Cours du 12 octobre 2017

LTL- (premier fragment)

Syntaxe: $P \in AP$

$\phi,\psi ::= P \mid \neg\phi \mid \phi\vee\psi \mid \phi\wedge\psi \mid \mathbf{X}\ \phi \mid \mathbf{F}\ \phi \mid \mathbf{X}^{-1}\ \phi \mid \mathbf{F}^{-1}\ \phi$

$\mathbf{X}\ \phi$: demain ϕ
$\mathbf{F}\ \phi$: un jour dans le futur ϕ
$\mathbf{X}^{-1}\ \phi$: hier ϕ
$\mathbf{F}^{-1}\ \phi$: un jour dans le passé ϕ

→ on interprète les formule de LTL- sur une position **i** le long d'une exécution **ρ** d'un STE.

+L pour les val. des AP.

$\rho = s_0\ s_1\ s_2\ s_3 \ldots\ s_i\ s_{i+1} \ldots$

LTL- (premier fragment)

Syntaxe: $P \in AP$

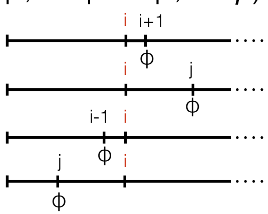
$\phi,\psi ::= P \mid \neg\phi \mid \phi\vee\psi \mid \phi\wedge\psi \mid \mathbf{X}\ \phi \mid \mathbf{F}\ \phi \mid \mathbf{X}^{-1}\ \phi \mid \mathbf{F}^{-1}\ \phi$

Sémantique:

soit ρ une exécution d'un STE $\mathbf{S} = (Q, Act, \rightarrow, q_0, AP, L)$
soit i un entier ≥ 0

$\rho,i \models P$ ssi $P \in L(\rho(i))$
$\rho,i \models \neg\phi$ ssi $\rho,i \not\models \phi$
$\rho,i \models \phi\wedge\psi$ ssi ($\rho,i \models \phi$ et $\rho,i \models \psi$)
$\rho,i \models \phi\vee\psi$ ssi ($\rho,i \models \phi$ ou $\rho,i \models \psi$)

$\rho,i \models \mathbf{X}\ \phi$ ssi $\rho,i+1 \models \phi$
$\rho,i \models \mathbf{F}\ \phi$ ssi ($\exists\, j \geq i.\ \rho,j \models \phi$)
$\rho,i \models \mathbf{X}^{-1}\ \phi$ ssi ($i>0$ et $\rho,i-1 \models \phi$)
$\rho,i \models \mathbf{F}^{-1}\ \phi$ ssi ($\exists\, j \leq i.\ \rho,j \models \phi$)



LTL-

$\mathbf{S} = (Q, Act, \rightarrow, q_0, AP, L)$

$\rho,i \models \phi$ est désormais défini !

Et $\mathbf{S} \models \phi$?

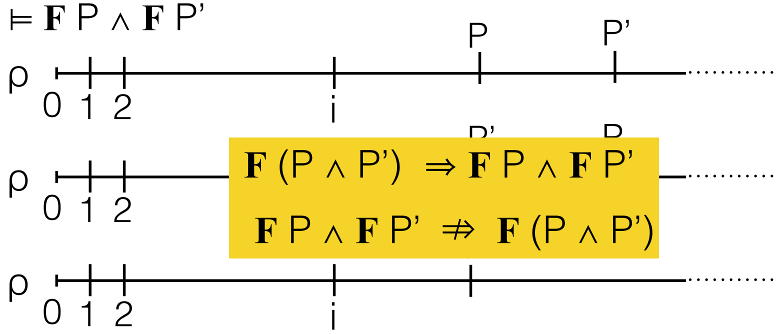
Rappel:
Avec les logiques de temps linéaire, le comportement d'un système est vu comme l'ensemble de ses exécutions prises séparément.

