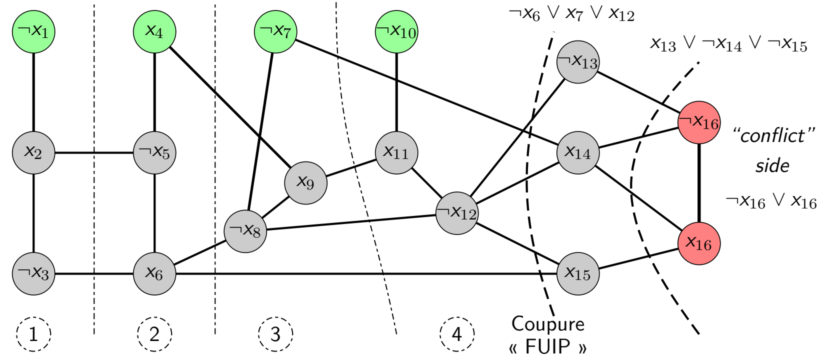
$x_7 \vee x_{12} \vee x_{14}$

$\neg x_6 \vee x_{12} \vee x_{15}$

$x_{13} \vee \neg x_{14} \vee \neg x_{16}$

$\neg x_{15} \vee \neg x_{14} \vee x_{16}$

CDCL rules the world since 2001



$x_1 \vee x_2$ | $\neg x_2 \vee \neg x_3$

$\neg x_2 \vee \neg x_4 \vee \neg x_5$ | $x_3 \vee x_5 \vee x_6$

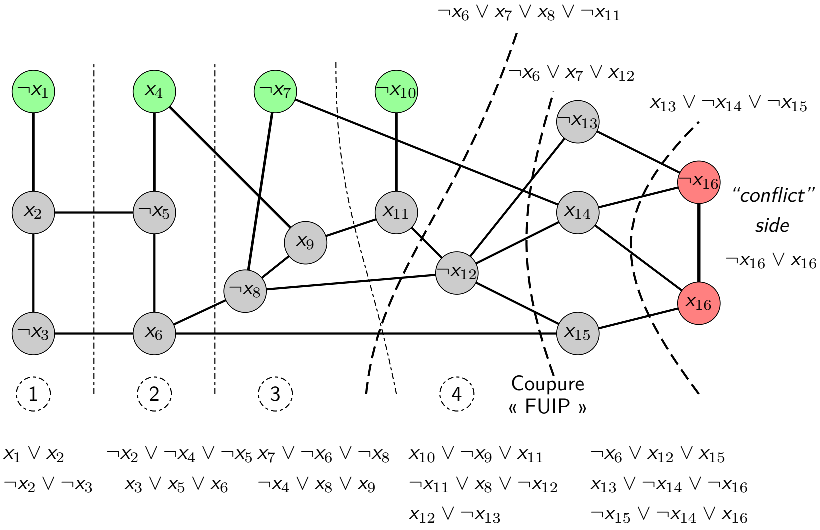
$x_7 \vee \neg x_6 \vee \neg x_8$ | $\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$ | $\neg x_{11} \vee x_8 \vee \neg x_{12}$ | $x_{12} \vee \neg x_{13}$

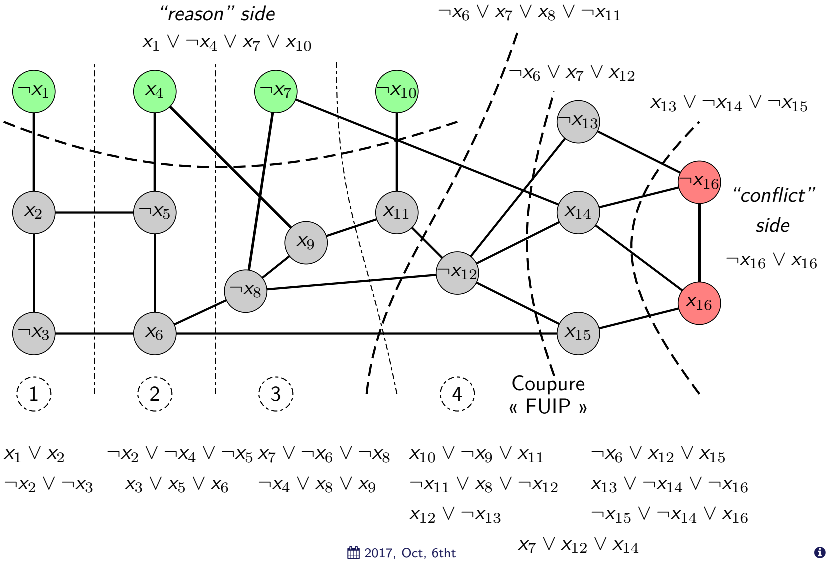
$\neg x_6 \vee x_{12} \vee x_{15}$ | $x_{13} \vee \neg x_{14} \vee \neg x_{16}$ | $\neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

