



Habilitation à diriger les recherches

Gilles Audemard

29 novembre 2010





Définitions : le problème SAT

$$\begin{array}{l} \overline{x_1} \vee \overline{x_2} \vee x_3 \\ \wedge \qquad \qquad \qquad \overline{x_3} \\ \wedge x_1 \vee x_2 \\ \wedge \qquad \qquad x_2 \vee x_3 \end{array}$$

- Variables : $x_1 \dots x_3$
- Littéraux : $x_1, \overline{x_1}$
- Clauses : $\overline{x_1} \vee \overline{x_2} \vee x_3$
- Formule CNF
- Problème SAT : existe-il une interprétation des variables qui satisfait la formule ?

Définitions : le problème SAT

$$\begin{array}{l} \overline{x_1} \vee \overline{x_2} \vee x_3 \\ \wedge \qquad \qquad \qquad \overline{x_3} \\ \wedge x_1 \vee x_2 \\ \wedge \qquad \qquad x_2 \vee x_3 \end{array}$$

x_1	x_2	x_3
F	F	F

- Variables : $x_1 \dots x_3$
- Littéraux : $x_1, \overline{x_1}$
- Clauses : $\overline{x_1} \vee \overline{x_2} \vee x_3$
- Formule CNF
- Problème SAT : existe-il une interprétation des variables qui satisfait la formule ?

Définitions : le problème SAT

$$\begin{array}{l} \overline{x_1} \vee \overline{x_2} \vee x_3 \\ \wedge \quad \quad \quad \overline{x_3} \\ \wedge \quad x_1 \vee x_2 \\ \wedge \quad \quad x_2 \vee x_3 \end{array}$$

x_1	x_2	x_3
F	F	F

- Variables : $x_1 \dots x_3$
- Littéraux : $x_1, \overline{x_1}$
- Clauses : $\overline{x_1} \vee \overline{x_2} \vee x_3$
- Formule CNF
- Problème SAT : existe-il une interprétation des variables qui satisfait la formule ?

Définitions : le problème SAT

$$\begin{array}{l} \overline{x_1} \vee \overline{x_2} \vee x_3 \\ \wedge \quad \quad \quad \overline{x_3} \\ \wedge \quad x_1 \vee x_2 \\ \wedge \quad \quad x_2 \vee x_3 \end{array}$$

x_1	x_2	x_3
F	V	F

- Variables : $x_1 \dots x_3$
- Littéraux : $x_1, \overline{x_1}$
- Clauses : $\overline{x_1} \vee \overline{x_2} \vee x_3$
- Formule CNF
- Problème SAT : existe-il une interprétation des variables qui satisfait la formule ?

Définitions : le problème SAT

$$\begin{array}{l}
 \overline{x_1} \vee \overline{x_2} \vee x_3 \\
 \wedge \quad \quad \quad \overline{x_3} \\
 \wedge \quad x_1 \vee x_2 \\
 \wedge \quad \quad x_2 \vee x_3
 \end{array}$$

x_1	x_2	x_3
F	V	F

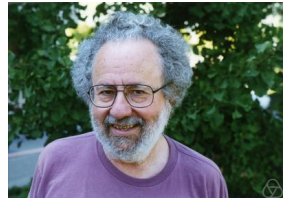


- Variables : $x_1 \dots x_3$
- Littéraux : $x_1, \overline{x_1}$
- Clauses : $\overline{x_1} \vee \overline{x_2} \vee x_3$
- Formule CNF
- Problème SAT : existe-il une interprétation des variables qui satisfait la formule ?
- Tester toutes les possibilités : illusoire !

Nombre d'instructions	Temps nécessaire
$2^3 = 8$	instantané
$2^{37} \approx 80 \times 10^9$	1 seconde
$2^{56} \approx 8 \times 10^{16}$	≈ 277 heures
$2^{60} \approx 10^{18}$	166 jours
$2^{128} \approx 340 \times 10^{38}$	≥ 3 milliards d'années

Historique

1960 DAVIS et PUTNAM



Martin DAVIS

Historique

1960 DAVIS et PUTNAM

1962 DAVIS, LOGEMANN et LOVELAND

...



Martin DAVIS

Historique

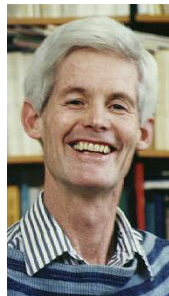
1960 DAVIS et PUTNAM

1962 DAVIS, LOGEMANN et LOVELAND

...

1971 SAT est NP-complet

...



Stephen COOK

Historique

1960 DAVIS et PUTNAM

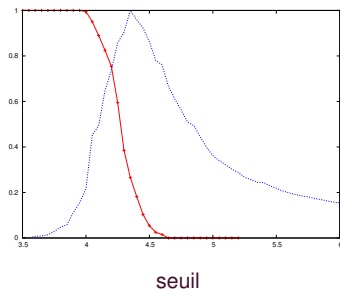
1962 DAVIS, LOGEMANN et LOVELAND

...

1971 SAT est NP-complet

...

1983 Formules aléatoires



Historique

1960 DAVIS et PUTNAM

1962 DAVIS, LOGEMANN et LOVELAND

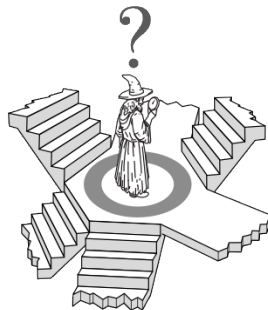
...

1971 SAT est NP-complet

...

1983 Formules aléatoires

1992 Recherche locale



Historique

1960 DAVIS et PUTNAM

1962 DAVIS, LOGEMANN et LOVELAND

...

1971 SAT est NP-complet

...

1983 Formules aléatoires

1992 Recherche locale

1999 BMC : Utilisation de SAT



Edmund CLARKE

Historique

1960 DAVIS et PUTNAM

1962 DAVIS, LOGEMANN et LOVELAND

...

