Model Checking CTL Formulas

Cesare Tinelli

tinelli@cs.uiowa.edu

The University of Iowa

An Abstract Algorithm

Given:

- a model $\mathcal{M} = (\{s_1, \ldots, s_n\}, \rightarrow, L)$ and a state s of $\mathcal{M}$
- a CTL formula ψ

Configurations: sat, $unsat$ or $F \parallel \phi \parallel P \parallel Q$

where F is a set of (CTL) formulas,
ϕ is a formula or _ ,
P and Q are sets of *labeled states* of the form
$s : \{\phi_1, \ldots, \phi_k\}$ where s is a state of $\mathcal{M}$ and
each ϕ_i is a formula.

An Abstract Algorithm

Given:

- a model $\mathcal{M} = (\{s_1, \ldots, s_n\}, \rightarrow, L)$ and a state s of $\mathcal{M}$
- a CTL formula ψ

Configurations: sat, $unsat$ or $F \parallel \phi \parallel P \parallel Q$

Initial configuration:

- $F \parallel \_ \parallel \{s_1 : \{\}, \ldots, s_n : \{\}\} \parallel \{\}$ where

  F consists of all the subformulas of ψ

Expected final configurations:

- sat, if $\mathcal{M}, s \models \psi$
- $unsat$, if $\mathcal{M}, s \not\models \psi$

Derivation Rules

Notation: F, ϕ abbreviates $F \cup \{\phi\}$, etc.
$\bar{\phi}$ same as $\neg\phi$

Choose

$$\frac{F, \phi \parallel \_ \parallel P \parallel Q}{F \parallel \phi \parallel P \parallel Q}$$ if ϕ has no subformulas in F

Bottom

$$\frac{F \parallel \bot \parallel P \parallel \{\}}{F \parallel \_ \parallel P \parallel \{\}}$$

Derivation Rules

Atom1

$$\frac{F \parallel p \parallel P,\ s : M \parallel Q}{F \parallel p \parallel P \parallel Q,\ (s : M, p)} \quad \text{if} \quad p \in L(s)$$

Atom2

$$\frac{F \parallel p \parallel P \parallel Q}{F \parallel \_ \parallel P \cup Q \parallel \{\}} \quad \text{if} \quad \textbf{Atom1} \text{ does not apply}$$

Derivation Rules

Not1

$$\frac{F \parallel \bar{\phi} \parallel P,\, s : M \parallel Q}{F \parallel \bar{\phi} \parallel P \parallel Q,\, (s : M, \bar{\phi})} \quad \text{if} \quad \phi \notin M$$

Not2

$$\frac{F \parallel \bar{\phi} \parallel P \parallel Q}{F \parallel \_ \parallel P \cup Q \parallel \{\}} \quad \text{if} \quad \textbf{Not1} \text{ does not apply}$$

Derivation Rules

And1

$$\frac{F \parallel \phi_1 \wedge \phi_2 \parallel P,\ s : M \parallel Q}{F \parallel \phi_1 \wedge \psi_2 \parallel P \parallel Q,\ (s : M, \phi_1 \wedge \phi_2)} \quad \text{if} \quad \phi_1, \phi_2 \in M$$

And2

$$\frac{F \parallel \phi_1 \wedge \phi_2 \parallel P \parallel Q}{F \parallel \_ \parallel P \cup Q \parallel \{\}} \quad \text{if} \quad \textbf{And1} \text{ does not apply}$$

Derivation Rules

EX1

$$\frac{F \parallel \mathrm{EX}\,\phi \parallel P,\ s : M,\ q : N \parallel Q}{F \parallel \mathrm{EX}\,\phi \parallel P,\ q : N \parallel Q,\ (s : M, \mathrm{EX}\,\phi)} \text{ if } \begin{cases} \phi \in N, \\ s \rightarrow q \end{cases}$$

EX2

$$\frac{F \parallel \mathrm{EX}\,\phi \parallel P \parallel Q}{F \parallel \_ \parallel P \cup Q \parallel \{\}}$$ if **EX1** does not apply

Derivation Rules

AF1

$$\frac{F \parallel \mathrm{AF}\,\phi \parallel P,\, s : M \parallel Q}{F \parallel \mathrm{AF}\,\phi \parallel P \parallel Q,\, (s : M, \mathrm{AF}\,\phi)} \quad \text{if} \quad \phi \in M$$

AF2

$$\frac{F \parallel \mathrm{AF}\,\phi \parallel P,\, s : M \parallel Q,\, q_1 : M_1,\, \ldots,\, q_k : M_k}{F \parallel \mathrm{AF}\,\phi \parallel P \parallel Q,\, q_1 : M_1,\, \ldots,\, q_k : M_k,\, (s : M, \mathrm{AF}\,\phi)} \quad \text{if} \quad *$$

$$* = \begin{cases} q_1, \ldots, q_k \text{ are all the successors of } s, \\ \mathrm{AF}\,\phi \in M_i \text{ for } i = 1, \ldots, k \end{cases}$$

