

Lógicas Modales

Usos de Bisimulaciones

Carlos Areces & Raul Fervari

1er Cuatrimestre 2017,
Córdoba, Argentina

Temario

- ▶ Propiedad de *tree model*.
- ▶ *n*-bisimulación.
- ▶ Propiedad de modelo finito vía selección.
- ▶ Propiedad de modelo finito vía filtraciones.

Bibliografía

- ▶ Capítulo 2 y apéndice A del Modal Logic Book (Blackburn, Venema & de Rijke)

Propiedad de modelo finito

Los resultados de invariancia pueden verse en forma negativa o positiva:

- ▶ (-): Nos hablan de los límites de la expresividad de los lenguajes modales.
- ▶ (+): Son una herramienta para transformar modelos en otros, modificando propiedades estructurales sin afectar la satisfacibilidad.

Propiedad de modelo finito

Vamos a probar que el lenguaje modal básico tiene la propiedad de *modelo finito*: Si una fórmula es satisfecha en un modelo arbitrario, entonces es satisfacible en un modelo finito.

- **Propiedad de modelo finito.** Sea C una clase de modelos. Decimos que un lenguaje tiene la propiedad de modelo finito con respecto a C si vale lo siguiente: Si φ es una fórmula del lenguaje que es satisfacible en un modelo de C , entonces φ es satisfecha en un modelo finito de C .

Por ahora nos vamos a preocupar sólo por el caso en el que C es la clase de *todos* los modelos de la lógica modal básica.

Propiedad de modelo finito

De nuevo podemos ver este resultado desde dos perspectivas:

- (-): El lenguaje modal básico carece del poder expresivo suficiente para forzar la existencia de modelos infinitos.
- (+): No tenemos que preocuparnos por modelos infinitos arbitrarios, porque siempre vamos a poder encontrar uno finito equivalente. Más adelante, esto nos va a permitir probar resultados de decidibilidad.

En particular, vamos a probar esta propiedad a través de un procedimiento llamado *de selección*.

Propiedad de modelo finito

Podemos empezar con la siguiente pregunta: ¿Cuánto del modelo ve una fórmula modal desde el estado actual?

- Intuitivamente, depende de cuál es el anidamiento de modalidades que la fórmula contiene.

El *grado* de una fórmula está definido de la siguiente manera:

$$\begin{aligned} \deg(p) &= 0 \\ \deg(\neg\varphi) &= \deg(\varphi) \\ \deg(\varphi \wedge \psi) &= \max\{\deg(\varphi), \deg(\psi)\} \\ \deg(\Diamond\varphi) &= 1 + \deg(\varphi) \end{aligned}$$

Propiedad de modelo finito

Veamos primero la siguiente propiedad.

Prop 1: Sea un lenguaje con una signatura finita (esto es, finitos símbolos proposicionales y modalidades).

- I. Para todo n , sólo hay un conjunto finito de fórmulas de grado a lo sumo n que no son lógicamente equivalentes.
- II. Para todo n , modelo \mathcal{M} y estado w de \mathcal{M} , el conjunto de todas las fórmulas de grado a lo sumo n que son satisfechas en w es equivalente a una sola fórmula.

Demostración: i) Por inducción en n . ii) Es inmediato de i).

Propiedad de modelo finito

Veamos también que hay una manera de aproximarnos en forma finita a la noción de bisimulación. Esto nos va a servir más adelante para buscar un modelo finito.

n -bisimulación: Sean dos modelos \mathcal{M} y \mathcal{M}' , y w y w' dos mundos de \mathcal{M} y \mathcal{M}' respectivamente. Decimos que w y w' son n -bisimilares (notación $w \leftrightarrow_n w'$) si existe una secuencia de relaciones binarias $Z_n \subseteq \dots \subseteq Z_0$ con las siguientes propiedades (con $i + 1 \leq n$):

- I. $w Z_n w'$
- II. Si $v Z_0 v'$ entonces v y v' acuerdan en todas las proposiciones.
- III. Si $v Z_{i+1} v'$ y Rvu , entonces existe u' con $R'v'u'$ y $u Z_i u'$
- IV. Si $v Z_{i+1} v'$ y $R'v'u'$, entonces existe u con Rvu y $u Z_i u'$

Propiedad de modelo finito

La intuición nos dice que:

- ▶ Si $w \leftrightarrow_n w'$ entonces w y w' son bisimilares hasta el nivel n .
- ▶ Si $w \leftrightarrow w'$ entonces $w \leftrightarrow_n w'$ para todo n .
- ▶ Pero la vuelta no vale (ejercicio: Pensar un **contraejemplo**).

