



Chronological vs Non-Chronological Backtracking in SMT

Master Thesis Defense

Robin Coutelier

U. Liège, Liège, Belgium
`robin.coutelier@student.uliege.be`

4 September 2023

Introduction

- SMT used in verification
- Core of SMT solvers: SAT solver
- Modern SAT solvers use CDCL
- [Nadel and Ryvchin, 2018, Möhle and Biere, 2019] re-introduced chronological backtracking
- What is the impact of CB on SMT solving?

SMT Solver

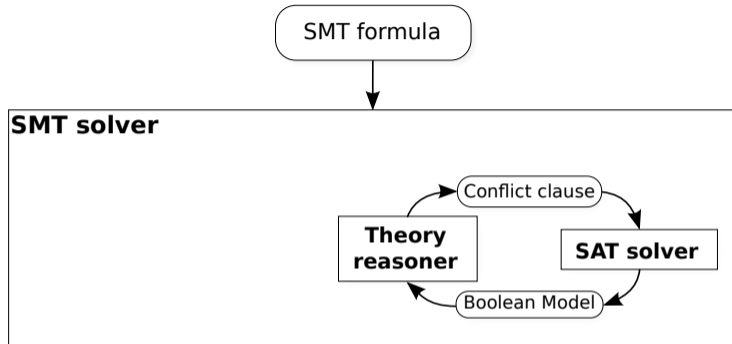


Figure: Schematic of a typical SMT solver (from [Fontaine and Boigelot, 2023]).

What is Chronological Backtracking? [Nadel and Ryvchin, 2018]

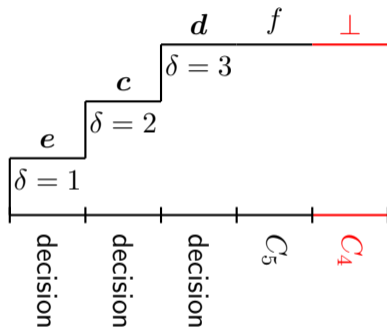
$$C_1 = a \vee b \vee c$$

$$C_2 = \neg b \vee d$$

$$C_3 = \neg a \vee d$$

$$C_4 = \neg e \vee \neg d \vee \neg f$$

$$C_5 = \neg d \vee f$$



What is Chronological Backtracking? [Nadel and Ryvchin, 2018]

$$C_1 = a \vee b \vee c$$

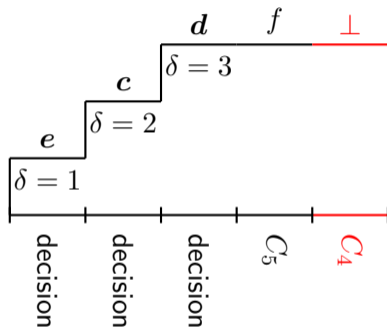
$$C_2 = \neg b \vee d$$

$$C_3 = \neg a \vee d$$

$$C_4 = \neg e \vee \neg d \vee \neg f$$

$$C_5 = \neg d \vee f$$

$$C_6 = \neg d \vee \neg e$$



What is Chronological Backtracking? [Nadel and Ryvchin, 2018]

$$C_1 = a \vee b \vee c$$

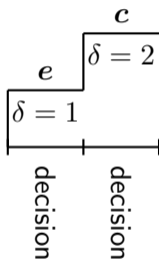
$$C_2 = \neg b \vee d$$

$$C_3 = \neg a \vee d$$

$$C_4 = \neg e \vee \neg d \vee \neg f$$

$$C_5 = \neg d \vee f$$

$$C_6 = \neg d \vee \neg e$$



What is Chronological Backtracking? [Nadel and Ryvchin, 2018]

$$C_1 = a \vee b \vee c$$

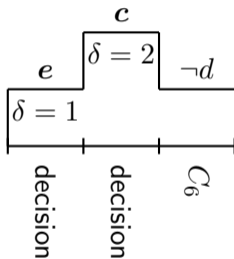
$$C_2 = \neg b \vee d$$

$$C_3 = \neg a \vee d$$

$$C_4 = \neg e \vee \neg d \vee \neg f$$

$$C_5 = \neg d \vee f$$

$$C_6 = \neg d \vee \neg e$$



What is Chronological Backtracking? [Nadel and Ryvchin, 2018]

$$C_1 = a \vee b \vee c$$

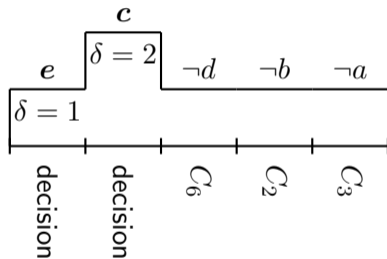
$$C_2 = \neg b \vee d$$

$$C_3 = \neg a \vee d$$

$$C_4 = \neg e \vee \neg d \vee \neg f$$

$$C_5 = \neg d \vee f$$

$$C_6 = \neg d \vee \neg e$$



What is Chronological Backtracking? [Nadel and Ryvchin, 2018]

$$C_1 = a \vee b \vee c$$

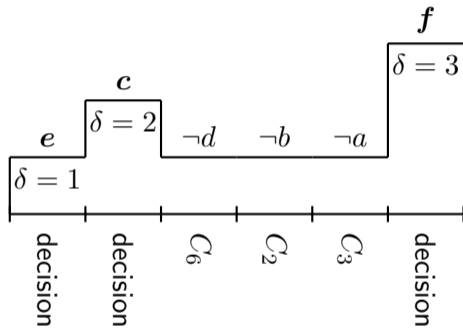
$$C_2 = \neg b \vee d$$

$$C_3 = \neg a \vee d$$

$$C_4 = \neg e \vee \neg d \vee \neg f$$

$$C_5 = \neg d \vee f$$

$$C_6 = \neg d \vee \neg e$$



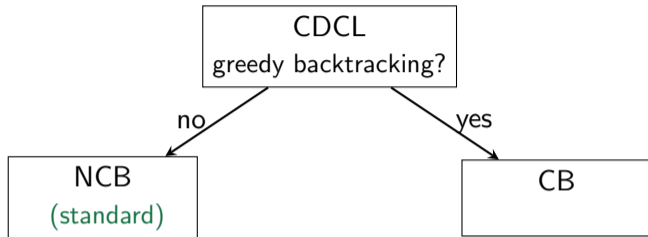
Backtracking Strategies

CDCL

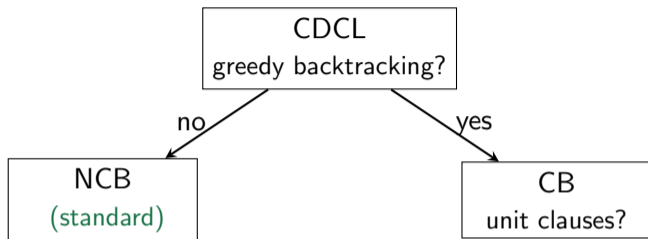
Backtracking Strategies

CDCL
greedy backtracking?

