Computation Tree Logic

EECS 4315

www.eecs.yorku.ca/course/4315/

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists \bigcirc f \mid \exists(f \; \mathsf{U} \; f) \mid \forall \bigcirc f \mid \forall(f \; \mathsf{U} \; f)$$

Semantics of CTL

$$
\begin{array}{rcl}
s \models a & \text{iff} & a \in \ell(s) \\
s \models f_1 \wedge f_2 & \text{iff} & s \models f_1 \text{ and } s \models f_2 \\
s \models \neg f & \text{iff} & \text{not}(s \models f) \\
s \models \exists \bigcirc f & \text{iff} & \exists p \in Paths(s) : p[1] \models f \\
s \models \exists (f_1 \mathbin{\mathsf{U}} f_2) & \text{iff} & \exists p \in Paths(s) : \\
 & & \exists i \geq 0 : p[i] \models f_2 \text{ and } \forall 0 \leq j < i : p[j] \models f_1 \\
s \models \forall \bigcirc f & \text{iff} & \forall p \in Paths(s) : p[1] \models f \\
s \models \forall (f_1 \mathbin{\mathsf{U}} f_2) & \text{iff} & \forall p \in Paths(s) : \\
 & & \exists i \geq 0 : p[i] \models f_2 \text{ and } \forall 0 \leq j < i : p[j] \models f_1
\end{array}
$$

Semantics of CTL

The *satisfaction set* $Sat(f)$ is defined by

$$Sat(f) = \{ s \in S \mid s \models f \}.$$

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists \bigcirc f \mid \exists (f \,\mathrm{U}\, f) \mid \forall \bigcirc f \mid \forall (f \,\mathrm{U}\, f)$$

Question

What is $Sat(a)$?

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists\bigcirc f \mid \exists(f \mathbin{\mathsf{U}} f) \mid \forall\bigcirc f \mid \forall(f \mathbin{\mathsf{U}} f)$$

Question

What is $Sat(a)$?

Answer

$Sat(a) = \{ s \in S \mid a \in \ell(s) \}$

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists \bigcirc f \mid \exists(f \, \mathsf{U} \, f) \mid \forall \bigcirc f \mid \forall(f \, \mathsf{U} \, f)$$

Question

What is $Sat(f_1 \wedge f_2)$?

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists \bigcirc f \mid \exists (f \ \mathsf{U} \ f) \mid \forall \bigcirc f \mid \forall (f \ \mathsf{U} \ f)$$

Question

What is $Sat(f_1 \wedge f_2)$?

Answer

$Sat(f_1 \wedge f_2) = Sat(f_1) \cap Sat(f_2)$

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists\bigcirc f \mid \exists(f \, \mathrm{U} \, f) \mid \forall\bigcirc f \mid \forall(f \, \mathrm{U} \, f)$$

Question

What is $Sat(\neg f)$?

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists\bigcirc f \mid \exists(f \; \mathsf{U} \; f) \mid \forall\bigcirc f \mid \forall(f \; \mathsf{U} \; f)$$

Question

What is $Sat(\neg f)$?

Answer

$Sat(\neg f) = S \setminus Sat(f)$

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists \bigcirc f \mid \exists(f \; \mathsf{U} \; f) \mid \forall \bigcirc f \mid \forall(f \; \mathsf{U} \; f)$$

Question

What is $Sat(\exists \bigcirc f)$?

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists\bigcirc f \mid \exists(f \,\mathsf{U}\, f) \mid \forall\bigcirc f \mid \forall(f \,\mathsf{U}\, f)$$

Question

What is $Sat(\exists\bigcirc f)$?

Answer

$Sat(\exists\bigcirc f) = \{ s \in S \mid Post(s) \cap Sat(f) \neq \emptyset \}$ where
$Post(s) = \{ s' \in S \mid s \rightarrow s' \}$.

Model checking CTL

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists\bigcirc f \mid \exists(f \; \mathsf{U} \; f) \mid \forall\bigcirc f \mid \forall(f \; \mathsf{U} \; f)$$

Question

What is $Sat(\exists(f_1 \; \mathsf{U} \; f_2))$?

