Cálculo de tableaux para fórmulas elementales en lógicas de separación

Licenciatura en Ciencias de la Computación

Andrés R. Saravia

Universidad Nacional de Córdoba, Facultad de Matemática, Astronomía y Física

10/III/2020

Motivación

Situaciones modeladas por medio de estructuras relacionales:

- grafos,
- bases de datos,
- el flujo de ejecución de un programa,
- el manejo de memoria dinámica,
- o relaciones entre varios elementos.

Lógicas modales

- Extensión de la lógica proposicional.
- Nuevos operadores que describen diferentes modos de verdad.
- Buen balance entre la expresividad y el comportamiento computacional.
- Sirven para razonar y extraer información de las estructuras relacionales.

Lógicas modales dinámicas

Permiten modificar la estructura a medida que se evalúa una fórmula.
Ejemplos:

- *frames reactivos*,
- *lógicas modales de sabotaje*,
- y las *lógicas de anuncios públicos*.

Lógicas de Separación *SL*

- Extensión de la lógica de Hoare.
- Razonamiento sobre programas con estructuras de datos mutables.
- Se interpreta sobre una abstracción de la memoria de un programa.

Reinterpretación de las *SL*

- Las abstracciones pueden ser representadas como modelos relacionales de lógica modal, donde la relación es finita y funcional.
- Permite expresar tanto propiedades *modales* como *de separación*.

Modal Logics + Separation Logics = Modal Separation Logics

Nuestra contribución

- Nos interesa razonar o extraer información usando MSL.
- Existen distintas tareas de razonamiento.
- Satisfacibilidad: dada una fórmula decidir si es satisfacible.
- Desarrollamos un cálculo de tableaux que decida la satisfacibilidad de un fragmento de MSL, expresada de una cierta manera.

Sintaxis de MSL($*, \Diamond$)

Sea $\mathrm{PROP} = \{p, q, \ldots\}$ un conjunto infinito enumerable de símbolos proposicionales. Las fórmulas de MSL($*, \Diamond$) están definidas por la siguiente gramática:

$$\phi ::= \top \mid p \mid \mathtt{emp} \mid \neg\phi \mid \phi \wedge \phi \mid \Diamond\phi \mid \phi * \phi,$$

donde $p \in \mathrm{PROP}$. Los demás operadores y constantes se definen de la forma usual.

Modelos en MSL($*, \Diamond$)

Un *modelo* es una tupla $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$ tal que:

- el conjunto de los números naturales $\mathbb{N}$ es el conjunto de *mundos*,
- $\mathfrak{R} \subseteq \mathbb{N} \times \mathbb{N}$ es una relación finita y funcional $((\mathfrak{l}, \mathfrak{l}') \in \mathfrak{R}$ y $(\mathfrak{l}, \mathfrak{l}'') \in \mathfrak{R}$ implica $\mathfrak{l}' = \mathfrak{l}'')$,
- y $\mathfrak{V} : \mathrm{PROP} \to \mathcal{P}(\mathbb{N})$ es una valuación.

Semántica de MSL$(*, \diamond)$

Sea $\mathfrak{M} = \langle \mathbb{N}, \mathfrak{R}, \mathfrak{V} \rangle$ y $\mathfrak{l} \in \mathbb{N}$, la relación $\models$ está definida como:

$$
\begin{array}{lcl}
\mathfrak{M}, \mathfrak{l} \models \top & \stackrel{\text{def}}{\Leftrightarrow} & \text{siempre}, \\
\mathfrak{M}, \mathfrak{l} \models p & \stackrel{\text{def}}{\Leftrightarrow} & \mathfrak{l} \in \mathfrak{V}(p), \\
\mathfrak{M}, \mathfrak{l} \models \neg\phi & \stackrel{\text{def}}{\Leftrightarrow} & \mathfrak{M}, \mathfrak{l} \not\models \phi, \\
\mathfrak{M}, \mathfrak{l} \models \phi_1 \wedge \phi_2 & \stackrel{\text{def}}{\Leftrightarrow} & \mathfrak{M}, \mathfrak{l} \models \phi_1 \text{ y } \mathfrak{M}, \mathfrak{l} \models \phi_2, \\
\mathfrak{M}, \mathfrak{l} \models \diamond\phi & \stackrel{\text{def}}{\Leftrightarrow} & \text{existe un } \mathfrak{l}' \in \mathbb{N} \ (\mathfrak{l}, \mathfrak{l}') \in \mathfrak{R}, \text{ tal que } \mathfrak{M}, \mathfrak{l}' \models \phi, \\
\mathfrak{M}, \mathfrak{l} \models \mathtt{emp} & \stackrel{\text{def}}{\Leftrightarrow} & \mathfrak{R} = \emptyset, \\
\mathfrak{M}, \mathfrak{l} \models \phi_1 * \phi_2 & \stackrel{\text{def}}{\Leftrightarrow} & \langle \mathbb{N}, \mathfrak{R}_1, \mathfrak{V} \rangle, \mathfrak{l} \models \phi_1 \text{ y } \langle \mathbb{N}, \mathfrak{R}_2, \mathfrak{V} \rangle, \mathfrak{l} \models \phi_2, \\
 & & \text{para alguna partición } \{\mathfrak{R}_1, \mathfrak{R}_2\} \text{ de } \mathfrak{R}.
\end{array}
$$

Una fórmula ϕ en MSL$(*, \diamond)$ es satisfacible si existe un modelo $\mathfrak{M}$ y un mundo $\mathfrak{l}$ tal que $\mathfrak{M}, \mathfrak{l} \models \phi$. Caso contrario, ϕ es insatisfacible.