1971 SAT est NP-complet

...

1983 Formules aléatoires

1992 Recherche locale

1999 BMC : Utilisation de SAT

2001 Solveur CDCL : ZCHAFF



Joao MARQUES-SILVA



Karem SAKALLAH

Historique

1960 DAVIS et PUTNAM

1962 DAVIS, LOGEMANN et LOVELAND

...

1971 SAT est NP-complet

...

1983 Formules aléatoires

1992 Recherche locale

1999 BMC : Utilisation de SAT

2001 Solveur CDCL : ZCHAFF



Lintao ZHANG



Sharad MALIK

Contributions

■ Amélioration des démonstrateurs CDCL

- ▶ Étude expérimentale intensive [CP 2008]
- ▶ Un cadre étendu pour l'analyse des conflits [SAT 2008]
- ▶ Qualité des clauses apprises [IJCAI 2009]
- ▶ Utilisation de la résolution étendue dans les solveurs CDCL [AAAI 2010]

Contributions

■ Amélioration des démonstrateurs CDCL

- ▶ Étude expérimentale intensive [CP 2008]
- ▶ Un cadre étendu pour l'analyse des conflits [SAT 2008]
- ▶ Qualité des clauses apprises [IJCAI 2009]
- ▶ Utilisation de la résolution étendue dans les solveurs CDCL [AAAI 2010]

■ Recherche locale pour l'insatisfiabilité

- ▶ GUNSAT, une méthode qui navigue au sein de l'espace de recherche par résolution [IJCAI 2007]
- ▶ Généralisation des graphes conflits aux méthodes de RL [ICTAI 2009]
- ▶ Méthode hybride [LPAR 2010]

Contributions

■ Amélioration des démonstrateurs CDCL

- ▶ Étude expérimentale intensive [CP 2008]
- ▶ Un cadre étendu pour l'analyse des conflits [SAT 2008]
- ▶ Qualité des clauses apprises [IJCAI 2009]
- ▶ Utilisation de la résolution étendue dans les solveurs CDCL [AAAI 2010]

■ Recherche locale pour l'insatisfiabilité

- ▶ GUNSAT, une méthode qui navigue au sein de l'espace de recherche par résolution [IJCAI 2007]
- ▶ Généralisation des graphes conflits aux méthodes de RL [ICTAI 2009]
- ▶ Méthode hybride [LPAR 2010]

■ Travaux connexes

- ▶ Codage basé sur les circuits [SAT 2007]
- ▶ Représentation graphique des CNF [JALIC 2008]

Contributions

■ Amélioration des démonstrateurs CDCL

- ▶ Étude expérimentale intensive [CP 2008]
- ▶ Un cadre étendu pour l'analyse des conflits [SAT 2008]
- ▶ **Qualité des clauses apprises** [IJCAI 2009]
- ▶ Utilisation de la résolution étendue dans les solveurs CDCL [AAAI 2010]

■ Recherche locale pour l'insatisfiabilité

- ▶ **GUNSAT, une méthode qui navigue au sein de l'espace de recherche par résolution** [IJCAI 2007]
- ▶ **Généralisation des graphes conflits aux méthodes de RL** [ICTAI 2009]
- ▶ Méthode hybride [LPAR 2010]

■ Travaux connexes

- ▶ Codage basé sur les circuits [SAT 2007]
- ▶ Représentation graphique des CNF [JALIC 2008]

Qualité des clauses apprises

Un bref aperçu des démonstrateurs CDCL

Séquence de décision, Propagation

$$C_1 = x_1 \vee x_4$$

$$C_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$$

$$C_3 = x_1 \vee x_8 \vee x_{12}$$

$$C_4 = x_2 \vee x_{11}$$

$$C_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$

$$C_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$

$$C_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$$

Un bref aperçu des démonstrateurs CDCL

Séquence de décision, Propagation

DL 1



$$C_1 = \overline{x_1} \vee x_4$$

$$C_2 = \overline{x_1} \vee \overline{x_3} \vee \overline{x_8}$$

$$C_3 = \overline{x_1} \vee x_8 \vee x_{12}$$

$$C_4 = x_2 \vee x_{11}$$

$$C_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$

$$C_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$

$$C_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$$

Un bref aperçu des démonstrateurs CDCL

Séquence de décision, Propagation

DL 1



$$c_1 = x_1 \vee x_4$$

$$c_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$$

$$c_3 = x_1 \vee x_8 \vee x_{12}$$

$$c_4 = x_2 \vee x_{11}$$

$$c_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$

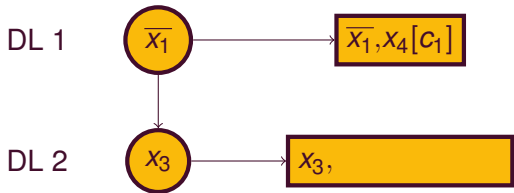
$$c_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$

$$c_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$$

Un bref aperçu des démonstrateurs CDCL

Séquence de décision, Propagation

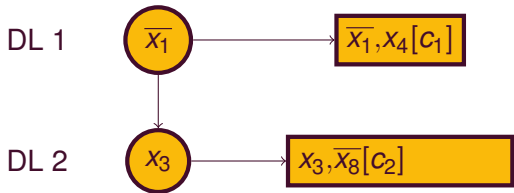
$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$



Un bref aperçu des démonstrateurs CDCL

Séquence de décision, Propagation

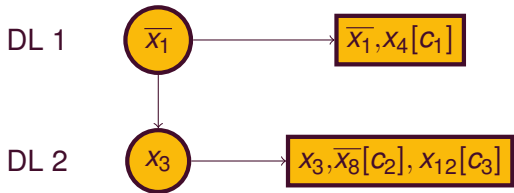
$$\begin{aligned}C_1 &= x_1 \vee x_4 \\C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\C_3 &= x_1 \vee x_8 \vee x_{12} \\C_4 &= x_2 \vee x_{11} \\C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}\end{aligned}$$



