Teoría de modelos finitos: Motivación

IIC3263

Poder expresivo de una lógica: Caso finito

En este curso nos vamos a concentrar (mayormente) en las estructuras finitas.

- Estructuras que tienen dominio finito

Poder expresivo de una lógica: Caso finito

En este curso nos vamos a concentrar (mayormente) en las estructuras finitas.

- Estructuras que tienen dominio finito

Notación

Dado un vocabulario $\mathcal{L}$, $\textsc{Struct}[\mathcal{L}]$ es el conjunto de todas las $\mathcal{L}$-estructuras finitas.

Poder expresivo de una lógica: Caso finito

Una propiedad $\mathcal{P}$ de las $\mathcal{L}$-estructuras finitas es un subconjunto de $\textsc{Struct}[\mathcal{L}]$.

Ejemplo

El conjunto de las $\mathcal{L}$-estructuras finitas con dos elementos en el dominio.

Poder expresivo de una lógica: Caso finito

Una propiedad $\mathcal{P}$ de las $\mathcal{L}$-estructuras finitas es un subconjunto de $\textsc{Struct}[\mathcal{L}]$.

Ejemplo

El conjunto de las $\mathcal{L}$-estructuras finitas con dos elementos en el dominio.

Decimos que una propiedad $\mathcal{P}$ es expresable en lógica de primer orden si existe una $\mathcal{L}$-oración φ tal que para toda $\mathfrak{A} \in \textsc{Struct}[\mathcal{L}]$:

$$\mathfrak{A} \in \mathcal{P} \quad \text{si y sólo si} \quad \mathfrak{A} \models \varphi$$

Poder expresivo de una lógica: Caso finito

Una propiedad $\mathcal{P}$ de las $\mathcal{L}$-estructuras finitas es un subconjunto de $\textsc{Struct}[\mathcal{L}]$.

Ejemplo

El conjunto de las $\mathcal{L}$-estructuras finitas con dos elementos en el dominio.

Decimos que una propiedad $\mathcal{P}$ es expresable en lógica de primer orden si existe una $\mathcal{L}$-oración φ tal que para toda $\mathfrak{A} \in \textsc{Struct}[\mathcal{L}]$:

$$\mathfrak{A} \in \mathcal{P} \quad \text{si y sólo si} \quad \mathfrak{A} \models \varphi$$

Importante

Siempre vamos a poder identificar por el contexto si estamos hablando de definibilidad sobre todas las estructuras o en el caso de las estructuras finitas.

Teorema de compacidad: Caso finito

Sea $\mathcal{L} = \{E(\cdot,\cdot), a, b\}$ y $\mathcal{P}$ el conjunto de todas las $\mathcal{L}$-estructuras finitas que tienen un camino entre a y b.

Usando el teorema de compacidad, demostramos que $\mathcal{P}$ no es expresable en primer orden si consideramos estructuras tanto finitas como infinitas.

- ¿Es la demostración válida para el caso finito?
- ¿Cómo debería ser enunciado el teorema de compacidad para que la demostración fuera válida? ¿Es esta versión del teorema cierta?

Teorema de compacidad: Caso finito

Notación

Un conjunto Σ de oraciones tiene un modelo finito si existe una estructura finita que satisface Σ.

Versión "finita" del teorema de compacidad: Si cada subconjunto finito de Σ tiene un modelo finito, entonces Σ tiene un modelo finito.

- ¿Es esta versión cierta?

Teorema de compacidad: Caso finito

Vamos a demostrar que la versión finita del teorema de compacidad no es cierta. Sean:

$$\begin{aligned} \lambda_k &= \exists x_1 \ldots \exists x_k \left(\bigwedge_{1 \leq i < j \leq k} \neg (x_i = x_j) \right) \\ \Sigma &= \{\lambda_k \mid k \geq 2\} \end{aligned}$$

Teorema de compacidad: Caso finito

Vamos a demostrar que la versión finita del teorema de compacidad no es cierta. Sean:

$$\begin{aligned} \lambda_k &= \exists x_1 \ldots \exists x_k \left(\bigwedge_{1 \leq i < j \leq k} \neg(x_i = x_j) \right) \\ \Sigma &= \{\lambda_k \mid k \geq 2\} \end{aligned}$$

Cada subconjunto finito de Σ tiene un modelo finito, pero Σ no tiene un modelo finito.

