NuSMV: Lógicas Temporales

Francisco J. Martín Mateos

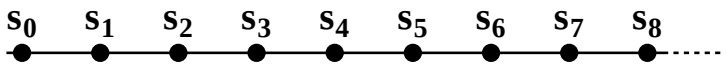
Dpto. Ciencias de la Computación e Inteligencia Artificial
Universidad de Sevilla

¿Qué son las lógicas temporales?

- Las lógicas temporales son lógicas diseñadas para modelar el tiempo y expresar propiedades sobre el mismo
- El tiempo se modela como secuencias infinitas de estados
- Cada estado tiene propiedades estáticas que se expresan en lógica proposicional o de primer orden
- Las propiedades temporales se expresan con conectivas especiales
- Algunas de estas lógicas son
  - Lógica Temporal Lineal (LTL)
  - Lógica Temporal Computacional (CTL)

Lógica Temporal Lineal (LTL)

- LTL es una lógica temporal en la que el tiempo se modela como una secuencia infinita de estados



- Se considera un conjunto infinito de propiedades atómicas $\mathcal{A}$ que representan hechos que pueden ocurrir en algún estado
  - *"La impresora Q5 está ocupada"*
  - *"El contenido del registro R1 es mayor que 6"*
- Estas propiedades pueden cambiar de un estado al siguiente

LTL: Fórmulas

- Cualquier propiedad atómica (elementos de $\mathcal{A}$) es una fórmula
- Los símbolos $\top$ y $\bot$ son fórmulas
- Si ϕ y ψ son fórmulas entonces también son fórmulas:
  - $(\neg\phi)$: negación de ϕ
  - $(\phi \wedge \psi)$: conjunción de ϕ y ψ
  - $(\phi \vee \psi)$: disyunción de ϕ y ψ
  - $(\phi \rightarrow \psi)$: ϕ implica ψ
  - $(\mathbf{X}\phi)$: ϕ ocurre en el siguiente estado
  - $(\mathbf{F}\phi)$: ϕ ocurre en algún estado futuro
  - $(\mathbf{G}\phi)$: ϕ ocurre en todos los estados futuros
  - $(\phi\mathbf{U}\psi)$: ϕ ocurre hasta que ocurre ψ
  - $(\phi\mathbf{W}\psi)$: ϕ ocurre mientras ψ no ocurra
  - $(\phi\mathbf{R}\psi)$: ψ ocurre mientras ϕ no ocurra

LTL: Fórmulas

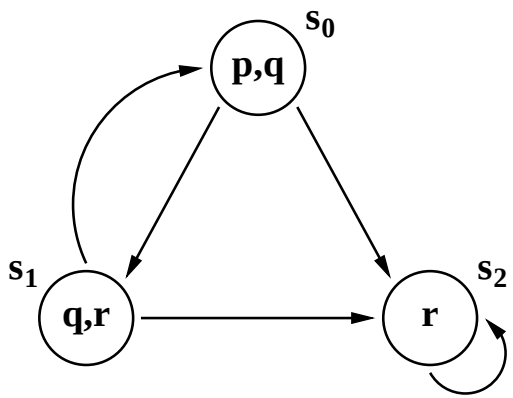
- Eliminación de paréntesis
  - Las conectivas unarias son más prioritarias que las binarias
  - La prioridad entre las conectivas binarias es la siguiente: **U**, **R**, **W**, $\wedge$, $\vee$ y $\rightarrow$ (de mayor a menor)
  - Los paréntesis externos se pueden eliminar
- Ejemplos de fórmulas
  - **FG**ϕ: En algún momento la propiedad ϕ se cumplirá para siempre
  - **GF**ϕ: La propiedad ϕ se cumple una cantidad infinita de veces
  - **G(**$\phi \rightarrow$ **F**ψ**)**: Siempre que ϕ se cumpla, en algún momento después se cumplirá ψ

LTL: Semántica

- Los sistemas para los cuales utilizaremos la lógica LTL pueden ser modelados como sistemas de transición
- Sistemas de transición: $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$, donde $\mathbf{S}$ es un conjunto finito de estados, $\rightarrow_{\mathcal{M}}$ es una relación binaria sobre $\mathbf{S}$ tal que para todo $\mathbf{s} \in \mathbf{S}$ existe un $\mathbf{s'} \in \mathbf{S}$ tal que $\mathbf{s} \rightarrow_{\mathcal{M}} \mathbf{s'}$ y $\mathbf{L}$ es una función de etiquetado $\mathbf{L} : \mathbf{S} \Rightarrow \mathcal{P}(\mathcal{A})$
  - $\rightarrow_{\mathcal{M}}$ representa las transiciones entre estados
  - $\mathcal{P}(\mathcal{A})$ es el conjunto formado por los subconjuntos de $\mathcal{A}$
  - $\mathbf{L(s)}$ representa el conjunto de propiedades atómicas que son ciertas en el estado $\mathbf{s}$
  - En lo sucesivo diremos que $\mathcal{M}$ es un modelo