Ejemplos

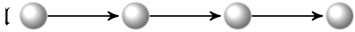
La siguiente fórmula es insatisfacible en MSL$(*, \Diamond)$:

$$\neg(\neg\mathtt{emp} * \neg\mathtt{emp}) \wedge (\neg\mathtt{emp} * \neg\mathtt{emp} * \neg\mathtt{emp})$$

Ejemplos

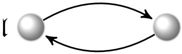
La expresividad de MSL$(*, \Diamond)$ puede definir caminos y ciclos:

$$\Diamond\Diamond\Diamond\Box\,\bot$$



$$(\neg\mathtt{emp} * \neg\mathtt{emp}) \wedge \neg(\neg\mathtt{emp} * \neg\mathtt{emp} * \neg\mathtt{emp}) \wedge \Diamond\Diamond\Diamond\top\wedge$$

$$\neg(\neg\mathtt{emp} * \Diamond\Diamond\Diamond\top) \wedge \neg\Diamond(\neg\mathtt{emp} * \Diamond\Diamond\Diamond\top)$$



Razonar sobre MSL$(*, \Diamond)$

- Los lenguajes dinámicos son difíciles de comprender y manipular.
- En general no tienen buenas propiedades para hacer inferencia.
- Sin embargo, podemos transformarlas en fórmulas más manejables.

Fórmulas elementales

- Fórmulas en MSL$(*, \Diamond)$.
- Describen propiedades esenciales de los modelos.
- Dos familias:
  - *Fórmulas size*:
    - Expresan el tamaño del modelo en términos de la relación.
    - Expresiones de la forma $\texttt{size} \geq \beta$.
    - $\texttt{size} \geq \beta$ es verdadera sii $\mathfrak{R}$ tiene al menos β elementos.
  - *Fórmulas grafo*: expresan propiedades de la forma del modelo desde el mundo actual.

Gramática de $\mathcal{G}$

Expresión derivada del elemento $\mathcal{G}$ no terminal de la siguiente gramática:

$$\ell := \top \mid \bot \mid p \mid \neg p, \qquad Q := \ell \mid Q \wedge Q,$$

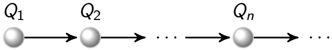
$$\mathcal{G} := |Q,\ldots,Q\rangle \mid |Q,\ldots,Q] \mid |Q,\ldots,Q,\ldots,Q|,$$

donde $p \in \mathrm{PROP}$ y $\mathcal{G}$ debe contener al menos una conjunción Q.

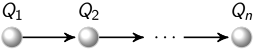
Semántica de $\mathcal{G}$

Representan caminos que satisfacen una conjunción de literales Q en cada posición.

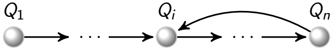
$|Q_1,\ldots, Q_n\rangle$



$|Q_1,\ldots, Q_n]$



$|Q_1,\ldots, Q_i,\ldots, Q_n|$



Equivalencia

Lema

Toda fórmula elemental ϕ es lógicamente equivalente a una fórmula en $MSL(*, \Diamond)$.

Lema

Sea ϕ una fórmula en $MSL(*, \Diamond)$, existe una fórmula elemental ψ tal que:

1. $\psi = \bigvee_{i=1}^{n} (\mathcal{G}_i \wedge \mathcal{S}_i)$, *con* $\mathcal{S}_i = (\texttt{size} \geq \beta_i)$ *ó* $(\texttt{size} \geq \beta_i \wedge \neg \texttt{size} \geq \alpha_i)$,
2. *y ψ y ϕ son equivalentes.*

Cálculo de tableaux

- Un procedimiento en el que se decide la satisfacibilidad de una fórmula dada utilizando la satisfacibilidad de sus subfórmulas.
- Uso de reglas de inferencia previamente establecidas.
- Toma una fórmula como input, decide si es satisfacible o no y, en caso afirmativo, devuelve un modelo el cual satisface dicha fórmula.
- Se utiliza una estructura de datos de árbol.

Recapitulación

Lema

Sea ϕ una fórmula en $\mathsf{MSL}(*, \Diamond)$, existe una fórmula elemental ψ equivalente tal que:

$$\psi = \bigvee_{i=1}^{n} (\mathcal{G}_i \wedge \mathcal{S}_i), \text{ con } \mathcal{S}_i = (\texttt{size} \geq \beta_i) \text{ ó } (\texttt{size} \geq \beta_i \wedge \neg\texttt{size} \geq \alpha_i).$$

Desarrollaremos un cálculo con etiquetas para este tipo de fórmulas. Las etiquetas serán los números naturales y representarán los mundos del modelo. Por definición, empezaremos desde la etiqueta $i = 1$.

