Un algoritmo de Verificación para CTL

Dante Zanarini

LCC

03 de diciembre de 2019

Preguntas

¿Qué queremos?

Un algoritmo que, tomando como entrada una fórmula $\phi \in$ CTL y un sistema de transiciones $\mathcal{M}$, decida si $\mathcal{M} \models \phi$

Preguntas

¿Qué queremos?

Un algoritmo que, tomando como entrada una fórmula $\phi \in$ CTL y un sistema de transiciones $\mathcal{M}$, decida si $\mathcal{M} \models \phi$

¿Cuándo lo queremos?

Para hoy, a más tardar,

Preguntas

¿Qué queremos?

Un algoritmo que, tomando como entrada una fórmula $\phi \in \mathsf{CTL}$ y un sistema de transiciones $\mathcal{M}$, decida si $\mathcal{M} \models \phi$

¿Cuándo lo queremos?

Para hoy, a más tardar,

¿Podemos lograrlo?

Y..., no sé.

Preguntas

¿Qué queremos?

Un algoritmo que, tomando como entrada una fórmula $\phi \in$ CTL y un sistema de transiciones $\mathcal{M}$, decida si $\mathcal{M} \models \phi$

¿Cuándo lo queremos?

Para hoy, a más tardar,

¿Podemos lograrlo?

Y..., no sé. Depende de si CTL es **decidible**

Hoja de ruta

Hoja de ruta

1. Primero, transformaremos ϕ en una nueva fórmula $\psi \in$ CTL tal que $\psi \equiv \phi$, pero ψ utiliza sólo los conectivos temporales $\exists\bigcirc$, $\exists\,\mathsf{U}$ y $\forall\Diamond$

Hoja de ruta

1. Primero, transformaremos ϕ en una nueva fórmula $\psi \in$ CTL tal que $\psi \equiv \phi$, pero ψ utiliza sólo los conectivos temporales $\exists\bigcirc$, $\exists \mathsf{U}$ y $\forall\Diamond$
2. Luego, calcularemos el conjunto de estados

$$\mathsf{Sat}(\psi) = \{s \in S \mid \mathcal{M}, s \models \psi\}$$

Hoja de ruta

1. Primero, transformaremos ϕ en una nueva fórmula $\psi \in$ CTL tal que $\psi \equiv \phi$, pero ψ utiliza sólo los conectivos temporales $\exists\bigcirc$, $\exists\,\mathsf{U}$ y $\forall\Diamond$
2. Luego, calcularemos el conjunto de estados

$$\mathsf{Sat}(\psi) = \{s \in S \mid \mathcal{M}, s \models \psi\}$$

3. Si $I \subseteq \mathsf{Sat}(\psi)$, entonces $\mathcal{M} \models \phi$

Pre-primer paso

- Recordemos la semántica de lo que serán nuestros *operadores básicos*:

  1. $\mathcal{M}, s \models \exists[\phi \, \mathsf{U} \, \psi]$ sii para alguna traza $s = s_0 \to s_1 \to s_2 \to \ldots$, existe $j \in \mathbb{N}$ tal que:
     - $\mathcal{M}, s_j \models \psi$
     - $\mathcal{M}, s_i \models \phi$, para todo $i < j$
  2. $\mathcal{M}, s \models \exists \bigcirc \phi$ sii para algún s' tal que $s \to s'$, $\mathcal{M}, s' \models \phi$
  3. $\mathcal{M}, s \models \forall \Diamond \phi$ sii para toda traza $s = s_0 \to s_1 \to s_2 \to \ldots$, existe j tal que $\mathcal{M}, s_j \models \phi$

Primer paso

$$
\begin{array}{lcl}
T(p) & = & p \\
T(\bot) & = & \bot \\
T(\phi \wedge \psi) & = & T(\phi) \wedge T(\psi) \\
T(\neg\phi) & = & \neg T(\phi) \\
T(\exists\bigcirc\phi) & = & \exists\bigcirc T(\phi) \\
T(\exists[\phi \,\mathsf{U}\, \psi]) & = & \exists[T(\phi) \,\mathsf{U}\, T(\psi)] \\
T(\forall\Diamond\phi) & = & \forall\Diamond T(\phi)
\end{array}
$$