El caso finito ...

Para estudiar el caso de los modelos finito, necesitamos herramientas nuevas.

Pero antes de desarrollar esta herramientas, hay que responder una pregunta natural: **¿Por qué nos interesa tanto el caso finito?**

- Veamos dos aplicaciones: Bases de datos y verificación formal de software

Más adelante en el curso vamos a ver otras aplicaciones.

Primera aplicación: Bases de datos

Tabla *Vuelo* almacena información sobre vuelos directos:

Partida	Llegada
Santiago	Toronto
Santiago	Lima
Lima	Los Angeles
Lima	Toronto
Lima	Santiago
Toronto	Los Angeles

Primera aplicación: Bases de datos

¿Qué lenguaje usamos para consultar bases de datos?

- Lenguaje estándar: Algebra relacional

Algebra relacional tiene operadores: selección (σ), proyección (π), join ($\bowtie$), unión ($\cup$) y diferencia ($-$).

Primera aplicación: Bases de datos

¿Qué lenguaje usamos para consultar bases de datos?

- Lenguaje estándar: Algebra relacional

Algebra relacional tiene operadores: selección (σ), proyección (π), join ($\bowtie$), unión ($\cup$) y diferencia ($-$).

¿Por qué se utiliza el álgebra relacional como lenguaje de consulta?

Primera aplicación: Bases de datos

¿Qué lenguaje usamos para consultar bases de datos?

- Lenguaje estándar: Algebra relacional

Algebra relacional tiene operadores: selección (σ), proyección (π), join ($\bowtie$), unión ($\cup$) y diferencia ($-$).

¿Por qué se utiliza el álgebra relacional como lenguaje de consulta?

- Es un lenguaje fácil de optimizar

Primera aplicación: Bases de datos

¿Cómo podemos estudiar el poder expresivo del álgebra relacional?

- ¿Por qué necesitamos estudiar esto?

Primera aplicación: Bases de datos

¿Cómo podemos estudiar el poder expresivo del álgebra relacional?

- ¿Por qué necesitamos estudiar esto?

Un resultado fundamental (Codd)

Algebra relacional y lógica de primer orden tienen el mismo poder expresivo.

Bases de datos y lógica de primer orden

1. ¿Hay un vuelo directo entre Santiago y Lima?

Bases de datos y lógica de primer orden

1. ¿Hay un vuelo directo entre Santiago y Lima?

$$\mathit{Vuelo}(\text{Santiago}, \text{Lima})$$

Bases de datos y lógica de primer orden

1. ¿Hay un vuelo directo entre Santiago y Lima?

$$\mathit{Vuelo}(\text{Santiago}, \text{Lima})$$

2. ¿Cuál es la lista de ciudades a las que se puede llegar sin escala desde Santiago?

Bases de datos y lógica de primer orden

1. ¿Hay un vuelo directo entre Santiago y Lima?

$$Vuelo(\text{Santiago}, \text{Lima})$$

2. ¿Cuál es la lista de ciudades a las que se puede llegar sin escala desde Santiago?

$$Vuelo(\text{Santiago}, x)$$

Bases de datos y lógica de primer orden

1. ¿Hay un vuelo directo entre Santiago y Lima?

$$Vuelo(\text{Santiago}, \text{Lima})$$

2. ¿Cuál es la lista de ciudades a las que se puede llegar sin escala desde Santiago?

$$Vuelo(\text{Santiago}, x)$$

3. ¿Hay un vuelo con escala entre Santiago y Los Angeles?

Bases de datos y lógica de primer orden

1. ¿Hay un vuelo directo entre Santiago y Lima?

$$Vuelo(\text{Santiago}, \text{Lima})$$

2. ¿Cuál es la lista de ciudades a las que se puede llegar sin escala desde Santiago?

$$Vuelo(\text{Santiago}, x)$$

3. ¿Hay un vuelo con escala entre Santiago y Los Angeles?

$$\exists x \, (Vuelo(\text{Santiago}, x) \wedge Vuelo(x, \text{Los Angeles}))$$

Bases de datos y lógica de primer orden

4. ¿Cuál es la lista de ciudades a las que se puede llegar con dos escalas desde Santiago?

