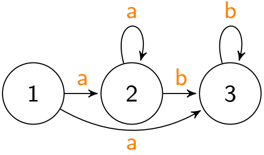
Bisimulation: entre Théorie des Modèles de la Logique Modale et Vérification

Raphaëlle Crubillé
mail: raphaelle.crubille@lis-lab.fr

AMU-LIS

Master IMD

$\mathcal{M}$:=



$+$ *val* : Etats x Variables $\rightarrow \{$true, false$\}$.

Modèle de Kripke pour LM

Équivalence Modale:
$(\mathcal{M}, w) \equiv^{LM} (\mathcal{M}', w')$ quand $\forall \phi$ LM-formula, $\mathcal{M}, w \models \phi \Leftrightarrow \mathcal{M}', w' \models \phi$.

Système de Transition Labellés (LTS)

modélisent des systèmes réactifs

Bisimulation: équivalence structurelle sur les LTSs.

Objectifs de ce cours:

- Peut-on comparer l'équivalence modale et la bisimulation ?
- Uttilisation de bisimulations pour des problèmes de théorie des modèles: construction de modèles, résultats de (non)-définissabilité

Definition (Langages poly-modaux)

$\Psi = \{P, Q, \ldots\}$: un ensemble dénombrable de variable propositionnelles,
$\tau = \{\alpha, \beta, \ldots\}$: un ensemble de *modalités*.

$$\phi, \psi \in LM(\Psi, \tau) := \bot \mid P \mid \phi \to \psi \mid \diamond_\alpha \phi \qquad \text{avec } P \in \Psi, \alpha \in \tau.$$

Remarque

Avec cette syntaxe minimale, on peut encoder $\neg$, $\top$, $\vee$, $\wedge$, $\square_\alpha$...

Definition (Structure de Kripke)

Un cadre (frame) de Kripke : $\mathcal{L} = (W, (R_\alpha)_{\alpha \in \tau})$,

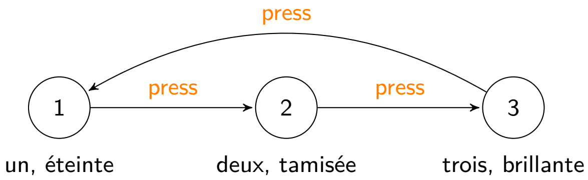
- W : ensemble des *états* (ou *mondes possibles*)
- R_α: relation d'accessibilité.

Une structure de Kripke: $\mathcal{S} = (\mathcal{L}, val)$, où $val : \Psi \to \{0, 1\}$ est une *fonction de valuation*.

Notation: $\omega \xrightarrow{\alpha} \omega'$ when $(\omega, \omega') \in R_\alpha$.

Un système d'éclairage:

$\mathcal{S}$:=

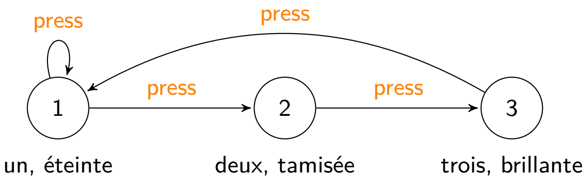


Kripke structure

- $\Psi = \{\text{un}, \text{deux}, \text{trois}, \text{brillante}, \text{tamisée}, \text{éteinte}\}$
- $\alpha = \{\text{press}\}$
- $W = \{1, 2, 3\}$
- $R_{\text{press}} = \{(1, 2), (2, 3), (3, 1)\}$
- $val(1)(\text{un}) = 1;\ val(1)(\text{éteinte}) = 1;\ val(1)(\text{deux}) = 0\ldots$

Exemple: un système d'éclairage dysfonctionnel

$\mathcal{S}_{dys}$:=



Exercice

Trouver une formule ϕ telle que $\mathcal{S} \models \phi$ and $\mathcal{S}_{dys} \models \neg\phi$.

Exercice

Écrire une structure de Kripke qui modélise une machine à café. Contraintes:

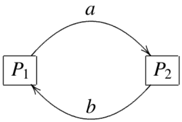
- l'utilisateur peut choisir de payer en espèce ou par carte;
- la machine propose de thé et du café.