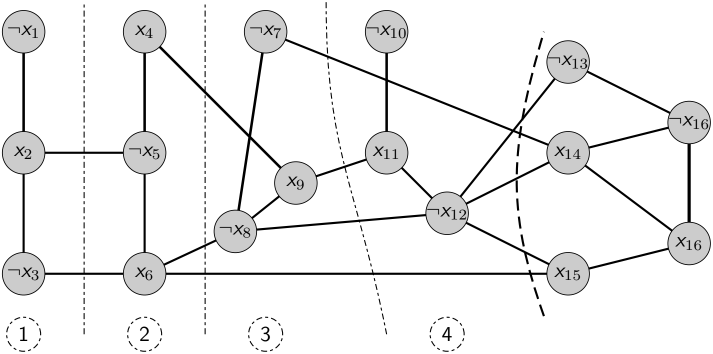
CDCL rules the world since 2001



CDCL rules the world since 2001



CDCL rules the world since 2001



$x_1 \vee x_2$
$\neg x_2 \vee \neg x_3$

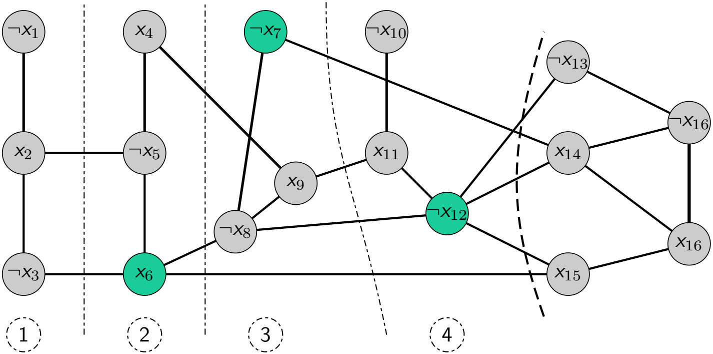
$\neg x_2 \vee \neg x_4 \vee \neg x_5$
$x_3 \vee x_5 \vee x_6$

$x_7 \vee \neg x_6 \vee \neg x_8$
$\neg x_4 \vee x_8 \vee x_9$

$x_{10} \vee \neg x_9 \vee x_{11}$
$\neg x_{11} \vee x_8 \vee \neg x_{12}$
$x_{12} \vee \neg x_{13}$
$x_7 \vee x_{12} \vee x_{14}$

$\neg x_6 \vee x_{12} \vee x_{15}$
$x_{13} \vee \neg x_{14} \vee \neg x_{16}$
$\neg x_{15} \vee \neg x_{14} \vee x_{16}$

CDCL rules the world since 2001



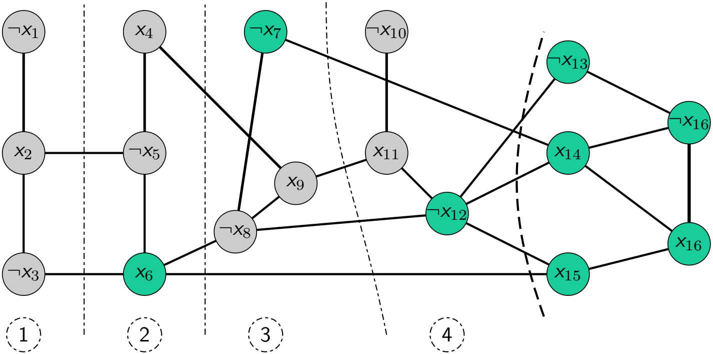
$x_1 \vee x_2$ | $\neg x_2 \vee \neg x_4 \vee \neg x_5$ | $x_7 \vee \neg x_6 \vee \neg x_8$ | $x_{10} \vee \neg x_9 \vee x_{11}$ | $\neg x_6 \vee x_{12} \vee x_{15}$