LTL: Semántica

- Los sistemas de transición se representan de forma concisa usando grafos dirigidos cuyos nodos están etiquetados con propiedades atómicas que son ciertas en el estado que representa



LTL: Semántica

- Un *camino* en un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ es una secuencia infinita de estados $\mathbf{s_1}, \mathbf{s_2}, \mathbf{s_3}, \ldots$ tales que para cada $\mathbf{i} \geq \mathbf{1}, \mathbf{s_i} \rightarrow_{\mathcal{M}} \mathbf{s_{i+1}}$
- Un camino representa un posible futuro de un sistema de transición
- Sea $\pi = \mathbf{s_1}, \mathbf{s_2}, \mathbf{s_3}, \ldots$ un camino, entonces para todo $\mathbf{i} \geq \mathbf{1}$, $\pi^{\mathbf{i}}$ es el camino que comienza en el estado $\mathbf{s_i}$, es decir, $\pi^{\mathbf{i}} = \mathbf{s_i}, \mathbf{s_{i+1}}, \mathbf{s_{i+3}}, \ldots$
- La semántica de las fórmulas LTL se expresa con respecto a un camino π cualquiera

LTL: Semántica

- Dado un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ y un camino $\pi = \mathbf{s_1}, \mathbf{s_2}, \mathbf{s_3}, \ldots$ en $\mathcal{M}$, la semántica de las fórmulas LTL se define como sigue:
  - $\pi \models \top$
  - $\pi \not\models \bot$
  - $\pi \models \mathbf{p}$ si y sólo si $\mathbf{p} \in \mathbf{L(s_1)}$
  - $\pi \models \neg\phi$ si y sólo si $\pi \models \phi$
  - $\pi \models \phi \wedge \psi$ si y sólo si $\pi \models \phi$ y $\pi \models \psi$
  - $\pi \models \phi \vee \psi$ si y sólo si $\pi \models \phi$ o $\pi \models \psi$
  - $\pi \models \phi \rightarrow \psi$ si y sólo si $\pi \models \psi$ cuando $\pi \models \phi$

LTL: Semántica

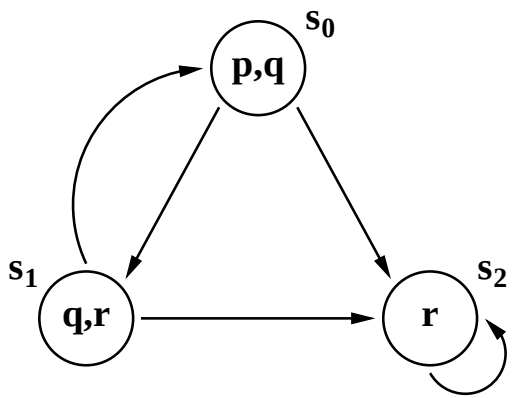
- Dado un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ y un camino $\pi = \mathbf{s_1}, \mathbf{s_2}, \mathbf{s_3}, \ldots$ en $\mathcal{M}$, la semántica de las fórmulas LTL se define como sigue:
  - $\pi \models \mathbf{X}\phi$ si y sólo si $\pi^{\mathbf{2}} \models \phi$
  - $\pi \models \mathbf{F}\phi$ si y sólo si existe $\mathbf{i} \geq \mathbf{1}$ tal que $\pi^{\mathbf{i}} \models \phi$
  - $\pi \models \mathbf{G}\phi$ si y sólo si para todo $\mathbf{i} \geq \mathbf{1}$ se tiene que $\pi^{\mathbf{i}} \models \phi$
  - $\pi \models \phi \mathbf{U} \psi$ si y sólo si existe $\mathbf{i} \geq \mathbf{1}$ tal que $\pi^{\mathbf{i}} \models \psi$ y para todo $\mathbf{j} = \mathbf{1}, \ldots, \mathbf{i} - \mathbf{1}$ se tiene que $\pi^{\mathbf{j}} \models \phi$
  - $\pi \models \phi \mathbf{W} \psi$ si y sólo si existe $\mathbf{i} \geq \mathbf{1}$ tal que $\pi^{\mathbf{i}} \models \psi$ y para todo $\mathbf{j} = \mathbf{1}, \ldots, \mathbf{i} - \mathbf{1}$ se tiene que $\pi^{\mathbf{j}} \models \phi$; o para todo $\mathbf{i}$ se tiene que $\pi^{\mathbf{i}} \models \phi$
  - $\pi \models \phi \mathbf{R} \psi$ si y sólo si existe $\mathbf{i} \geq \mathbf{1}$ tal que $\pi^{\mathbf{i}} \models \phi$ y para todo $\mathbf{j} = \mathbf{1}, \ldots, \mathbf{i}$ se tiene que $\pi^{\mathbf{j}} \models \psi$; o para todo $\mathbf{i}$ se tiene que $\pi^{\mathbf{i}} \models \psi$