Primer paso

$$
\begin{array}{lcl}
T(p) & = & p \\
T(\bot) & = & \bot \\
T(\phi \wedge \psi) & = & T(\phi) \wedge T(\psi) \\
T(\neg\phi) & = & \neg T(\phi) \\
T(\exists\bigcirc\phi) & = & \exists\bigcirc T(\phi) \\
T(\exists[\phi \,\mathsf{U}\, \psi]) & = & \exists[T(\phi) \,\mathsf{U}\, T(\psi)] \\
T(\forall\Diamond\phi) & = & \forall\Diamond T(\phi) \\
 & & \\
T(\forall\bigcirc\phi) & = & T(\neg\exists\bigcirc\neg\phi) = \neg\exists\bigcirc\neg T(\phi)
\end{array}
$$

Primer paso

$$\begin{array}{lcl}
T(p) & = & p \\
T(\bot) & = & \bot \\
T(\phi \wedge \psi) & = & T(\phi) \wedge T(\psi) \\
T(\neg\phi) & = & \neg T(\phi) \\
T(\exists\bigcirc\phi) & = & \exists\bigcirc T(\phi) \\
T(\exists[\phi\,\mathsf{U}\,\psi]) & = & \exists[T(\phi)\,\mathsf{U}\,T(\psi)] \\
T(\forall\Diamond\phi) & = & \forall\Diamond T(\phi)
\end{array}$$

$$\begin{array}{lcl}
T(\forall\bigcirc\phi) & = & T(\neg\exists\bigcirc\neg\phi) = \neg\exists\bigcirc\neg T(\phi) \\
T(\forall[\phi\,\mathsf{U}\,\psi]) & = & T(\neg(\exists[\neg\psi\,\mathsf{U}\,(\neg\phi \wedge \neg\psi)] \vee \exists\Box\neg\psi))
\end{array}$$

Primer paso

$$
\begin{array}{lcl}
T(p) & = & p \\
T(\bot) & = & \bot \\
T(\phi \wedge \psi) & = & T(\phi) \wedge T(\psi) \\
T(\neg\phi) & = & \neg T(\phi) \\
T(\exists\bigcirc\phi) & = & \exists\bigcirc T(\phi) \\
T(\exists[\phi\,\mathsf{U}\,\psi]) & = & \exists[T(\phi)\,\mathsf{U}\,T(\psi)] \\
T(\forall\Diamond\phi) & = & \forall\Diamond T(\phi) \\
 & & \\
T(\forall\bigcirc\phi) & = & T(\neg\exists\bigcirc\neg\phi) = \neg\exists\bigcirc\neg T(\phi) \\
T(\forall[\phi\,\mathsf{U}\,\psi]) & = & T(\neg(\exists[\neg\psi\,\mathsf{U}\,(\neg\phi \wedge \neg\psi)] \vee \exists\Box\neg\psi)) \\
 & = & \ldots \\
 & = & \neg T(\exists[\neg\psi\,\mathsf{U}\,(\neg\phi \wedge \neg\psi)]) \wedge \neg T(\neg\forall\Diamond\psi) \\
 & = & \ldots \\
 & = & \text{algo que sólo utiliza los operadores de más arriba} \\
 & & \text{y los argumentos de T son } \phi, \psi
\end{array}
$$

Segundo paso

- Definimos $\psi = T(\phi)$
- Debemos calcular el conjunto $\mathsf{Sat}(\psi)$

Segundo paso

- Definimos $\psi = T(\phi)$
- Debemos calcular el conjunto Sat(ψ)
- Lo haremos por recursión en la fórmula, asumiendo que sabemos calcular Sat(ψ_1), para cualquier subfórmula ψ_1 de ψ.

