Comparaison de logiques

Pouvoir de distinction et d'expression

Comparaisons

- Logiques temporelles.
  - CTL: formules d'états.
  - LTL: formules de chemins/traces.
  - CTL*: formules mixtes.
- Questions.
  - Comment les comparer?
  - Quand est-ce que deux états satisfont les mêmes formules?

- Solutions.
  1. *Pouvoir de distinction*: est-ce qu'une formule φ d'une logique Φ peut distinguer l'état s de l'état s'?

     On dit qu'une formule φ distingue deux états s et t si elle est satisfaite par exactement un des deux états.
  2. *Pouvoir d'expression*: est-ce qu'une formule φ d'une logique Φ est équivalente à une formule ψ d'une logique Ψ?

Équivalence d'états

- Définition: une *équivalence d'états* est une famille de relations qui contient pour chaque structure de Kripke $M = (S, S_0, R, L)$ une relation d'équivalence $\simeq_M$ sur les états de M.
- Exemples.
  1. Égalité d'états: $s \simeq t$ si $s = t$.
  2. Équivalence observationnelle: $s \approx t$ si $L(s) = L(t)$.
  3. Bissimilarité, similarité, équivalence de trace: cf plus loin.

- Définitions.
  - Un équivalence d'états $\simeq^1$ est *aussi distinguante* qu'une équivalence d'états $\simeq^2$, si pour tout M, $\simeq^1_M$ raffine $\simeq^2_M$.
  - L'équivalence d'état $\simeq^1$ est *plus distinguante* si le contraire n'est pas vrai.

Bissimilarité

- Définition: la bissimilarité $\simeq^B$ est l'équivalence d'état qui correspond à $min_M(\approx)$, où $\approx$ est l'équivalence observationnelle.
  I.e. $\simeq^B_M = min_M(\approx)$ pour tout M.

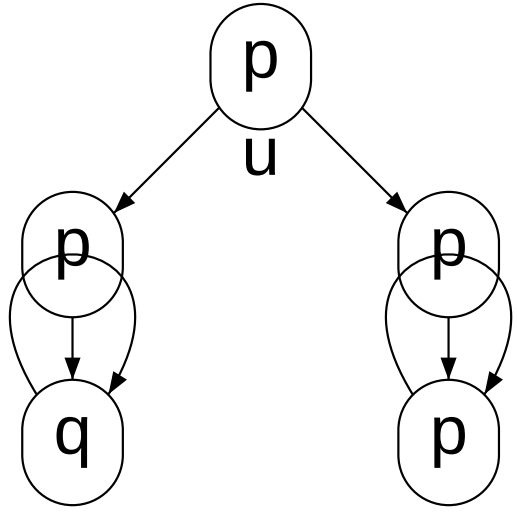
Bissimilarité

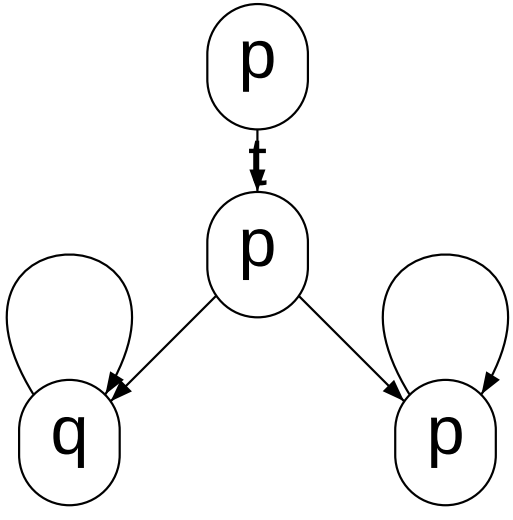
- Définition équivalente:
  1. une relation $\sim$ sur les états S d'une structure de Kripke $M = (S, S_0, R, L)$ est une bissimulation si pour tout s,t avec $s \sim t$,
     - $L(s) = L(t)$.
     - $R(s, s')$ alors il existe t' avec $R(t, t')$ et $s' \sim t'$.
     - $R(t, t')$ alors il existe s' avec $R(s, s')$ et $s' \sim t'$.
  2. Deux états s et t sont bissimilaires, noté $s \simeq^B t$, ou $s \leq^B t$, s'il existe une bissimulation $\sim$ avec $s \sim t$.