Reglas

Capas en la aplicación de las reglas de derivación.

$$\bigvee_{i=1}^{n} \varphi_i \Longrightarrow (\mathcal{G}_k \wedge \mathcal{S}_k) \Longrightarrow \mathcal{G}_k \Longrightarrow Q \Longrightarrow \ell$$

$\bigvee_{i=1}^{n} \varphi_i \implies (\mathcal{G}_k \wedge \mathcal{S}_k)$

$$\frac{i : \quad \varphi_k \vee \bigvee_{j \neq k} \varphi_j}{i : \varphi_k \mid i : \bigvee_{j \neq k} \varphi_j} \vee \text{ para } \varphi_j\text{'s}$$

Siendo $\bigvee_{j \neq k} \varphi_j$ una disyunción de una o más fórmulas.

$(\mathcal{G}_k \wedge \mathcal{S}_k) \Longrightarrow \mathcal{G}_k$

Cada rama tendrá exactamente una fórmula $\varphi_k = (\mathcal{G}_k \wedge \mathcal{S}_k)$.

$$\dfrac{i : \mathcal{G} \wedge \texttt{size} \geq \beta}{\begin{array}{c} i : \mathcal{G} \\ \texttt{size} \geq \beta \end{array}} \wedge(\mathrm{I}) \qquad \dfrac{i : \mathcal{G} \wedge \texttt{size} \geq \beta \wedge \neg\texttt{size} \geq \alpha}{\begin{array}{c} i : \mathcal{G} \\ \texttt{size} \geq \beta \\ \neg\texttt{size} \geq \alpha \end{array}} \wedge(\mathrm{II})$$

$\mathcal{G}_k \implies Q$

$$\frac{i : |Q_i\rangle}{\begin{array}{c} i : Q_i \\ iR(i+1) \\ \texttt{size} \geq 1 \end{array}} \text{ Continuada I} \qquad \frac{i : |Q_i, \alpha, Q_n\rangle}{\begin{array}{c} i : Q_i \\ iR(i+1) \\ \texttt{size} \geq n - i + 1 \\ i+1 : |\alpha, Q_n\rangle \end{array}} \text{ Continuada II}$$

Siendo α cero o más conjunciones.

$Q \Longrightarrow \ell$

$$\frac{i : \ell \wedge Q}{\begin{array}{c} i : \ell \\ i : Q \end{array}} \wedge \text{ para literales}$$

Con Q siendo una conjunción de uno o más literales.

Ramas cerradas, abiertas y saturadas

Una rama $\mathcal{B}$ es cerrada si y solamente si sucede al menos una de las siguientes situaciones:

- $(i : \perp) \in \mathcal{B}$ para algún $i \in \mathbb{N}$;
- $(i : p), (i : \neg p) \in \mathcal{B}$ para algún $i \in \mathbb{N}$, $p \in \mathrm{PROP}$;
- $\texttt{size} \geq \beta, \neg\texttt{size} \geq \alpha \in \mathcal{B}$ con $\alpha \leq \beta$;
- $\neg\texttt{size} \geq 0 \in \mathcal{B}$;

Una rama es abierta si no es cerrada, y una rama está saturada si no se le pueden aplicar más reglas.

Resultados del cálculo

Completitud

Sea $\psi = \bigvee_{i=1}^{n}(\mathcal{G}_i \wedge \mathcal{S}_i)$ con $\mathcal{S}_i = \texttt{size} \geq \beta_i$ ó $(\texttt{size} \geq \beta_i \wedge \neg\texttt{size} \geq \alpha_i)$. Si el tableaux para ψ tiene una rama abierta y saturada, entonces ψ es satisfacible.

Corrección

Sea $\psi = \bigvee_{i=1}^{n}(\mathcal{G}_i \wedge \mathcal{S}_i)$ con $\mathcal{S}_i = \texttt{size} \geq \beta_i$ ó $(\texttt{size} \geq \beta_i \wedge \neg\texttt{size} \geq \alpha_i)$. Si ψ es satisfacible, entonces el tableaux para ψ tiene una rama abierta y saturada.

Características del cálculo

- Ventajas:
  - Fácil tratamiento computacional.
  - Es polinomial.
- Desventajas:
  - La traducción de MSL$(*, \Diamond)$ a fórmulas elementales contiene una explosión exponencial.
  - No es polinomial a la hora de decidir la satisfacibilidad de una fórmula en MSL$(*, \Diamond)$.

Trabajos futuros

- Pasantía en LSV, ENS Paris-Saclay (Stéphane Demri):
  - Estudio sobre la complejidad de los fragmentos de MSL.
- Tesis doctoral: Lógicas Epistémicas con Estrategias (Raúl Fervari):
  - Lenguajes provistos de agentes capaces de aprender estrategias.