LTL: Semántica

- Dado un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$, $\mathbf{s} \in \mathbf{S}$ y una fórmula LTL ϕ, decimos que ϕ es válida en $\mathcal{M}$ a partir del estado $\mathbf{s}$, $\mathcal{M}, \mathbf{s} \models \phi$, si y sólo si para cualquier camino π en $\mathcal{M}$ que comience en $\mathbf{s}$ se tiene que $\pi \models \phi$
- Si el modelo $\mathcal{M}$ está claro en el contexto, se suele escribir $\mathbf{s} \models \phi$ en lugar de $\mathcal{M}, \mathbf{s} \models \phi$

LTL: Semántica

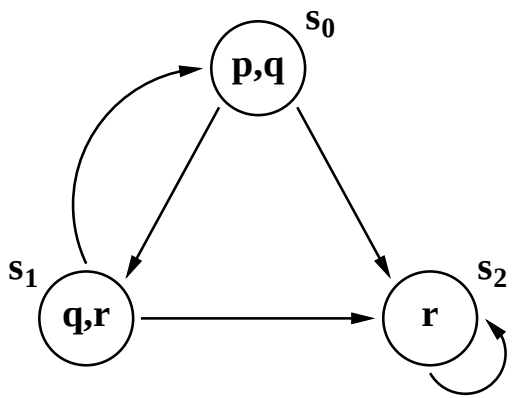
- Consideremos el modelo $\mathcal{M}$ representado por el siguiente sistema de transición



- Se verifican
  - $\mathcal{M}, s_0 \models \mathbf{p} \wedge \mathbf{q}$
  - $\mathcal{M}, s_0 \models \neg \mathbf{r}$
  - $\mathcal{M}, s_0 \models \top$
  - $\mathcal{M}, s_0 \models \mathbf{X}\mathbf{r}$

LTL: Semántica

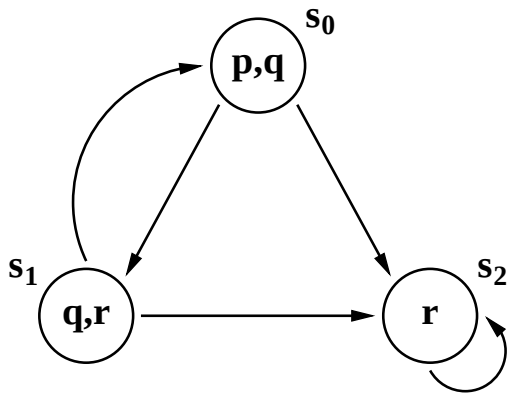
- Consideremos el modelo $\mathcal{M}$ representado por el siguiente sistema de transición



- Se verifican
  - $\mathcal{M}, \mathbf{s_0} \not\models \mathbf{X(q \wedge r)}$
  - $\mathcal{M}, \mathbf{s_0} \models \mathbf{G\neg(p \wedge r)}$
  - $\mathcal{M}, \mathbf{s_2} \models \mathbf{Gr}$
  - Para cualquier $\mathbf{s}$ se tiene $\mathcal{M}, \mathbf{s} \models \mathbf{F(\neg q \wedge r) \rightarrow FGr}$

LTL: Semántica

- Consideremos el modelo $\mathcal{M}$ representado por el siguiente sistema de transición



- Se verifican
  - $\mathcal{M}, s_0 \not\models \mathbf{GFp}$
  - $\mathcal{M}, s_0 \models \mathbf{GFp} \rightarrow \mathbf{GFr}$
  - $\mathcal{M}, s_0 \not\models \mathbf{GFr} \rightarrow \mathbf{GFp}$

LTL: Semántica

- Decimos que dos fórmulas son equivalentes, $\phi \equiv \psi$ si y sólo si para todo modelo $\mathcal{M}$ y para todo camino π en $\mathcal{M}$ se tiene que $\pi \models \phi$ si y sólo si $\pi \models \psi$
- Relaciones entre las conectivas
  - $\neg(\phi \wedge \psi) \equiv \neg\phi \vee \neg\psi$
  - $\neg(\phi \vee \psi) \equiv \neg\phi \wedge \neg\psi$
  - $\neg \mathbf{F}\phi \equiv \mathbf{G}\neg\phi$
  - $\neg \mathbf{G}\phi \equiv \mathbf{F}\neg\phi$
  - $\neg \mathbf{X}\phi \equiv \mathbf{X}\neg\phi$
  - $\neg(\phi \mathbf{U} \psi) \equiv \neg\phi \mathbf{R} \neg\psi$
  - $\neg(\phi \mathbf{R} \psi) \equiv \neg\phi \mathbf{U} \neg\psi$
  - $\phi \mathbf{W} \psi \equiv \phi \mathbf{U} \psi \vee \mathbf{G}\phi$
- Estas equivalencias permiten la interiorización de la negación en las fórmulas LTL