Bases de datos y lógica de primer orden

4. ¿Cuál es la lista de ciudades a las que se puede llegar con dos escalas desde Santiago?

$$\exists y \exists z \, (\mathit{Vuelo}(\text{Santiago}, y) \wedge \mathit{Vuelo}(y, z) \wedge \mathit{Vuelo}(z, x)).$$

Bases de datos y lógica de primer orden

4. ¿Cuál es la lista de ciudades a las que se puede llegar con dos escalas desde Santiago?

$$\exists y \exists z \, (\mathit{Vuelo}(\text{Santiago}, y) \wedge \mathit{Vuelo}(y, z) \wedge \mathit{Vuelo}(z, x)).$$

5. **¿Cuál es la lista de ciudades a las que se puede llegar desde Santiago?**

Bases de datos y lógica de primer orden

4. ¿Cuál es la lista de ciudades a las que se puede llegar con dos escalas desde Santiago?

$$\exists y \exists z \, (\mathit{Vuelo}(\text{Santiago}, y) \wedge \mathit{Vuelo}(y, z) \wedge \mathit{Vuelo}(z, x)).$$

5. **¿Cuál es la lista de ciudades a las que se puede llegar desde Santiago?**

   Necesitamos recursión.

Bases de datos y lógica de primer orden

4. ¿Cuál es la lista de ciudades a las que se puede llegar con dos escalas desde Santiago?

$$\exists y \exists z \, (\mathit{Vuelo}(\text{Santiago}, y) \wedge \mathit{Vuelo}(y, z) \wedge \mathit{Vuelo}(z, x)).$$

5. **¿Cuál es la lista de ciudades a las que se puede llegar desde Santiago?**

   Necesitamos recursión.

6. **¿Hay más vuelos desde Santiago que desde Lima?**

Bases de datos y lógica de primer orden

4. ¿Cuál es la lista de ciudades a las que se puede llegar con dos escalas desde Santiago?

$$\exists y \exists z \, (\mathit{Vuelo}(\text{Santiago}, y) \wedge \mathit{Vuelo}(y, z) \wedge \mathit{Vuelo}(z, x)).$$

5. **¿Cuál es la lista de ciudades a las que se puede llegar desde Santiago?**

   Necesitamos recursión.

6. **¿Hay más vuelos desde Santiago que desde Lima?**

   Necesitamos la habilidad de contar.

Bases de datos: Problemas a resolver

- ¿Podemos demostrar que la lógica de primer orden no tiene recursión?
- ¿Podemos demostrar que la lógica de primer orden no puede contar?
- ¿Cómo podemos agregar estas habilidades a la lógica de primer orden?

Bases de datos: Problemas a resolver

- ¿Son estas dos habilidades independientes?
  - ¿Si tenemos una lógica con recursión podemos contar?
  - ¿Si tenemos una lógica con la habilidad de contar entonces tenemos recursión?

Bases de datos: Problemas a resolver

- ¿Son estas dos habilidades independientes?
  - ¿Si tenemos una lógica con recursión podemos contar?
  - ¿Si tenemos una lógica con la habilidad de contar entonces tenemos recursión?

Queremos desarrollar herramientas que nos permitan solucionar estos problemas ...

Segunda aplicación: Verificación formal de software

Ejemplo

Queremos verificar si funciona correctamente el software diseñado para manejar un semáforo.

- El semáforo tiene tres estados: R (rojo), A (amarillo) y V (verde), que indican cuál es el color que ven los automovilistas.
- El semáforo además tiene un botón que permite a los peatones ponerlo en rojo.