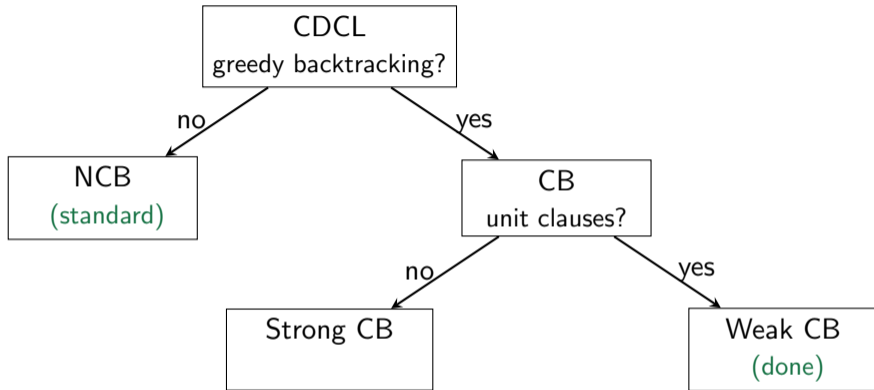
Backtracking Strategies



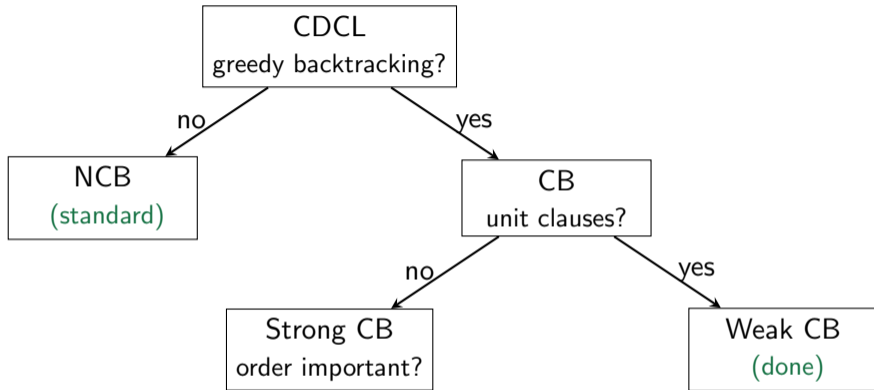
Backtracking Strategies



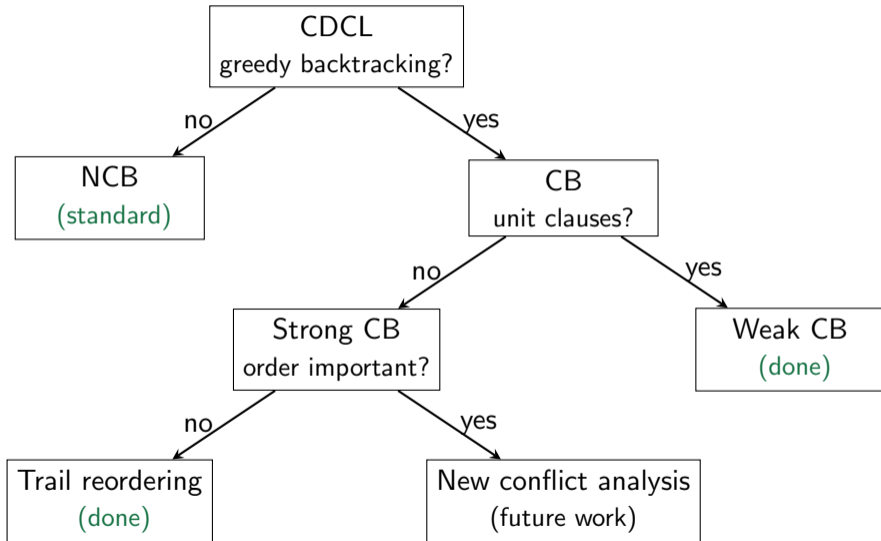
Backtracking Strategies



Backtracking Strategies



Backtracking Strategies



Example Reminder

$$C_1 = a \vee b \vee c$$

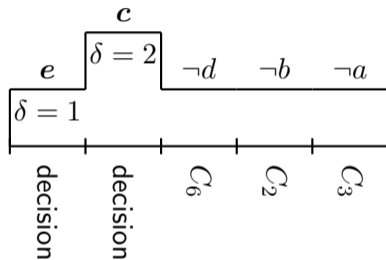
$$C_2 = \neg b \vee d$$

$$C_3 = \neg a \vee d$$

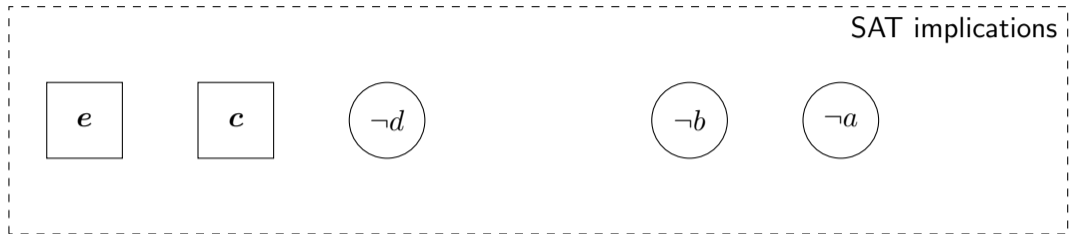
$$C_4 = \neg e \vee \neg d \vee \neg f$$