LTL: Semántica

- Decimos que dos fórmulas son equivalentes, $\phi \equiv \psi$ si y sólo si para todo modelo $\mathcal{M}$ y para todo camino π en $\mathcal{M}$ se tiene que $\pi \models \phi$ si y sólo si $\pi \models \psi$
- Relaciones entre las conectivas
  - $\mathbf{F}(\phi \vee \psi) \equiv \mathbf{F}\phi \vee \mathbf{F}\psi$
  - $\mathbf{G}(\phi \wedge \psi) \equiv \mathbf{G}\phi \wedge \mathbf{G}\psi$
  - $\mathbf{F}\phi \equiv \top \mathbf{U} \phi$
  - $\mathbf{G}\phi \equiv \bot \mathbf{R} \phi$
  - $\phi \mathbf{U} \psi \equiv \phi \mathbf{W} \psi \wedge \mathbf{F}\psi$
  - $\phi \mathbf{W} \psi \equiv \psi \mathbf{R} (\phi \vee \psi)$
  - $\phi \mathbf{R} \psi \equiv \psi \mathbf{W} (\phi \wedge \psi)$

Patrones de especificación

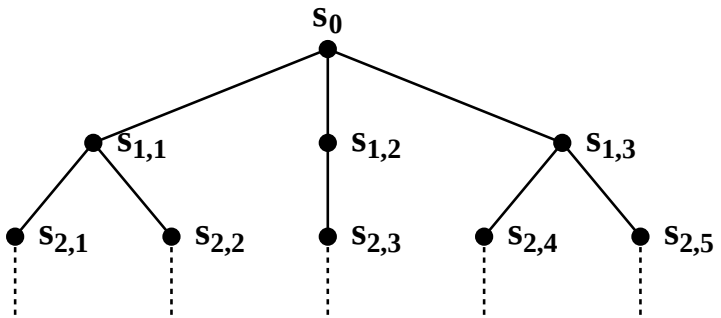
- (Liveness) *Si se realiza alguna petición, entonces es finalmente atendida*: **G(peticion $\rightarrow$ Fatendida)**
- (Deadlock) *Ocurra lo que ocurra, el proceso terminará quedando permanentemente inactivo*: **FG$\neg$activo**
- (Fairness) *En cualquier situación el proceso se activará una cantidad infinita de veces*: **GFactivo**
- (Fairness) *Si un proceso queda activo una cantidad infinita de veces entonces es ejecutado una cantidad infinita de veces*: **GFactivo $\rightarrow$ GFejecucion**

Patrones de especificación

- (Safety) *Es imposible alcanzar una situación en la que el proceso esté ejecutandose y no esté activo*:
  G¬(ejecucion $\wedge$ **¬activo)**
- En LTL no se pueden expresar propiedades que afirme la existencia de un camino con una propiedad concreta (Reachability), ya que la semántica definida se establece sobre todos los caminos existentes:
  - *Es posible alcanzar un estado en el que hay una petición y el proceso está inactivo*

Lógica Temporal Computacional (CTL)

- CTL es una lógica temporal en la que el tiempo se modela como un árbol en el que la ramificación de cada nodo representa todos los posibles futuros que se pueden dar a partir de un estado



- Se considera un conjunto infinito de propiedades atómicas $\mathcal{A}$ que representan hechos que pueden ocurrir en algún estado

CTL: Fórmulas

- Cualquier propiedad atómica (elementos de $\mathcal{A}$) es una fórmula
- Los símbolos $\top$ y $\bot$ son fórmulas
- Si ϕ y ψ son fórmulas entonces también son fórmulas:
  - $(\neg\phi)$: negación de ϕ
  - $(\phi \wedge \psi)$: conjunción de ϕ y ψ
  - $(\phi \vee \psi)$: disyunción de ϕ y ψ
  - $(\phi \rightarrow \psi)$: ϕ implica ψ
  - **(AX** ϕ**)**: ϕ inevitablemente ocurre en el estado siguiente
  - **(EX** ϕ**)**: ϕ posiblemente ocurre en algún estado siguiente
  - **(AF** ϕ**)**: ϕ inevitablemente ocurre en algún estado futuro
  - **(EF** ϕ**)**: ϕ posiblemente ocurre en algún estado futuro
  - **(AG** ϕ**)**: ϕ inevitablemente ocurre en todos los estados futuros
  - **(EG** ϕ**)**: ϕ posiblemente ocurre en todos los estados futuros
  - **A[**ϕ**U**ψ**]**: ϕ inevitablemente ocurre hasta que ocurre ψ
  - **E[**ϕ**U**ψ**]**: ϕ posiblemente ocurre hasta que ocurre ψ