$\mathbf{S} \models \phi$ si et seulement si $\rho,0 \models \phi \quad \forall\, \rho \in Exec(q_0)$

Exemples de formules

Comparer $\mathbf{F}\, P \wedge \mathbf{F}\, P'$ et $\mathbf{F}\,(P \wedge P')$

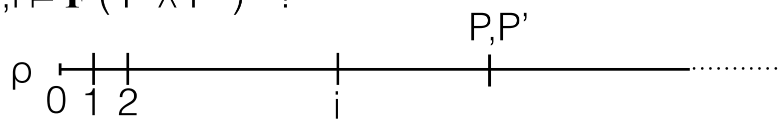
$\rho, i \models \mathbf{F}\, P \wedge \mathbf{F}\, P'$



$\mathbf{F}\,(P \wedge P') \Rightarrow \mathbf{F}\, P \wedge \mathbf{F}\, P'$

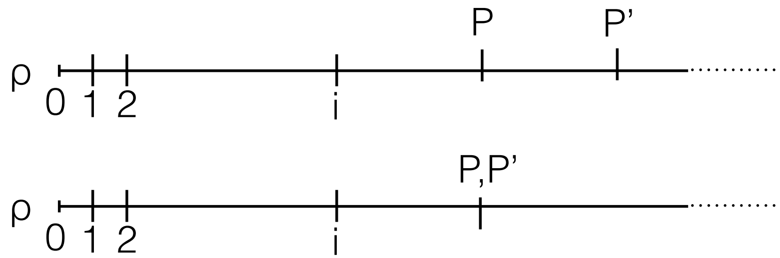
$\mathbf{F}\, P \wedge \mathbf{F}\, P' \not\Rightarrow \mathbf{F}\,(P \wedge P')$

$\rho, i \models \mathbf{F}\,(P \wedge P')$?

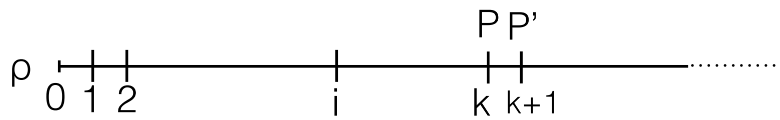


Exemples de formules

$\rho, i \models \mathbf{F}\,(P \wedge \mathbf{F}\, P')$?

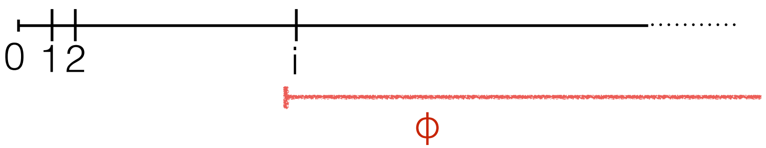


$\rho, i \models \mathbf{F}\,(P \wedge \mathbf{X}\, P')$?



Exemples de formules

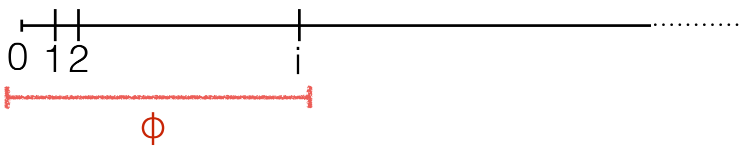
$\rho, i \models \neg\, \mathbf{F} \neg \phi$??



→ ϕ est vrai pour tous les états i, i+1, i+2,…
« toujours dans le futur »
On le note: $\mathbf{G}\, \phi = \neg\, \mathbf{F} \neg \phi$

Exemples de formules

$\rho, i \models \neg\, \mathbf{F}^{-1} \neg \phi$??



→ ϕ est vrai pour tous les états du passé: i, i-1, i-2…
« toujours dans le passé »
On le note: $\mathbf{G}^{-1}\, \phi = \neg\, \mathbf{F}^{-1} \neg \phi$

Exemples de formules

$\rho, i \models \neg \mathbf{X}\, \phi$

$\Leftrightarrow \ \rho, i \models \mathbf{X}\, \neg \phi$ (car exécutions infinies)

(sans cette hypothèse, on aurait:
$\rho, i \models \mathbf{X}\, \neg \phi \quad \Rightarrow \quad \rho, i \models \neg \mathbf{X}\, \phi$)