Segundo paso

- Definimos $\psi = T(\phi)$
- Debemos calcular el conjunto $\mathsf{Sat}(\psi)$
- Lo haremos por recursión en la fórmula, asumiendo que sabemos calcular $\mathsf{Sat}(\psi_1)$, para cualquier subfórmula ψ_1 de ψ.
- Empecemos por los casos fáciles:

$$
\begin{array}{lcl}
\mathsf{Sat}(\bot) & = & \emptyset \\
\mathsf{Sat}(p_i) & = & \{s \in S \mid p_i \in L(s)\} \\
\mathsf{Sat}(\neg\psi_1) & = & S - \mathsf{Sat}(\psi_1) \\
\mathsf{Sat}(\psi_1 \wedge \psi_2) & = & \mathsf{Sat}(\psi_1) \cap \mathsf{Sat}(\psi_1)
\end{array}
$$

Segundo paso, definiciones auxiliares

- Para trabajar con los operadores temporales, definimos las siguientes funciones sobre conjuntos:

$$
\begin{aligned}
\text{pre}_{\exists}(Y) &= \{s \in S \mid \text{existe } s' \text{ tal que } s \rightarrow s' \text{ y } s' \in Y\} \\
\text{pre}_{\forall}(Y) &= \{s \in S \mid \text{para todo } s' \text{ tal que } s \rightarrow s' \text{ se cumple } s' \in Y\}
\end{aligned}
$$

Segundo paso, definiciones auxiliares

- Para trabajar con los operadores temporales, definimos las siguientes funciones sobre conjuntos:

$$
\begin{aligned}
\mathrm{pre}_{\exists}(Y) &= \{s \in S \mid \text{existe } s' \text{ tal que } s \to s' \text{ y } s' \in Y\} \\
\mathrm{pre}_{\forall}(Y) &= \{s \in S \mid \text{para todo } s' \text{ tal que } s \to s' \text{ se cumple } s' \in Y\}
\end{aligned}
$$

- Un estado está en $\mathrm{pre}_{\exists}(Y)$ sii tiene algún sucesor en Y

Segundo paso, definiciones auxiliares

- Para trabajar con los operadores temporales, definimos las siguientes funciones sobre conjuntos:

$$
\begin{aligned}
\mathrm{pre}_{\exists}(Y) &= \{s \in S \mid \text{existe } s' \text{ tal que } s \to s' \text{ y } s' \in Y\} \\
\mathrm{pre}_{\forall}(Y) &= \{s \in S \mid \text{para todo } s' \text{ tal que } s \to s' \text{ se cumple } s' \in Y\}
\end{aligned}
$$

- Un estado está en $\mathrm{pre}_{\exists}(Y)$ sii tiene algún sucesor en Y
- Un estado está en $\mathrm{pre}_{\forall}(Y)$ sii todos sus sucesores están en Y

Segundo paso, operador $\exists\bigcirc$

- Supongamos que tenemos Sat(ψ_1),

Segundo paso, operador $\exists\bigcirc$

- Supongamos que tenemos $\mathrm{Sat}(\psi_1)$,
- Calculemos

$$
\begin{aligned}
& s \models \exists\bigcirc\psi_1 \\
\Longleftrightarrow\ & \text{definición de } \models \\
& \text{existe } s' \text{ tal que } s \to s' \text{ y } s' \models \psi_1 \\
\Longleftrightarrow\ & \text{definición de Sat} \\
& \text{existe } s' \text{ tal que } s \to s' \text{ y } s' \in \mathrm{Sat}(\psi_1) \\
\Longleftrightarrow\ & \text{definición de } \mathrm{pre}_\exists \\
& s \in \mathrm{pre}_\exists(\mathrm{Sat}(\psi_1))
\end{aligned}
$$

Segundo paso, operador $\exists\bigcirc$

- Supongamos que tenemos $\mathsf{Sat}(\psi_1)$,
- Calculemos

$$
\begin{aligned}
& s \models \exists\bigcirc\psi_1 \\
\iff & \text{definición de } \models \\
& \text{existe } s' \text{ tal que } s \to s' \text{ y } s' \models \psi_1 \\
\iff & \text{definición de Sat} \\
& \text{existe } s' \text{ tal que } s \to s' \text{ y } s' \in \mathsf{Sat}(\psi_1) \\
\iff & \text{definición de } \mathsf{pre}_\exists \\
& s \in \mathsf{pre}_\exists(\mathsf{Sat}(\psi_1))
\end{aligned}
$$

- Obtenemos entonces

$$\mathsf{Sat}(\exists\bigcirc\psi) \quad = \quad \mathsf{pre}_\exists(\mathsf{Sat}(\psi))$$

Segundo paso, operador $\forall\Diamond$

- Conociendo Sat(ψ_1), ¿Cómo calculo Sat($\forall\Diamond\psi_1$)?