$$C_5 = \neg d \vee f$$

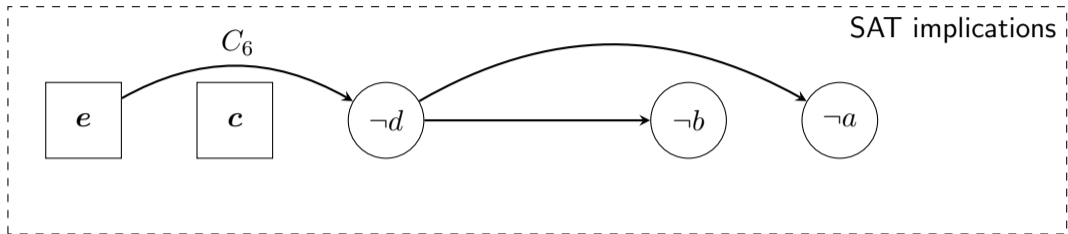
$$C_6 = \neg d \vee \neg e$$



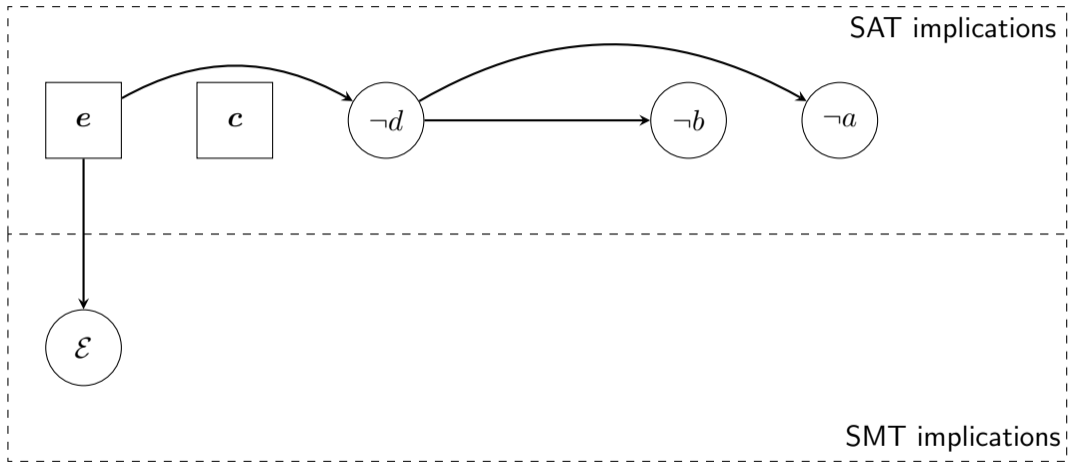
SAT and SMT Trails



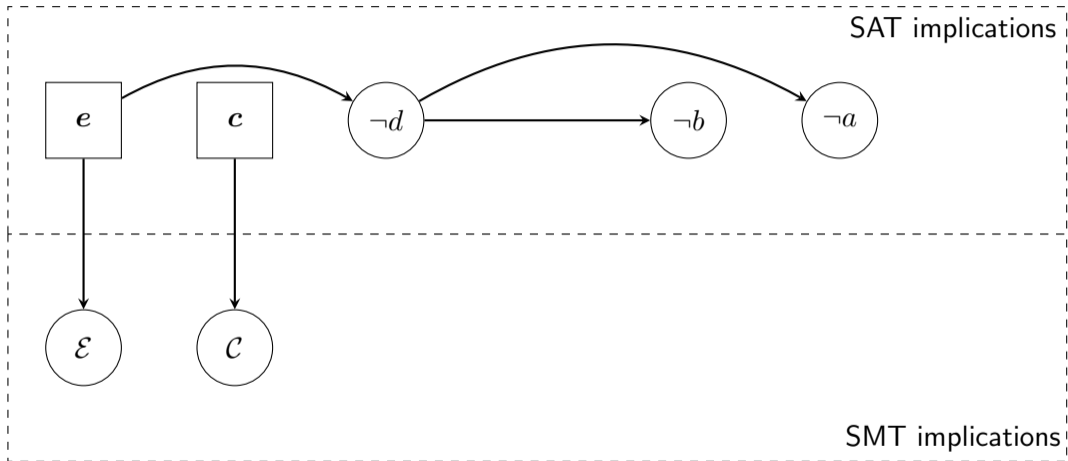
SAT and SMT Trails



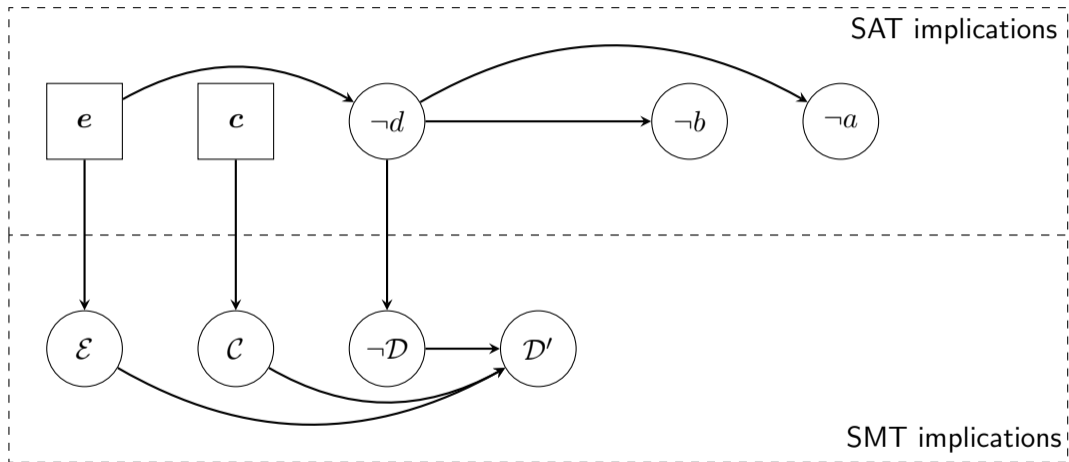
SAT and SMT Trails



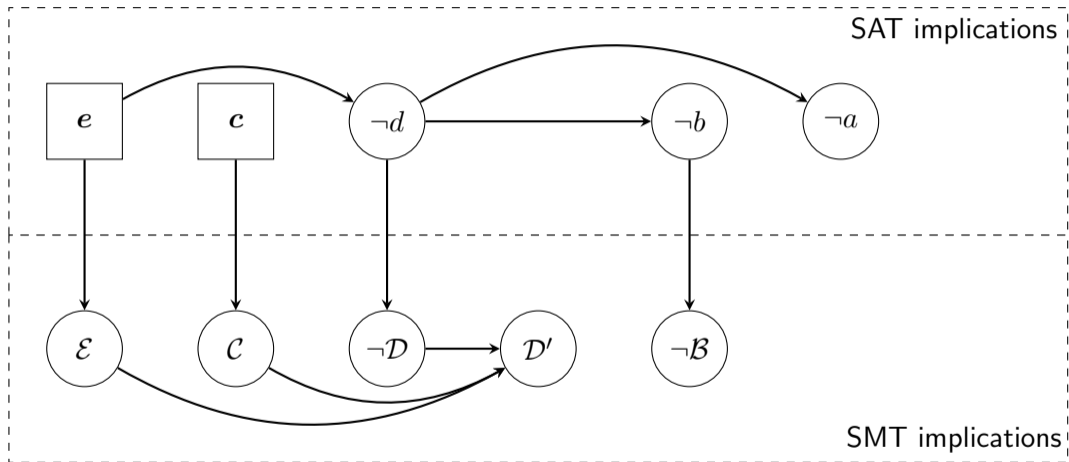
SAT and SMT Trails



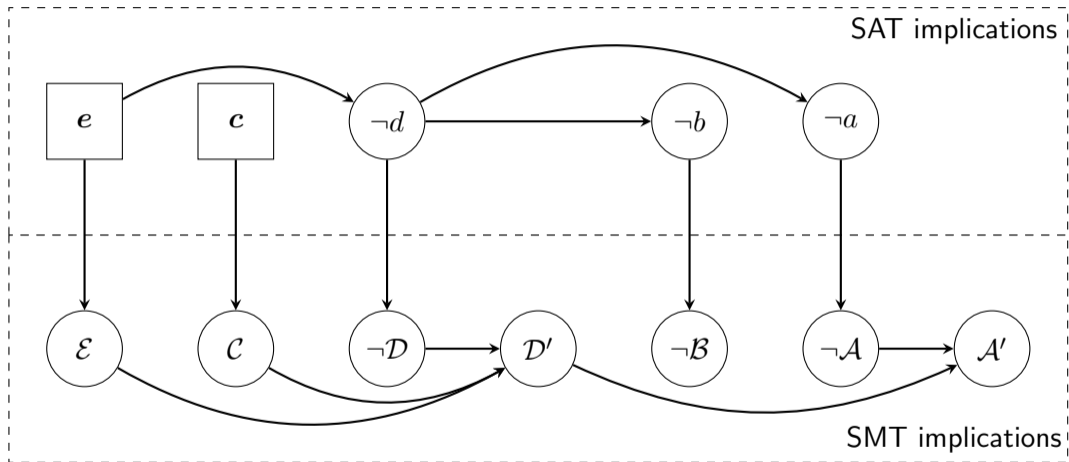
SAT and SMT Trails



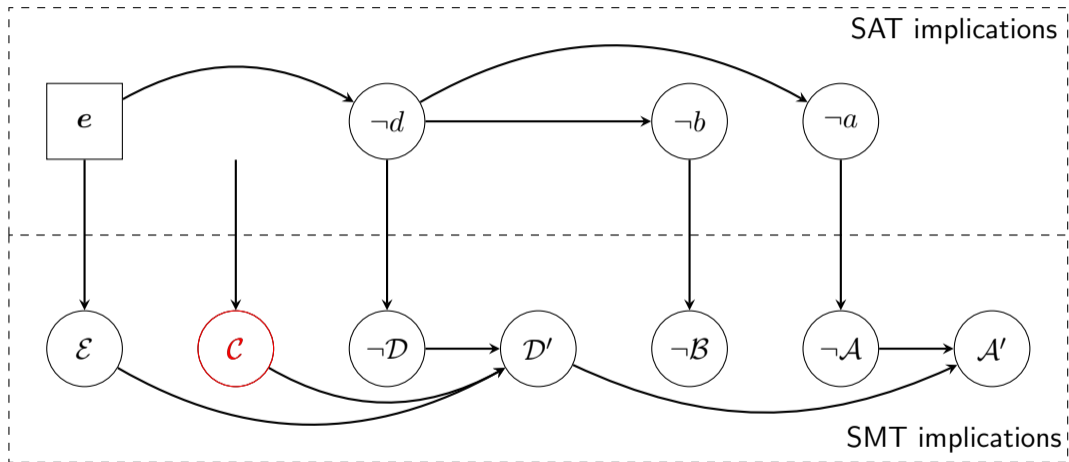
SAT and SMT Trails



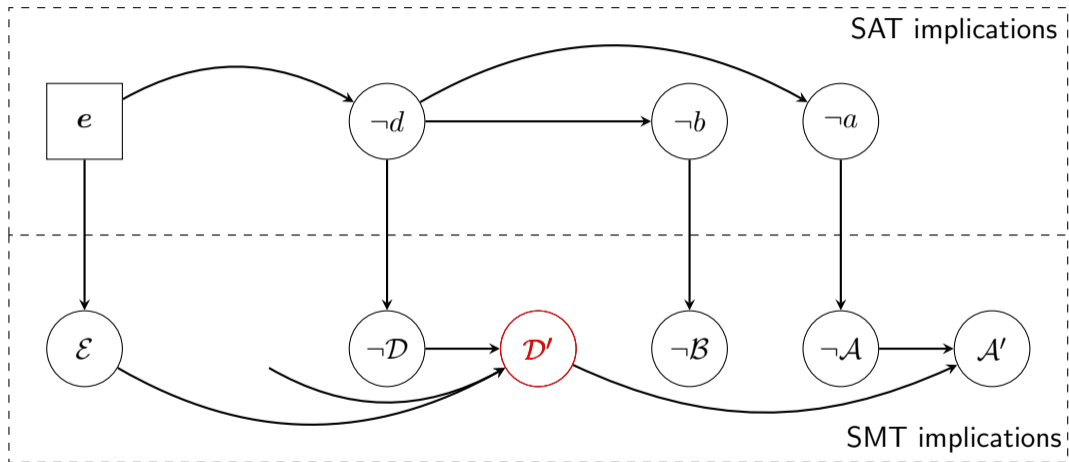
SAT and SMT Trails



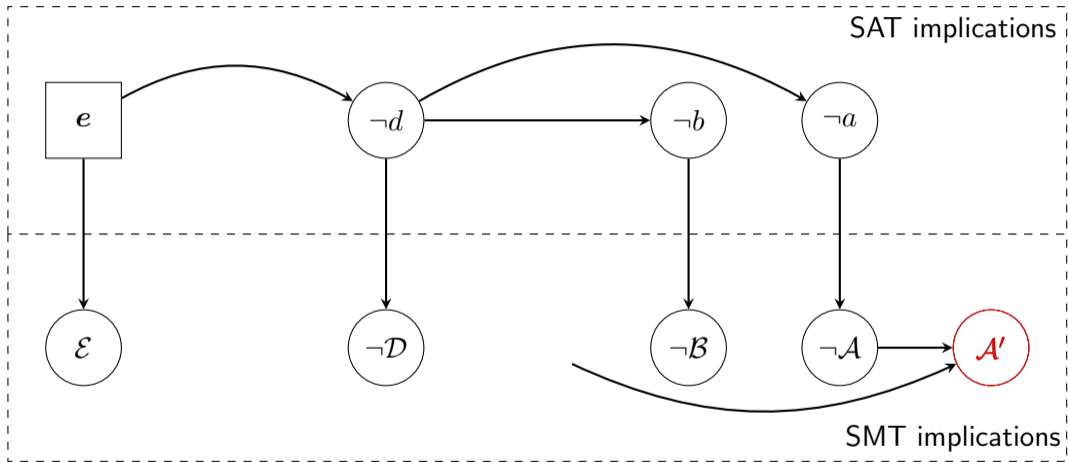
SAT and SMT Trails



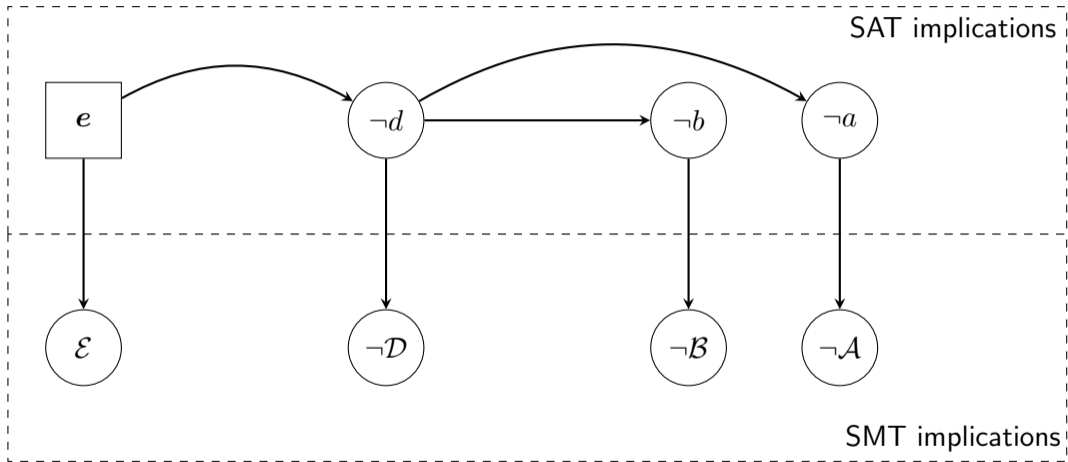
SAT and SMT Trails



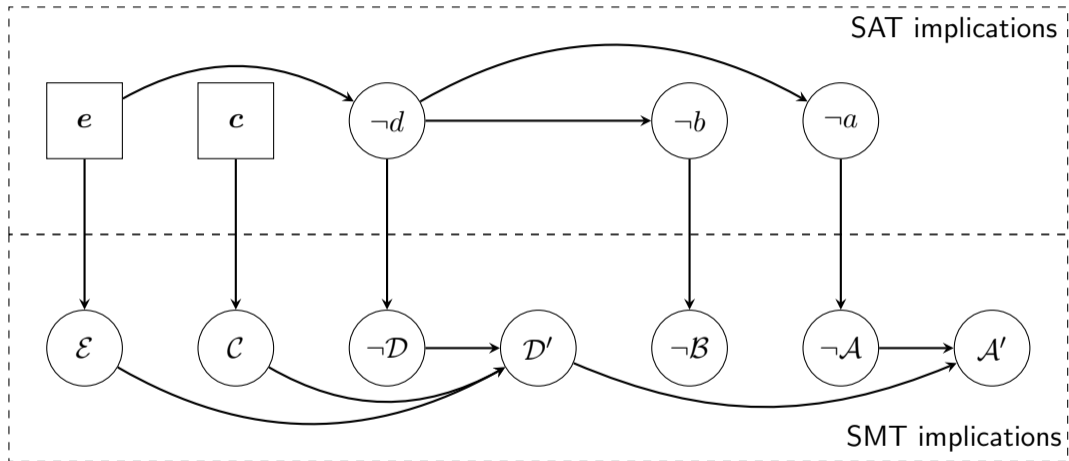
SAT and SMT Trails



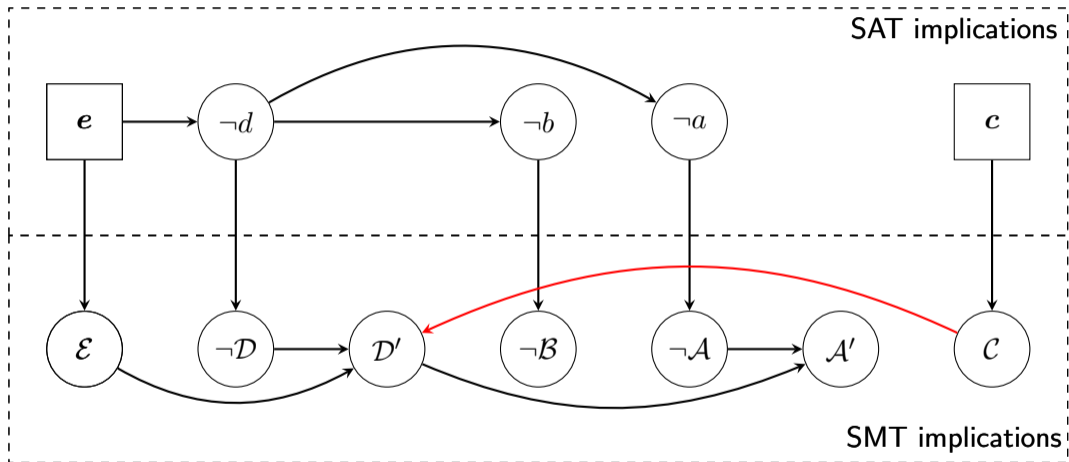
SAT and SMT Trails



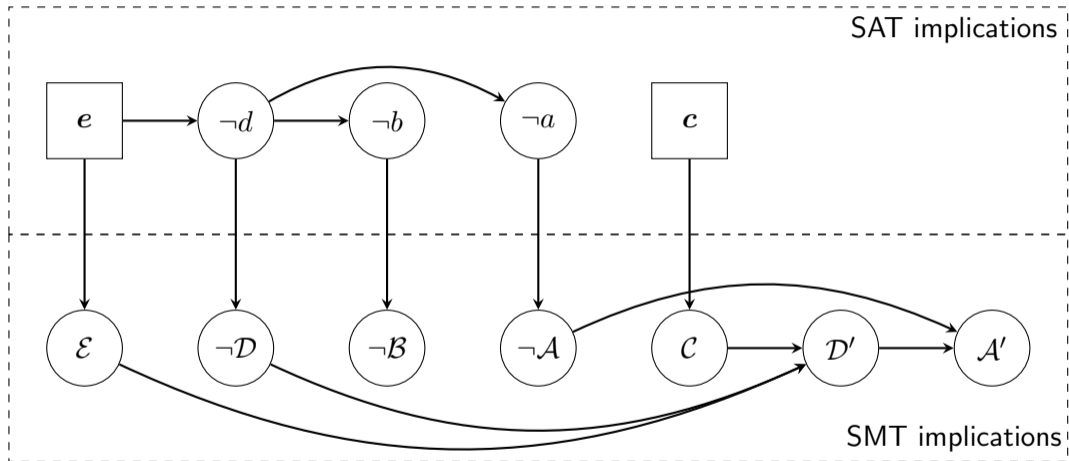
Moving Literals



Moving Literals



Moving Literals



Results

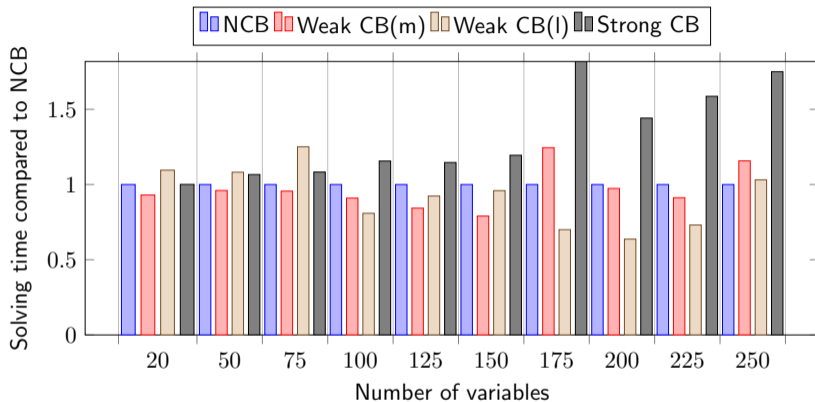