$\neg x_2 \vee \neg x_3$ | $x_3 \vee x_5 \vee x_6$ | $\neg x_4 \vee x_8 \vee x_9$ | $\neg x_{11} \vee x_8 \vee \neg x_{12}$ | $x_{13} \vee \neg x_{14} \vee \neg x_{16}$

$x_{12} \vee \neg x_{13}$ | $\neg x_{15} \vee \neg x_{14} \vee x_{16}$

$x_7 \vee x_{12} \vee x_{14}$

CDCL rules the world since 2001



$x_1 \lor x_2$ $\neg x_2 \lor \neg x_4 \lor \neg x_5$ $x_7 \lor \neg x_6 \lor \neg x_8$ $x_{10} \lor \neg x_9 \lor x_{11}$ $\neg x_6 \lor x_{12} \lor x_{15}$

$\neg x_2 \lor \neg x_3$ $x_3 \lor x_5 \lor x_6$ $\neg x_4 \lor x_8 \lor x_9$ $\neg x_{11} \lor x_8 \lor \neg x_{12}$ $x_{13} \lor \neg x_{14} \lor \neg x_{16}$

$x_{12} \lor \neg x_{13}$ $\neg x_{15} \lor \neg x_{14} \lor x_{16}$

$x_7 \lor x_{12} \lor x_{14}$

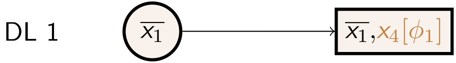
CDCL, learning and resolution

Decisions – Propagations

$\phi_1 = x_1 \vee x_4$
$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$
$\phi_3 = x_1 \vee x_8 \vee x_{12}$
$\phi_4 = x_2 \vee x_{11}$
$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$
$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$
$\phi_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$

CDCL, learning and resolution

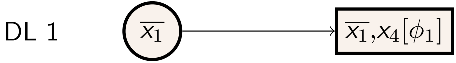
Decisions – Propagations



$$\phi_1 = x_1 \vee x_4$$
$$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$$
$$\phi_3 = x_1 \vee x_8 \vee x_{12}$$
$$\phi_4 = x_2 \vee x_{11}$$
$$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$
$$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$
$$\phi_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$$

CDCL, learning and resolution

Decisions – Propagations



$\phi_1 = x_1 \vee x_4$

$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$

$\phi_3 = x_1 \vee x_8 \vee x_{12}$

$\phi_4 = x_2 \vee x_{11}$

$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$

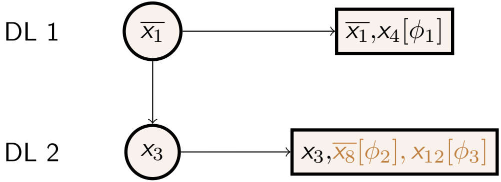
$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$

$\phi_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$

CDCL, learning and resolution

Decisions – Propagations

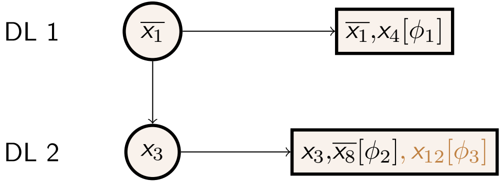
$\phi_1 = x_1 \vee x_4$
$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$
$\phi_3 = x_1 \vee x_8 \vee x_{12}$
$\phi_4 = x_2 \vee x_{11}$
$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$
$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$
$\phi_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$



CDCL, learning and resolution

Decisions – Propagations

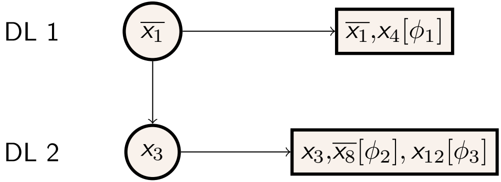
$$\phi_1 = x_1 \lor x_4$$
$$\phi_2 = x_1 \lor \overline{x_3} \lor \overline{x_8}$$
$$\phi_3 = x_1 \lor x_8 \lor x_{12}$$
$$\phi_4 = x_2 \lor x_{11}$$
$$\phi_5 = \overline{x_3} \lor \overline{x_7} \lor x_{13}$$
$$\phi_6 = \overline{x_3} \lor \overline{x_7} \lor \overline{x_{13}} \lor x_9$$
$$\phi_7 = x_8 \lor \overline{x_7} \lor \overline{x_9}$$