Propiedad de modelo finito

Vamos a ver ahora que con lenguajes de signatura finita, hay una coincidencia exacta entre equivalencia modal y n -bisimilaridad para todo n .

Prop 2: Sea un lenguaje con una signatura finita, y dos modelos \mathcal{M} y \mathcal{M}' de este lenguaje. Entonces, para todo w de \mathcal{M} y w' de \mathcal{M}' los siguientes puntos son equivalentes:

- I. $w \leftrightarrow_n w'$
- II. w y w' acuerdan en todas las fórmulas modales de grado a lo sumo n .

De esto se sigue que la noción de “ n -bisimilaridad para todo n ” y equivalencia modal coinciden.

Demostración: i) \Rightarrow ii) por inducción en n . La converso se puede usar un argumento similar al de la prueba de Henessy-Milner.

Propiedad de modelo finito

- ▶ Vamos a definir la *altura* de un modelo rooted de la siguiente manera: Sea \mathcal{M} un modelo con raíz w . El único elemento con altura 0 es w . Los estados con altura $n + 1$ son los inmediatos sucesores de los estados con altura n que todavía no fueron asignados con una altura menor a $n + 1$.
- ▶ La altura de un modelo \mathcal{M} es el máximo n tal que existe un estado en \mathcal{M} con altura n , si es que tal máximo existe. Si no existe, la altura de \mathcal{M} es infinita. La altura de w la notamos $height(w)$.
- ▶ Para un natural k , la restricción de \mathcal{M} a k (notación: $\mathcal{M} \upharpoonright k$) está definida como: $(\mathcal{M} \upharpoonright k) = (W_k, \{R_{ik}\}, V_k)$ donde $W_k = \{v \mid height(v) \leq k\}$, $R_{ik} = R_i \cap (W_k \times W_k)$, y para cada p , $V_k(p) = V(p) \cap W_k$.

Propiedad de modelo finito

Ahora podemos decir más formalmente cuánto de un modelo ve una fórmula en relación a su profundidad modal.

Prop 3: Sea \mathcal{M} un modelo rooted, y sea k un número natural. Entonces, por cada estado w de $(\mathcal{M} \upharpoonright k)$ vale que $(\mathcal{M} \upharpoonright k), w \xleftrightarrow{l} \mathcal{M}, w$, donde $l = k - \text{height}(w)$.

Demostración: Tomar la relación de identidad sobre $(\mathcal{M} \upharpoonright k)$.

- Poniendo juntas las proposiciones 2 y 3, podemos concluir que cualquier fórmula satisfacible puede ser satisfecha en un modelo de *altura finita*. Esto nos acerca a lo que buscamos, pero el modelo resultante todavía puede tener *branching infinito*.

Propiedad de modelo finito

Vamos a obtener un modelo finito *seleccionando* puntos y descartando ramas no deseadas.

Teorema: Modelo Finito - vía selección. Sea φ una fórmula de la lógica modal básica. Si φ es satisfacible, entonces es satisfacible en un modelo finito.

Demostración: Sea φ una fórmula con $\text{deg}(\varphi) = k$. Vamos a restringir la signatura a los operadores modales y proposiciones que aparezcan en φ . Sea \mathcal{M}_1, w_1 tal que $\mathcal{M}_1, w_1 \models \varphi$.

1. Por la *tree model property*, existe \mathcal{M}_2 con forma de árbol y raíz w_2 tal que $\mathcal{M}_2, w_2 \models \varphi$.
2. Sea $\mathcal{M}_3 = (\mathcal{M}_2 \upharpoonright k)$. Por la **Prop 3**, vale $\mathcal{M}_2, w_2 \xleftrightarrow{k} \mathcal{M}_3, w_2$, y por la **Prop 2**, tenemos que $\mathcal{M}_3, w_2 \models \varphi$.