Un bref aperçu des démonstrateurs CDCL

Séquence de décision, Propagation

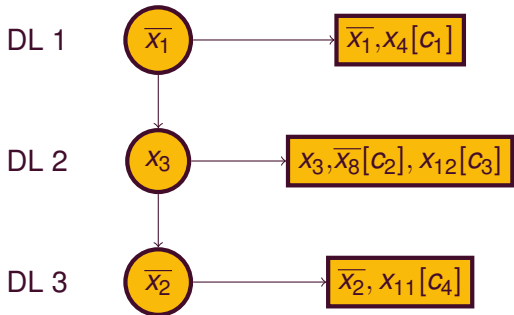
$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$



Un bref aperçu des démonstrateurs CDCL

Séquence de décision, Propagation

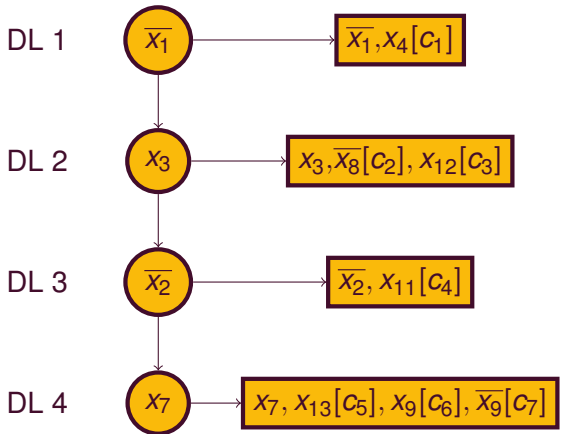
$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$



Un bref aperçu des démonstrateurs CDCL

Séquence de décision, Propagation

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$



Un bref aperçu des démonstrateurs CDCL

Analyse de conflits

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$

DL 4



Un bref aperçu des démonstrateurs CDCL

Analyse de conflits

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$

DL 4



$$d^* = c_7 \otimes_{x_9} c_6 = \overline{x_3} \vee x_8 \vee \overline{x_7} \vee \overline{x_{13}}$$

Un bref aperçu des démonstrateurs CDCL

Analyse de conflits

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$

DL 4



$$d^* = c_7 \otimes_{x_9} c_6 = \overline{x_3} \vee x_8 \vee \overline{x_7} \vee \overline{x_{13}}$$

$$d_1 = d^* \otimes_{x_{13}} c_5 = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

Un bref aperçu des démonstrateurs CDCL

Analyse de conflits

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$

DL 4



$$d^* = c_7 \otimes_{x_9} c_6 = \overline{x_3} \vee x_8 \vee \overline{x_7} \vee \overline{x_{13}}$$

$$d_1 = d^* \otimes_{x_{13}} c_5 = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

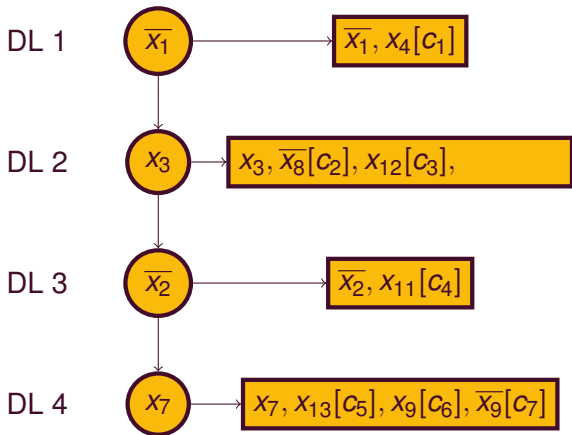
- Première résolvante qui ne contient qu'un littéral du niveau de décision courant
- Schéma d'apprentissage appelé le premier UIP
- d_1 est ajoutée à la base des clauses apprises, et...

Un bref aperçu des démonstrateurs CDCL

Backjumping

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$

$$d_1 = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

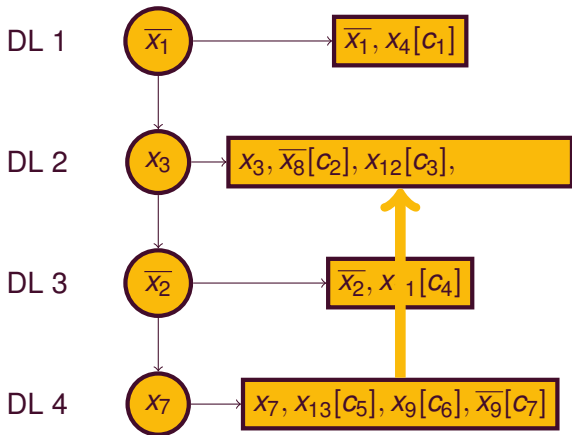


Un bref aperçu des démonstrateurs CDCL

Backjumping

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$

$$d_1 = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

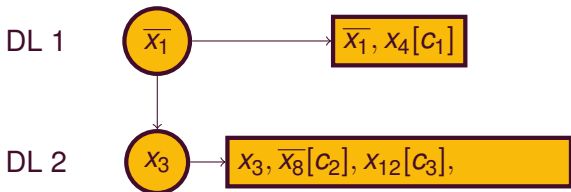


Un bref aperçu des démonstrateurs CDCL

Backjumping

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$

$$d_1 = \overline{x_3} \vee x_8 \vee \overline{x_7}$$

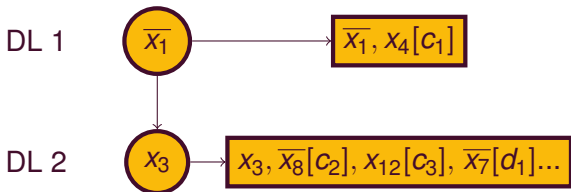


Un bref aperçu des démonstrateurs CDCL

Backjumping

$$\begin{aligned}
 C_1 &= x_1 \vee x_4 \\
 C_2 &= x_1 \vee \overline{x_3} \vee \overline{x_8} \\
 C_3 &= x_1 \vee x_8 \vee x_{12} \\
 C_4 &= x_2 \vee x_{11} \\
 C_5 &= \overline{x_3} \vee \overline{x_7} \vee x_{13} \\
 C_6 &= \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9 \\
 C_7 &= x_8 \vee \overline{x_7} \vee \overline{x_9}
 \end{aligned}$$

$$d_1 = \overline{x_3} \vee x_8 \vee \overline{x_7}$$



Autres composants essentiels

- Heuristique de choix de variables
 - ▶ Dynamiques : récompensent les variables les plus récemment utilisées dans l'analyse de conflits
 - ▶ Enregistrement de la phase