CDCL, learning and resolution

Decisions – Propagations

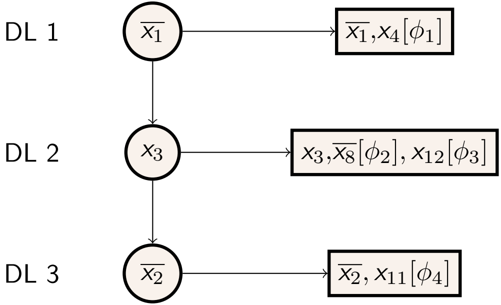
$\phi_1 = x_1 \vee x_4$
$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$
$\phi_3 = x_1 \vee x_8 \vee x_{12}$
$\phi_4 = x_2 \vee x_{11}$
$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$
$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$
$\phi_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$



CDCL, learning and resolution

Decisions – Propagations

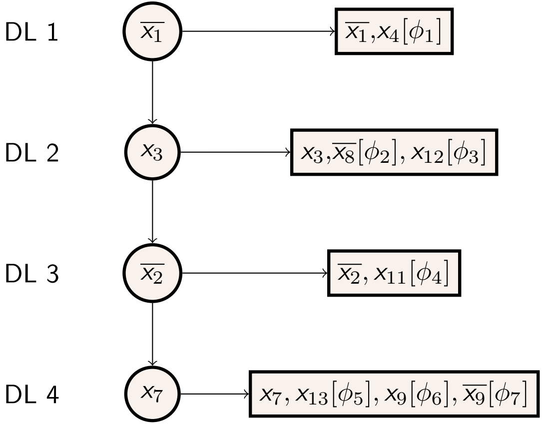
$$
\begin{aligned}
\phi_1 &= x_1 \vee x_4 \\
\phi_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
\phi_3 &= x_1 \vee x_8 \vee x_{12} \\
\phi_4 &= x_2 \vee x_{11} \\
\phi_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
\phi_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
\phi_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
\end{aligned}
$$



CDCL, learning and resolution

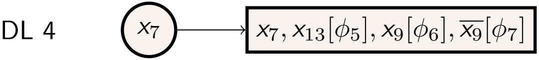
Decisions – Propagations

$$\phi_1 = x_1 \vee x_4$$
$$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$$
$$\phi_3 = x_1 \vee x_8 \vee x_{12}$$
$$\phi_4 = x_2 \vee x_{11}$$
$$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$
$$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$
$$\phi_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$$



CDCL, learning and resolution

Conflict Analysis



$$
\begin{aligned}
\phi_1 &= x_1 \lor x_4 \\
\phi_2 &= x_1 \lor \overline{x_3} \lor \overline{x_8} \\
\phi_3 &= x_1 \lor x_8 \lor x_{12} \\
\phi_4 &= x_2 \lor x_{11} \\
\phi_5 &= \overline{x_3} \lor \overline{x_7} \lor x_{13} \\
\phi_6 &= \overline{x_3} \lor \overline{x_7} \lor \overline{x_{13}} \lor x_9 \\
\phi_7 &= x_8 \lor \overline{x_7} \lor \overline{x_9}
\end{aligned}
$$

CDCL, learning and resolution

Conflict Analysis

DL 4 $x_7 \rightarrow x_7, x_{13}[\phi_5], x_9[\phi_6], \overline{x_9}[\phi_7]$

$$\beta_1 = res(x_9, \phi_7, \phi_6) = \overline{x_3} \vee x_8 \vee \overline{x_7} \vee \overline{x_{13}}$$

$$\phi_1 = x_1 \vee x_4$$
$$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$$
$$\phi_3 = x_1 \vee x_8 \vee x_{12}$$
$$\phi_4 = x_2 \vee x_{11}$$
$$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$
$$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$
$$\phi_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$$

