Verificación de Modelos

Dante Zanarini

LCC

November 5, 2015

Verificación Formal

Ingredientes:

- Un lenguaje para describir sistemas
- Un lenguaje de especificación
- Un mecanismo para verificar que la descripción de un sistema satisface la especificación

Una forma: Verificación de Modelos

- Es una técnica automática usada principalmente para sistemas reactivos y concurrentes
- Estos sistemas están diseñados, en general, para tener un comportamiento infinito
- Por lo tanto, los métodos que vimos en primer año no son suficientes para verificar sus propiedades

Verificación de Modelos, ingredientes más comunes

- Los sistemas se describen mediante un sistema de transiciones $\mathcal{M}$ (finito)
- Las propiedades se expresan como fórmulas ϕ en alguna lógica temporal (la validez de una fórmula puede depender de dónde estoy parado en la ejecución de un programa)
- El mecanismo de verificación es automatizable, es decir, existe un programa que
  - Responde Sí en caso que $\mathcal{M} \models \phi$
  - En caso que $\mathcal{M} \not\models \phi$, responde No + un camino en el modelo que no cumple la propiedad

La lógica CTL

- *Computation Tree Logic* es una lógica **temporal**
- Se utiliza para expresar propiedades sobre las ejecuciones de un programa
- Sintaxis:
  1. $\bot \in \mathbf{CTL}$
  2. $p_i \in \mathbf{CTL}$, $i \in \mathbb{N}$
  3. Si $\phi \in \mathbf{CTL}$, entonces $(\neg\phi) \in \mathbf{CTL}$
  4. Si $\phi, \psi \in \mathbf{CTL}$, entonces $(\phi \wedge \psi) \in \mathbf{CTL}$
  5. Si $\phi \in \mathbf{CTL}$, entonces $\forall\bigcirc\phi$, $\exists\bigcirc\phi \in \mathbf{CTL}$
  6. Si $\phi, \psi \in \mathbf{CTL}$, entonces $\forall[\phi\,\mathbf{U}\,\psi]$, $\exists[\phi\,\mathbf{U}\,\psi] \in \mathbf{CTL}$
- Precedencia de los operadores: $\neg$, $\forall\bigcirc$, $\exists\bigcirc$, $\wedge$, $\forall\,\mathbf{U}$, $\exists\,\mathbf{U}$
- Definimos $\top$, $\vee$ y $\rightarrow$ usando sus equivalencias proposicionales con $\neg$, $\bot$ y $\wedge$

Algunas fórmulas (y no-fórmulas)

- $p_1 \rightarrow \forall \bigcirc p_2$
- $\forall [p_1 \; \mathbf{U} \; (p_2 \wedge p_3)]$
- $\exists \bigcirc p_0 \rightarrow \forall \bigcirc \forall \bigcirc p_1$
- $\forall \bigcirc (\forall [p_0 \; \mathbf{U} \; (\exists [p_1 \; \mathbf{U} \; p_2])])$
- $[p_1 \; \mathbf{U} \; p_2]$
- $\exists (p_1 \wedge p_2)$
- $\forall [p_1 \; \mathbf{U} \; \bigcirc p_2]$
- $\forall [(p_1 \; \mathbf{U} \; p_2) \wedge (p_3 \; \mathbf{U} \; p_4)]$

Semántica

- Las fórmulas de CTL se interpretan sobre **sistemas de transiciones**
- Un sistema de transiciones $\mathcal{M}$ es una tupla $(S, \rightarrow, I, L)$, donde:
  - S es un conjunto finito de estados
  - $I \subseteq S$ es el conjunto de estados iniciales
  - $\rightarrow \subseteq S \times S$ es una relación de transición entre estados
  - $L : S \rightarrow \mathcal{P}(AT)$ es una función de etiquetado
- Asumimos que $\rightarrow$ es no bloqueante $(\forall s \exists s' (s, s') \in \rightarrow)$

Sistemas de transiciones

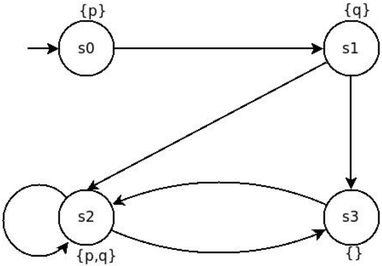
- AT es un conjunto de proposiciones atómicas, que depende de qué quiero especificar
- Si $s, s' \in \rightarrow$, escribimos $s \rightarrow s'$

Definición

Una traza es una secuencia infinita de estados $s_1, s_2, \ldots$ *tal que, para todo* $i \in \mathbb{N}$, $s_i \rightarrow s_{i+1}$

- Notación para trazas: $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \ldots$.