- Redémarrages : statiques ou dynamiques

- Un composant sous-estimé : le nettoyage de la base de clauses
 - ▶ Pour éviter une explosion de la mémoire utilisée, il est nécessaire de supprimer certaines clauses apprises
 - ▶ Lesquelles ?
 - ▶ Jusqu'à récemment : les clauses intéressantes étaient supposées être celles utilisées récemment dans l'analyse de conflits

Déterminer les clauses apprises importantes

Expérimentations intensives

■ Solveurs de type lookahead

« Si on veut savoir où aller, on doit savoir où l'on est »

- ▶ Implantation d'idées visant à réduire/équilibrer l'arbre de recherche
- ▶ Heuristiques, failed literal
- ▶ L'explication des performances est (relativement) simple

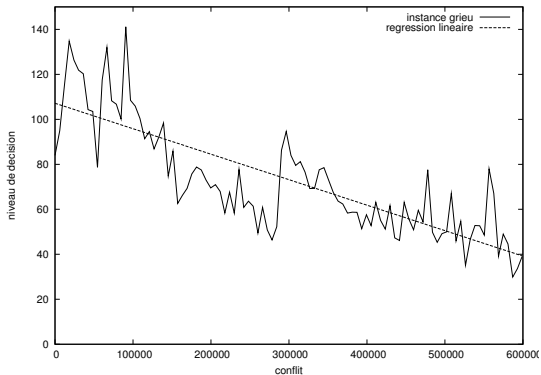
■ Solveurs de type lookback (CDCL)

« On ne sait pas où l'on est, mais on sait où l'on va »

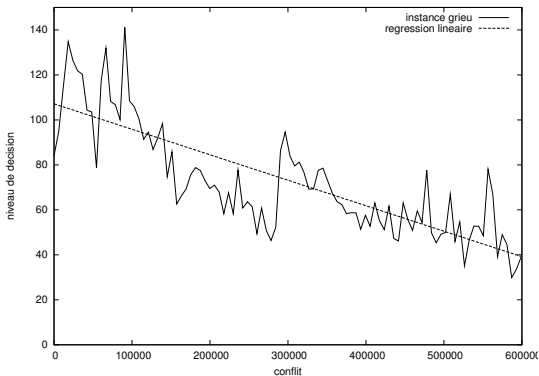
- ▶ De nombreuses variables
- ▶ Des redémarrages
- ▶ Explication des performances plus difficile

Besoin d'expérimentations solides pour comprendre le fonctionnement et améliorer les performances

Décroissance



Décroissance



Series	#Benchs	% Decr.
een	8	62%
goldb	11	100%
grieu	7	71%
hoons	5	100%
ibm-2002	7	71%
ibm-2004	13	92%
manol-pipe	55	91%
miz	13	0%
schup	5	80%
simon	10	90%
vange	3	66%
velev	54	92%
all	199	83%

La mesure LBD

- Nombreuses tentatives pour déterminer la qualité d'une clause apprise
- Nombreux échecs aussi !
- Intuition : plus les niveaux de décision vont décroître vite, plus vite l'instance sera résolue
- Plus elle établit de liens forts entre blocs de propagations, meilleure est la clause

Literal Block Distance – LBD

Nombre de blocs différents de littéraux propagés

- Mesure calculée à la création de la clause

Retour sur un exemple

$$c_1 = x_1 \vee x_4$$

$$c_2 = x_1 \vee \overline{x_3} \vee \overline{x_8}$$

$$c_3 = x_1 \vee x_8 \vee x_{12}$$

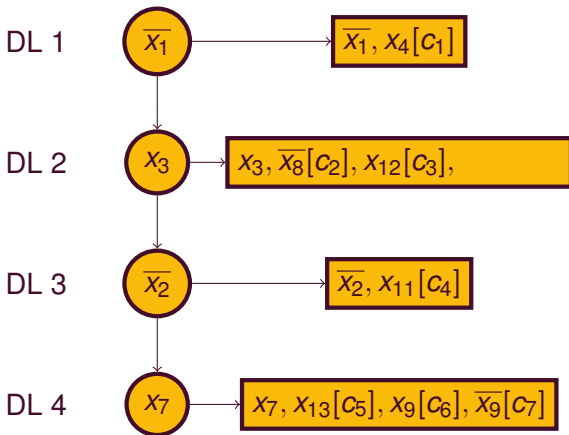
$$c_4 = x_2 \vee x_{11}$$

$$c_5 = \overline{x_3} \vee \overline{x_7} \vee x_{13}$$

$$c_6 = \overline{x_3} \vee \overline{x_7} \vee \overline{x_{13}} \vee x_9$$

$$c_7 = x_8 \vee \overline{x_7} \vee \overline{x_9}$$

$$d_1 = \overline{x_3} \vee x_8 \vee \overline{x_7}$$



d_1 a un LBD égal à 2

Les clauses glues

- Les clauses de LBD égal à 2 sont très importantes : elles collent deux blocs de propagations entre eux
- Ce sont les clauses glues



Les clauses glues

- Les clauses de LBD égal à 2 sont très importantes : elles collent deux blocs de propagations entre eux
- Ce sont les clauses glues