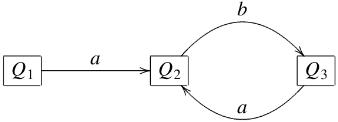
On fixe Ψ (variables propositionnelles) et τ (modalités).

Definition

Soit $\mathcal{S}$, $\mathcal{S}'$ deux structures de Kripke. $\mathcal{S}, w \equiv^{LM} \mathcal{S}', w'$ quand $\forall \phi \in LM(\Psi, \tau)$, $\mathcal{S}, w \models \phi \Leftrightarrow \mathcal{S}', w' \models \phi$.

Example



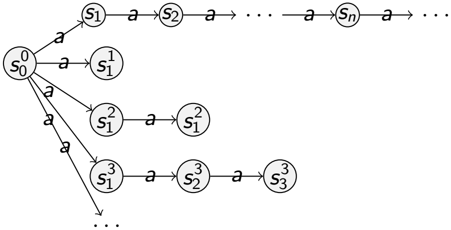


Exo(TD)

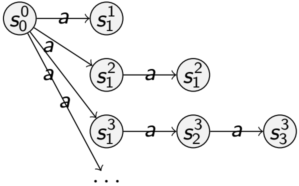
$\forall i, j, val(P_i) = val(Q_j) = \top := (P \in \Psi \mapsto 1)$.

Équivalence Modale: Exercice.

$\mathcal{L}_1$:



$\mathcal{L}_2$:



Question:

Est ce que $(\mathcal{L}_1, s_0) \equiv_{LM} (\mathcal{L}_2, s_1)$?

Definition

- Structure de Kripke pointée: $\mathcal{S}_p = ((W, (R_\alpha)_{\alpha\in\tau}, val), w)$ avec $w \in W$.
  $Thm(\mathcal{S}_p) = \{\phi \mid (W, (R_\alpha)_{\alpha\in\tau}, val), w) \models \phi\}$.
- Structure de Kripke: $\mathcal{S} = (W, (R_\alpha)_{\alpha\in\tau}, val)$
  $Thm(\mathcal{S}) = \{\phi \mid \forall w \in W,\ (W, (R_\alpha)_{\alpha\in\tau}, val), w) \models \phi\}$.
- Frame de Kripke pointée: $\mathcal{F}_p((W, (R_\alpha)_{\alpha\in\tau}), w)$ avec $w \in W$
  $Thm(\mathcal{F}_p) = \{\phi \mid \forall val \in 2^{\Psi},\ (W, (R_\alpha)_{\alpha\in\tau}, val), w) \models \phi\}$.
- Frame de Kripke : $\mathcal{F} = (W, (R_\alpha)_{\alpha\in\tau})$.
  $Thm(\mathcal{F}) = \{\phi \mid \forall val \in 2^{\Psi}, \forall w \in W,\ (W, (R_\alpha)_{\alpha\in\tau}, val), w) \models \phi\}$.

Definition

$\mathcal{L}$: structure de Kripke (pointée)/ Frame de Kripke (pointée).

$$\mathcal{L} \equiv^{LM} \mathcal{L}' \text{ quand } Thm(\mathcal{L}) = Thm(\mathcal{L}').$$

Towards Bisimulation (1)

Que veut-on-dire par **équivalence structurelle** sur les structures de Kripke ?

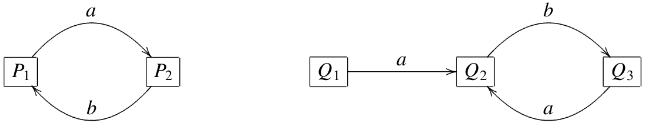
Une première tentative: isomorphisme de graphe

$(W, (R_\alpha)_{\alpha\in\tau}, val) \equiv (W', (R'_\alpha)_{\alpha\in\tau}, val')$ si il existe une bijection $\rho : W \to W'$, tel que:

- ρ est un isomorphisme de graphe;
- $\forall w \in W,\ val'(\rho(w)) = val(w)$.