Model checking CTL

$s \in Sat(\exists(f_1 \; \mathrm{U} \; f_2))$

iff $\quad s \models \exists(f_1 \; \mathrm{U} \; f_2)$

iff $\quad s \models f_2 \vee (s \models f_1 \wedge \exists s \to t : t \models \exists(f_1 \; \mathrm{U} \; f_2))$

iff $\quad s \in Sat(f_2) \vee (s \in Sat(f_1) \wedge \exists t \in Post(s) : t \in Sat(\exists(f_1 \; \mathrm{U} \; f_2))$

iff $\quad s \in Sat(f_2) \cup \{ s \in Sat(f_1) \mid Post(s) \cap Sat(\exists(f_1 \; \mathrm{U} \; f_2)) \neq \emptyset \}$

$s \in Sat(\exists(f_1 \ \mathsf{U} \ f_2))$

iff $s \models \exists(f_1 \ \mathsf{U} \ f_2)$

iff $s \models f_2 \lor (s \models f_1 \land \exists s \to t : t \models \exists(f_1 \ \mathsf{U} \ f_2))$

iff $s \in Sat(f_2) \lor (s \in Sat(f_1) \land \exists t \in Post(s) : t \in Sat(\exists(f_1 \ \mathsf{U} \ f_2))$

iff $s \in Sat(f_2) \cup \{ s \in Sat(f_1) \mid Post(s) \cap Sat(\exists(f_1 \ \mathsf{U} \ f_2)) \neq \emptyset \}$

Proposition

$Sat(\exists(f_1 \ \mathsf{U} \ f_2))$ is the smallest subset T of S such that

$$T = Sat(f_2) \cup \{ s \in Sat(f_1) \mid Post(s) \cap T \neq \emptyset \}.$$

$Sat(f)$:
switch (f):

$$
\begin{array}{rcl}
a & : & \textbf{return } \{\, s \in S \mid a \in \ell(s) \,\} \\
f_1 \wedge f_2 & : & \textbf{return } Sat(f_1) \cap Sat(f_2) \\
\neg f & : & \textbf{return } S \setminus Sat(f) \\
\exists \bigcirc f & : & \textbf{return } \{\, s \in S \mid Post(s) \cap Sat(f) \neq \emptyset \,\} \\
\exists (f_1 \, \mathsf{U} \, f_2) & : & T := \emptyset \\
 & & \textbf{while } T \neq F(T) \\
 & & \qquad T := F(T) \\
 & & \textbf{return } T
\end{array}
$$

...

where $F(T) = Sat(f_2) \cup \{\, s \in Sat(f_1) \mid Post(s) \cap T \neq \emptyset \}$.

$Sat(f)$:
switch (f):

...

$\exists(f_1 \; \mathsf{U} \; f_2)$: $E := Sat(f_2)$
$T := E$
while $E \neq \emptyset$
let $t \in E$
$E := E \setminus \{t\}$
for all $s \in Pre(t)$
if $s \in Sat(f) \setminus T$
$E := E \cup \{s\}$
$T := T \cup \{s\}$
return T

...

where $Pre(t) = \{ s \in S \mid s \to t \}$.

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists\bigcirc f \mid \exists(f \, \mathsf{U} \, f) \mid \forall\bigcirc f \mid \forall(f \, \mathsf{U} \, f)$$

Question

What is $Sat(\forall\bigcirc f)$?

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists \bigcirc f \mid \exists(f \; \mathsf{U} \; f) \mid \forall \bigcirc f \mid \forall(f \; \mathsf{U} \; f)$$

Question

What is $Sat(\forall \bigcirc f)$?

Answer

$Sat(\forall \bigcirc f) = \{ s \in S \mid Post(s) \subseteq Sat(f) \}$.

Definition

The *formulas* are defined by

$$f ::= a \mid f \wedge f \mid \neg f \mid \exists \bigcirc f \mid \exists(f \text{ U } f) \mid \forall \bigcirc f \mid \forall(f \text{ U } f)$$

Question

What is $Sat(\forall(f_1 \text{ U } f_2))$?