Figure: Computation time for SAT instances of SAT-LIB problems [Hoos and Stützle, 2000] with different backtracking strategies.

Future Work

- Implement SAT solver for modulariT
- New algorithm for conflict analysis
- Minimize cost of Strong CB
- Complete interaction between SAT and SMT solvers
- Benchmark CB in SMT

References I

 Fontaine, P. and Boigelot, B. (2023).
Introduction to computer systems verification.

 Hoos, H. H. and Stützle, T. (2000).
SATLIB: An online resource for research on SAT.
Sat, 2000:283–292.

 Möhle, S. and Biere, A. (2019).
Backing backtracking.
In Janota, M. and Lynce, I., editors, *Theory and Applications of Satisfiability Testing - SAT 2019 - 22nd International Conference, SAT 2019, Lisbon, Portugal, July 9-12, 2019*,

References II

Proceedings, volume 11628 of *Lecture Notes in Computer Science*, pages 250–266. Springer.



Nadel, A. and Ryvchin, V. (2018).

Chronological backtracking.

In Beyersdorff, O. and Wintersteiger, C. M., editors, *Theory and Applications of Satisfiability Testing - SAT 2018 - 21st International Conference, SAT 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 9-12, 2018, Proceedings*, volume 10929 of *Lecture Notes in Computer Science*, pages 111–121. Springer.

Example

```
procedure max(a, b, c)  
  var m  
  if  $a \geq b \wedge a \geq c$  then  
    |  $m \leftarrow a$   
  else if  $b \geq c$  then  
    |  $m \leftarrow b$   
  else  
    |  $m \leftarrow c$   
  assert  $m \geq a \wedge m \geq b \wedge m \geq c$   
  return m
```

Example

```
procedure  $\max(a, b, c)$   
  var  $m$   
  if  $a \geq b \wedge a \geq c$  then  
     $m \leftarrow a$   
  else if  $b \geq c$  then  
     $m \leftarrow b$   
  else  
     $m \leftarrow c$   
  assert  $m \geq a \wedge m \geq b \wedge m \geq c$   
  return  $m$ 
```