Propiedad de modelo finito

3. Por inducción en $i \leq k$ vamos a definir los conjuntos S_0, \dots, S_k y modelo final \mathcal{M}_4 con dominio $S_0 \cup \dots \cup S_k$. Los puntos en cada S_i van a tener altura i .
4. Definimos $S_0 = \{w_2\}$ y supongamos que S_0, \dots, S_i ya fueron definidos. Fijemos un elemento v de S_i . Por la **Prop 1** hay sólo finitas fórmulas no equivalentes con grado a lo sumo k . Llamémoslas ψ_1, \dots, ψ_m . Para cada una de esas fórmulas de la forma $\langle a \rangle \rho$ que vale en \mathcal{M}_3 en el punto v , seleccionemos un estado u de \mathcal{M}_3 tal que $R_a v u$ y $\mathcal{M}_3, u \models \rho$. Agreguemos todos los puntos u a S_{i+1} y repitamos este proceso de selección para cada punto de S_i .
5. Definimos a S_{i+1} como el conjunto de todos los puntos seleccionados de esta manera.

Propiedad de modelo finito

6. Finalmente, definimos \mathcal{M}_4 como:

- I. Su dominio es $S_0 \cup \dots \cup S_k$. Como cada S_i es finito, \mathcal{M}_4 es finito.
- II. Sus relaciones y valuaciones se obtienen restringiendo las relaciones y valuaciones de \mathcal{M}_3 al dominio de \mathcal{M}_4 .

7. No es difícil probar que $\mathcal{M}_4, w_2 \xleftrightarrow{k} \mathcal{M}_3, w_2$, y por lo tanto $\mathcal{M}_4, w_2 \models \varphi$.

Propiedad de modelo finito

El método que acabamos de ver tiene sus ventajas y desventajas:

- ▶ (+): En muchos casos el método se adapta bien a distintas lógicas. Son los casos en los que las nociones de **árbol**, **n -bisimulación** y el **procedimiento de selección** en sí se adaptan bien.
- ▶ (-): El modelo de entrada puede satisfacer **relaciones estructurales** importantes para nosotros, pero el resultado es siempre un árbol finito, y esas propiedades usualmente se pierden. Eso hace que si queremos probar la propiedad de modelo finito para alguna clase de modelos en especial, probablemente tengamos que hacer más trabajo adicional.

Aparecen las filtraciones

- ▶ Otro método de probar la propiedad de modelos finitos
- ▶ Idea:
 - ▶ No se *seleccionan* finitos sucesores (en un árbol)
 - ▶ En cambio, se *cocientan* todos los elementos del modelo
 - ▶ El criterio para cocientar es: “cosas que φ no puede distinguir”
- ▶ Aclaración:
 - ▶ En lo que sigue asumimos que hay una única relación
 - ▶ Pero la generalización es trivial

Preliminares

Definición (Conjunto cerrado por subfórmulas)

Un conjunto de fórmulas Σ está *cerrado por subfórmulas* si para todo par de fórmulas φ y ψ , si $\varphi \in \Sigma$ y ψ es subfórmula de φ , entonces $\psi \in \Sigma$

Definición

Sea Σ un conjunto cerrado por subfórmulas, y sea $\mathcal{M} = \langle W, R, V \rangle$. Llamamos \sim_{Σ} a la relación de equivalencia sobre W dada por

$$\sim_{\Sigma} := \{(w, v) \mid \text{para todo } \varphi \in \Sigma, \mathcal{M}, w \models \varphi \text{ si y solo si } \mathcal{M}, v \models \varphi\}$$

Con ustedes, las filtraciones

Definición (Filtración)

Sea $\mathcal{M} = \langle W, R, V \rangle$ y sea Σ un conjunto cerrado por subfórmulas. Se llama *filtración de \mathcal{M} vía Σ* a cualquier modelo $\mathcal{M}^f = \langle W^f, R^f, V^f \rangle$ que cumpla

- $W^f = W / \sim_{\Sigma}$
- Si $R w v$, entonces $R^f [w][v]$
- Si $R^f [w][v]$ y $\Diamond \varphi \in \Sigma$, entonces $\mathcal{M}, v \models \varphi$ implica $\mathcal{M}, w \models \Diamond \varphi$
- $V^f(p) = \{[w] \mid \mathcal{M}, w \models p\}$ para todo $p \in \Sigma$

- ▶ Intuitivamente, las condiciones ?? y ?? nos dicen qué pares tiene que tener R^f como mínimo (??) y como máximo (??).

Filtraciones... ¿para que?

Teorema (Filtration Theorem)

Sea \mathcal{M}^f una filtración vía Σ de \mathcal{M} , donde Σ es un conjunto de fórmulas de la lógica modal básica, cerrado por subfórmulas. Para toda fórmula $\varphi \in \Sigma$ y todo elemento w de \mathcal{M} ,
 $\mathcal{M}, w \models \varphi$ sii $\mathcal{M}^f, [w] \models \varphi$

Demostración.