Segundo paso, operador $\forall\Diamond$

- Conociendo Sat(ψ_1), ¿Cómo calculo Sat($\forall\Diamond\psi_1$)?
- Algunas pistas:

1. Si vale ahora, es inevitable: Sat(ψ_1) $\subseteq$ Sat($\forall\Diamond\psi_1$)

Segundo paso, operador $\forall\Diamond$

- Conociendo Sat(ψ_1), ¿Cómo calculo Sat($\forall\Diamond\psi_1$)?
- Algunas pistas:

1. Si vale ahora, es inevitable: Sat(ψ_1) $\subseteq$ Sat($\forall\Diamond\psi_1$)
2. Si para todos mis sucesores ψ_1 es inevitable, para mi también

Segundo paso, operador $\forall\Diamond$

- Conociendo Sat(ψ_1), ¿Cómo calculo Sat($\forall\Diamond\psi_1$)?
- Algunas pistas:

1. Si vale ahora, es inevitable: Sat(ψ_1) $\subseteq$ Sat($\forall\Diamond\psi_1$)
2. Si para todos mis sucesores ψ_1 es inevitable, para mi también
3. Es decir, si todos mis sucesores están en Sat(ψ_1), pertenezco a Sat($\forall\Diamond\psi_1$)

Segundo paso, operador $\forall\Diamond$

- Conociendo $\mathsf{Sat}(\psi_1)$, ¿Cómo calculo $\mathsf{Sat}(\forall\Diamond\psi_1)$?
- Algunas pistas:

1. Si vale ahora, es inevitable: $\mathsf{Sat}(\psi_1) \subseteq \mathsf{Sat}(\forall\Diamond\psi_1)$
2. Si para todos mis sucesores ψ_1 es inevitable, para mi también
3. Es decir, si todos mis sucesores están en $\mathsf{Sat}(\psi_1)$, pertenezco a $\mathsf{Sat}(\forall\Diamond\psi_1)$
4. Por lo tanto, si yo estoy en $\mathsf{pre}_\forall(\mathsf{Sat}(\psi_1))$, ψ_1 es inevitable para mi

Segundo paso, operador $\forall\Diamond$

- Conociendo $\mathsf{Sat}(\psi_1)$, ¿Cómo calculo $\mathsf{Sat}(\forall\Diamond\psi_1)$?
- Algunas pistas:

1. Si vale ahora, es inevitable: $\mathsf{Sat}(\psi_1) \subseteq \mathsf{Sat}(\forall\Diamond\psi_1)$
2. Si para todos mis sucesores ψ_1 es inevitable, para mi también
3. Es decir, si todos mis sucesores están en $\mathsf{Sat}(\psi_1)$, pertenezco a $\mathsf{Sat}(\forall\Diamond\psi_1)$
4. Por lo tanto, si yo estoy en $\mathsf{pre}_\forall(\mathsf{Sat}(\psi_1))$, ψ_1 es inevitable para mi
5. Es decir, $\mathsf{Sat}(\psi_1) \cup \mathsf{pre}_\forall(\mathsf{Sat}(\psi_1)) \subseteq \mathsf{Sat}(\forall\Diamond\psi_1)$

Segundo paso, operador $\forall\Diamond$

- Conociendo Sat(ψ_1), ¿Cómo calculo Sat($\forall\Diamond\psi_1$)?
- Algunas pistas:

1. Si vale ahora, es inevitable: Sat(ψ_1) $\subseteq$ Sat($\forall\Diamond\psi_1$)
2. Si para todos mis sucesores ψ_1 es inevitable, para mi también
3. Es decir, si todos mis sucesores están en Sat(ψ_1), pertenezco a Sat($\forall\Diamond\psi_1$)
4. Por lo tanto, si yo estoy en $\text{pre}_\forall$(Sat(ψ_1)), ψ_1 es inevitable para mi
5. Es decir, Sat(ψ_1) $\cup$ $\text{pre}_\forall$(Sat(ψ_1)) $\subseteq$ Sat($\forall\Diamond\psi_1$)
6. Volver a la pista (2)