CDCL, learning and resolution

Conflict Analysis

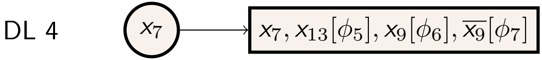
DL 4 $x_7 \longrightarrow x_7, x_{13}[\phi_5], x_9[\phi_6], \overline{x_9}[\phi_7]$

$$\beta_1 = res(x_9, \phi_7, \phi_6) = \overline{x_3} \vee x_8 \vee \overline{x_7} \vee \overline{x_{13}}$$
$$\beta = res(x_{13}, \beta_1, \phi_5) = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

$$\phi_1 = x_1 \vee x_4$$
$$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$$
$$\phi_3 = x_1 \vee x_8 \vee x_{12}$$
$$\phi_4 = x_2 \vee x_{11}$$
$$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$
$$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$
$$\phi_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$$

CDCL, learning and resolution

Conflict Analysis



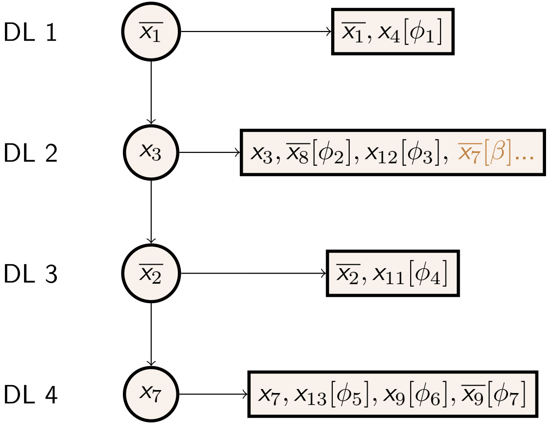
$$\beta_1 = res(x_9, \phi_7, \phi_6) = \overline{x_3} \vee x_8 \vee \overline{x_7} \vee \overline{x_{13}}$$
$$\beta = res(x_{13}, \beta_1, \phi_5) = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

- Stops as soon as the resolvant has a unique literal from the last decision level (FUIP).
- β is added to the clauses databases (ensure a systematic search)

CDCL, learning and resolution

Non Chronological Backtrackings

$\phi_1 = x_1 \vee x_4$
$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$
$\phi_3 = x_1 \vee x_8 \vee x_{12}$
$\phi_4 = x_2 \vee x_{11}$
$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$
$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$
$\phi_7 = \overline{x_8} \vee \overline{x_7} \vee \overline{x_9}$

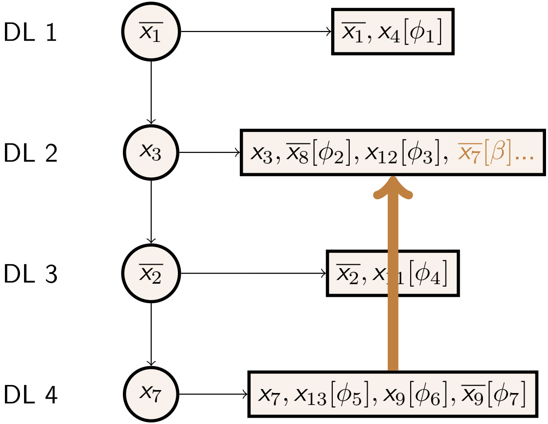


$\beta = \overline{x_3} \vee x_8 \vee \overline{x_7}$

CDCL, learning and resolution

Non Chronological Backtrackings

$\phi_1 = x_1 \vee x_4$
$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$
$\phi_3 = x_1 \vee x_8 \vee x_{12}$
$\phi_4 = x_2 \vee x_{11}$
$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$
$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$
$\phi_7 = \overline{x_8} \vee \overline{x_7} \vee \overline{x_9}$