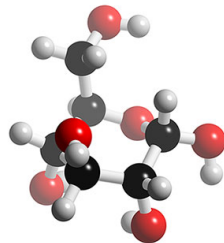
	2	3	4	5
LBD	2452	295	136	80
taille	1827	884	305	195

Moyenne d'utilisation des clauses apprises
dans l'analyse de conflits



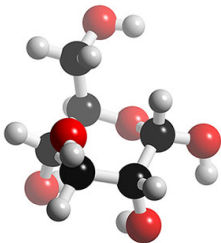
GLUCOSE, un solveur qui aime les clauses glues

- Les clauses intéressantes sont identifiées



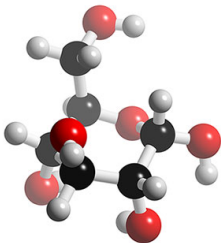
GLUCOSE, un solveur qui aime les clauses glues

- Les clauses intéressantes sont identifiées
- Politique agressive de suppression des *mauvaises* clauses apprises
 - ▶ Conservation d'un bon taux de propagation unitaire
 - ▶ Sans désavantager le solveur



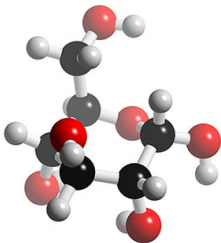
GLUCOSE, un solveur qui aime les clauses glues

- Les clauses intéressantes sont identifiées
- Politique agressive de suppression des *mauvaises* clauses apprises
 - ▶ Conservation d'un bon taux de propagation unitaire
 - ▶ Sans désavantager le solveur
- Récompenser les bonnes variables
- Stratégie de redémarrage dynamique : favoriser la décroissance



GLUCOSE, un solveur qui aime les clauses glues

- Les clauses intéressantes sont identifiées
- Politique agressive de suppression des *mauvaises* clauses apprises
 - ▶ Conservation d'un bon taux de propagation unitaire
 - ▶ Sans désavantager le solveur
- Récompenser les bonnes variables
- Stratégie de redémarrage dynamique : favoriser la décroissance
- GLUCOSE a gagné la compétition SAT 2009, catégorie application, UNSAT
- Mesure aujourd'hui utilisée dans de nombreux solveurs



Recherche locale pour l'insatisfiabilité

Introduction



- Exploration d'autres voies de recherche
- Le recherche locale a surtout été utilisée pour trouver un modèle à une formule
- L'adapter à l'insatisfiabilité [ANR UNLOC]
- Challenge pour la communauté (proposé en 1997 par SELMAN et al.)

Recherche locale pour la satisfiabilité

- Méthode incomplète :
répond SAT ou ?

Recherche locale pour la satisfiabilité

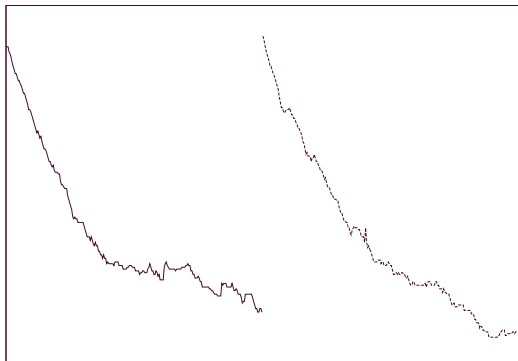
- Méthode incomplète :
répond SAT ou ?
- Interprétation complète
- Étape :
changer la valeur d'une variable

Recherche locale pour la satisfiabilité

- Méthode incomplète :
répond SAT ou ?
- Interprétation complète
- Étape :
changer la valeur d'une variable
- Distance d'une solution ?
- Réduire le nombre de clauses
UNSAT

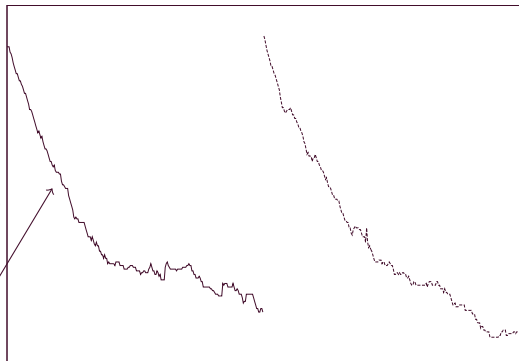
Recherche locale pour la satisfiabilité

- Méthode incomplète :
répond SAT ou ?
- Interprétation complète
- Étape :
changer la valeur d'une variable
- Distance d'une solution ?
- Réduire le nombre de clauses
UNSAT



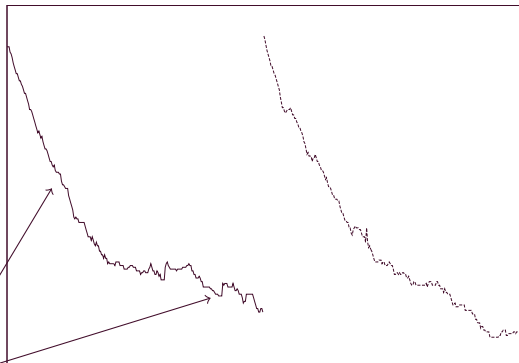
Recherche locale pour la satisfiabilité

- Méthode incomplète :
répond SAT ou ?
- Interprétation complète
- Étape :
changer la valeur d'une variable
- Distance d'une solution ?
- Réduire le nombre de clauses
UNSAT



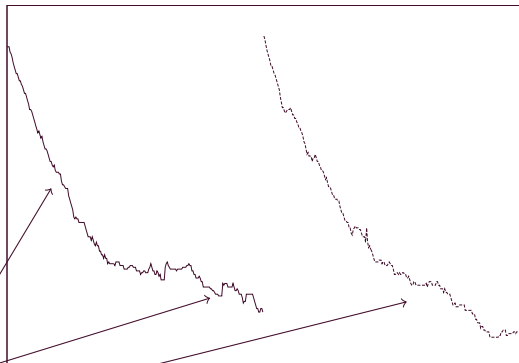
Recherche locale pour la satisfiabilité

- Méthode incomplète :
répond SAT ou ?
- Interprétation complète
- Étape :
changer la valeur d'une variable
- Distance d'une solution ?
- Réduire le nombre de clauses
UNSAT
- Critère d'échappement des
minimum locaux