Segunda aplicación: Verificación formal de software

Ejemplo

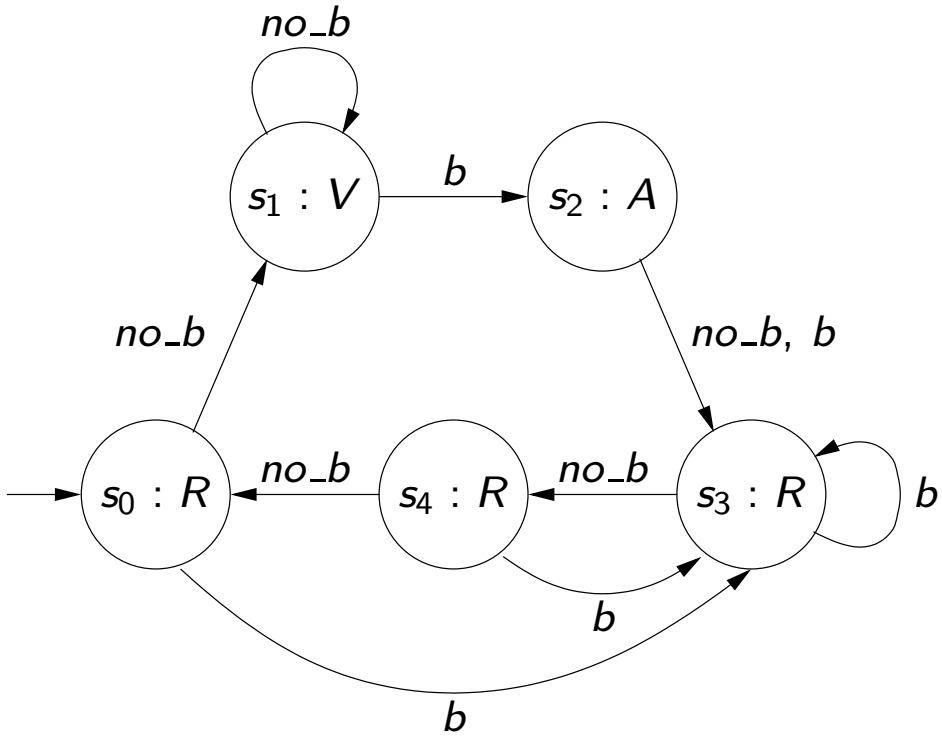
Queremos verificar si funciona correctamente el software diseñado para manejar un semáforo.

- El semáforo tiene tres estados: R (rojo), A (amarillo) y V (verde), que indican cuál es el color que ven los automovilistas.
- El semáforo además tiene un botón que permite a los peatones ponerlo en rojo.

Para analizar un programa, generalmente se utiliza alguna herramienta que permite *abstraer* el funcionamiento del código.

