Pouvoir de distinction

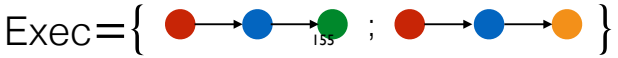
Pouvoir de distinction:
→ capacité à distinguer deux modèles **S** et **S'**.

distinguer = trouver une formule vraie pour l'un et fausse pour l'autre.

Pouvoir de distinction de LTL

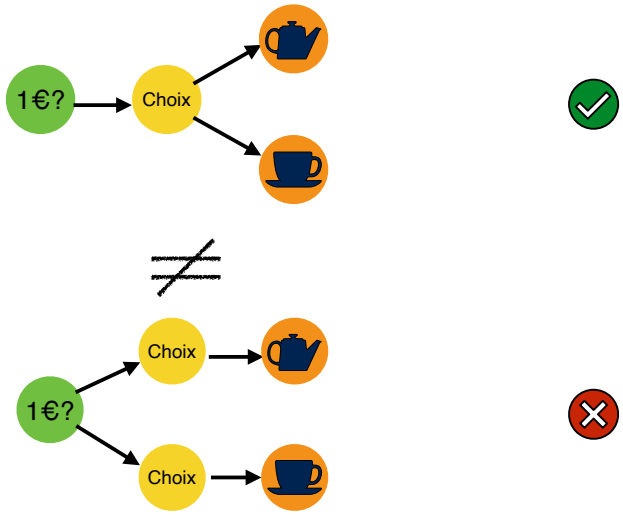
→ Si deux STE ont le même ensemble d'exécutions (*), alors ils vérifient les mêmes formules de LTL.

(*) on dit qu'ils sont « trace-equivalent »



A-t-on envie que ce soit équivalent ?

Une machine à café… deux implémentations.



Pouvoir de distinction

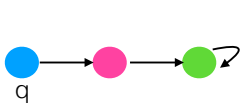
Et CTL ?

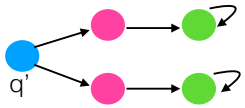
$q \not\models \mathbf{EX}\,(\mathbf{EX}\ \mathbf{P} \wedge \mathbf{EX}\ \mathbf{P})$ $\quad q' \models \mathbf{EX}\,(\mathbf{EX}\ \mathbf{P} \wedge \mathbf{EX}\ \mathbf{P})$

$q \models \mathbf{EX}\,(\mathbf{AX}\ \mathbf{P})$ $\quad q' \not\models \mathbf{EX}\,(\mathbf{AX}\ \mathbf{P})$

Pouvoir de distinction

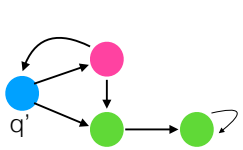
Peut-on distinguer n'importe quels STE avec CTL ?

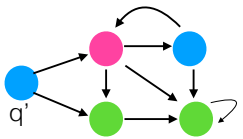




q et q' vérifient les mêmes formules de CTL !

ICI





q et q' vérifient les mêmes formules de CTL !

Comment définir l'équivalence entre des machines ?

- systèmes réactifs (interaction avec un environnement)

Pouvoir de distinction

deux STE vérifient les mêmes formules de CTL
ssi
ils sont ***bisimilaires****.
(Hennessy, 1980)

Rappel: on considère ici des STE finis.

(*) *fortement* bisimilaires

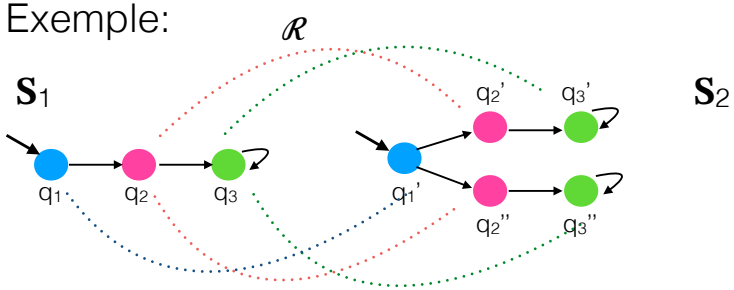
Bisimulation (forte)

Soient $\mathbf{S}_1 = \langle Q_1, q^0_1, R_1, \ell_1 \rangle$ et $\mathbf{S}_2 = \langle Q_2, q^0_2, R_2, \ell_2 \rangle$
Une relation $\mathcal{R} \subseteq Q_1 \times Q_2$ est une bisimulation ssi $\forall (q_1,q_2) \in \mathcal{R}$ on a:

- $\ell_1(q_1) = \ell_2(q_2)$
- $\forall\ q_1 \rightarrow_{R1} q_1'$, $\exists\ q_2 \rightarrow_{R2} q_2'$ t.q. $(q_1',q_2') \in \mathcal{R}$
- $\forall\ q_2 \rightarrow_{R2} q_2'$, $\exists\ q_1 \rightarrow_{R1} q_1'$ t.q. $(q_1',q_2') \in \mathcal{R}$

$\mathbf{S}_1$ et $\mathbf{S}_2$ sont bisimilaires ($\mathbf{S}_1 \approx \mathbf{S}_2$) ssi il existe une bisimulation $\mathcal{R}$ telle que $(q^0_1, q^0_2) \in \mathcal{R}$.