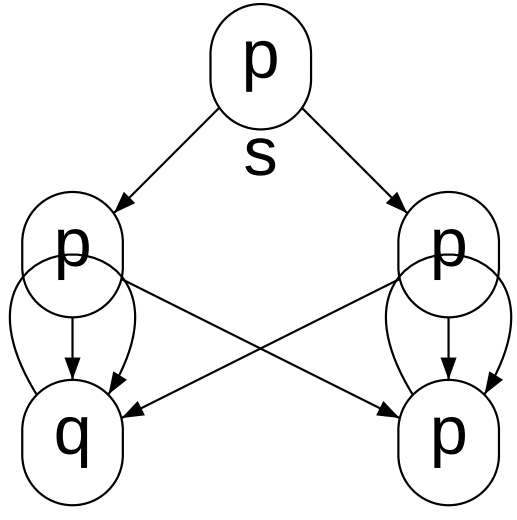
Démonstration. La deuxième définition donne bien une relation stable qui raffine l'équivalence observationnelle. La relation définie est donc incluse dans $min_M(\approx)$. Réciproquement, $min_M(\approx)$ est une bissimulation particulière et donc les deux relations se correspondent.

Exemples

- Soit M:







- s et t sont bissimilaires.
- t n'est pas bissimilaire avec u.

Bissimilarité

Plusieurs autres définitions alternatives:

- théorie des jeux,
- plus grand point fixe,
- limite de relations moins distinguantes.

Exemple de définition équivalente: hi

- Deux états s et t sont dits bissimilaires en i-étapes si dans un jeu de bissimilarité l'adversaire n'a aucune stratégie gagnante qui requiert au plus i-étapes.
- Formellement, on définit:
  - $\approx^0 = \approx$
  - Étant donné $\approx^i$, on définit $s \approx_M^{i+1} t$ ssi
    1. $L(s) = L(t)$
    2. $R(s, s')$ alors il existe t' avec $R(t, t')$ et $s' \approx^i t'$.
    3. $R(t, t')$ alors il existe s' avec $R(s, s')$ et $s' \approx^i t'$.

- Théorème: pour tout i, $\approx^{i+1}$ est aussi distinguante que $\approx^{i}$.

  Démonstration. Récurrence immédiate sur i.

- Équivalence de bissimilarité s'obtient par

$$\simeq^{B} = \bigcap_{i \in \mathbb{N}} \approx^{i} .$$

Démonstration. $\bigcap_{i\in\mathbb{N}} \approx^i$ raffine $min_M(\approx)$: en effet, on vérifie facilement que $\bigcap_{i\in\mathbb{N}} \approx^i$ est une relation stable et puisque chaque $\approx^i$ raffine $\approx^0 = \approx$, $\bigcap_{i\in\mathbb{N}} \approx^i$ raffine $\approx$. Réciproquement, il suffit de montrer que $min_M(\approx)$ raffine $\approx^i$ pour tout i: par récurrence. $min_M(\approx)$ raffine $\approx^0 = \approx$. Suppose hypothèse au rang i et $s\ min_M(\approx)\ t$. Suppose $R(s, s')$. Puisque $min_M(\approx)$ est stable, il doit exister t' avec $s'\ min_M(\approx)\ t'$. Par hypothèse de récurrence, cela implique $s' \approx^i t'$. Même chose en inversant s et t. Et donc $s \approx_M^{i+1} t$.

Équivalence d'états associée à une log

- Chaque logique Φ induit une équivalence d'états $\simeq^{\Phi}$: $s \simeq^{\Phi} t$ si pour toute formule $\varphi \in \Phi$, $s \models_M \varphi$ ssi $t \models_M \varphi$.
- Pouvoir distinction d'une logique Φ.
  comparer les pouvoirs distinctions de deux logiques = comparer les équivalences induites.
- Définition: une équivalence d'état aussi distinguante que $\simeq^{\Phi}$ est appelé *une sémantique abstraite de la logique* Φ.
- Définition: l'équivalence d'états $\simeq^{\Phi}$ est appelé *sémantique abstraite complète de la logique* Φ.

CTL

- Théorème: la bissimilarité est la sémantique abstraite complète de CTL.
- I.e.
  1. deux états bissimilaires satisfont les mêmes formules CTL.
  2. si deux états sont non bissimilaires, alors on peut les distinguer par une formule CTL.