Example

Deux systèmes non isomorphes (de graphe)



$\forall i, j, val(P_i) = val(Q_j) = \top := (P \in \Psi \mapsto 1).$

Une deuxième tentative: équivalence de trace

Inspirée par la théorie des automates.
Deux automates sont équivalents si ils reconnaissent le même language.

Definition (Traces)

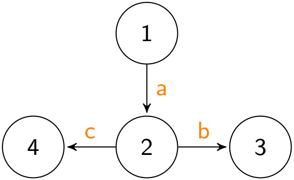
Une **trace** est une séquence finie alternée $v_0 a_0 v_1 a_1 \ldots . v_n$, où $v_i \in 2^{\Psi}$, et $a_i \in \tau$.

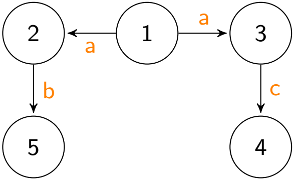
Definition

- Une trace $t = v_0 a_0 v_1 \ldots . v_n$ est **reconnue** par une structure de Kripke $\mathcal{S} = (W, (R_\alpha)_{\alpha \in \tau}, val)$ quand $\exists s_0, \ldots, s_n \in W$ tel que $s_i \xrightarrow{a_i} s_{i+1}$ for $0 \leq i \leq n$, and $val(s_i) = v_i$.
- Deux structures de Kripke sont en **équivalence de trace** si elles reconnaissent le même ensemble de trace.

Équivalence modale et équivalence de trace

Example





Est ce que ces 2 structures de Kripke:

- sont en équivalence de trace ?
- sont en équivalence modale ?
- ont intuitivement un comportement équivalent vu comme des systèmes réactifs ?

Bisimulation

Intuition

On veut que deux systèmes réactifs/machines soient équivalents quand:

- Si une action peut-être faite par une machine, la même action peut être faite par l'autre machine;
- Quelque soit l'état dans lequel l'une des deux machines évolue, l'autre peut évoluer dans un état équivalent.

Definition

$\mathcal{S} = (W, (R_\alpha)_{\alpha \in \tau}, val)$ une structure de Kripke. Une relation binaire réflexive $R \subseteq W \times W$ est une **bisimulation** sur $\mathcal{S}$ quand:
$(s, s') \in R$ implique:

1. $val(s) = val(s')$;
2. si $s \xrightarrow{a} t$, alors il existe $t' \in W$ avec $s' \xrightarrow{a} t'$, et $t \, R \, t'$;
3. si $s' \xrightarrow{a} t'$, alors il existe $t \in W$ avec $s \xrightarrow{a} t$, et $t \, R \, t'$.

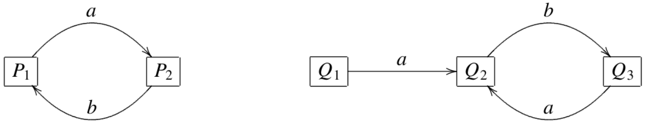
On appelle **bisimilarité** l'union de toutes les bisimulations:
$\sim_{\mathcal{S}} := \bigcup_{R \mid R \text{ est une bisimulation}} R$.

Uttiliser la bisimulation pour comparer une paire de SK pointées.

Definition

$\mathcal{S}, w \sim \mathcal{S}', w' := w \sim_{\mathcal{S} \cup \mathcal{S}'} w'$, where $\mathcal{S} \cup \mathcal{S}'$ is the **disjoint** union of $\mathcal{S}$ and $\mathcal{S}'$.

Example



$\forall i, j, val(P_i) = val(Q_j) = \top := (P \in \Psi \mapsto 1)$.

Proof.

Au tableau. □

Theorem

$(\mathcal{S}, w) \sim (\mathcal{S}', w') \Rightarrow (\mathcal{S}, w) \sim^{ML} (\mathcal{S}', w')$.

Proposition

La bisimilarité $\sim_{\mathcal{S}}$ est une bisimulation, et de plus c'est une relation d'équivalence (réflexive, transitive et symmétrique).