AF3

$$\frac{F \parallel \mathrm{AF}\,\phi \parallel P \parallel Q}{F \parallel \_ \parallel P \cup Q \parallel \{\}} \quad \text{if} \quad \textbf{AF1/AF2} \text{ does not apply}$$

Derivation Rules

EU1

$$\frac{F \parallel \mathrm{E}[\phi \,\mathrm{U}\, \psi] \parallel P,\ s : M \parallel Q}{F \parallel \mathrm{E}[\phi \,\mathrm{U}\, \psi] \parallel P \parallel Q,\ (s : M, \mathrm{E}[\phi \,\mathrm{U}\, \psi])} \quad \text{if} \quad \psi \in M$$

EU2

$$\frac{F \parallel \mathrm{E}[\phi \,\mathrm{U}\, \psi] \parallel P,\ s : M \parallel Q,\ q : N}{F \parallel \mathrm{E}[\phi \,\mathrm{U}\, \psi] \parallel P \parallel Q,\ q : N,\ (s : M, \mathrm{E}[\phi \,\mathrm{U}\, \psi])} \quad \text{if} \quad *$$

$$* = \begin{cases} \phi \in M, \\ s \to q,\ \mathrm{E}[\phi \,\mathrm{U}\, \psi] \in N \end{cases}$$

EU3

$$\frac{F \parallel \mathrm{E}[\phi \,\mathrm{U}\, \psi] \parallel P \parallel Q}{F \parallel \_ \parallel P \cup Q \parallel \{\}} \quad \text{if} \quad \textbf{EU1/EU2} \text{ does not apply}$$

Derivation Rules

Sat

$$\frac{F \parallel * \parallel P \parallel Q,\ s : M}{sat} \text{ if } \psi \in M$$

$*$ stands any for either a formula or _

Unsat

$$\frac{\{\} \parallel \_ \parallel P,\ s : M \parallel \{\}}{unsat} \text{ if } \psi \notin M$$

Example

- **System $\mathcal{M}$:** the one in Figure 3.8 of [Huth&Ryan], with
  1. s_8 instead of s_9,
  2. c abbreviating c_1, and
  3. d abbreviating c_2

- **Formula ψ:** $\mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

- **State s:** s_0

Derivation Example

F : $c,\ d,\ \bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ : –

P : $s_0 : \{\},\ s_1 : \{\},\ s_2 : \{\},\ s_3 : \{\},\ s_4 : \{\},$
$s_5 : \{\},\ s_6 : \{\},\ s_7 : \{\},\ s_8 : \{\}$

Q :

$\Downarrow$ **Choose**

F : $d,\ \bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ : c

P : $s_0 : \{\},\ s_1 : \{\},\ s_2 : \{\},\ s_3 : \{\},\ s_4 : \{\},$
$s_5 : \{\},\ s_6 : \{\},\ s_7 : \{\},\ s_8 : \{\}$

Q :

Derivation Example

F : $d,\ \bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ : c

P : $s_0 : \{\},\ s_1 : \{\},\ s_2 : \{\},\ s_3 : \{\},\ s_4 : \{\},$
$s_5 : \{\},\ s_6 : \{\},\ s_7 : \{\},\ s_8 : \{\}$

Q :

$\Downarrow$ **Atom1**^{2}

F : $d,\ \bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ : c

P : $s_0 : \{\},\ s_1 : \{\},\ s_3 : \{\}$
$s_5 : \{\},\ s_6 : \{\},\ s_7 : \{\},\ s_8 : \{\}$

Q : $s_2 : \{c\},\ s_4 : \{c\}$

Derivation Example

F : $d,\ \bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ : c

P : $s_0 : \{\},\ s_1 : \{\},\ s_3 : \{\}$

$s_5 : \{\},\ s_6 : \{\},\ s_7 : \{\},\ s_8 : \{\}$

Q : $s_2 : \{c\},\ s_4 : \{c\}$

$\Downarrow$ **Atom2**

F : $d,\ \bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ :

P : $s_0 : \{\},\ s_1 : \{\},\ s_2 : \{c\},\ s_3 : \{\},\ s_4 : \{c\}$

$s_5 : \{\},\ s_6 : \{\},\ s_7 : \{\},\ s_8 : \{\}$

Q :

Derivation Example

F : $d,\ \bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ :

P : $s_0 : \{\},\ s_1 : \{\},\ s_2 : \{c\},\ s_3 : \{\},\ s_4 : \{c\}$
$s_5 : \{\},\ s_6 : \{\},\ s_7 : \{\},\ s_8 : \{\}$