Démonstration de 1.

Démonstration de 1. Par induction structurelle sur la formule CTL φ.
Suppose φ formule propositionnelle. $\simeq^B$ raffine l'équivalence observationnelle $\approx$ et donc les états bissimilaires vérifient les même formules propositionnelles.
Suppose $\varphi = \psi \exists U \chi$. Par hypothèse de récurrence, les états bissimilaires concordent sur ψ et χ. Suppose $s \models \varphi$. Il existe une trajectoire $s = s_0 s_1 \dots s_m$ avec $s_i \models \psi$ pour $0 \leq i < m$ et $s_m \models \chi$.
Puisque $\simeq^B$ est stable à partir d'un t tq $s \simeq^B t$, on construit facilement une trajectoire $t = t_0 t_1 \dots t_m$ avec $s_i \simeq^B t_i$ pour $0 \leq i \leq m$. On obtient $t \models \varphi$.
Les cas $\varphi = \exists \circ \psi$ et $\varphi = \exists \Box \psi$ sont laissés en exercice.
De même pour les cas $\varphi = \varphi_1 \vee \varphi_2$, $\varphi = \varphi_1 \wedge \varphi_2$ et $\varphi = \neg \varphi_1$.

Démonstration de 2.

Démonstration de 2. Supposons que $\neg(s \simeq^B t)$. Puisque $\simeq^B = \bigcap_{i\in\mathbb{N}} \approx^i$, on a $\neg(s \approx^{i_0} t)$ pour un certain i_0.

On montre par récurrence sur i que pour chaque classe d'équivalence σ de $\approx^i$ on peut construire une formule φ_σ qui caractérise σ: $[\![\varphi_\sigma]\!] = \sigma$.

Pour $i = 0$, $\approx^i = \approx$. Prendre $\varphi_\sigma = L(s)$ pour un $s \in \sigma$.

Pour $i = k + 1$, il y a au plus un nombre fini de classes d'équivalence τ de $\approx^k$ tel que $R(s, t)$ pour $s \in \sigma$, $t \in \tau$. On note $\sigma \to \tau$ pour une telle classe.

Considère $\varphi_\sigma = \wedge_{\{\tau\in\approx^k|\sigma\to\tau\}} \exists \circ \varphi_\tau \wedge \forall \circ \vee_{\{\tau\in\approx^k|\neg(\sigma\to\tau)\}} \neg\varphi_\tau$. Vérifier que cette formule convient.

Fragments de CTL

- Fragments de CTL:

  Rappel: CTL= formules sur la grammaire
  $\varphi ::= p|\varphi \vee \varphi|\neg\varphi|\exists \circ \varphi|\varphi \exists U \varphi|\varphi \exists \Box \varphi$.

  1. STL: fragment de CTL obtenu en considérant uniquement les formules sur la grammaire $\varphi ::= p|\varphi \vee \varphi|\neg\varphi|\exists \circ \varphi|\varphi \exists U \varphi$. (i.e. on considère seulement les propriétés de sûreté). (i.e. STL= CTL sans $\exists \Box \varphi$).
  2. $STL\circ$: seulement $\varphi ::= p|\varphi \vee \varphi|\neg\varphi|\exists \circ \varphi$
  3. $STLU$: seulement $\varphi ::= p|\varphi \vee \varphi|\neg\varphi|\varphi \exists U \varphi$

- Théorème: si deux états ne sont pas bissimilaires, alors il existe une formule $STL\circ$ qui les distingue.
  Démonstration: il suffit d'observer les formules construites dans la démonstration de 2.
- Corollaire: sémantique abstraite complète de CTL = sémantique abstraite complète de STL = sémantique abstraite complète de $STL\circ$ = bissimilarité.

Graphe quotient

Remarque: Pour $M = (S, S_0, R, L)$ une structure de Kripke, et une relation d'équivalence $\simeq$ qui raffine l'équivalence observationnelle, on peut bien associer une **structure de Kripke** quotient $M/\simeq$.

On considère $M/\simeq = (S/\simeq, S_0/\simeq, R/\simeq, L/\simeq)$
où $(S/\simeq, S_0/\simeq, R/\simeq)$ est le graphe quotient du système de transition (S, S_0, R) comme auparavant
et on définit $L/\simeq(\sigma)$ pour une région σ par $L/\simeq(\sigma) = L(s)$ pour n'importe quel $s \in \sigma$: puisque $\simeq$ raffine l'équivalence observationnelle , pour tout $s, t \in \Sigma$, on a bien $L(s) = L(t)$ et donc cette définition est non ambigue.