Model checking CTL

$$s \in Sat(\forall(f_1 \, \mathsf{U} \, f_2))$$
$$\text{iff} \quad s \models \forall(f_1 \, \mathsf{U} \, f_2)$$
$$\text{iff} \quad s \models f_2 \vee (s \models f_1 \wedge \forall s \rightarrow t : t \models \forall(f_1 \, \mathsf{U} \, f_2))$$
$$\text{iff} \quad s \in Sat(f_2) \vee (s \in Sat(f_1) \wedge \forall t \in Post(s) : t \in Sat(\forall(f_1 \, \mathsf{U} \, f_2))$$
$$\text{iff} \quad s \in Sat(f_2) \cup \{ s \in Sat(f_1) \mid Post(s) \subseteq Sat(\forall(f_1 \, \mathsf{U} \, f_2))\}$$

Model checking CTL

$s \in Sat(\forall(f_1 \; \mathrm{U} \; f_2))$

iff $\quad s \models \forall(f_1 \; \mathrm{U} \; f_2)$

iff $\quad s \models f_2 \vee (s \models f_1 \wedge \forall s \rightarrow t : t \models \forall(f_1 \; \mathrm{U} \; f_2))$

iff $\quad s \in Sat(f_2) \vee (s \in Sat(f_1) \wedge \forall t \in Post(s) : t \in Sat(\forall(f_1 \; \mathrm{U} \; f_2))$

iff $\quad s \in Sat(f_2) \cup \{ s \in Sat(f_1) \mid Post(s) \subseteq Sat(\forall(f_1 \; \mathrm{U} \; f_2))\}$

Proposition

$Sat(\forall(f_1 \; \mathrm{U} \; f_2))$ is the smallest subset T of S such that

$$T = Sat(f_2) \cup \{ s \in Sat(f_1) \mid Post(s) \subseteq T \}.$$

Model checking CTL

$s \in Sat(\forall(f_1 \; \mathrm{U} \; f_2))$

iff $s \models \forall(f_1 \; \mathrm{U} \; f_2)$

iff $s \models f_2 \vee (s \models f_1 \wedge \forall s \to t : t \models \forall(f_1 \; \mathrm{U} \; f_2))$

iff $s \in Sat(f_2) \vee (s \in Sat(f_1) \wedge \forall t \in Post(s) : t \in Sat(\forall(f_1 \; \mathrm{U} \; f_2))$

iff $s \in Sat(f_2) \cup \{ s \in Sat(f_1) \mid Post(s) \subseteq Sat(\forall(f_1 \; \mathrm{U} \; f_2))\}$

Proposition

$Sat(\forall(f_1 \; \mathrm{U} \; f_2))$ is the smallest subset T of S such that

$$T = Sat(f_2) \cup \{ s \in Sat(f_1) \mid Post(s) \subseteq T\}.$$

Question

Does such a smallest subset exist?

Size of a CTL formula

$$
\begin{array}{rcl}
|a| & = & 1 \\
|f_1 \wedge f_2| & = & 1 + |f_1| + |f_2| \\
|\neg f| & = & 1 + |f| \\
|\exists \bigcirc f| & = & 1 + |f| \\
|\forall \bigcirc f| & = & 1 + |f| \\
|\exists \bigcirc (f_1 \; \mathsf{U} \; f_2)| & = & 1 + |f_1| + |f_2| \\
|\forall \bigcirc (f_1 \; \mathsf{U} \; f_2)| & = & 1 + |f_1| + |f_2|
\end{array}
$$

Time Complexity of CTL Model Checking

By improving the model checking algorithm (see, for example the textbook of Baier and Katoen for details), we obtain

Theorem

For a transition system TS, with N states and K transitions, and a CTL formula f, the model checking problem $TS \models f$ can be decided in time $\mathcal{O}((N + K) \cdot |f|)$.

Time Complexity of CTL Model Checking

By improving the model checking algorithm (see, for example the textbook of Baier and Katoen for details), we obtain

Theorem

For a transition system TS, with N states and K transitions, and a CTL formula f, the model checking problem $TS \models f$ can be decided in time $\mathcal{O}((N + K) \cdot |f|)$.

Theorem

For a transition system TS, with N states and K transitions, and a LTL formula g, the model checking problem $TS \models g$ can be decided in time $\mathcal{O}((N + K) \cdot 2^{|g|})$.

Time Complexity of CTL Model Checking

By improving the model checking algorithm (see, for example the textbook of Baier and Katoen for details), we obtain

Theorem

For a transition system TS, with N states and K transitions, and a CTL formula f, the model checking problem $TS \models f$ can be decided in time $\mathcal{O}((N + K) \cdot |f|)$.

Theorem

For a transition system TS, with N states and K transitions, and a LTL formula g, the model checking problem $TS \models g$ can be decided in time $\mathcal{O}((N + K) \cdot 2^{|g|})$.

Theorem

If P $\neq$ NP then there exist LTL formulas g_n whose size is a polynomial in n, for which equivalent CTL formulas exist, but not of size polynomial in n.