CTL: Fórmulas

- Eliminación de paréntesis
  - Las conectivas unarias son más prioritarias que las binarias
  - La prioridad entre las conectivas binarias es la siguiente: $\wedge$, $\vee$, $\rightarrow$, **AU** y **EU** (de mayor a menor)
  - Los paréntesis externos se pueden eliminar
- Ejemplos de fórmulas
  - **AF AG** ϕ: Inevitablemente la propiedad ϕ se cumplirá para siempre
  - **EF AG** ϕ: Posiblemente la propiedad ϕ se cumplirá para siempre
  - **AG AF** ϕ: La propiedad ϕ se cumple una cantidad infinita de veces
- **AX** ϕ en CTL equivale a **X**ϕ en LTL
- **AF** ϕ en CTL equivale a **F**ϕ en LTL
- **AG** ϕ en CTL equivale a **G**ϕ en LTL
- **A**[ϕ**U**ψ] en CTL equivale a ϕ**U**ψ en LTL

CTL: Semántica

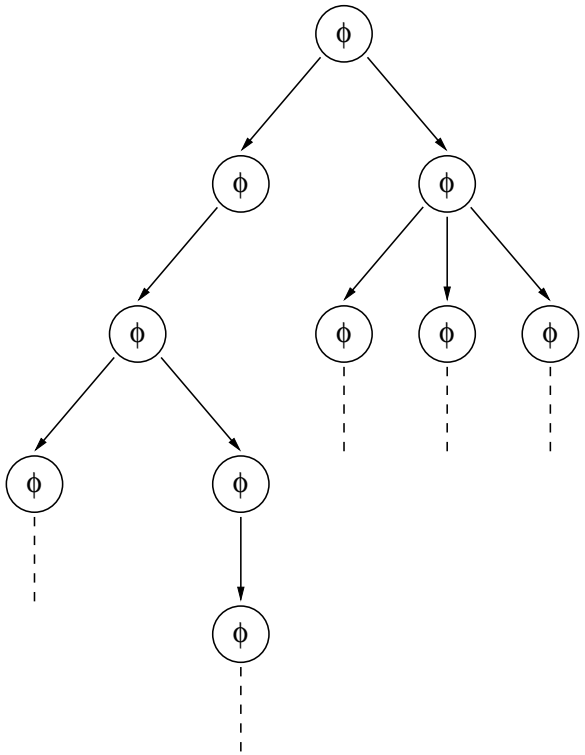
- Las fórmulas CTL se interpretan sobre sistemas de transición
- Sea $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ un modelo, $\mathbf{s} \in \mathbf{S}$ y ϕ una fórmula CTL, la definición de $\mathcal{M}, \mathbf{s} \models \phi$ es intuitivamente la siguiente:
  - Si ϕ es atómica, su satisfaccibilidad está determinada por **L**
  - Si la conectiva principal de ϕ es booleana, su satisfaccibilidad se resuelve como en lógica proposicional
  - Si la conectiva principal de ϕ comienza por **A**, su satisfacibilidad se tiene si todos los caminos que comienzan en **s** satisfacen la fórmula LTL obtenida eliminado el símbolo **A**
  - Si la conectiva principal de ϕ comienza por **E**, su satisfacibilidad se tiene si algún camino que comienze en **s** satisface la fórmula LTL obtenida eliminado el símbolo **E**