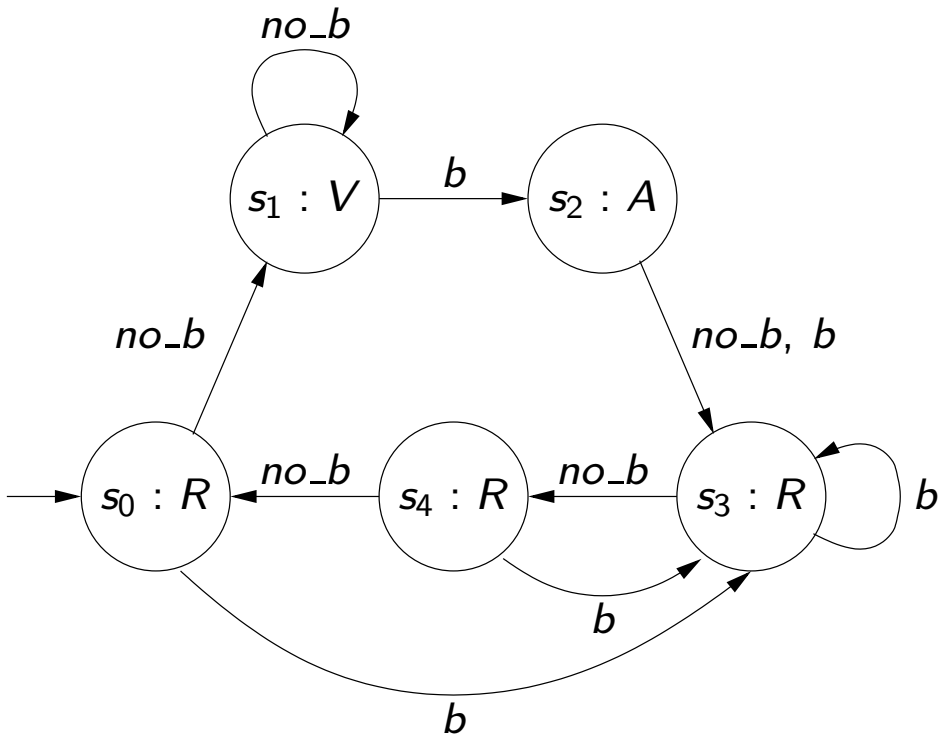
Verificación formal de software

Ejemplo (especificación del semáforo)



Verificación formal de software

Ejemplo (especificación del semáforo)



Representamos el comportamiento del programa como un autómata con etiquetas en los nodos.

Verificación formal de software

¿Cómo podemos verificar si un programa funciona bien?

Verificación formal de software

¿Cómo podemos verificar si un programa funciona bien?

El significado de *funcionar bien* es dado por el usuario.

- El usuario debe indicar cuáles son las propiedades que el programa debería satisfacer.

Verificación formal de software

¿Cómo podemos verificar si un programa funciona bien?

El significado de *funcionar bien* es dado por el usuario.

- El usuario debe indicar cuáles son las propiedades que el programa debería satisfacer.
- La satisfacción de estas propiedades debería ser verificada de manera automática.

Verificación formal de software

¿Cómo podemos verificar si un programa funciona bien?

El significado de *funcionar bien* es dado por el usuario.

- El usuario debe indicar cuáles son las propiedades que el programa debería satisfacer.
- La satisfacción de estas propiedades debería ser verificada de manera automática.

Necesitamos un lenguaje para poder expresar propiedades de programas (o de sus versiones abstractas).

Verificación formal de software: Lógica temporal

Para expresar propiedades de programas se utiliza lógica temporal.

- Linear Temporal Logic (LTL)

Verificación formal de software: Lógica temporal

Para expresar propiedades de programas se utiliza lógica temporal.

- Linear Temporal Logic (LTL)

φ es una fórmula en LTL sobre un alfabeto Γ si:

- $\varphi = a$ y $a \in \Gamma$.
- $\varphi = (\neg\psi)$ y ψ es una fórmula en LTL.
- $\varphi = (\psi \star \theta)$, $\star \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$ y ψ, θ son fórmulas en LTL.
- $\varphi = (\mathbf{X}\,\psi)$ y ψ es una fórmula en LTL.
- $\varphi = (\psi\,\mathbf{U}\,\theta)$ y ψ, θ son fórmulas en LTL.

LTL: Semántica

X y **U** son conectivos temporales:

- $\mathbf{X}\,\varphi$: En el siguiente estado se cumple φ
- $\varphi\,\mathbf{U}\,\psi$: φ se cumple hasta que se cumple ψ

LTL: Semántica

X y **U** son conectivos temporales:

- $\mathbf{X}\,\varphi$: En el siguiente estado se cumple φ
- $\varphi\,\mathbf{U}\,\psi$: φ se cumple hasta que se cumple ψ

Para definir la semántica de LTL tenemos que hablar de caminos.

LTL: Semántica

X y **U** son conectivos temporales:

- $\mathbf{X}\,\varphi$: En el siguiente estado se cumple φ
- $\varphi\,\mathbf{U}\,\psi$: φ se cumple hasta que se cumple ψ

Para definir la semántica de LTL tenemos que hablar de caminos.