Application

- Application: pour résoudre un problème de vérification $M \models ?\varphi$ avec φ CTL (respectivement CTL^*,STL, $STL\circ$) on peut:
  1. calculer la partition de bissimilarité $\simeq^B = min_M(\approx)$;
  2. et travailler sur $M/\simeq^B$:

$$M/\simeq^B \models \varphi \text{ ssi } M \models \varphi.$$

- Démonstration: 2 états équivalents pour $\simeq^B$ satisfont les mêmes formules. $[[\varphi]]_M$ est donc un bloc de $\simeq^B$, pour toute formule φ. On vérifie que pour ces logiques: $[[\varphi]]_M = \bigcup [[\varphi]]_{M/\simeq^B}$.

Amélioration

- En fait, ces logiques Φ admettent l'abstraction: pour toute $\simeq$ qui raffine $\simeq^{\Phi}$, $[[\varphi]]_M = \bigcup [[\varphi]]_{M/\simeq}$.
- Conséquence, pour une telle logique, pour toute $\simeq$ qui raffine $\simeq^{\Phi}$,

$$M/\simeq \models \varphi \text{ ssi } M \models \varphi.$$

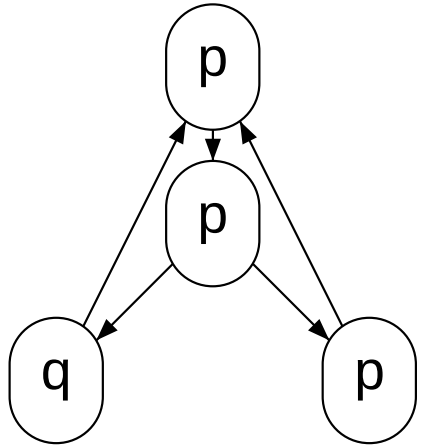
- Remarque: toutes les logiques n'admettent pas cette propriété.

Bégaiements (stuttering)

- Une structure de Kripke bégaie lorsque les états observables peuvent rester inchangés par une transition.
  i.e. elle possède des chemins $\pi = s_0 s_1 \ldots s_n s_{n+1} \ldots$ avec $L(s_n) = L(s_{n+1})$.
- Motivation: essayer d'avoir une équivalence avec encore moins de classes d'équivalence en ignorant les bégaiements.

- Clôture par bégaiement d'une structure de Kripke $M = (S, S_0, R, L)$.
  - On note $R_{beg}(s,t)$ s'il existe un chemin $s_0 s_1 \ldots s_n$ avec $s_0 = s$, $s_n = t$ et $L(s_0) = L(s_1) = \ldots = L(s_{n-1})$.
  - La *clôture par bégaiement de* M est la structure de Kripke $M_{beg} = (S, S_0, R_{beg}, L)$.
- Définition: la *clôture par bégaiement d'une* ***équivalence d'états*** $\simeq$ est l'équivalence d'états $\simeq_{beg}$ telle que $s \simeq_{beg} t$ sur M si et seulement si $s \simeq t$ sur M_{beg}.
  (rappel: une équivalence d'états associe à chaque structure de Kripke une partition).
- Définition: une équivalence d'états est dite *insensible par bégaiement* si $\simeq_{beg} = \simeq$.

- Propriété: la bissimilarité n'est pas insensible par bégaiement.
  Contre Exemple:



- On appelle *bissimilarité faible* la clôture par bégaiement de la bissimilarité.
  Propriété: la bissimilarité faible est moins distinguante que la bissimilarité.
  Démonstration: immédiat.
- Définition: une logique est dite *insensible au bégaiement* si $\simeq^{\Phi}$ l'est.

- Corollaire: CTL, STL ne sont pas insensibles au bégaiement.
  Intuitivement, $\exists\circ$ permet de distinguer des états bissimilaires faiblement.
- Théorème: la bissimilarité faible est la sémantique abstraite complète de $STLU$.
  Démonstration: laissée en exercice.
- Corollaire: $STL\circ$ et CTL sont plus distinguantes que $STLU$.