CTL: Semántica

- La satisfacibilidad de una fórmula CTL ϕ en un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ a partir de un estado $\mathbf{s} \in \mathbf{S}$, $\mathcal{M}, \mathbf{s} \models \phi$, se define como sigue:
  - $\mathcal{M}, \mathbf{s} \models \top$
  - $\mathcal{M}, \mathbf{s} \not\models \bot$
  - $\mathcal{M}, \mathbf{s} \models \mathbf{p}$ si y sólo si $\mathbf{p} \in \mathbf{L(s)}$
  - $\mathcal{M}, \mathbf{s} \models \neg\phi$ si y sólo si $\mathcal{M}, \mathbf{s} \not\models \phi$
  - $\mathcal{M}, \mathbf{s} \models \phi \wedge \psi$ si y sólo si $\mathcal{M}, \mathbf{s} \models \phi$ y $\mathcal{M}, \mathbf{s} \models \psi$
  - $\mathcal{M}, \mathbf{s} \models \phi \vee \psi$ si y sólo si $\mathcal{M}, \mathbf{s} \models \phi$ o $\mathcal{M}, \mathbf{s} \models \psi$
  - $\mathcal{M}, \mathbf{s} \models \phi \rightarrow \psi$ si y sólo si $\mathcal{M}, \mathbf{s} \not\models \phi$ o $\mathcal{M}, \mathbf{s} \models \psi$
  - $\mathcal{M}, \mathbf{s} \models \mathbf{AX}\ \phi$ si y sólo si para todo $\mathbf{s'}$ sucesor de $\mathbf{s}$ en $\mathcal{M}$ se tiene $\mathcal{M}, \mathbf{s'} \models \phi$
  - $\mathcal{M}, \mathbf{s} \models \mathbf{EX}\ \phi$ si y sólo si existe $\mathbf{s'}$ sucesor de $\mathbf{s}$ en $\mathcal{M}$ tal que $\mathcal{M}, \mathbf{s'} \models \phi$

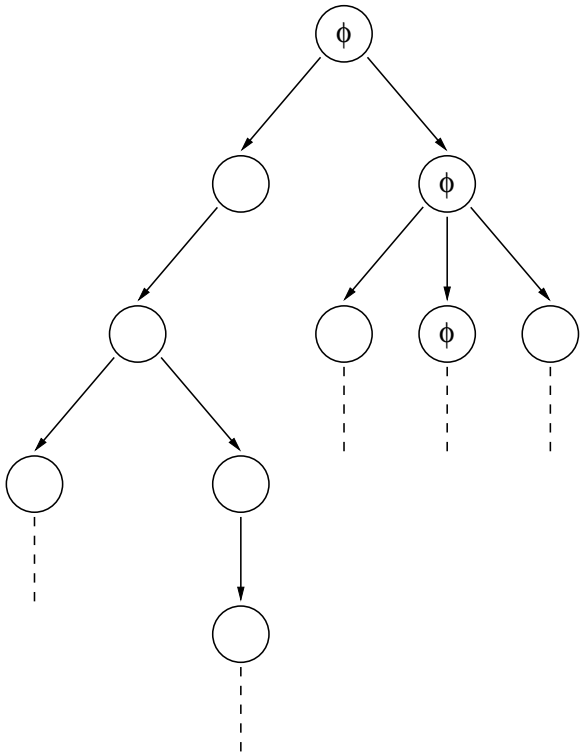
CTL: Semántica

- La satisfacibilidad de una fórmula CTL ϕ en un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ a partir de un estado $\mathbf{s} \in \mathbf{S}$, $\mathcal{M}, \mathbf{s} \models \phi$, se define como sigue:
  - $\mathcal{M}, \mathbf{s} \models \mathbf{AG}\ \phi$ si y sólo si para todo $\mathbf{s'}$ en cualquier camino que comience en $\mathbf{s}$ se tiene $\mathcal{M}, \mathbf{s'} \models \phi$



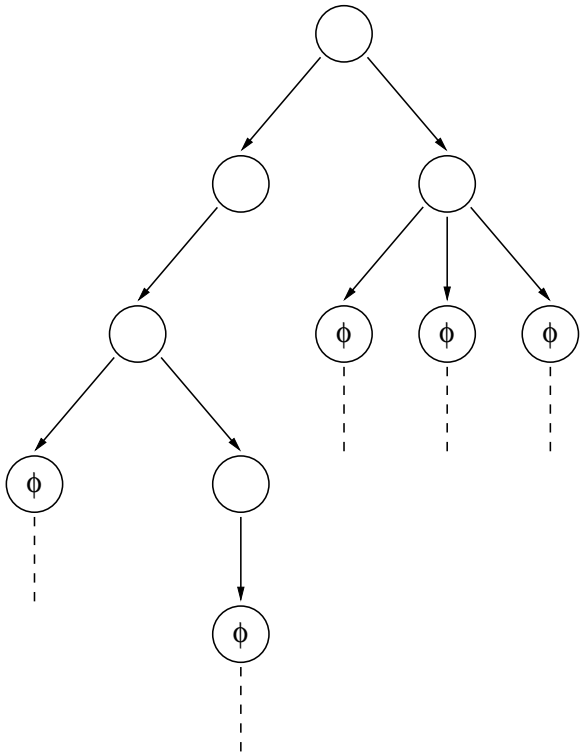
CTL: Semántica

- La satisfacibilidad de una fórmula CTL ϕ en un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ a partir de un estado $\mathbf{s} \in \mathbf{S}$, $\mathcal{M}, \mathbf{s} \models \phi$, se define como sigue:
  - $\mathcal{M}, \mathbf{s} \models \mathbf{EG}\ \phi$ si y sólo si existe un camino que comienza en $\mathbf{s}$ en el que todos los elementos $\mathbf{s'}$ cumplen $\mathcal{M}, \mathbf{s'} \models \phi$