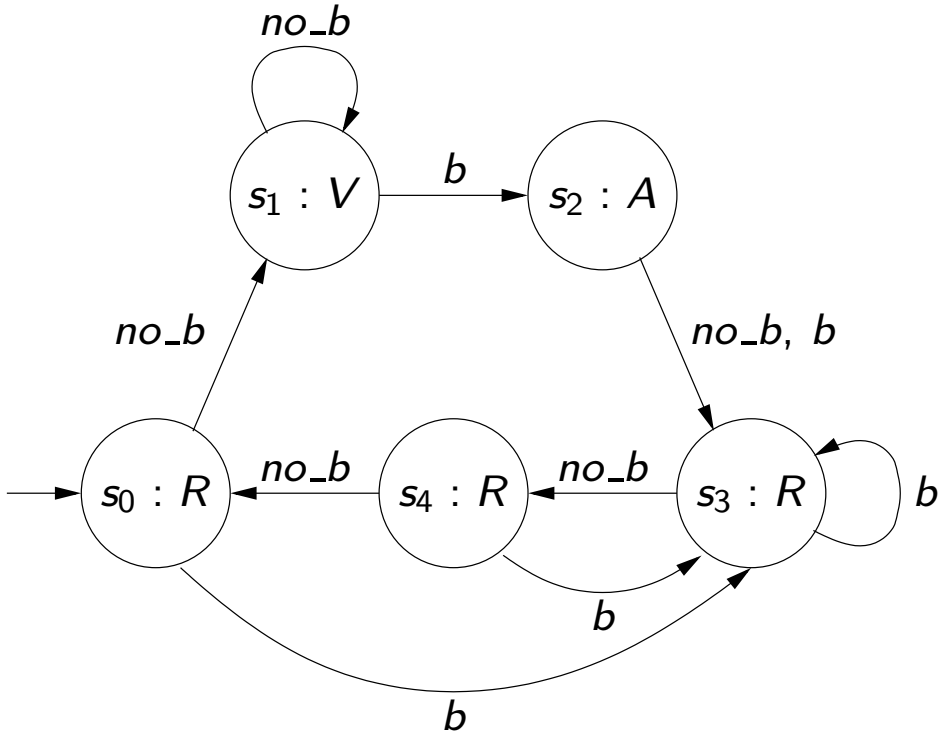
Notación

Una secuencia infinita $\pi = q_1 q_2 q_3 \cdots$ *es un camino en un autómata* $\mathcal{A}$ *si para cada* $i \geq 1$*:*

- q_i *es un estado de* $\mathcal{A}$*,*
- *existe un arco en* $\mathcal{A}$ *de* q_i *a* q_{i+1}*.*

LTL: Caminos

Ejemplo

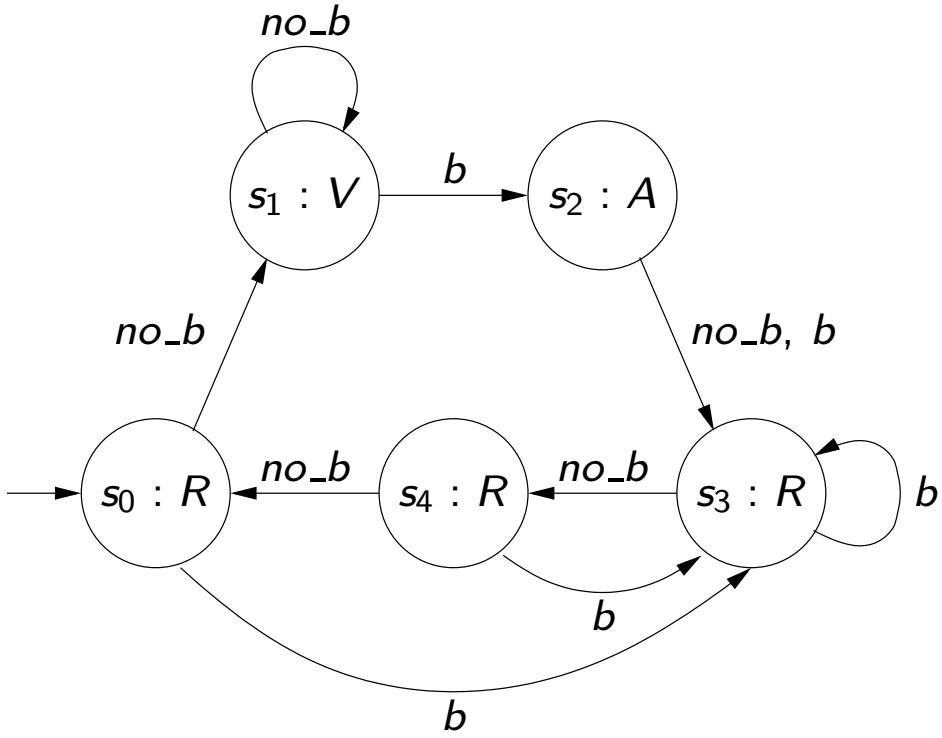


Aquí son caminos:

$s_0 s_1 \cdots s_1 \cdots$ $\quad$ $s_1 \cdots s_1 \cdots$ $\quad$ $s_0 s_1 s_2 s_3 s_4 s_0 s_1 s_2 s_3 s_4 \cdots$

LTL: Caminos

Ejemplo



Aquí son caminos:

$s_0 s_1 \cdots s_1 \cdots$ $s_1 \cdots s_1 \cdots$ $s_0 s_1 s_2 s_3 s_4 s_0 s_1 s_2 s_3 s_4 \cdots$

¿Qué ejecuciones representan estos caminos?

LTL: Semántica

Dada una fórmula LTL φ, un autómata $\mathcal{A}$ y un camino $\pi = q_1 q_2 q_3 \cdots$ en $\mathcal{A}$:

- φ se evalúa en una posición $i \geq 1$ de π

LTL: Semántica

Dada una fórmula LTL φ, un autómata $\mathcal{A}$ y un camino $\pi = q_1 q_2 q_3 \cdots$ en $\mathcal{A}$:

- φ se evalúa en una posición $i \geq 1$ de π

Definición (Semántica de LTL)

Decimos que φ es satisfecha en la posición i de π, denotado como $\pi, i \models \varphi$, si:

- $\varphi = a$ *y la etiqueta de* q_i *en* $\mathcal{A}$ *es* a.
- $\varphi = (\neg\psi)$ *y no es verdad que* $\pi, i \models \psi$.
- $\varphi = (\psi \wedge \theta)$, $\pi, i \models \psi$ *y* $\pi, i \models \theta$.

LTL: Semántica

Dada una fórmula LTL φ, un autómata $\mathcal{A}$ y un camino $\pi = q_1 q_2 q_3 \cdots$ en $\mathcal{A}$:

- φ se evalúa en una posición $i \geq 1$ de π

Definición (Semántica de LTL)

Decimos que φ es satisfecha en la posición i de π, denotado como $\pi, i \models \varphi$, si:

- $\varphi = a$ *y la etiqueta de* q_i *en* $\mathcal{A}$ *es* a.
- $\varphi = (\neg\psi)$ *y no es verdad que* $\pi, i \models \psi$.
- $\varphi = (\psi \wedge \theta)$, $\pi, i \models \psi$ *y* $\pi, i \models \theta$.
- $\varphi = (\mathbf{X}\,\psi)$ *y* $\pi, i+1 \models \psi$.

LTL: Semántica

Dada una fórmula LTL φ, un autómata $\mathcal{A}$ y un camino $\pi = q_1 q_2 q_3 \cdots$ en $\mathcal{A}$:

- φ se evalúa en una posición $i \geq 1$ de π

Definición (Semántica de LTL)

Decimos que φ es satisfecha en la posición i de π, denotado como $\pi, i \models \varphi$, si:

- $\varphi = a$ *y la etiqueta de* q_i *en* $\mathcal{A}$ *es* a.
- $\varphi = (\neg\psi)$ *y no es verdad que* $\pi, i \models \psi$.
- $\varphi = (\psi \wedge \theta)$, $\pi, i \models \psi$ *y* $\pi, i \models \theta$.
- $\varphi = (\mathbf{X}\,\psi)$ *y* $\pi, i+1 \models \psi$.
- $\varphi = (\psi\,\mathbf{U}\,\theta)$ *y existe* $k \geq i$ *tal que* $\pi, k \models \theta$ *y para todo* $i \leq j < k$ *se tiene que* $\pi, j \models \psi$.

LTL: Ejemplos

Sea $\pi = s_0 s_1 \cdots s_1 \cdots$ un camino para el autómata del semáforo.