Prove validity of:

$$\begin{aligned} & (a \geq b \wedge a \geq c) \Rightarrow m = a \\ & \wedge (\neg(a \geq b \wedge a \geq c) \wedge b \geq c) \Rightarrow m = b \\ & \wedge (\neg(a \geq b \wedge a \geq c \wedge b \geq c)) \Rightarrow m = c \\ & \Rightarrow m \geq a \wedge m \geq b \wedge m \geq c \end{aligned}$$

Example

```
procedure max(a, b, c)  
  var m  
  if  $a \geq b \wedge a \geq c$  then  
    |  $m \leftarrow a$   
  else if  $b \geq c$  then  
    |  $m \leftarrow b$   
  else  
    |  $m \leftarrow c$   
  assert  $m \geq a \wedge m \geq b \wedge m \geq c$   
  return m
```

Prove unsatisfiability of:

$$\begin{aligned} & (a \geq b \wedge a \geq c) \Rightarrow m = a \\ & \wedge (\neg(a \geq b \wedge a \geq c) \wedge b \geq c) \Rightarrow m = b \\ & \wedge (\neg(a \geq b \wedge a \geq c \wedge b \geq c)) \Rightarrow m = c \\ & \wedge \neg(m \geq a \wedge m \geq b \wedge m \geq c) \end{aligned}$$