Recherche locale pour la satisfiabilité

- Méthode incomplète :
répond SAT ou ?
- Interprétation complète
- Étape :
changer la valeur d'une variable
- Distance d'une solution ?
- Réduire le nombre de clauses
UNSAT
- Critère d'échappement des
minimum locaux
- Redémarrages



Difficultés d'adaptation à UNSAT

■ Recherche locale et SAT

- ▶ Taille du certificat linéaire
- ▶ Mesure indiquant la distance à une solution (nombre de clauses UNSAT)

■ Recherche locale et UNSAT

- ▶ Taille du certificat n'est plus bornée polynomialement
- ▶ Comment savoir la distance qui nous sépare de la preuve ?

■ 2 propositions

GUNSAT, un solveur qui aime les contradictions

- Transposition des méthodes de recherche locales à UNSAT
- Un flip est une clause obtenue par résolution
- On essaie de se rapprocher de la contradiction
- Score basé sur des couples de littéraux : combien de modèles sont supposés être filtrés par ce couple
- Introduction de la résolution étendue
- Des performances *mauvaises*

CDLS, un solveur éclectique

- Algorithme de recherche locale classique
- Extension de l'analyse de conflits
 - ▶ Pas de littéraux de décision
 - ▶ Pas de littéraux propagés
- Propriétés des minimums locaux (clauses critiques et liées)
- L'apprentissage nous sert également à sortir des minimums
- CDLS est capable de prouver SAT et UNSAT
- Bonnes *performances*
- Base d'un solveur hybride

En résumé

Atouts de SAT

- Aujourd'hui, SAT est une technologie éprouvée !
- De nombreux progrès théoriques et pratiques
- Utilisé dans de nombreux domaines (cryptographie, vérification. . .)



Edmund CLARKE

« La résolution pratique du problème SAT est une technologie clé pour l'informatique du 21ème siècle. »

Points faibles de SAT

- Des instances de plus en plus dures sont proposées
- Tailles des formules
- Perte de la structure
- Manque d'expressivité



Points faibles de SAT

- Des instances de plus en plus dures sont proposées
- Tailles des formules
- Perte de la structure
- Manque d'expressivité
- D'autres formulations
 - ▶ Clauses de cardinalité
 - ▶ Formules Pseudo Booléennes
 - ▶ Formules Booléennes Quantifiées
 - ▶ SAT Modulo Théories



Contributions autour de SAT

■ Autour de QBF

- ▶ Détection et suppression des symétries
- ▶ QBFBDD Un solveur qui s'abstrait de l'ordre

[SAT 2004,IJCAI 2007]

[SAT 2005]

Contributions autour de SAT

■ Autour de QBF

- ▶ Détection et suppression des symétries [SAT 2004,IJCAI 2007]
- ▶ QBFBDD Un solveur qui s'abstrait de l'ordre [SAT 2005]

■ Autour de SMT

- ▶ MATHSAT, un solveur SMT avec des équations mathématiques [CADE 2002]
- ▶ Application aux automates temporels [FORTE 2002]

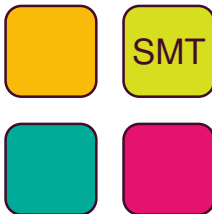
Contributions autour de SAT

■ Autour de QBF

- ▶ Détection et suppression des symétries [SAT 2004,IJCAI 2007]
- ▶ QBFBDD Un solveur qui s'abstrait de l'ordre [SAT 2005]

■ Autour de SMT

- ▶ MATHSAT, un solveur SMT avec des équations mathématiques [CADE 2002]
- ▶ Application aux automates temporels [FORTE 2002]



Le problème SMT

Décider de la satisfiabilité d'une formule SAT contenant des atomes d'une théorie donnée T

- Égalité sur des fonctions non interprétées
- Lecture, écriture dans un tableau
- Arithmétique linéaire

Le problème SMT

Décider de la satisfiabilité d'une formule SAT contenant des atomes d'une théorie donnée T

- Égalité sur des fonctions non interprétées
- Lecture, écriture dans un tableau
- Arithmétique linéaire

Le problème SMT

Décider de la satisfiabilité d'une formule SAT contenant des atomes d'une théorie donnée T

$$\begin{aligned}
 & \overline{(2v_2 - v_3 > 2)} \vee x_1 \\
 & \overline{x_2} \vee (2v_1 - 4v_5 > 3) \\
 & (3v_1 - 2v_2 \leq 3) \vee x_2 \\
 & \overline{(2v_3 + v_4 \geq 5)} \vee \overline{(3v_1 - v_3 \leq 6)} \vee \overline{x_1} \\
 & x_1 \vee (3v_1 - 2v_2 \leq 3) \\
 & (v_1 - v_5 \leq 1) \vee (v_5 = 5 - 3v_4) \vee \overline{x_1} \\
 & x_1 \vee (v_3 = 3v_5 + 4) \vee x_2
 \end{aligned}$$

 x_1 x_2 v_1 v_2 v_3 v_4 v_5

Le problème SMT

Décider de la satisfiabilité d'une formule SAT contenant des atomes d'une théorie donnée T

$$\begin{aligned}
 & \overline{(2v_2 - v_3 > 2)} \vee x_1 \\
 & \overline{x_2} \vee (2v_1 - 4v_5 > 3) \\
 & (3v_1 - 2v_2 \leq 3) \vee x_2 \\
 & \overline{(2v_3 + v_4 \geq 5)} \vee \overline{(3v_1 - v_3 \leq 6)} \vee \overline{x_1} \\
 & x_1 \vee (3v_1 - 2v_2 \leq 3) \\
 & (v_1 - v_5 \leq 1) \vee (v_5 = 5 - 3v_4) \vee \overline{x_1} \\
 & x_1 \vee (v_3 = 3v_5 + 4) \vee x_2
 \end{aligned}$$

