

Verificación de Modelos

Dante Zanarini

LCC

2 de diciembre de 2020

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, necesitamos métodos para razonar sobre *cómputos infinitos*

Verificación de Modelos, ingredientes más comunes

- Los sistemas se describen mediante un **sistema de transiciones** \mathcal{M} (finito)

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)

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 $\perp \in \text{CTL}$
 - 2 $p_i \in \text{CTL}, i \in \mathbb{N}$

La lógica CTL

- *Computation Tree Logic* es una lógica **temporal**
- Se utiliza para expresar propiedades sobre las ejecuciones de un programa
- Sintaxis:
 - 1 $\perp \in \text{CTL}$
 - 2 $p_i \in \text{CTL}, i \in \mathbb{N}$
 - 3 Si $\phi \in \text{CTL}$, entonces $(\neg\phi) \in \text{CTL}$
 - 4 Si $\phi, \psi \in \text{CTL}$, entonces $(\phi \wedge \psi) \in \text{CTL}$
 - 5 Si $\phi \in \text{CTL}$, entonces $\forall\bigcirc\phi, \exists\bigcirc\phi \in \text{CTL}$
 - 6 Si $\phi, \psi \in \text{CTL}$, entonces $\forall[\phi \text{ U } \psi], \exists[\phi \text{ U } \psi] \in \text{CTL}$

La lógica CTL

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

Algunas fórmulas (y no-fórmulas)

- $p_1 \rightarrow \forall \bigcirc p_2$
- $\forall[p_1 \cup (p_2 \wedge p_3)]$
- $\exists \bigcirc p_0 \rightarrow \forall \bigcirc \forall \bigcirc p_1$
- $\forall \bigcirc (\forall[p_0 \cup (\exists[p_1 \cup p_2])])$
- $[p_1 \cup p_2]$
- $\exists(p_1 \wedge p_2)$
- $\forall[p_1 \cup \bigcirc p_2]$
- $\forall[(p_1 \cup p_2) \wedge (p_3 \cup p_4)]$

- Las fórmulas de CTL se interpretan sobre **sistemas de transiciones**

- 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

- 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

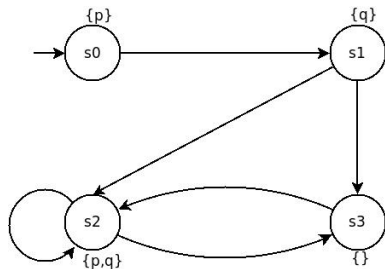
- AT es un conjunto de proposiciones atómicas, que depende de qué quiero especificar
- Si $s, s' \in \rightarrow$, escribimos $s \rightarrow s'$

Definición

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

- Notación para trazas: $s_1 \rightarrow s_2 \rightarrow s_3 \rightarrow \dots$

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 :

- $\mathcal{M}, s \not\models \perp$
- $\mathcal{M}, s \models p_i$ sii $p_i \in L(s)$

Semántica

Definimos la relación \models por inducción en ϕ :

- $\mathcal{M}, s \not\models \perp$
- $\mathcal{M}, s \models \neg\phi$ sii $\mathcal{M}, s \not\models \phi$
- $\mathcal{M}, s \models \phi \wedge \psi$ sii $\mathcal{M}, s \models \phi$ y $\mathcal{M}, s \models \psi$
- $\mathcal{M}, s \models p_i$ sii $p_i \in L(s)$

Semántica

Definimos la relación \models por inducción en ϕ :

- $\mathcal{M}, s \not\models \perp$
- $\mathcal{M}, s \models p_i$ 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 $\mathcal{M}, s \models \psi$
- $\mathcal{M}, s \models \forall\Box\phi$ sii para todo s' tal que $s \rightarrow s'$, se cumple $\mathcal{M}, s' \models \phi$
- $\mathcal{M}, s \models \exists\Box\phi$ sii para algún s' tal que $s \rightarrow s'$, se cumple $\mathcal{M}, s' \models \phi$

Semántica

Definimos la relación \models por inducción en ϕ :

- $\mathcal{M}, s \not\models \perp$
- $\mathcal{M}, s \models p_i$ 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 $\mathcal{M}, s' \models \phi$
- $\mathcal{M}, s \models \forall[\phi \cup \psi]$ sii para cada traza $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots$ 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

Definimos la relación \models por inducción en ϕ :

- $\mathcal{M}, s \not\models \perp$
- $\mathcal{M}, s \models p_i$ 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 $\mathcal{M}, s \models \psi$
- $\mathcal{M}, s \models \forall\phi$ sii para todo s' tal que $s \rightarrow s'$, se cumple $\mathcal{M}, s' \models \phi$
- $\mathcal{M}, s \models \exists\phi$ sii para algún s' tal que $s \rightarrow s'$, se cumple $\mathcal{M}, s' \models \phi$
- $\mathcal{M}, s \models \forall[\phi \cup \psi]$ sii para cada traza $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots$ 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 $i < j$
- $\mathcal{M}, s \models \exists[\phi \cup \psi]$ sii para alguna traza $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots$ 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 $i < j$