Example

procedure $\text{max}(a, b, c)$

var m

if $a \geq b \wedge a \geq c$ **then**

$m \leftarrow a$

else if $b \geq c$ **then**

$m \leftarrow b$

else

$m \leftarrow c$

assert $m \geq a \wedge m \geq b \wedge m \geq c$

return m

$(a < b \vee a \geq c \vee m = a)$

$\wedge (a \geq b \vee b < c \vee m = b)$

$\wedge (a \geq c \vee b < c \vee m = b)$

$\wedge (a \geq b \vee m = c)$

$\wedge (a \geq c \vee m = c)$

$\wedge (b \geq c \vee m = c)$

$\wedge (m < a \vee m < b \vee m < c)$

Example

$$\begin{aligned} & (a < b \vee a \geq c \vee m = a) \\ \wedge & (a \geq b \vee b < c \vee m = b) \\ \wedge & (a \geq c \vee b < c \vee m = b) \\ \wedge & (a \geq b \vee m = c) \\ \wedge & (a \geq c \vee m = c) \\ \wedge & (b \geq c \vee m = c) \\ \wedge & (m < a \vee m < b \vee m < c) \end{aligned}$$

Example

$$\begin{aligned} & (a < b \vee a \geq c \vee m = a) \\ \wedge & (a \geq b \vee b < c \vee m = b) \\ \wedge & (a \geq c \vee b < c \vee m = b) \\ \wedge & (a \geq b \vee m = c) \\ \wedge & (a \geq c \vee m = c) \\ \wedge & (b \geq c \vee m = c) \\ \wedge & (m < a \vee m < b \vee m < c) \end{aligned}$$

$$v_{a < b} \Leftrightarrow a < b$$

$$v_{a < c} \Leftrightarrow a < c$$

$$v_{b < c} \Leftrightarrow b < c$$

$$v_{m = a} \Leftrightarrow m = a$$

$$v_{m = b} \Leftrightarrow m = b$$

$$v_{m = c} \Leftrightarrow m = c$$

$$v_{m < a} \Leftrightarrow m < a$$

$$v_{m < b} \Leftrightarrow m < b$$

$$v_{m < c} \Leftrightarrow m < c$$

Example

$$\begin{aligned} & (a < b \vee a \geq c \vee m = a) \\ \wedge & (a \geq b \vee b < c \vee m = b) \\ \wedge & (a \geq c \vee b < c \vee m = b) \\ \wedge & (a \geq b \vee m = c) \\ \wedge & (a \geq c \vee m = c) \\ \wedge & (b \geq c \vee m = c) \\ \wedge & (m < a \vee m < b \vee m < c) \end{aligned}$$

$$v_{a < b} \Leftrightarrow a < b$$

$$v_{a < c} \Leftrightarrow a < c$$

$$v_{b < c} \Leftrightarrow b < c$$

$$v_{m = a} \Leftrightarrow m = a$$

$$v_{m = b} \Leftrightarrow m = b$$

$$v_{m = c} \Leftrightarrow m = c$$

$$v_{m < a} \Leftrightarrow m < a$$

$$v_{m < b} \Leftrightarrow m < b$$

$$v_{m < c} \Leftrightarrow m < c$$

$$C_1 : v_{a < b} \vee v_{a < c} \vee v_{m = a}$$

$$C_2 : \neg v_{a < b} \vee v_{b < c} \vee v_{m = b}$$

$$C_3 : \neg v_{a < c} \vee v_{b < c} \vee v_{m = b}$$

$$C_4 : \neg v_{a < b} \vee v_{m = c}$$

$$C_5 : \neg v_{a < c} \vee v_{m = c}$$

$$C_6 : \neg v_{b < c} \vee v_{m = c}$$

$$C_7 : v_{m < a} \vee v_{m < b} \vee v_{m < c}$$

Example

$$C_1 : v_a < b \vee v_a < c \vee v_m = a$$

$$C_2 : \neg v_a < b \vee v_b < c \vee v_m = b$$

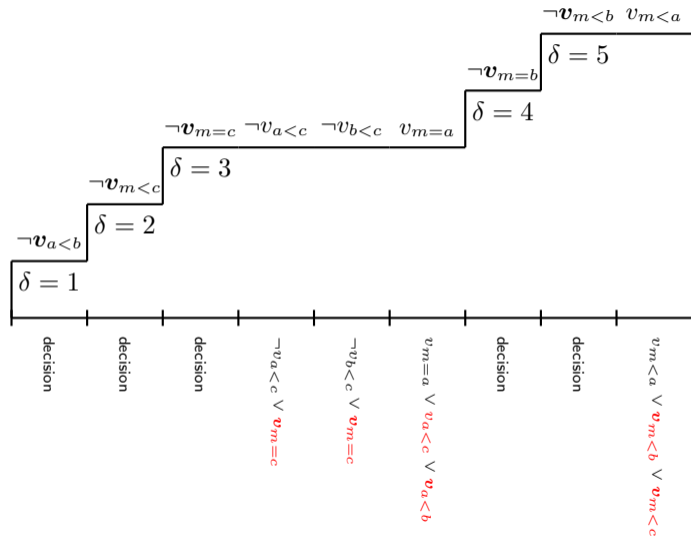
$$C_3 : \neg v_a < c \vee v_b < c \vee v_m = b$$