$$x_1 = F$$

$$x_2 = F$$

$$v_1 = 0$$

$$v_2 = -1.5$$

$$v_3 = -5$$

$$v_4$$

$$v_5 = -3$$

Le problème SMT

Décider de la satisfiabilité d'une formule SAT contenant des atomes d'une théorie donnée T

$$\begin{aligned}
 & \overline{(2v_2 - v_3 > 2)} \vee x_1 \\
 & \overline{x_2} \vee (2v_1 - 4v_5 > 3) \\
 & (3v_1 - 2v_2 \leq 3) \vee x_2 \\
 & \overline{(2v_3 + v_4 \geq 5)} \vee \overline{(3v_1 - v_3 \leq 6)} \vee \overline{x_1} \\
 & x_1 \vee (3v_1 - 2v_2 \leq 3) \\
 & (v_1 - v_5 \leq 1) \vee (v_5 = 5 - 3v_4) \vee \overline{x_1} \\
 & x_1 \vee (v_3 = 3v_5 + 4) \vee x_2
 \end{aligned}$$

$$x_1 = F$$

$$x_2 = F$$

$$v_1 = 0$$

$$v_2 = -1.5$$

$$v_3 = -5$$

$$v_4$$

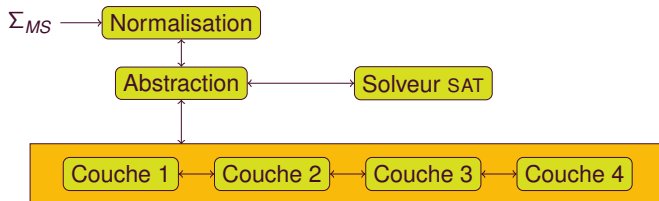
$$v_5 = -3$$

MATHSAT

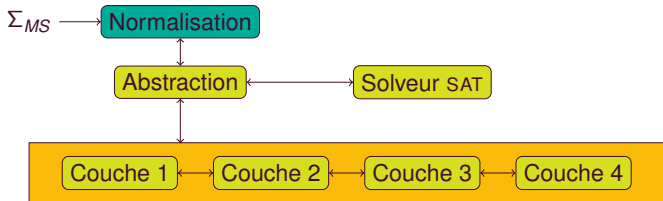
MATHSAT, un solveur qui aime les maths

- MATHSAT est un solveur utilisant l'approche paresseuse
- Utilisation d'un solveur SAT classique
- Abstraction :
 - ▶ Les atomes mathématiques sont associés à des nouvelles variables propositionnelles
- On va commencer par chercher un modèle propositionnel
- Architecture sous forme de couches

ARCHITECTURE DE MATHSAT



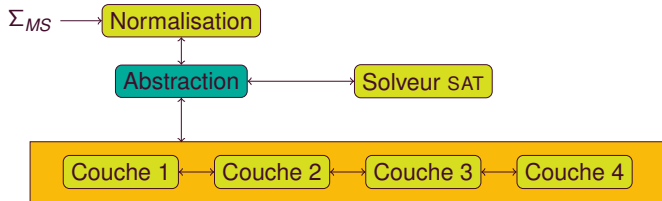
ARCHITECTURE DE MATHSAT



Normalisation

- Très importante
- Découvrir les atomes mathématiques sémantiquement équivalents mais syntaxiquement différents : $(v_1 - v_2) \leq 0$ et $v_1 \leq v_2$

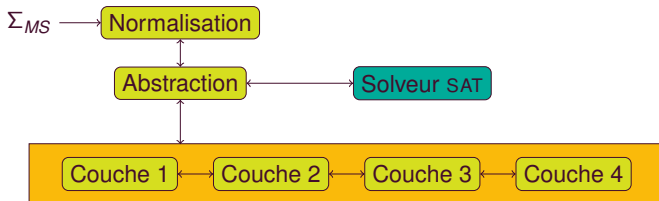
ARCHITECTURE DE MATHSAT



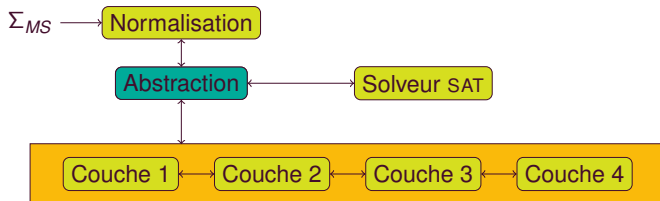
Abstraction

- Introduction d'une variable propositionnelle par atome mathématique différent
- La formule est considérée comme une formule SAT classique

ARCHITECTURE DE MATHSAT



ARCHITECTURE DE MATHSAT

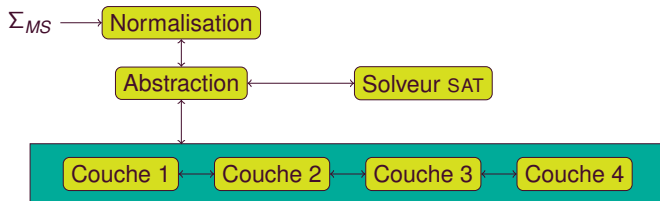


Abstraction

- Extraction des atomes mathématiques affectés à vrai ou faux

$$\overline{x_1}, \overline{x_2}, \overline{(2v_2 - v_3 > 2)}, (2v_1 - 4v_5 > 3), (3v_1 - 2v_2 \leq 3), (v_3 = 3v_5 + 4)$$