Q :

$\Downarrow$ **Choose Atom1^2 Atom2**

F : $\bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ :

P : $s_0 : \{\},\ s_1 : \{\},\ s_2 : \{c\},\ s_3 : \{\},\ s_4 : \{c\}$
$s_5 : \{\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\}$

Q :

Derivation Example

F : $\bar{d},\ \mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ :

P : $s_0 : \{\},\ s_1 : \{\},\ s_2 : \{c\},\ s_3 : \{\},\ s_4 : \{c\}$
$s_5 : \{\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\}$

Q :

$\Downarrow$ **Choose Not1^2 Not2**

F : $\mathrm{E}[\bar{d}\,\mathrm{U}\,c]$

ϕ :

P : $s_0 : \{\bar{d}\},\ s_1 : \{\bar{d}\},\ s_2 : \{c, \bar{d}\},\ s_3 : \{\bar{d}\},\ s_4 : \{c, \bar{d}\}$
$s_5 : \{\bar{d}\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\bar{d}\}$

Q :

Derivation Example

F : $\mathrm{E}[\bar{d}\,\mathrm{U}\,c]$ $(= \psi)$

ϕ :

P : $s_0 : \{\bar{d}\},\ s_1 : \{\bar{d}\},\ s_2 : \{c, \bar{d}\},\ s_3 : \{\bar{d}\},\ s_4 : \{c, \bar{d}\}$
$s_5 : \{\bar{d}\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\bar{d}\}$

Q :

$\Downarrow$ **Choose EU1**^{2}

F :

ϕ : $\mathrm{E}[\bar{d}\,\mathrm{U}\,c]$ $(= \psi)$

P : $s_0 : \{\bar{d}\},\ s_1 : \{\bar{d}\},\ s_3 : \{\bar{d}\}$
$s_5 : \{\bar{d}\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\bar{d}\}$

Q : $s_2 : \{c, \bar{d}, \psi\},\ s_4 : \{c, \bar{d}, \psi\}$

Derivation Example

F :

ϕ : $\quad \mathrm{E}[\bar{d}\,\mathrm{U}\,c]\ (=\psi)$

P : $\quad s_0 : \{\bar{d}\},\ s_1 : \{\bar{d}\},\ s_3 : \{\bar{d}\}$

$\quad\quad s_5 : \{\bar{d}\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\bar{d}\}$

Q : $\quad s_2 : \{c, \bar{d}, \psi\},\ s_4 : \{c, \bar{d}, \psi\}$

$\Downarrow$ **EU2**

F :

ϕ : $\quad \mathrm{E}[\bar{d}\,\mathrm{U}\,c]\ (=\psi)$

P : $\quad s_0 : \{\bar{d}\},\ s_3 : \{\bar{d}\}$

$\quad\quad s_5 : \{\bar{d}\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\bar{d}\}$

Q : $\quad s_1 : \{\bar{d}, \psi\},\ s_2 : \{c, \bar{d}, \psi\},\ s_4 : \{c, \bar{d}, \psi\}$

Derivation Example

F :

ϕ : $\quad \mathrm{E}[\bar{d}\,\mathrm{U}\,c]\ (=\psi)$

P : $\quad s_0 : \{\bar{d}\},\ s_3 : \{\bar{d}\}$

$\quad\quad s_5 : \{\bar{d}\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\bar{d}\}$

Q : $\quad s_1 : \{\bar{d}, \psi\},\ s_2 : \{c, \bar{d}, \psi\},\ s_4 : \{c, \bar{d}, \psi\}$

$\Downarrow$ **EU2**

F :

ϕ : $\quad \mathrm{E}[\bar{d}\,\mathrm{U}\,c]\ (=\psi)$

P : $\quad s_3 : \{\bar{d}\}$

$\quad\quad s_5 : \{\bar{d}\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\bar{d}\}$

Q : $\quad s_0 : \{\bar{d}, \psi\},\ s_1 : \{\bar{d}, \psi\},\ s_2 : \{c, \bar{d}, \psi\},\ s_4 : \{c, \bar{d}, \psi\}$

Derivation Example

F :

ϕ : $\quad \mathrm{E}[\bar{d}\,\mathrm{U}\,c]\ (=\psi)$

P : $\quad s_3 : \{\bar{d}\}$

$\quad\quad s_5 : \{\bar{d}\},\ s_6 : \{d\},\ s_7 : \{d\},\ s_8 : \{\bar{d}\}$

Q : $\quad s_0 : \{\bar{d}, \psi\},\ s_1 : \{\bar{d}, \psi\},\ s_2 : \{c, \bar{d}, \psi\},\ s_4 : \{c, \bar{d}, \psi\}$

$\Downarrow$ **Sat**

sat