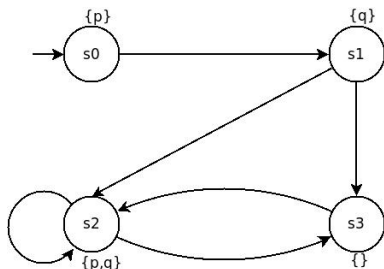
Definición

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:
 - ▶ $\exists[\phi_1 \cup \phi_2] \rightarrow (\phi_2 \vee (\phi_1 \wedge \exists \circ \exists[\phi_1 \cup \phi_2]))$
 - ▶ $\forall \circ p \rightarrow \exists \circ p$
- Algunas fórmulas que no son válidas:
 - ▶ $\forall \circ p \rightarrow p$
 - ▶ $\exists[\top \cup p] \rightarrow \forall[\top \cup p]$
 - ▶ $\forall[p \cup q] \rightarrow q \vee (p \wedge \forall \circ q) \vee (p \wedge \forall \circ p \wedge \forall \circ \forall \circ q)$

Semántica, ejemplos

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



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

Operadores derivados

- ϕ es inevitable:

$$\forall \Diamond \phi \equiv \forall [\top \cup \phi]$$

- ϕ es posible:

$$\exists \Diamond \phi \equiv \exists [\top \cup \phi]$$

- ϕ es invariante:

$$\forall \Box \phi \equiv \neg \exists \Diamond \neg \phi$$

- ϕ es invariante para alguna traza:

$$\exists \Box \phi \equiv \neg \forall \Diamond \neg \phi$$

Operadores derivados, ejemplos

Algunas fórmulas válidas

- $\forall \Box \phi \rightarrow \exists \Box \phi$
- $\forall \Box \phi \rightarrow (\phi \wedge \forall \bigcirc \forall \Box \phi)$
- $\exists \Diamond (p \vee q) \rightarrow \exists \Diamond p \vee \exists \Diamond q$

Fórmulas que no son válidas

- $\forall \Diamond (p \vee q) \rightarrow \forall \Diamond p \vee \forall \Diamond q$
- $\exists \Box p \wedge \exists \Box q \rightarrow \exists \Box (p \wedge q)$

Semántica de los Operadores Derivados

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

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

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 $\forall \Diamond$

$$\mathcal{M}, s \models \forall [\top \cup \phi]$$

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 $\forall \Diamond$

$$\mathcal{M}, s \models \forall [\top \cup \phi]$$

\iff definición de \models para $\forall \cup$

para cada traza $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots / s = s_0$,

existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \phi$ y $\mathcal{M}, s_i \models \top, \forall i < j$

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 $\forall \Diamond$

$$\mathcal{M}, s \models \forall [\top \cup \phi]$$

\iff definición de \models para $\forall \cup$

para cada traza $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots / s = s_0$,

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 $s_0 \rightarrow s_1 \rightarrow s_2 \rightarrow \dots / s = s_0$,

existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \phi$

Semántica de los Operadores Derivados

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

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

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 $\exists \Box$

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

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

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

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 $s_0 \rightarrow s_1 \rightarrow \dots / s = s_0$,
existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \neg \phi$

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 $s_0 \rightarrow s_1 \rightarrow \dots / s = s_0$,
existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \neg \phi$

\iff intercambio de cuantificadores

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

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 $s_0 \rightarrow s_1 \rightarrow \dots / s = s_0$,
existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \models \neg \phi$

\iff intercambio de cuantificadores

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

\iff definición de \models

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

\iff intercambio de cuantificadores

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

\iff definición de \models

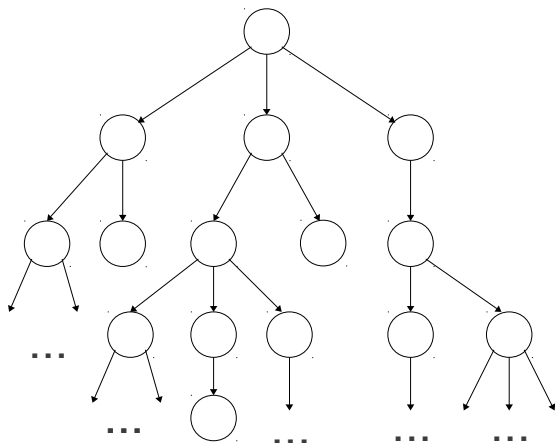
para alguna traza $s_0 \rightarrow s_1 \rightarrow \dots / s = s_0$, no existe $j \in \mathbb{N}$ tal que $\mathcal{M}, s_j \not\models \phi$