Segundo paso, operador $\forall\Diamond$

- Proponemos el siguiente procedimiento para calcular $\mathrm{Sat}(\forall\Diamond\psi_1)$:

$$
\begin{array}{l}
\mathit{inev}(Y)\{ \\
\quad \textbf{while } (\mathrm{Y} \neq \mathrm{Y} \cup \mathrm{pre}_{\forall}(Y)) \ \textbf{ do} \\
\qquad \mathrm{Y} \leftarrow \mathrm{Y} \cup \mathrm{pre}_{\forall}(Y) \ ; \\
\quad \textbf{return } \ Y \\
\}
\end{array}
$$

- Tenemos entonces

$$\mathrm{Sat}(\forall\Diamond\psi_1) = \mathit{inev}(\mathrm{Sat}(\psi_1))$$

- Debemos ver que este programa termina y es correcto

Segundo paso, operador $\exists \mathsf{U}$

- Conociendo $\mathrm{Sat}(\psi_1)$ y $\mathrm{Sat}(\psi_2)$, cómo calculo $Y = \mathrm{Sat}(\exists[\psi_1 \, \mathsf{U} \, \psi_2])$?
- Pistas:

Segundo paso, operador $\exists\,\mathrm{U}$

- Conociendo Sat(ψ_1) y Sat(ψ_2), cómo calculo $Y = \mathrm{Sat}(\exists[\psi_1 \,\mathrm{U}\, \psi_2])$?
- Pistas:

1. Si un estado satisface ψ_2, entonces está en Y

Segundo paso, operador $\exists$ U

- Conociendo Sat(ψ_1) y Sat(ψ_2), cómo calculo $Y = \text{Sat}(\exists[\psi_1 \, \text{U} \, \psi_2])$?
- Pistas:

1. Si un estado satisface ψ_2, entonces está en Y
2. Si un estado satisface ψ_1, y tiene algún sucesor en Y, entonces debería estar en Y

Segundo paso, operador $\exists\,\mathsf{U}$

- Conociendo $\mathsf{Sat}(\psi_1)$ y $\mathsf{Sat}(\psi_2)$, cómo calculo $Y = \mathsf{Sat}(\exists[\psi_1 \,\mathsf{U}\, \psi_2])$?
- Pistas:

1. Si un estado satisface ψ_2, entonces está en Y
2. Si un estado satisface ψ_1, y tiene algún sucesor en Y, entonces debería estar en Y
3. Por lo tanto, si $s \in \mathsf{Sat}(\psi_1) \cap \mathsf{pre}_{\exists}(Y)$, entonces debería pertenecer a Y

Segundo paso, operador $\exists$ U

- Proponemos el siguiente prodedimiento para calcular $\mathsf{Sat}(\exists[\psi_1 \,\mathsf{U}\, \psi_2])$
  ex-until$(X, Y)\{$
  while $(\mathsf{Y} \neq \mathsf{Y} \cup (X \cap \mathsf{pre}_{\exists}(Y)))$ **do**
  $\mathsf{Y} \leftarrow \mathsf{Y} \cup (X \cap \mathsf{pre}_{\exists}(Y))$;
  return Y
  $\}$

- Tenemos entonces

$$\mathsf{Sat}(\exists[\psi_1 \,\mathsf{U}\, \psi_2]) = \textit{ex-until}(\mathsf{Sat}(\psi_1), \mathsf{Sat}(\psi_2))$$

- Nuevamente, dejamos terminación y correctitud para más adelante

Juntando...

$$
\begin{array}{lcl}
\mathsf{Sat}(\bot) & = & \emptyset \\
\mathsf{Sat}(p_i) & = & \{s \in S \mid p_i \in L(s)\} \\
\mathsf{Sat}(\neg\psi_1) & = & S - \mathsf{Sat}(\psi_1) \\
\mathsf{Sat}(\psi_1 \wedge \psi_2) & = & \mathsf{Sat}(\psi_1) \cap \mathsf{Sat}(\psi_1) \\
\mathsf{Sat}(\exists\bigcirc\psi) & = & \mathsf{pre}_{\exists}(\mathsf{Sat}(\psi)) \\
\mathsf{Sat}(\forall\Diamond\psi_1) & = & \mathit{inev}(\mathsf{Sat}(\psi_1)) \\
\mathsf{Sat}(\exists[\psi_1 \,\mathsf{U}\, \psi_2]) & = & \mathit{ex\text{-}until}(\mathsf{Sat}(\psi_1), \mathsf{Sat}(\psi_2))
\end{array}
$$