Proof.

Au tableau. $\square$

Definition (Morphisme zig-zag)

Un morphisme zig-zag est une fonction $\rho : W \to W'$, dont le graphe est une bisimulation.

Un exemple d'application de la bisimilarité en logique modale.

Problématique

Comment construire des modèles (avec des contraintes structurelles) ?
Ou: quelles **constructions** sur les modèles **préservent la valeur de vérité** des formules ?

Definition

On définit un *pré-ordre d'inclusion* sur les structures de Kripke par:
pour $\mathcal{L} = (W, (R_\alpha)_{\alpha\in\tau}, val)$, $\mathcal{L}' = (W', (R'_\alpha)_{\alpha\in\tau}, val')$, $\mathcal{L} \subseteq \mathcal{L}'$ quand:

- $W \subseteq W'$, $R_\alpha = R'_\alpha \cap (W \times W)$, $val = val'_{|W}$,
- $\forall w \in W, \forall a \in \tau$, $(w \xrightarrow{a}_{\mathcal{L}'} w' \Rightarrow w' \in W)$.

Definition (Structure engendrée par un état w)

Soit $\mathcal{L} = (W, (R_\alpha)_{\alpha\in\tau}, val)$ une structure de Kripke, $w \in W$. On définit:

- $G^n(w) :=$ {états atteignables en partant de w en $\leq n$ étapes}.
- $G(w) := \cup_{n\in\mathbb{N}} G^n(w)$
- $\mathcal{L}[w] := (G(w), (R_\alpha \cap (G(w) \times G(w)))_{\alpha\in\tau}, val_{|G(w)})$.

Example (Au tableau)

Proposition

La sous-structure de $\mathcal{L}$ engendré par un état est ***incluse*** *dans $\mathcal{L}$, i.e. $\mathcal{L}[w] \subseteq \mathcal{L}$.*

Proposition (Validité dans un sous-modèle)

Si $\mathcal{L} \subseteq \mathcal{L}'$, et w est un état de $\mathcal{L}$, alors $\mathcal{L}, w \equiv^{LM} \mathcal{L}', w$.

Proof.

L'inclusion $W \to W'$ est un morphisme zig-zag + invariance par bisimulation. □

Conséquence

Toute formule satisfiable est satisfiable dans un modèle «enraciné», c'est à dire de la forme $\mathcal{L}[w]$.

« Unfolding» d'arbres

Definition (Chemins)

Un chemin sur $\mathcal{L}$ est une suite finie d'état $w_0, \ldots, w_n$, tel que pour tout $i \leq n-1$, $\exists \alpha \in \tau$, $w_i \xrightarrow{\alpha} w_{i+1}$. On note $\vec{W}$ pour l'ensemble des chemins sur $\mathcal{L}$.

Definition («Unfolding» d'une structure de Kripke)

Soit $\mathcal{L} = (W, (R_\alpha)_{\alpha \in \tau}, val)$, et $w \in W$. On définit une SK $\vec{\mathcal{L}}[w]$ par:

- ensemble d'états: $\{p \in \vec{W} \mid p_0 = w\}$
- relation de transition: $p \xrightarrow{a} p'$ si $p' = p.w$, et $last(p) \xrightarrow{a} w$;
- fonction de valuation: $val(p) = val(last(p))$.

Example (Au tableau)

Proposition

Soit $\mathcal{L} = (W, (R_\alpha)_{\alpha \in \tau}, val)$, *et* $w \in W$. $\vec{\mathcal{L}}[w], [w] \equiv^{LM} \mathcal{L}, w$.

Conséquence

Toute formule satisfiable est satisfiable à la racine d'un **arbre**.

Proposition

Toute structure de Kripke est l'image par un morphisme zig-zag d'une union disjointe de structures Arbre.

Proof.

$$f : \bigcup_{w \in W} \vec{\mathcal{L}}[w] \to \mathcal{L}$$

$\square$

Conséquence

Si une propriété sur les modèles de Kripke est invariante par bisimulation, il suffit de la montrer sur les unions disjointes de structure d'arbre.