$$C_4 : \neg v_a < b \vee v_m = c$$

$$C_5 : \neg v_a < c \vee v_m = c$$

$$C_6 : \neg v_b < c \vee v_m = c$$

$$C_7 : v_m < a \vee v_m < b \vee v_m < c$$



Example

$$C_1 : v_a < b \vee v_a < c \vee v_m = a$$

$$C_2 : \neg v_a < b \vee v_b < c \vee v_m = b$$

$$C_3 : \neg v_a < c \vee v_b < c \vee v_m = b$$

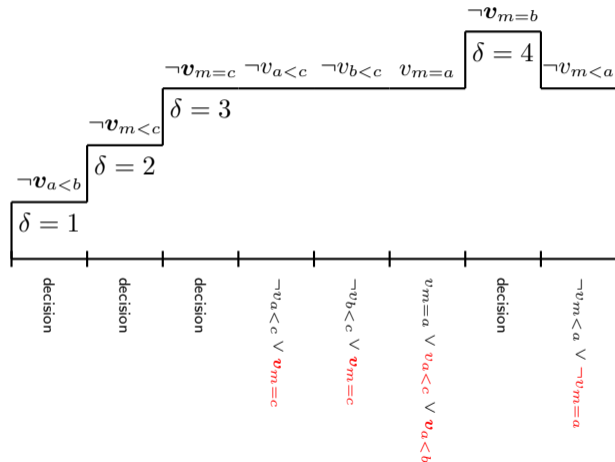
$$C_4 : \neg v_a < b \vee v_m = c$$

$$C_5 : \neg v_a < c \vee v_m = c$$

$$C_6 : \neg v_b < c \vee v_m = c$$

$$C_7 : v_m < a \vee v_m < b \vee v_m < c$$

$$C_8 : \neg v_m = a \vee \neg v_m < a$$



Example

$$C_1 : v_a < b \vee v_a < c \vee v_m = a$$

$$C_2 : \neg v_a < b \vee v_b < c \vee v_m = b$$

$$C_3 : \neg v_a < c \vee v_b < c \vee v_m = b$$

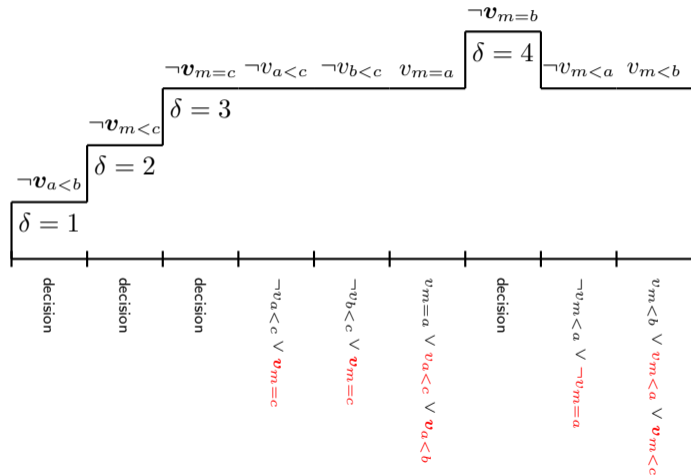
$$C_4 : \neg v_a < b \vee v_m = c$$

$$C_5 : \neg v_a < c \vee v_m = c$$

$$C_6 : \neg v_b < c \vee v_m = c$$

$$C_7 : v_m < a \vee v_m < b \vee v_m < c$$

$$C_8 : \neg v_m = a \vee \neg v_m < a$$



Example

$$C_1 : v_{a < b} \vee v_{a < c} \vee v_{m = a}$$

$$C_2 : \neg v_{a < b} \vee v_{b < c} \vee v_{m = b}$$

$$C_3 : \neg v_{a < c} \vee v_{b < c} \vee v_{m = b}$$

$$C_4 : \neg v_{a < b} \vee v_{m = c}$$

$$C_5 : \neg v_{a < c} \vee v_{m = c}$$

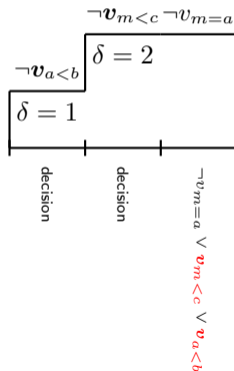
$$C_6 : \neg v_{b < c} \vee v_{m = c}$$

$$C_7 : v_{m < a} \vee v_{m < b} \vee v_{m < c}$$

$$C_8 : \neg v_{m = a} \vee \neg v_{m < a}$$

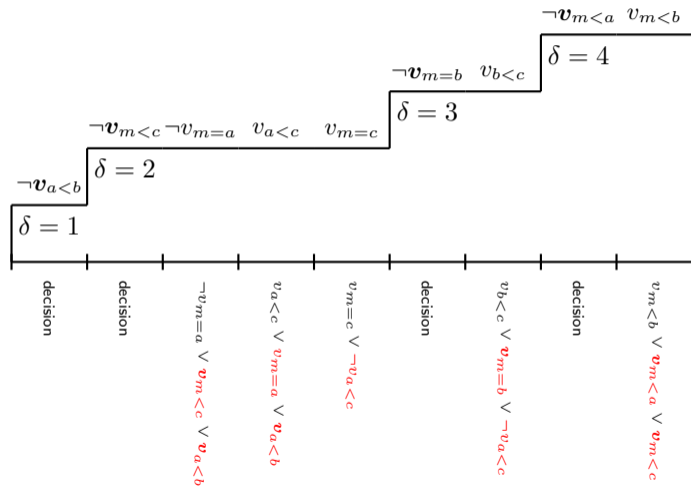
$$C_9 : v_{a < b} \vee \neg v_{m = a} \vee \neg v_{m < b}$$

$$C_{10} : v_{a < b} \vee \neg v_{m = a} \vee v_{m < c}$$



Example

- $C_1 : v_a < b \vee v_a < c \vee v_m = a$
 $C_2 : \neg v_a < b \vee v_b < c \vee v_m = b$
 $C_3 : \neg v_a < c \vee v_b < c \vee v_m = b$
 $C_4 : \neg v_a < b \vee v_m = c$
 $C_5 : \neg v_a < c \vee v_m = c$
 $C_6 : \neg v_b < c \vee v_m = c$
 $C_7 : v_m < a \vee v_m < b \vee v_m < c$
 $C_8 : \neg v_m = a \vee \neg v_m < a$
 $C_9 : v_a < b \vee \neg v_m = a \vee \neg v_m < b$
 $C_{10} : v_a < b \vee \neg v_m = a \vee v_m < c$



Example

$$C_1 : v_a < b \vee v_a < c \vee v_m = a$$

$$C_2 : \neg v_a < b \vee v_b < c \vee v_m = b$$

$$C_3 : \neg v_a < c \vee v_b < c \vee v_m = b$$

$$C_4 : \neg v_a < b \vee v_m = c$$

$$C_5 : \neg v_a < c \vee v_m = c$$

$$C_6 : \neg v_b < c \vee v_m = c$$

$$C_7 : v_m < a \vee v_m < b \vee v_m < c$$

$$C_8 : \neg v_m = a \vee \neg v_m < a$$

$$C_9 : v_a < b \vee \neg v_m = a \vee \neg v_m < b$$

$$C_{10} : v_a < b \vee \neg v_m = a \vee v_m < c$$

...

$$C_{22} : \neg v_a < b \vee \neg v_m = b \vee \neg v_m < a$$