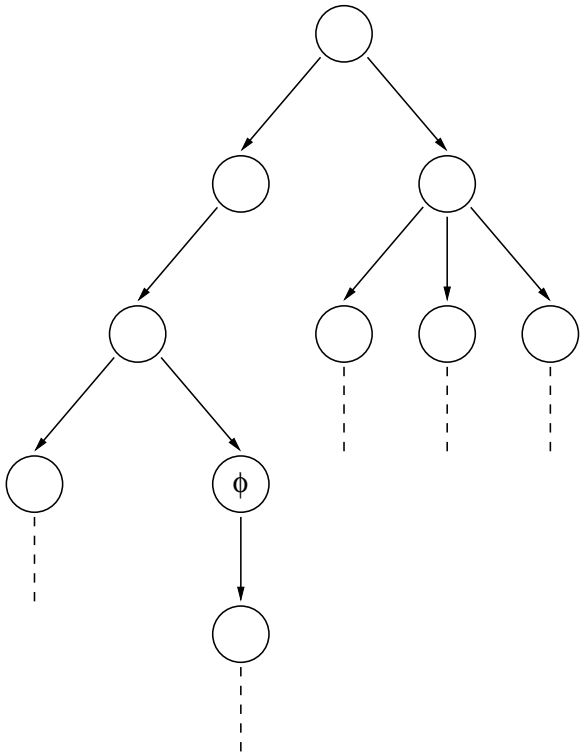
CTL: Semántica

- La satisfacibilidad de una fórmula CTL ϕ en un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ a partir de un estado $\mathbf{s} \in \mathbf{S}$, $\mathcal{M}, \mathbf{s} \models \phi$, se define como sigue:
  - $\mathcal{M}, \mathbf{s} \models \mathbf{AF}\ \phi$ si y sólo si existe $\mathbf{s'}$ en cualquier camino que comienze en $\mathbf{s}$ que cumple $\mathcal{M}, \mathbf{s'} \models \phi$



CTL: Semántica

- La satisfacibilidad de una fórmula CTL ϕ en un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ a partir de un estado $\mathbf{s} \in \mathbf{S}$, $\mathcal{M}, \mathbf{s} \models \phi$, se define como sigue:
  - $\mathcal{M}, \mathbf{s} \models \mathbf{EF}\ \phi$ si y sólo si existe un camino que comienza en $\mathbf{s}$ en el que hay un elemento $\mathbf{s'}$ que cumple $\mathcal{M}, \mathbf{s'} \models \phi$

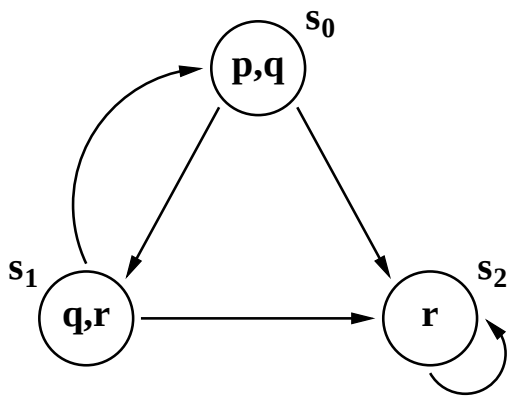


CTL: Semántica

- La satisfacibilidad de una fórmula CTL ϕ en un modelo $\mathcal{M} = (\mathbf{S}, \rightarrow_{\mathcal{M}}, \mathbf{L})$ a partir de un estado $\mathbf{s} \in \mathbf{S}$, $\mathcal{M}, \mathbf{s} \models \phi$, se define como sigue:
  - $\mathcal{M}, \mathbf{s} \models \mathbf{A}[\phi \mathbf{U} \psi]$ si y sólo si todos los caminos que comienzan en $\mathbf{s}$ se cumple la propiedad ϕ hasta que se alcanza un estado en el que se cumple ψ
  - $\mathcal{M}, \mathbf{s} \models \mathbf{E}[\phi \mathbf{U} \psi]$ si y sólo si en algún camino que comienza en $\mathbf{s}$ se cumple la propiedad ϕ hasta que se alcanza un estado en el que se cumple ψ