Sistemas de transiciones, ejemplo



- $S = \{s_0, s_1, s_2, s_3\}$
- $I = \{s_0\}$
- $L(s_0) = \{p\}$,
- $L(s_1) = \{q\}$,
- $L(s_2) = \{p, q\}$,
- $L(s_3) = \emptyset$

Semántica

Definimos la relación $\models$ por inducción en ϕ:

- $\mathcal{M}, s \not\models \bot$
- $\mathcal{M}, s \models p_i$ sii $p_i \in L(s)$
- $\mathcal{M}, s \models \neg\phi$ sii $\mathcal{M}, s \not\models \phi$
- $\mathcal{M}, s \models \phi \wedge \psi$ sii $\mathcal{M}, s \models \phi$ y $\mathcal{M}, s \models \psi$
- $\mathcal{M}, s \models \forall\bigcirc\phi$ sii para todo s' tal que $s \rightarrow s'$, se cumple $\mathcal{M}, s' \models \phi$
- $\mathcal{M}, s \models \exists\bigcirc\phi$ sii para algún s' tal que $s \rightarrow s'$, se cumple $\mathcal{M}, s' \models \phi$
- $\mathcal{M}, s \models \forall[\phi \,\mathbf{U}\, \psi]$ sii para cada traza $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$ con $s = s_0$, existe $j \in \mathbb{N}$ tal que:
  - $\mathcal{M}, s_j \models \psi$
  - $\mathcal{M}, s_i \models \phi$, para todo $i < j$
- $\mathcal{M}, s \models \exists[\phi \,\mathbf{U}\, \psi]$ sii para alguna traza $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \ldots$ con $s = s_0$, existe $j \in \mathbb{N}$ tal que:
  - $\mathcal{M}, s_j \models \psi$
  - $\mathcal{M}, s_i \models \phi$, para todo $i < j$

Semántica

Definición

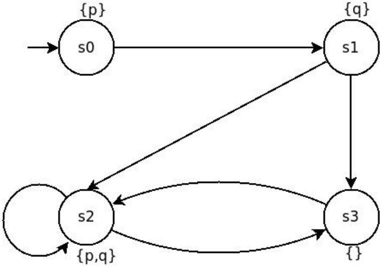
Sea $\mathcal{M} = (S, \rightarrow, I, L)$.

- *Decimos que* $\mathcal{M} \models \phi$ *sii para todo* $s \in I, \mathcal{M}, s \models \phi$
- ϕ *es válida* ($\models \phi$) *sii* $\mathcal{M}, s \models \phi$, *para todo* $\mathcal{M}$, s

- Cualquier tautología proposicional es válida
- Otros ejemplos de fórmulas válidas:
  - $\forall\Box\phi \rightarrow \exists\Box\phi$
  - $\forall\Box\phi \rightarrow (\phi \wedge \forall\bigcirc\forall\Box\phi)$
  - $\exists[\phi_1 \,\mathbf{U}\, \phi_2] \rightarrow (\phi_2 \vee (\phi_1 \wedge \exists\bigcirc\exists[\phi_1 \,\mathbf{U}\, \phi_2]))$
- Algunas fórmulas que no son válidas:
  - $\forall\bigcirc p \rightarrow p$
  - $\exists\Box p \rightarrow \forall\Box p$
  - $\forall\Diamond(p \vee q) \rightarrow \forall\Diamond p \vee \forall\Diamond q$

Semántica, ejemplos

Observemos que, para todo s, $\mathcal{M}, s \models \top$, donde $\top = \neg\bot$



- $\mathcal{M}, s_0 \models p$
- $\mathcal{M}, s_0 \not\models q$
- $\mathcal{M}, s_1 \models \exists\bigcirc p$
- $\mathcal{M}, s_1 \not\models \forall\bigcirc p$
- $\mathcal{M}, s_3 \models \forall\bigcirc p \wedge \forall\bigcirc q$
- $\mathcal{M}, s_0 \models \forall[\top \,\mathbf{U}\, (p \wedge q)]$
- $\mathcal{M}, s_0 \models \exists[(p \vee q) \,\mathbf{U}\, (\neg p \wedge \neg q)]$
- $\mathcal{M}, s_0 \not\models \exists[p \,\mathbf{U}\, (\neg p \wedge \neg q)]$