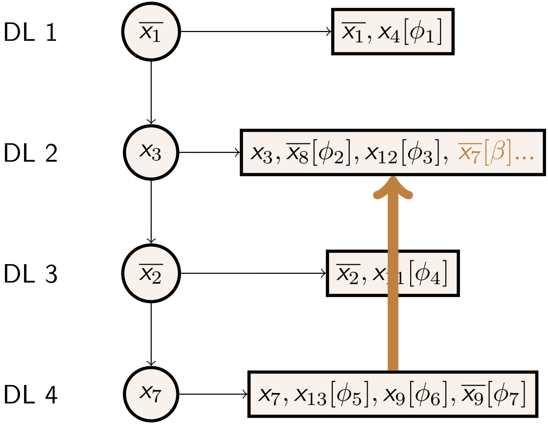


$$\beta = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

CDCL, learning and resolution

Non Chronological Backtrackings

$$\phi_1 = x_1 \vee x_4$$
$$\phi_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$$
$$\phi_3 = x_1 \vee x_8 \vee x_{12}$$
$$\phi_4 = x_2 \vee x_{11}$$
$$\phi_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$
$$\phi_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$
$$\phi_7 = \overline{x_8} \vee \overline{x_7} \vee \overline{x_9}$$



$$\beta = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

From LookAhead to Lookback

All solvers are now turned to lazily detect Unit Propagation

No way to maintain counters for "smart" branching

Look ahead heuristics were "easy" to understand

Look back heuristics are very hard to study

Ingredients of an efficient SAT solver

Preprocessing
(and inprocessing)

Restarting

Branching

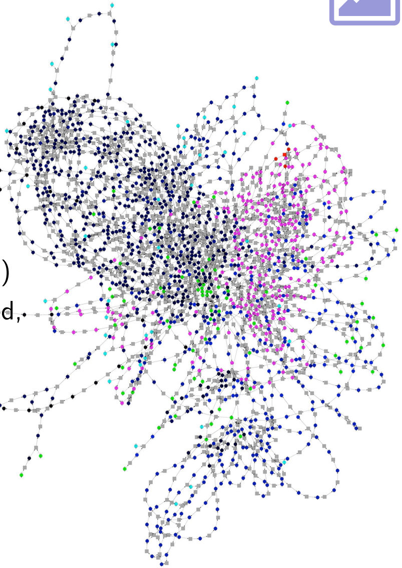
Conflict Analysis

Clause Database Cleaning

CDCL solvers are complex systems – Illustration

Example of a real conflict analysis :

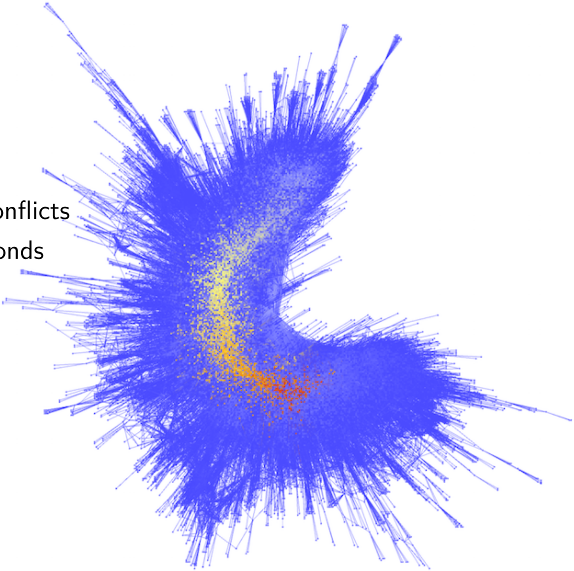
- Many resolutions at each conflict
- Very reactive VSIDS (1/10s lifetime)
- All components are tightly connected, side effects are everywhere



At least we know that we don't know

How to understand this (trivial) proof ?

- Less than 70 000 conflicts
- Solved in a few seconds
- A very dense proof
- Hard to understand



Bounded Model Checking at a glance

We have a system to verify, modeled by an automaton, encoding its state transitions

Correctness : No bugs A special state "error" is used in the model. The problem is about its reachability.

Liveness : No infinite loop Any state must be reachable from any other state, in any future.

Notice :

- Closely related to temporal logic ;
- Before SAT, BDD were used to solve these problems

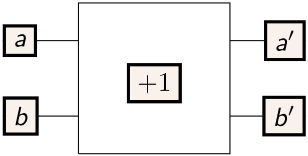
(Bounded) Model Checking at a glance

We fix a *bound* k, and increment it as we need

- The automaton is represented by the propositional logic function T that encodes the characteristics function of the reachable states.