Pouvoir d'expression

- Définition: une logique Φ est *aussi expressive* que la logique Ψ si pour toute formule $\varphi \in \Phi$ il existe une formule $\psi \in \Psi$ tq pour toute structure de Kripke $[\![\varphi]\!]_M = [\![\psi]\!]_M$.
- Définition: une logique Φ est *plus expressive* si elle est aussi expressive mais le contraire est faux.
- Remarque: pouvoir de distinction supérieur implique pouvoir d'expression supérieur.
  (réciproque fausse).

- Théorème.
  - STL est plus expressif que $STLU$.
  - $STL\circ$ est plus expressif que $STLU$.

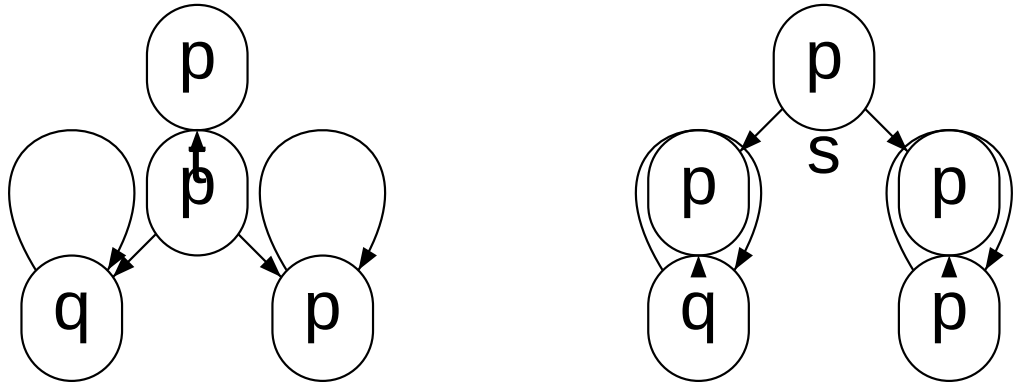
  Démonstration. Exercice: montrer que bissimilarité plus distinguante que bissimilarité faible.
  Remarque: intuition $\circ$ suffisant pour distinguer états bissimilaires mais pas pour exprimer U.

Équivalences de traces

- Question: Qu'en est-il des logiques de traces? ex: LTL.
- Définition: deux états s et t d'une structure de Kripke M sont *traces équivalents*, noté $s \simeq^L t$, si $L_M(s) = L_M(t)$, i.e. l'ensemble des traces des chemins partant de s et de t coïncident.
- Propriété: l'équivalence de trace est une équivalence d'états moins distinguante que la bissimilarité.

Équivalences de traces vs Bissimilarit

Démonstration. Clairement deux états bissimilaires sont traces équivalents. Réciproquement, s et t sont traces équivalents mais non-bissimilaires dans le système suivant.



- En clair: $s \simeq^B t$ implique $s \simeq^L t$. (mais réciproque fausse).

Logiques de traces vs CTL, STL

- Théorème: l'équivalence de trace est la sémantique abstraite complète de LTL.
  I.e.
  - Aucune formule LTL ne distingue deux états traces équivalents.
  - si s et t sont non traces équivalents, alors il existe une formule LTL qui les distingue.
- Corollaire: LTL est moins distinguant que STL et CTL.

  Démonstration: l'équivalence de trace est moins distinguante que la bissimilarité.

Démonstrations

Démonstration de 1: puisque LTL est une logique de traces, elle ne peut pas distinguer des états trace équivalents.
Démonstration de 2: pour deux états s et t non trace équivalents, quitte à inverser le rôle de s et t, il existe une trace $\sigma \in L(s)$ qui n'est pas dans $L(t)$. Considérer la formule φ LTL correspondant à l'existence d'une trajectoire commençant par la trace σ. On a $s \models \varphi$ et $\neg(t \models \varphi)$.

Application

- Application: pour résoudre un problème de vérification $M \models ?\varphi$ avec φ LTL on peut:
  1. calculer la partition de bissimilarité $\simeq^B = min_M(\approx)$;
  2. et travailler sur $M/\simeq^B$:

$$M/\simeq^B \models \varphi \text{ ssi } M \models \varphi.$$

- Démonstration: deux états bissimilaires sont traces équivalents. Ils vérifient donc les mêmes formules LTL.