\iff intercambio de cuantificadores

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

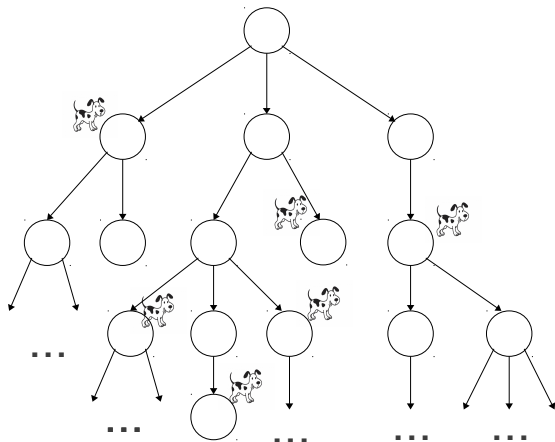
Ejemplos

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



Ejemplos

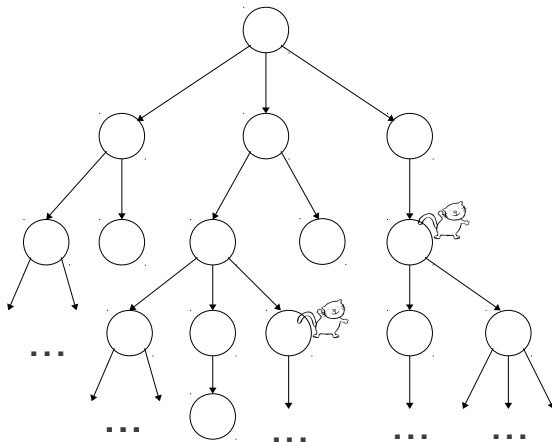
- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



$\forall \Diamond \text{perro}$

Ejemplos

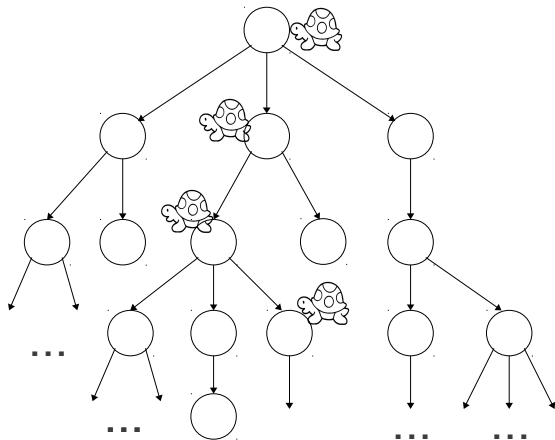
- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



$\exists \Diamond \text{gato}$

Ejemplos

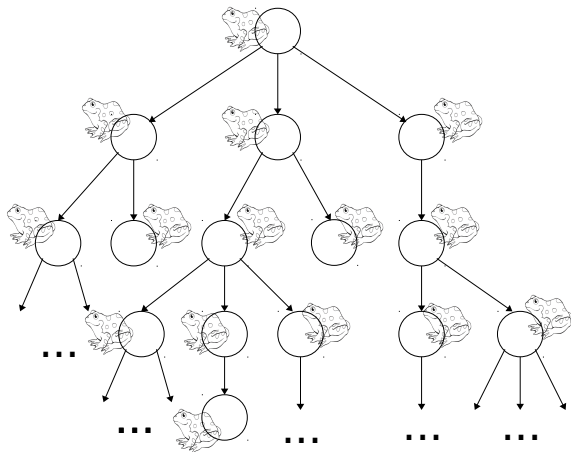
- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



$\exists \square \text{tortuga}$

Ejemplos

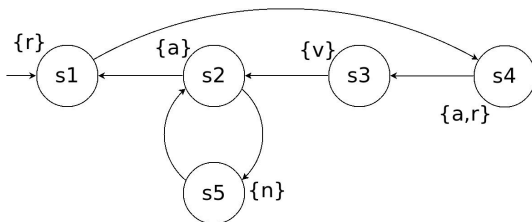
- Imaginemos que nuestras proposiciones atómicas refieren a animales,
- y consideremos el árbol de computaciones de un sistema de transición



$\forall \Box \textit{sapo}$

Ejercicio 1

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



- Determinar el conjunto de estados que satisface cada fórmula

- | | | |
|---|-------------------------------------|--------------------------------------|
| • $r \rightarrow \forall \bigcirc v$ | • $\forall \Diamond a$ | • $\forall (n U \neg n)$ |
| • $a \rightarrow \forall \bigcirc \bigcirc a$ | • $\forall \Box a$ | • $\forall (\neg n U n)$ |
| • $\exists \Box \neg v$ | • $\forall \Box \forall \Diamond a$ | • $\exists (n U r)$ |
| • $\forall \Diamond v$ | • $\forall \Diamond v$ | • $r \rightarrow \forall \Diamond v$ |

Ejercicio 2

¿Cuáles de las siguientes afirmaciones son válidas?

① $\models \phi \rightarrow \forall \Box \phi$

② Si $\models \phi$ entonces $\models \forall \Box \phi$

③ $\models \exists \Box \phi \rightarrow \forall \Diamond \phi$

④ $\models \forall [\perp \cup \phi] \rightarrow \phi$