Example (2-bits 1-adder) :

$$(a' \leftrightarrow \neg a) \land (b' \leftrightarrow a \oplus b)$$



$$(0,0) \rightarrow (1,0) \rightarrow (0,1) \rightarrow (1,1) \rightarrow (0,0) \rightarrow \dots$$

(Bounded) Model Checking at a glance

We fix a *bound* k, and increment it as we need

- The automaton is represented by the propositional logic function T that encodes the characteristics function of the reachable states. Example (2-bits 1-adder) : $(a' \leftrightarrow \neg a) \wedge (b' \leftrightarrow a \oplus b)$
- The property to check is (for instance) : $a \wedge b$ (is the state (11) reachable ?)
- The initial state is an assignment of variables at time step 0

BMC : Unrolling loops

Let us check whether the state (11) is reachable in 2 iterations

$I(s_0) = \neg a_0 \wedge \neg b_0$

$T(s_0, s_1) = (a_1 \leftrightarrow \neg a_0) \wedge (b_1 \leftrightarrow a_0 \oplus b_0)$

$T(s_1, s_2) = (a_2 \leftrightarrow \neg a_1) \wedge (b_2 \leftrightarrow a_1 \oplus b_1)$

$p(s_2) = a_2 \wedge b_2$

$p(s_0) = a_0 \wedge b_0$

$p(s_1) = a_1 \wedge b_1$

Finally, is the formula

$(\neg a_0 \wedge \neg b_0) \wedge ((a_1 \leftrightarrow \neg a_0) \wedge (b_1 \leftrightarrow a_0 \oplus b_0)) \wedge ((a_2 \leftrightarrow \neg a_1)$
$\wedge (b_2 \leftrightarrow a_1 \oplus b_1)) \wedge (a_2 \wedge b_2)$ satisfiable ?

BMC : Unrolling loops

Let us check whether the state (11) is reachable in 2 iterations

$I(s_0) = \neg a_0 \wedge \neg b_0$

$T(s_0, s_1) = (a_1 \leftrightarrow \neg a_0) \wedge (b_1 \leftrightarrow a_0 \oplus b_0)$

$T(s_1, s_2) = (a_2 \leftrightarrow \neg a_1) \wedge (b_2 \leftrightarrow a_1 \oplus b_1)$

$p(s_2) = a_2 \wedge b_2$

$p(s_0) = a_0 \wedge b_0$

$p(s_1) = a_1 \wedge b_1$

Finally, is the formula

$(\neg a_0 \wedge \neg b_0) \wedge ((a_1 \leftrightarrow \neg a_0) \wedge (b_1 \leftrightarrow a_0 \oplus b_0)) \wedge ((a_2 \leftrightarrow \neg a_1)$
$\wedge (b_2 \leftrightarrow a_1 \oplus b_1)) \wedge (a_2 \wedge b_2)$ satisfiable ?

BMC : Unrolling loops

Let us check whether the state (11) is reachable in 2 iterations

$I(s_0) = \neg a_0 \wedge \neg b_0$

$T(s_0, s_1) = (a_1 \leftrightarrow \neg a_0) \wedge (b_1 \leftrightarrow a_0 \oplus b_0)$

$T(s_1, s_2) = (a_2 \leftrightarrow \neg a_1) \wedge (b_2 \leftrightarrow a_1 \oplus b_1)$

$p(s_2) = a_2 \wedge b_2$

$p(s_0) = a_0 \wedge b_0$

$p(s_1) = a_1 \wedge b_1$

Finally, is the formula

$(\neg a_0 \wedge \neg b_0) \wedge ((a_1 \leftrightarrow \neg a_0) \wedge (b_1 \leftrightarrow a_0 \oplus b_0)) \wedge ((a_2 \leftrightarrow \neg a_1)$
$\wedge (b_2 \leftrightarrow a_1 \oplus b_1)) \wedge (a_2 \wedge b_2)$ satisfiable ?

Unbounded Model Checking

$$I \wedge T_1 \wedge T_2 \wedge \ldots \wedge T_k \wedge BUG_k$$

How to ensure that BUG is unreachable ?