Inducción en φ . Caso base, por definición de V^f . Booleanos, por HI.

- ▶ Si $\Diamond\psi \in \Sigma$ y $\mathcal{M}, w \models \Diamond\psi$
 - ▶ Existe v tal que Rwv y $\mathcal{M}, v \models \psi$
 - ▶ Por ??, $R^f[w][v]$ y como $\psi \in \Sigma$, por HI $\mathcal{M}^f, [v] \models \psi$
 - ▶ Con lo cual $\mathcal{M}^f, [w] \models \Diamond\psi$
- ▶ Si $\Diamond\psi \in \Sigma$ y $\mathcal{M}^f, [w] \models \Diamond\psi$
 - ▶ Para algún $[v]$, $R^f[w][v]$ y $\mathcal{M}^f, [v] \models \psi$
 - ▶ Como $\psi \in \Sigma$, por HI, $\mathcal{M}, v \models \psi$; luego, por ?? $\mathcal{M}, w \models \Diamond\psi$

Filtraciones, mito o realidad

- ▶ Si \mathcal{M}^f cumple ciertas condiciones, vale el Filtration Theorem
- ▶ Preguntas:
 - ▶ ¿Serán condiciones que se pueden cumplir?
 - ▶ O sea, dado \mathcal{M} y Σ , existirá siempre una filtración de \mathcal{M} vía Σ

Filtraciones, ¡realidad!

Teorema

Sea $\mathcal{M} = \langle W, R, V \rangle$ y sea Σ un conjunto cerrado por subfórmulas. Llamemos W^f a W / \sim_{Σ} , y V^f a la valuación que cumple con ??. Entonces, $\mathcal{M}^s = \langle W^f, R^s, V^f \rangle$ y $\mathcal{M}^l = \langle W^f, R^l, V^f \rangle$ son filtraciones de \mathcal{M} vía Σ , donde

- $R^s[w][v]$ sii $\exists w' \in [w]$ y $\exists v' \in [v]$ tal que $Rw'v'$
 $R^l[w][v]$ sii para toda $\Diamond\varphi \in \Sigma$, $\mathcal{M}, v \models \varphi$ implica $\mathcal{M}, w \models \Diamond\varphi$

Además, si $\mathcal{M}^f = \langle W^f, R^f, V^f \rangle$ es una filtración de \mathcal{M} vía Σ , entonces $R^s \subseteq R^f \subseteq R^l$

Filtraciones, ¡realidad!

Demostración.

Veamos que $\mathcal{M}^s = \langle W^f, R^s, V^f \rangle$ es una filtración (el resto... **ejercicio!**). Alcanza con ver que R^s cumple con ?? y ??.

- ▶ R^s cumple ?? por definición
- ▶ Para ??, supongamos que $R^s[w][v]$ y que $\mathcal{M}, v \models \varphi$ para $\Diamond\varphi \in \Sigma$
- ▶ Necesitamos ver que $\mathcal{M}, w \models \Diamond\varphi$
- ▶ Como $R^s[w][v]$, existen $w' \in [w]$ y $v' \in [v]$ tales que $Rw'v'$
- ▶ Pero $\varphi \in \Sigma$, y $v' \sim_{\Sigma} v$, con lo cual $\mathcal{M}, v' \models \varphi$
- ▶ Luego, $\mathcal{M}, w' \models \Diamond\varphi$
- ▶ Pero como $w' \sim_{\Sigma} w$ y $\Diamond\varphi \in \Sigma$, $\mathcal{M}, w \models \Diamond\varphi$

□

Propiedad de modelos finitos vía filtraciones

Teorema

Sea φ una fórmula de la lógica modal básica. Si φ es satisfacible, es satisfacible en un modelo finito, que contiene a lo sumo 2^m nodos, donde m es la cantidad de subfórmulas de φ ($m \leq |\varphi|$)

Demostración.

- ▶ Supongamos que φ es satisfacible, i.e., $\mathcal{M}, w \models \varphi$
- ▶ Sea $\Sigma := \{\psi \mid \psi \text{ es subfórmula de } \varphi\}$. Observar que Σ es finito
- ▶ Sea, además, \mathcal{M}^f una filtración de \mathcal{M} vía Σ .
- ▶ Vale $\mathcal{M}^f, [w] \models \varphi$
- ▶ ¿Cuántos elementos tiene \mathcal{M}^f ?
- ▶ ¡A lo sumo $2^{|\Sigma|}$!