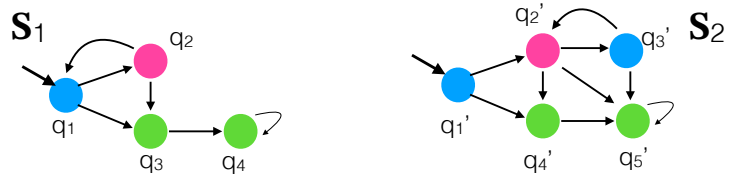
Exemple:



$\mathcal{R} = \{(q_1,q_1'), (q_2,q_2'),(q_2,q_2''),(q_3,q_3'),(q_3,q_3'')\}$

$\mathbf{S}_1 \approx \mathbf{S}_2$

Exemple:

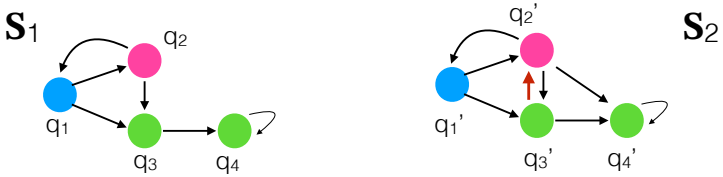


$\mathcal{R} = \{(q_1,q_1'), (q_1,q_3'), (q_2,q_2'),(q_3,q_4'),(q_3,q_5'), (q_4,q_4'),(q_4,q_5'),\}$

$\mathbf{S}_1 \approx \mathbf{S}_2$

Montrer que deux STE sont bisimilaires est FACILE: il suffit de donner une bisimulation !

Exemple:



q_3 et q_3' sont très différents !!
$\mathbf{S}_1$ et $\mathbf{S}_2$ ne sont pas bisimilaires.

Théorème: deux STE (à branchement fini) vérifient les mêmes formules de CTL ssi ils sont (fortement) bisimilaires. (Hennessy, 1980)

Preuve:

- $\mathbf{S}_1 \approx \mathbf{S}_2 \Rightarrow \mathbf{S}_1 \equiv_{CTL} \mathbf{S}_2$

On montre un résultat plus fort: si $\mathcal{R} \subseteq Q_1 \times Q_2$ est une bisimulation alors $\forall (q_1,q_2) \in \mathcal{R}$, on a: $q_1 \equiv_{CTL} q_2$

Par induction sur la taille des formules de CTL.

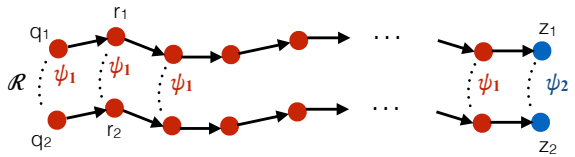
- $P \in AP$: $q_1 \models P \overset{def}{\iff} P \in L(q_1) \overset{q_1 \approx q_2}{\iff} P \in L(q_2) \iff q_2 \models P$
- $\psi_1 \wedge \psi_2$: $q_1 \models \psi_1 \wedge \psi_2 \overset{def}{\iff} q_1 \models \psi_1$ et $q_1 \models \psi_2 \overset{h.i.}{\iff} q_2 \models \psi_1$ et $q_2 \models \psi_2$ $\overset{def}{\iff} q_2 \models \psi_1 \wedge \psi_2$
- $\neg \psi$: $q_1 \models \neg \psi \overset{def}{\iff} q_1 \not\models \psi \overset{h.i.}{\iff} q_2 \not\models \psi \overset{def}{\iff} q_2 \models \neg \psi$

- $\mathbf{EX}\ \psi$: $q_1 \models \mathbf{EX}\ \psi \iff \exists\, q_1 \rightarrow q_1'$ t.q. $q_1' \models \psi$

  $(q_1,q_2) \in \mathcal{R} \Rightarrow \exists\, q_2 \rightarrow q_2'$ t.q. $(q_1',q_2') \in \mathcal{R}$.

  $(q_1',q_2') \in \mathcal{R}$, $q_1' \models \psi$ $\Rightarrow q_2' \models \psi$ et donc $q_2 \models \mathbf{EX}\ \psi$

- $\mathbf{E}\ \psi_1\ \mathbf{U}\ \psi_2$: $q_1 \models \mathbf{E}\ \psi_1\ \mathbf{U}\ \psi_2$



donc $q_2 \models \mathbf{E}\ \psi_1\ \mathbf{U}\ \psi_2$

- $\mathbf{A}\ \psi_1\ \mathbf{U}\ \psi_2$: ou plus simplement $\mathbf{AF}$ ou même $\mathbf{EG}$… même idée que pour le $\mathbf{E}\ \mathbf{U}$!