Idea : find an invariant Inv s.t. BUG is not reachable in $k > 0$ steps

- Inv characterizes an over approximation of the reachable states in j steps :

$$I \wedge T_1 \wedge \cdots \wedge T_j \rightarrow Inv$$

- Inv is an inductive property :

$$Inv \wedge T_1 \rightarrow Inv_1$$

- BUG is not reachable from Inv in k steps :

$$Inv \wedge T_1 \wedge T_2 \wedge \ldots \wedge T_k \wedge BUG_k \equiv \bot$$

- Incremental SAT Solving / Proof Analysis

The Erdös Discrepancy Problem (1932)

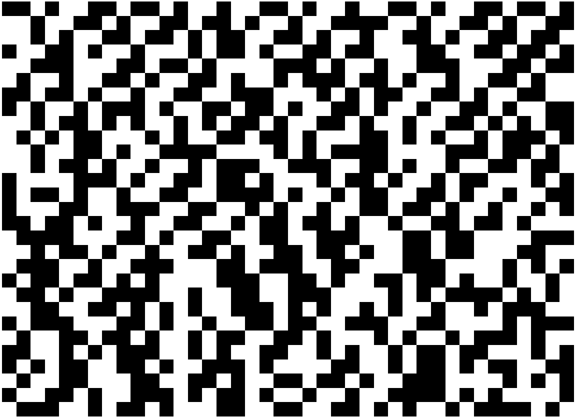
- Infinite series of +1 and -1 : $< -1, 1, 1, -1 - 1, 1, 1, \ldots >$
- $\forall C \; \exists k, d \;\; t.q. \;\; |\sum_{i=1}^{k} x_{i.d}| \geq C$

+	−	−	+	+	−	−	−	+	+	−	−1
	−		+		−		−		+		−1
		−			−			+			−1
			+				−				0
				+					+		+2

- Proven in 2014 for $C = 2$ (k=1161)
- The *proof* : UNSAT certificate (trace) from Glucose (13 Gb) [3]
- General case proven two years later by Terence Tao (previous proof considered as the biggest mathematical proof ever by T. Tao).

3. cgi.csc.liv.ac.uk/~konev/SAT14/

Solution for C=2, 1160 steps

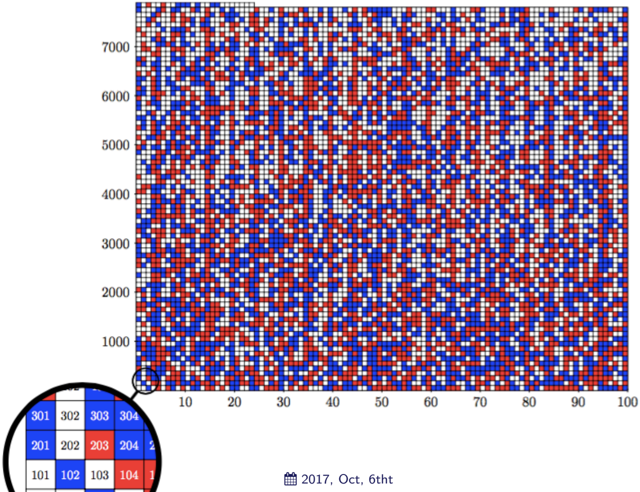


(For C=3, maximum solution is not yet known)

The "biggest proof" in the world

Boolean Pythagorean triples problem

Is it possible to colorize the n integers $\leq n$ in two colors s.t. no triplet (a, b, c) is $a^2 + b^2 = c^2$ monochromatic ?



The "biggest proof" in the world

No solution for n=7825

- Open question since 20 years
- 10^{2300} possible canidates
- SAT encoding
- Original problem splitted in 1,000,000 subproblems
- 800 CPUs

Proof is 200Tb long (Glucose's output)

- In practice the proof is not really kept

Other applications

Cryptography

- Find a crypto key / Hash function inversion

Biologie

- Metabolic Network Analysis
- Gene alignment

Software / Hardware verification

- Implementation complies with specifications
- Loop Invariants Discovery

Data Mining

- Not (yet) on Big Data

Optimisations problems

- Thousands calls to SAT solvers

Let us solve a Sudoku

A very simple example

		5		6	3			
9	4		8			7		
6						8		
						2	3	6
	6	7				9	5	
5	3	8						
		6						7
		4			5		2	1
			1	7		6		

Time for a (live) demo !

Conclusion

SAT solvers are efficient and not stalling

Many new and unexpected uses (incremental SAT)

You can prove your results (almost formally)

Parallel SAT Solvers is the new frontier (use as many CPU as you can)

Encode your problems now