Definition

- Une classe $\mathscr{P}_S$ de **Kripke structures pointées** (on τ, Φ) est **définissable** si $\exists \phi \in LM[\tau, \Phi]$ telle que: $(\mathcal{S}, w \models \phi) \Leftrightarrow (\mathcal{S}, w) \in \mathscr{P}_S$.
- Une classe $\mathscr{P}_F$ de **Kripke frames pointées** (on τ, Φ) est **définissable** si$\exists \phi \in LM[\tau, \Phi]$ telle que: $(\forall val,\ \mathcal{F}, w, val \models \phi) \Leftrightarrow (\mathcal{F}, w) \in \mathscr{P}_F$.
- Une classe $\mathscr{P}_F$ de **Kripke frames** (on τ, Φ) est **définissable** si$\exists \phi \in LM[\tau, \Phi]$ telle que: $(\forall val, \forall w\ \mathcal{F}, w, val \models \phi) \Leftrightarrow \mathcal{F} \in \mathscr{P}_F$.

Remarque:

" Quelles sont les classes de Kripke frames définissable ? "
$\equiv$ "Quelles propriétés d'une relation binaire peut-on axiomatiser en logique modale ? "

Definition

- Une classe $\mathscr{P}_S$ de **Kripke structures pointées** (on τ, Φ) est **définissable** si $\exists \phi \in LM[\tau, \Phi]$ telle que: $(\mathcal{S}, w \models \phi) \Leftrightarrow (\mathcal{S}, w) \in \mathscr{P}_S$.
- Une classe $\mathscr{P}_F$ de **Kripke frames pointées** (on τ, Φ) est **définissable** si$\exists \phi \in LM[\tau, \Phi]$ telle que: $(\forall val,\ \mathcal{F}, w, val \models \phi) \Leftrightarrow (\mathcal{F}, w) \in \mathscr{P}_F$.
- Une classe $\mathscr{P}_F$ de **Kripke frames** (on τ, Φ) est **définissable** si$\exists \phi \in LM[\tau, \Phi]$ telle que: $(\forall val, \forall w\ \mathcal{F}, w, val \models \phi) \Leftrightarrow \mathcal{F} \in \mathscr{P}_F$.

Proposition

- *si $\mathscr{P}_S$ sur PKSs est définissable, $(\mathcal{L}, w) \in \mathscr{P}_S$ et $(\mathcal{L}, w) \sim (\mathcal{L}', w')$, alors $(\mathcal{L}', w') \in \mathscr{P}_S$;*
- *si $\mathscr{P}_F$ sur KFs est définissable:*
  - *si $(\mathcal{F}, w) \in \mathscr{P}_S$ et $f : (\mathcal{F}, val_\perp, w) \rightarrow (F', val'_\perp, w')$ un morphisme zig-zag surjectif, alors $(\mathcal{F}', w) \in \mathscr{P}_S$.*
  - *si $\forall i \in I$, $(\mathcal{F}_i, w_i) \in \mathscr{P}_S$ et $f_i : (\mathcal{F}_i, val_\perp, w_i) \rightarrow (F', val'_\perp, w')$ un morphisme zig-zag tel que $\cup_i f_i$ est surjectif, alors $(\mathcal{F}', w) \in \mathscr{P}_S$.*

Example (Sur les structures de Kripke pointées)

- Réfléxivité: **Non-définissable**
  (Preuve: L'"unfolding" de n'importe quelle structure est non-réflexive + toute structure de Kripke est bisimilaire à son unfolding.)
- Plus généralement: tout propriété non-locale.

Example (Sur les frames (non pointées))

- Réflexivité: $\Box p \to p$
- Irréflexivité: **Non-définissable** (non préservé par zig-zag morphismes)
- Frames finies, frames connexes, frames avec une relation binaire unniverselle...:**Non-définissables** (Non préservé par union disjointe).
- Frame qui est un réflexive partial ordering: **Non-définissable** (pas préservé par zig-zag morphisme surjectif: /ex $((Z), \leq) \to \{\omega_0, \omega 1\}$).