Operadores derivados

- ϕ *es inevitable:*
$$\forall\Diamond\phi \equiv \forall[\top \,\mathbf{U}\, \phi]$$
- ϕ *es posible:*
$$\exists\Diamond\phi \equiv \exists[\top \,\mathbf{U}\, \phi]$$
- ϕ *es invariante:*
$$\forall\Box\phi \equiv \neg\exists\Diamond\neg\phi$$
- ϕ *es invariante para alguna traza:*
$$\exists\Box\phi \equiv \neg\forall\Diamond\neg\phi$$

Semántica de los Operadores Derivados

Veamos qué significa que $\mathcal{M}, s \models \forall\Diamond\phi$

$\mathcal{M}, s \models \forall\Diamond\phi$
$\iff$ definición de $\forall\Diamond$
$\mathcal{M}, s \models \forall[\top\, \mathbf{U}\, \phi]$
$\iff$ definición de $\models$ para $\forall\, \mathbf{U}$
para cada traza $s_0 \to s_1 \to s_2 \to \ldots / s = s_0$,
existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \phi$ y $\mathcal{M}, s_i \models \top, \forall i < j$
$\iff$ $\mathcal{M}, s \models \top, \forall s$
para cada traza $s_0 \to s_1 \to s_2 \to \ldots / s = s_0$,
existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \phi$

Semántica de los Operadores Derivados

Veamos qué significa que $\mathcal{M}, s \models \exists\Box\phi$

$\mathcal{M}, s \models \exists\Box\phi$

$\iff$ definición de $\exists\Box$

$\mathcal{M}, s \models \neg\forall\Diamond\neg\phi$

$\iff$ definición de $\models$

$\mathcal{M}, s \not\models \forall\Diamond\neg\phi$

$\iff$ slide anterior

no se cumple que, para cada traza $s_0 \rightarrow s_1 \rightarrow \ldots / s = s_0$,
existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \neg\phi$

$\iff$ intercambio de cuantificadores

para alguna traza $s_0 \rightarrow s_1 \rightarrow \ldots / s = s_0$,
no existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \neg\phi$

$\iff$ definición de $\models$

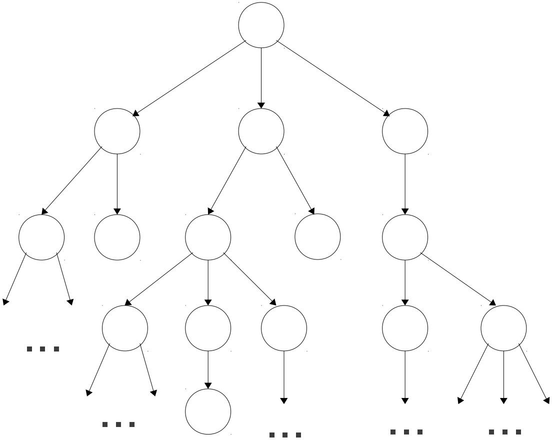
para alguna traza $s_0 \rightarrow s_1 \rightarrow \ldots / s = s_0$, no existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \not\models \phi$

$\iff$ intercambio de cuantificadores

para alguna traza $s_0 \rightarrow s_1 \rightarrow \ldots / s = s_0$, para todo $j \in \mathbb{N}$, $\mathcal{M}, s_j \models \phi$