CTL: Semántica

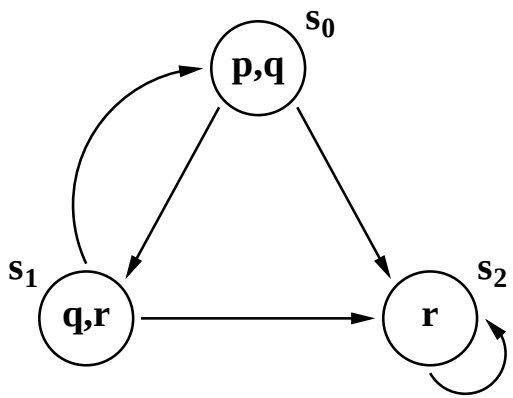
- Consideremos el modelo $\mathcal{M}$ representado por el siguiente sistema de transición



- Se verifican
  - $\mathcal{M}, s_0 \models \mathbf{p} \wedge \mathbf{q}$
  - $\mathcal{M}, s_0 \models \neg \mathbf{r}$
  - $\mathcal{M}, s_0 \models \top$
  - $\mathcal{M}, s_0 \models \mathbf{EX}\ (\mathbf{q} \wedge \mathbf{r})$

CTL: Semántica

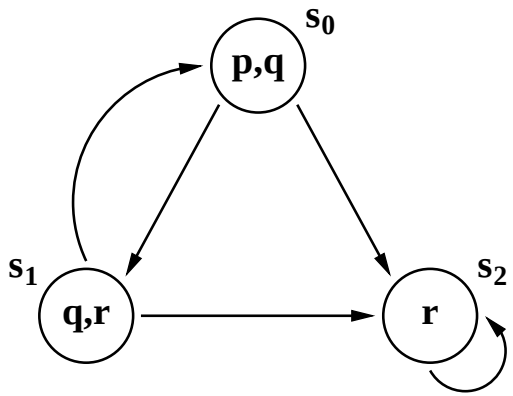
- Consideremos el modelo $\mathcal{M}$ representado por el siguiente sistema de transición



- Se verifican
  - $\mathcal{M}, s_0 \models \neg \mathbf{AX}\ (q \wedge r)$
  - $\mathcal{M}, s_0 \models \neg \mathbf{EF}\ (p \wedge r)$
  - $\mathcal{M}, s_2 \models \mathbf{EG}\ r$
  - $\mathcal{M}, s_0 \models \mathbf{AF}\ r$

CTL: Semántica

- Consideremos el modelo $\mathcal{M}$ representado por el siguiente sistema de transición



- Se verifican
  - $\mathcal{M}, \mathbf{s_0} \models \mathbf{E[(p \wedge q)Ur]}$
  - $\mathcal{M}, \mathbf{s_0} \models \mathbf{A[pUr]}$
  - $\mathcal{M}, \mathbf{s_0} \models \mathbf{AG\ (p \vee q \vee r \rightarrow EF\ EG\ r)}$

CTL: Semántica

- Decimos que dos fórmulas son equivalentes, $\phi \equiv \psi$ si y sólo si para todo modelo $\mathcal{M}$ y para todo estado $\mathbf{s}$ se tiene que $\mathcal{M}, \mathbf{s} \models \phi$ si y sólo si $\mathcal{M}, \mathbf{s} \models \psi$
- Relaciones entre las conectivas
  - $\neg \mathbf{AF}\ \phi \equiv \mathbf{EG}\ \neg\phi$
  - $\neg \mathbf{EF}\ \phi \equiv \mathbf{AG}\ \neg\phi$
  - $\neg \mathbf{AX}\ \phi \equiv \mathbf{EX}\ \neg\phi$
  - $\mathbf{AF}\ \phi \equiv \mathbf{A}[\top \mathbf{U} \phi]$
  - $\mathbf{EF}\ \phi \equiv \mathbf{E}[\top \mathbf{U} \phi]$

Patrones de especificación

- (Liveness) *Si se realiza alguna petición, entonces es finalmente atendida*: **AG (peticion → AF atendida)**
- (Deadlock) *Ocurra lo que ocurra, el proceso terminará quedando permanentemente inactivo*: **AF AG ¬activo**
- (Fairness) *En cualquier situación el proceso se activará una cantidad infinita de veces*: **AG AF activo**
- (Fairness) *Si un proceso queda activo una cantidad infinita de veces entonces es ejecutado una cantidad infinita de veces*: **AG AF activo → AG AF ejecucion**

Patrones de especificación

- (Safety) *Es imposible alcanzar una situación en la que el proceso esté ejecutandose y no esté activo*:
  AG $\neg$**(ejecucion** $\wedge$ $\neg$**activo)**
- (Reachability) *Es posible alcanzar un estado en el que hay una petición y el proceso está inactivo*: **EF (peticion** $\wedge$ $\neg$**activo)**
- (Reachability) *En cualquier situación es posible alcanzar un estado en el que el proceso está activo*: **AG EF activo**

Bibliografía

- Huth, M. and Ryan, M. *Logic in Computer Science: Modelling and Reasoning about Systems*. (Cambridge University Press, 2004)