1. ¿Cuáles de las siguientes afirmaciones son ciertas?

$$\begin{aligned} \pi, 1 &\models V \\ \pi, 1 &\models R \\ \pi, 1 &\models \mathbf{X}\, V \\ \pi, 2 &\models R \\ \pi, 2 &\models \mathbf{X}\, \mathbf{X}\, \neg V \end{aligned}$$

2. Sea $\top$ una tautología cualquiera (por ejemplo $A \vee \neg A$). ¿Es cierto que $\pi, 1 \models \top\, \mathbf{U}\, R$?

LTL: Otros conectivos temporales

Vamos a definir otros conectivos temporales usados en la práctica.

LTL: Otros conectivos temporales

Vamos a definir otros conectivos temporales usados en la práctica.

Notación

$$\begin{aligned} \mathbf{F}\,\varphi &= \top\,\mathbf{U}\,\varphi, \\ \mathbf{G}\,\varphi &= \neg(\top\,\mathbf{U}\,(\neg\varphi)). \end{aligned}$$

¿Cuál es el significado de estos conectivos?

LTL y el problema de verificación

Problema de verificación

Dada una fórmula LTL φ y un autómata $\mathcal{A}$:

- Verificar que para todos los caminos π que comienzan en el estado inicial del autómata se tiene que $\pi, 1 \models \varphi$.

LTL y el problema de verificación

Problema de verificación

Dada una fórmula LTL φ y un autómata $\mathcal{A}$:

- Verificar que para todos los caminos π que comienzan en el estado inicial del autómata se tiene que $\pi, 1 \models \varphi$.

¿Cuáles son las propiedades que queremos verificar en el caso del semáforo?

LTL y el problema de verificación

Ejemplo (verificación del funcionamiento del semáforo)

Nos gustaría verificar que si el semáforo está en rojo, entonces en algún momento en el futuro va a estar en verde.

- ¿Cómo se expresa está propiedad en LTL?

LTL y el problema de verificación

Ejemplo (verificación del funcionamiento del semáforo)

Nos gustaría verificar que si el semáforo está en rojo, entonces en algún momento en el futuro va a estar en verde.

- ¿Cómo se expresa está propiedad en LTL?

$$\varphi \quad = \quad \mathbf{G}\,(R \rightarrow \mathbf{F}\,V)$$

LTL y el problema de verificación

Ejemplo (verificación del funcionamiento del semáforo)

Nos gustaría verificar que si el semáforo está en rojo, entonces en algún momento en el futuro va a estar en verde.

- ¿Cómo se expresa está propiedad en LTL?

$$\varphi \quad = \quad \mathbf{G}\,(R \rightarrow \mathbf{F}\,V)$$

¿Por qué no usamos $R \rightarrow \mathbf{F}\,V$?

LTL y el problema de verificación

Ejemplo (verificación del funcionamiento del semáforo)

Nos gustaría verificar que si el semáforo está en rojo, entonces en algún momento en el futuro va a estar en verde.

- ¿Cómo se expresa está propiedad en LTL?

$$\varphi \quad = \quad \mathbf{G}\,(R \rightarrow \mathbf{F}\,V)$$

¿Por qué no usamos $R \rightarrow \mathbf{F}\,V$?

- ¿Es cierto que $\pi, 1 \models \varphi$ para todo camino π que comienza en el estado inicial del autómata del semáforo?

Verificación: Problemas a resolver

¿Cuál es la complejidad de resolver el problema de verificación para LTL? ¿Es decidible este problema?

- ¿Existen otras lógicas para las cuales la complejidad de este problema sea menor?

¿Cuál es el poder expresivo de LTL?

- ¿Hay mejores lógicas en términos de poder expresivo?

Verificación: Problemas a resolver

¿Cuál es la complejidad de resolver el problema de verificación para LTL? ¿Es decidible este problema?

- ¿Existen otras lógicas para las cuales la complejidad de este problema sea menor?

¿Cuál es el poder expresivo de LTL?

- ¿Hay mejores lógicas en términos de poder expresivo?

Queremos desarrollar herramientas que nos permitan responder este tipo de consultas ...