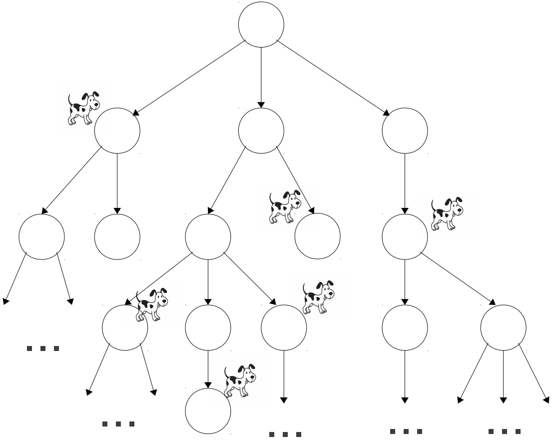
Ejemplos

- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



Ejemplos

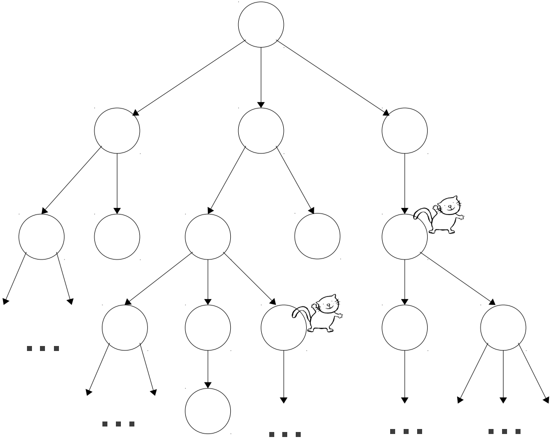
- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



$\forall\Diamond perro$

Ejemplos

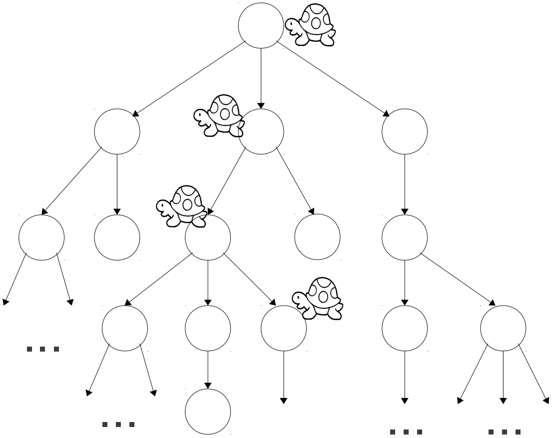
- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



$\exists\Diamond gato$

Ejemplos

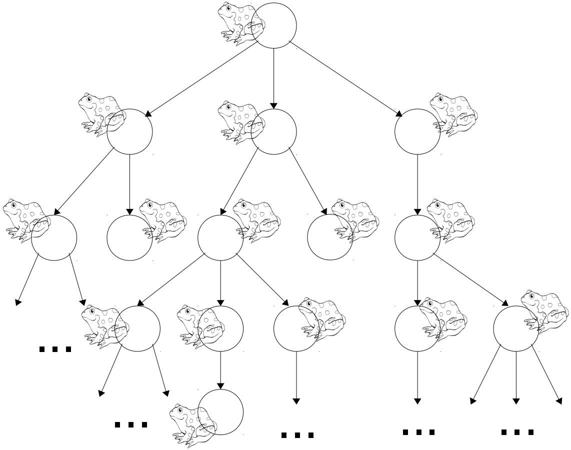
- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



$\exists\Box\, tortuga$

Ejemplos

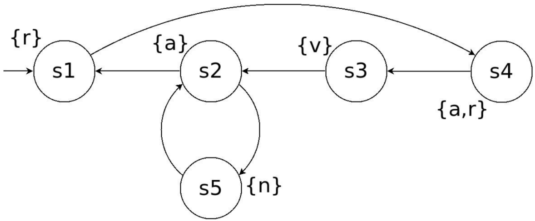
- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



$\forall\Box \mathit{sapo}$

Ejercicio 1

- Imaginemos un semáforo, que ocasionalmente puede quedar con la luz amarilla intermitente



- Determinar el conjunto de estados que satisface cada fórmula

- $r \rightarrow \forall\bigcirc v$
- $a \rightarrow \forall\bigcirc\forall\bigcirc a$
- $\exists\Box\neg v$
- $\forall\Diamond v$
- $\forall\Diamond a$
- $\forall\Box a$
- $\forall\Box\forall\Diamond a$
- $\forall\Diamond v$
- $\forall(n\,\mathbf{U}\,\neg n)$
- $\forall(\neg n\,\mathbf{U}\,n)$
- $\exists(n\,\mathbf{U}\,r)$
- $r \rightarrow \forall\Diamond v$

Ejercicio 2

¿Cuáles de las siguientes afirmaciones son válidas?

1. $\models \phi \to \forall\Box\phi$
2. Si $\models \phi$ entonces $\models \forall\Box\phi$
3. $\models \exists\Box\phi \to \forall\Diamond\phi$
4. $\models \forall[\bot \,\mathbf{U}\, \phi] \to \phi$