Exemples de formules

$\mathbf{G}$ (problème $\Rightarrow \mathbf{F}$ alarme)

$\mathbf{G}$ (alarme $\Rightarrow \mathbf{F}^{-1}$ problème)

$\mathbf{G}$ (request $\Rightarrow \mathbf{F}$ service)

$\mathbf{G}$ ($\neg$ bug)

Exemples de formules

$\mathbf{G}\, \mathbf{F}$ accueil

$\mathbf{F}\, \mathbf{G}$ ok

$\mathbf{GF}$ request $\Rightarrow \mathbf{GF}$ service

$\mathbf{GF}\,(a \wedge b)$ implique $\mathbf{GF}\, a \wedge \mathbf{GF}\, b$

$\mathbf{GF}\, a \wedge \mathbf{GF}\, b$ n'implique pas $\mathbf{GF}\,(a \wedge b)$

Exclusion mutuelle (suite)

- Exclusion mutuelle: Jamais les deux processus ne peuvent se trouver en SC au même moment.
  $\neg \mathbf{F}\,(SC_1 \wedge SC_2)$ $\qquad \mathbf{G}\,(\neg SC_1 \vee \neg SC_2)$
- Il n'y a jamais pas de blocage.
  $\mathbf{G}\,(\mathbf{X}\, \top)$ (NB: toujours vrai si $\rightarrow$ est totale)
- Absence de famine: Si un processus demande l'accès à la SC, il y arrivera un jour.
  $\mathbf{G}\,(D_1 \Rightarrow \mathbf{F}\; SC_1) \wedge \mathbf{G}\,(D_2 \Rightarrow \mathbf{F}\; SC_2)$
- Attente bornée: Si un processus demande l'accès à la SC, l'autre processus ne peut pas passer avant lui plus d'une fois.

il nous manque encore un opérateur… patience !

LTL

Syntaxe: $P \in AP$

$\phi,\psi ::= P \mid \neg\phi \mid \phi\vee\psi \mid \phi\wedge\psi \mid \mathbf{X}\,\phi \mid \psi\mathbf{U}\phi \mid \mathbf{X}^{-1}\,\phi \mid \psi\mathbf{S}\phi$

$\mathbf{U}$ = until $\mathbf{S}$ = since

$\rho,i \models \mathbf{X}\,\phi$ ssi $\rho,i+1 \models \phi$

$\rho,i \models \psi\mathbf{U}\phi$ ssi ($\exists\, j \geq i.$ ($\rho,j \models \phi$ et $\forall\, i\leq k<j$ on a $\rho,k \models \psi$)

$\rho,i \models \mathbf{X}^{-1}\,\phi$ ssi ($i>0$ et $\rho,i-1 \models \phi$)

$\rho,i \models \psi\mathbf{S}\phi$ ssi ($\exists\, j \leq i.$ ($\rho,j \models \phi$ et $\forall\, j<k\leq i$ on a $\rho,k \models \psi$)

Exemples de formules

$\mathbf{F}\,\phi$ = ?

$\mathbf{F}\,\phi = \top\ \mathbf{U}\ \phi$

def:

$\rho,i \models \mathbf{F}\,\phi$ ssi ($\exists\, j \geq i.$ $\rho,j \models \phi$)

$\rho,i \models \psi\mathbf{U}\phi$ ssi ($\exists\, j \geq i.$ ($\rho,j \models \phi$ et $\forall\, i\leq k<j$ on a $\rho,k \models \psi$)

$\rho,i \models \top\mathbf{U}\phi$ ssi ($\exists\, j \geq i.$ ($\rho,j \models \phi$ et $\forall\, i\leq k<j$ on a $\rho,k \models \top$)

$\Leftrightarrow$

($\exists\, j \geq i.$ $\rho,j \models \phi$)

$\Leftrightarrow$

$\rho,i \models \mathbf{F}\phi$

Exemples de formules

$\mathbf{F}^{-1}\,\phi = \top\ \mathbf{S}\ \phi$

def:

$\rho,i \models \mathbf{F}^{-1}\,\phi$ ssi ($\exists\, j \leq i.$ $\rho,j \models \phi$)

$\rho,i \models \psi\mathbf{S}\phi$ ssi ($\exists\, j \leq i.$ ($\rho,j \models \phi$ et $\forall\, j<k\leq i$ on a $\rho,k \models \psi$)

$\rho,i \models \top\mathbf{S}\phi$ ssi ($\exists\, j \leq i.$ ($\rho,j \models \phi$ et $\forall\, j<k\leq i$ on a $\rho,k \models \top$)

$\Leftrightarrow$

($\exists\, j \leq i.$ $\rho,j \models \phi$)

$\Leftrightarrow$

$\rho,i \models \mathbf{F}^{-1}\,\phi$

Pourquoi utiliser la logique temporelle ?

- une bonne expressivité

→ on peut exprimer beaucoup de choses

- une sémantique naturelle,

→ facilement et succinctement

- de bonnes propriétés de décision

→ des algorithmes et des outils

- beaucoup d'extensions

→ pour les systèmes probabilistes, temps-réel, les jeux, les données,…

Problèmes de vérification

Model-checking:
input: un modèle (STE) $\boldsymbol{S}$ et une formule φ
output: oui ssi $\boldsymbol{S} \models \varphi$.

Satisfaisabilité:
input: une formule φ
output: oui ssi il existe un modèle $\boldsymbol{S}$ t.q. $\boldsymbol{S} \models \varphi$.
(+ $\boldsymbol{S}$ si il existe !)

Synthèse de contrôleur:
input: un modèle partiel $\boldsymbol{S}$ une formule φ
output: un « controleur » $\boldsymbol{C}$ t.q. $\boldsymbol{S} \times \boldsymbol{C} \models \varphi$.

Spécifier un système réactif

On distingue plusieurs grandes familles de propriétés:

Propriétés de sûreté (safety):
"une mauvaise chose n'arrive jamais".
Ex: il y a au plus un processus en section critique.

Propriétés de vivacité (liveness):
"de bonnes choses arrivent un jour".
Ex: chaque demande d'accès à la SC est satisfaite un jour.

Propriétés d'équité (fairness):
→ Vérification d'exécution équitable.
Ex: Chaque processus doit « avancer » infiniment souvent.

Et encore de nouvelles modalités !

Weak until :

$$\rho,i \models \psi\ \mathbf{W}\ \phi \quad = \quad \text{ssi } (\ \forall\, k \geq i,\ \rho,k \models \psi \quad \text{ou} \quad \exists\, j \geq i.\ (\rho,j \models \phi \text{ et } \forall\, i \leq k < j \text{ on a } \rho,k \models \psi\ )$$

$$\rho,i \models \psi\ \mathbf{W}\ \phi \quad \Leftrightarrow \quad \rho,i \models \mathbf{G}\,\psi \ \vee\ \psi\ \mathbf{U}\ \phi \qquad (\forall\, \rho,\ \forall\, i)$$

Notation: $\psi\ \mathbf{W}\ \phi \quad \equiv \quad \mathbf{G}\,\psi \ \vee\ \psi\ \mathbf{U}\ \phi$

Definition:
$\phi \equiv \psi$ ssi ($\forall\, \rho,\ \forall\, i$, on a : $\rho,i \models \phi \Leftrightarrow \rho,i \models \psi$)

Et encore de nouvelles modalités !

Release

$$\rho,i \models \psi\ \mathbf{R}\ \phi \quad = \quad \text{ssi } (\ \forall\, k \geq i,\ (\rho,k \models \phi \text{ ou } \exists\, i \leq j < k\ \rho,j \models \psi\ ))$$

$$\rho,i \models \psi\ \mathbf{R}\ \phi \quad \Leftrightarrow \quad \rho,i \models \phi\ \mathbf{W}\ (\psi \wedge \phi) \qquad (\forall\, \rho,\ \forall\, i)$$

$$\psi\ \mathbf{R}\ \phi \quad \equiv \quad \phi\ \mathbf{W}\ (\psi \wedge \phi)$$