□

Algunas relaciones entre clases de complejidad

No se sabe si son estrictas

$$P \subseteq NP \subseteq NPSpace \subseteq EXPTIME \subseteq NEXPTIME \subseteq NEXPSPACE \subseteq 2EXP \dots$$

Se sabe que son iguales (Savitch)

$$\begin{array}{lcl} PSPACE & = & NPSpace \\ EXPSPACE & = & NEXPSPACE \\ & \vdots & \end{array}$$

Se sabe que son estrictas (Stearns & Hartmanis; Cook)

$$\begin{array}{lcl} P & \subset & EXPTIME \subset 2EXPTIME \subset 3EXPTIME \dots \\ NP & \subset & NEXPTIME \subset 2NEXPTIME \subset 3NEXPTIME \dots \\ PSPACE & \subset & EXPSPACE \subset 2EXPSPACE \subset 3EXPSPACE \dots \end{array}$$

Problemas clásicos de decisión (para una lógica \mathcal{L})

Model checking en \mathcal{L}

Dados \mathcal{M} y φ , decidir si $\mathcal{M} \models_{\mathcal{L}} \varphi$

Satisfacibilidad en \mathcal{L} (respecto a una clase de modelos \mathcal{C})

Dada φ decidir si **existe** \mathcal{M} tal que $\mathcal{M} \models_{\mathcal{L}} \varphi$ (con $\mathcal{M} \in \mathcal{C}$)

Validez en \mathcal{L} (respecto a una clase de modelos \mathcal{C})

Dada φ decidir si **para todo** \mathcal{M} vale $\mathcal{M} \models_{\mathcal{L}} \varphi$ (con $\mathcal{M} \in \mathcal{C}$)

Satisfacibilidad y validez son problemas duales

- ▶ φ es satisfacible sii $\neg\varphi$ no es válida
- ▶ φ es válida sii $\neg\varphi$ no es satisfacible

Aspectos computacionales de una lógica

Para cada uno de estos problemas vale preguntarse:

- I. ¿Es decidable?
- II. ¿Cuál es su complejidad de peor caso?
- III. ¿Hay algoritmos que sean eficientes en el caso promedio?

Aspectos computacionales de la lógica proposicional

Model checking proposicional

- I. Es decidable
- II. Es lineal en la fórmula (post-order en el árbol sintáctico)
- III. Es fácil de implementar de manera eficiente

Aspectos computacionales de la lógica proposicional

Satisfacibilidad proposicional

- I. Es decidable
- II. Está en **NP** (adivinar y chequear) y es completo (Cook)
- III. DPLL algorithm: problemas “reales” con $> 10K$ variables

Aspectos computacionales de la lógica modal básica

Model checking (sobre modelos finitos)

- I. Es decidable
- II. Está en **PTIME**: $O(|\varphi| \cdot |W|^2)$ (eg., usando prog. dinámica)
- III. Es fácil de implementar de manera eficiente

Aspectos computacionales de la lógica modal básica

Satisfacibilidad

- I. Ya habíamos visto que es decidable (reducciones a FO2)
- II. ??
- III.

Filtraciones como cota de complejidad

Filtraciones y la propiedad de modelos finitos (repaso)

- ▶ Sea Σ un conjunto finito cerrado bajo subfórmulas
- ▶ Y sea \mathcal{M}^f una filtración de \mathcal{M} via Σ
- ▶ Vimos que si $\mathcal{M}, w \models \varphi$ con $\varphi \in \Sigma$, entonces $\mathcal{M}^f, |w| \models \varphi$
- ▶ Pero \mathcal{M}^f es finito... cuántos estados tiene?

Corolario

- ▶ Si φ es satisfacible, tiene modelo de a lo sumo $2^{|\varphi|}$ estados
- ▶ Luego, podemos adivinar un modelo en $O(2^{|\varphi|})$
- ▶ Y podemos testear si satisface φ en tiempo polinomial
- ▶ Con lo cual, el problema seguro está en NEXPTIME

Aspectos computacionales de la lógica modal básica

Satisfacibilidad

- I. Ya habíamos visto que es decidible (reducciones a FO2)
- II. A lo sumo NEXPTIME (pero vamos a ver mejores cotas)