- $\mathbf{S}_1 \equiv_{CTL} \mathbf{S}_2 \Rightarrow \mathbf{S}_1 \approx \mathbf{S}_2$

Il suffit de trouver une bisimulation…

Soit $\mathcal{R} = \{ (q_1,q_2) \in \mathbf{S}_1 \times \mathbf{S}_2 \mid q_1 \equiv_{CTL} q_2 \}$

Vérifions que $\mathcal{R}$ est bien une bisimulation…

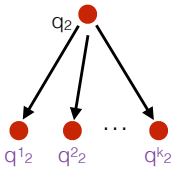
Def: Soient $\mathbf{S}_1 = \langle Q_1, q^0_1, R_1, \ell_1 \rangle$ et $\mathbf{S}_2 = \langle Q_2, q^0_2, R_2, \ell_2 \rangle$
Une relation $\mathcal{R} \subseteq Q_1 \times Q_2$ est une bisimulation ssi $\forall (q_1,q_2) \in \mathcal{R}$ on a:

- $\ell_1(q_1) = \ell_2(q_2)$
- $\forall\, q_1 \rightarrow_{R1} q_1'$, $\exists\ q_2 \rightarrow_{R2} q_2'$ t.q. $(q_1',q_2') \in \mathcal{R}$
- $\forall\, q_2 \rightarrow_{R2} q_2'$, $\exists\ q_1 \rightarrow_{R1} q_1'$ t.q. $(q_1',q_2') \in \mathcal{R}$

- $\mathbf{S_1} \equiv_{CTL} \mathbf{S_2} \Rightarrow \mathbf{S_1} \approx \mathbf{S_2}$

Il suffit de trouver une bisimulation…

Soit $\mathcal{R} = \{ (q_1,q_2) \in \mathbf{S_1}x\mathbf{S_2} \mid q_1 \equiv_{CTL} q_2 \}$



Vérifions que $\mathcal{R}$ est bien une bisimulation…
Soit $(q_1,q_2) \in \mathcal{R}$

- $L(q_1)=L(q_2)$ car $q_1 \equiv_{CTL} q_2$
- Supposons $q_1 \rightarrow q_1'$. Existe-t-il $q_2 \rightarrow q_2'$ t.q. $(q_1',q_2') \in \mathcal{R}$?

Supposons le contraire…
et donc que pour tout arc $q_2 \rightarrow q^i_2$, $(q_1',q^i_2) \notin \mathcal{R} \iff q_1' \not\equiv_{CTL} q^i_2$
$\iff \exists\, \psi^i$ tq $q_1' \models \neg\psi^i$ et $q_2 \models \psi^i$

Donc $q_1 \models \mathbf{EX}\ (\neg\, \psi^1 \wedge \neg\, \psi^2 \wedge \ldots \wedge \neg\, \psi^k)$
Et $q_2 \models \mathbf{AX}\,(\psi^1 \vee \psi^2 \vee \ldots \vee \psi^k)$ 169
c-à-d. $q_2 \models \neg\, \mathbf{EX}\ (\neg\, \psi^1 \wedge \neg\, \psi^2 \wedge \ldots \wedge \neg\, \psi^k)$ et donc $(q_1,q_2) \notin \mathcal{R}$

Si deux systèmes sont bisimilaires, alors ils sont « trace-equivalent » (mais l'inverse n'est pas tjs vrai).

Conséquence:
CTL a un pouvoir de distinction plus grand que LTL.

Pouvoir d'expression

Pouvoir d'expression

- LTL n'est pas aussi expressive que CTL.
  Par ex.:
  EX (EX P ∧ **EX** P') ou **AG (EF** P) n'ont pas d'équivalent en LTL.

Pour **AG (EF** P) :

Exec(q)=Exec(q')={ $\bullet^{\omega}$, $\bullet^{+}\bullet^{\omega}$ } 172 Et donc $q \equiv_{LTL} q'$

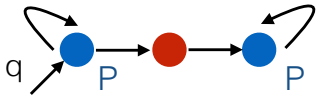
$q \models \mathbf{AG}\ (\mathbf{EF}\ P)$ et $q' \not\models \mathbf{AG}\ (\mathbf{EF}\ P)$

Pouvoir d'expression

- CTL n'est pas aussi expressive que LTL.
- Par ex.: **A FG** P n'a pas d'équivalent en CTL.

(Emerson, 1986)

- **A FG** P : sur tous les chemins, à partir d'une position, on a toujours P.
- Remarque: **A FG** P ≠ **A F AG** P:



q ⊨ **A FG** P
q ⊭ **AF AG** P

- **A FG** P ≡ ¬ **EGF** ¬ P
- **EGF** P' : Il existe un chemin où P' est vraie infiniment souvent.

Pouvoir d'expression

LTL et CTL sont incomparables.

La logique CTL* a été définie pour réunir LTL et CTL: elle contient des quantificateurs de chemins (**E** et **A**) pour exprimer des propriétés sur les états et elle permet aussi des propriétés complexes sur les exécutions…

CTL* est strictement plus expressive que CTL et LTL.

Par ex.: **A (GF** P **⇒ GF (EF** P'**))** ∈ CTL*

Pouvoir d'expression

On peut aussi comparer les logiques (CTL et LTL) à d'autres formalismes: logiques du 1er ou du second ordre, automates, μ-calcul, etc.