ARCHITECTURE DE MATHSAT

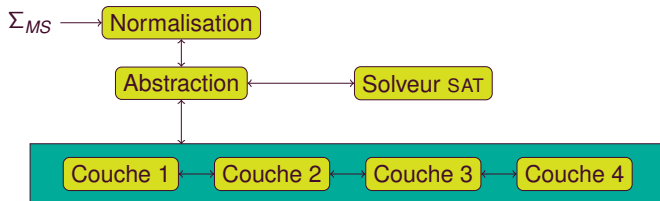


Abstraction

- Extraction des atomes mathématiques affectés à vrai ou faux

$$\overline{(2v_2 - v_3 > 2)}, (2v_1 - 4v_5 > 3), (3v_1 - 2v_2 \leq 3), (v_3 = 3v_5 + 4)$$

ARCHITECTURE DE MATHSAT



Les couches mathématiques

- Couche 1 : Raisonnement sur les égalités
- Couche 2 : Raisonnement sur les inéquations $v_i - v_j \leq c$
- Couche 3 : Raisonnement sur les inéquations quelconques : simplexe
- Couche 4 : Raisonnement sur les inégalités

BMC sur les automates temporels

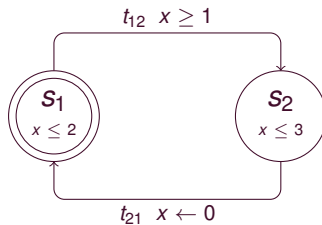

Bounded Model Checking

- Vérifier qu'un automate représentant un système quelconque vérifie une propriété donnée (atteignabilité d'un état. . .)
- Propriété exprimée sous forme LTL
- Plutôt que d'essayer de prouver que la propriété est vraie on va essayer de montrer qu'elle est fausse en bornant le nombre d'étapes
- Complémentaire à la vérification formelle, recherche de bugs dans le système
- Problème pouvant être encodé en SAT

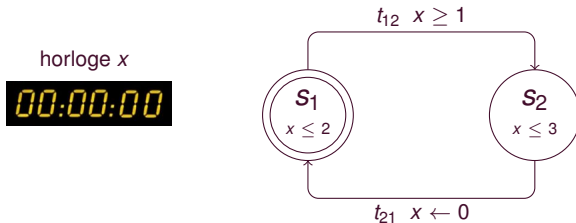
Extension aux automates temporels

Exemple

horloge x



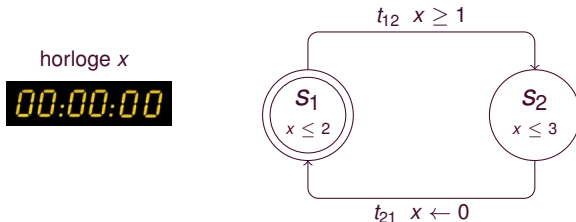
Exemple



■ A l'étape k

- ▶ Variable rationnelle z^k donne le temps courant
- ▶ Variable rationnelle associée 0_x^k à l'horloge : $x^k = 0_x^k - z^k$
- ▶ Variables booléennes pour les états : s_i^k est vrai si on est dans l'état s_i
- ▶ Variables booléennes pour les transitions : t_{ij}^k est vrai si on utilise la transition t_{ij} à l'étape k
- ▶ δ^k est vrai si on fait avancer le chronomètre

Exemple



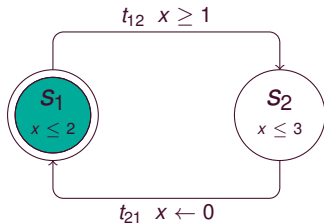
Quelques contraintes

- On se trouve dans un seul état : $(s_1^k \vee s_2^k) \wedge (\overline{s_1^k} \vee \overline{s_2^k})$
- On fait une seule action : $(\delta^k \vee t_{12}^k \vee t_{21}^k) \wedge (\overline{\delta^k} \vee \overline{t_{12}^k}) \wedge \dots$
- On fait avancer le temps : $(\overline{\delta^k} \vee (z^{k+1} - z^k < 0)) \wedge (\overline{\delta^k} \vee (0_x^k - 0_x^{k+1} = 0)) \wedge (\overline{\delta^k} \vee \overline{s_1^k} \vee s_1^{k+1}) \dots$
- de s_1 vers s_2 : $(\overline{s_1^k} \vee \overline{t_{12}^k} \vee \overline{(0_x^k - z^k \geq 1)}) \vee s_2^{k+1}$

Exemple

horloge x

00:00:00



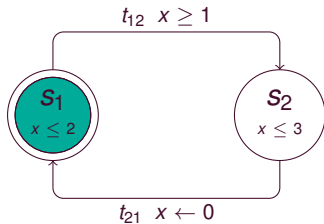
Étape 0

s_1	T
s_2	F
z	0
0_x	0

Exemple

horloge x

00:00:01



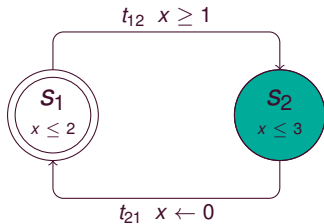
Étape 0 δ^0 1

s_1	T	T
s_2	F	F
z	0	-1
0_x	0	0

Exemple

horloge x

00:00:01

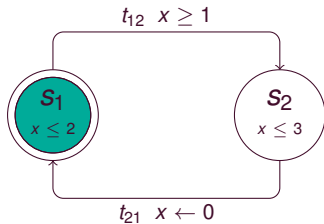


Étape	0	δ^0	1	t_{12}^1	2
s_1	T		T		F
s_2	F		F		T
z	0		-1		-1
0_x	0		0		0

Exemple

horloge x

00:00:00



Étape	0	δ^0	1	t_{12}^1	2	t_{21}^2	3
s_1	T		T		F		T
s_2	F		F		T		F
z	0		-1		-1		-1
0_x	0		0		0		-1

Perspectives

■ Autour de SAT

- ▶ Résolution étendue
- ▶ Solveurs CDCL
- ▶ Architecture multi-coeurs

■ Autour de SMT

- ▶ SMT et contraintes globales

■ Et après

- ▶ Problèmes d'optimisation MAXSAT, MAXSMT
- ▶ Applications : cryptanalyse asymétrique...