

Expression d'une politique, compatibilité d'un système vis à vis d'une politique

Julien Brunel

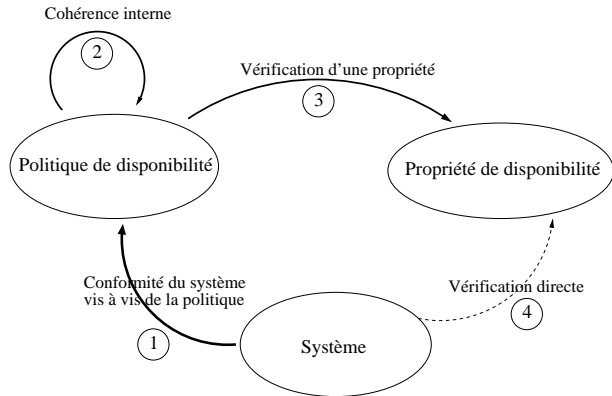
Institut de Recherche en Informatique de Toulouse

8-9 juin 2006 / Projet DISPO

Plan

- 1 Introduction
- 2 Formalisation de la problématique
 - Spécification d'une politique avec *SED-LTL*
 - Système et respect d'une politique
- 3 Produit de logiques
 - Concept pour l'expression de deux modalités
 - Sémantique du produit
- 4 Perspectives

Problématique



Différents concepts

Nous allons étudier la formalisation de différents concepts :

- langage pour spécifier une politique
 - ▷ cohérence interne d'une politique
 - ▷ s'assurer qu'une politique garantit une propriété
- modèle de comportement (temporisé)
- respect de la politique par un système
 - ▷ vérifier
 - ▷ contraindre

Plan

- 1 Introduction
- 2 **Formalisation de la problématique**
 - Spécification d'une politique avec *SED-LTL*
 - Système et respect d'une politique
- 3 Produit de logiques
 - Concept pour l'expression de deux modalités
 - Sémantique du produit
- 4 Perspectives

Expression de la politique

Formalisme basé sur

- la logique temporelle
- la logique déontique

Quelle logique ?

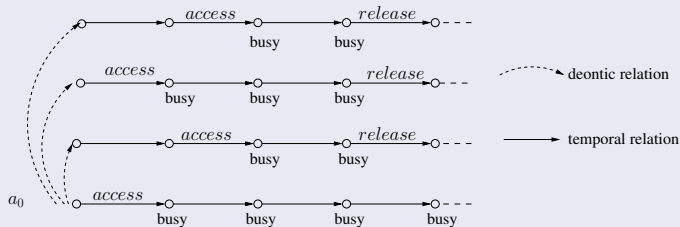
- Temps arborescent/linéaire
 - Actions / événements
 - Interaction entre les deux dimensions (déontique et temporelle)
- ⇒ [DEON'06] "A state/event temporal deontic logic" *SED-LTL*

SED-LTL

Syntaxe

$$\varphi ::= p \in P \mid e \in \mathcal{E} \mid \perp \mid \varphi \Rightarrow \varphi \mid \varphi U^+ \varphi \mid \mathbf{O}(\varphi)$$

Sémantique

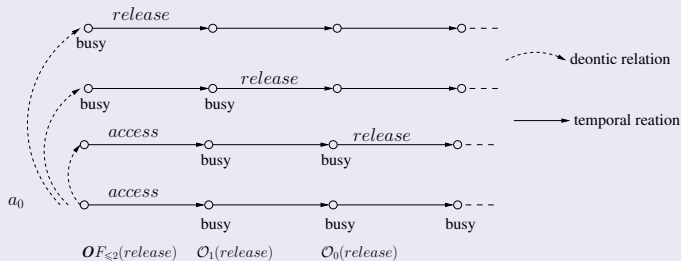


Obligation avec délai

Sémantique

$$\begin{aligned}
 a, \tau, i \models \mathcal{O}_k(\varphi) \text{ iff } & \exists k' \in \mathbb{N} & a, \tau, i - k' \models & \mathbf{OF}_{\leq k+k'} \varphi \\
 & \wedge \nexists k'' < k + k' & a, \tau, i - k' \models & \mathbf{OF}_{\leq k''} \varphi \\
 & & & \wedge \neg \varphi \mathbf{U}_{=k'} \top
 \end{aligned}$$

Illustration



La politique

Une formule de *SED-LTL*

- Si s_1 demande la ressource et s_2 ne l'utilise pas, alors s_1 est autorisé à l'utiliser

$$A\Box (request_1 \wedge \neg busy_2 \Rightarrow \mathbf{P} busy_1)$$

- Si s_i utilise la ressource sans permission, alors sanction

$$A\Box (busy_i \wedge \mathbf{I}(busy_i) \Rightarrow sanction)$$

- Si s_i demande la ressource et a la permission de l'utiliser, alors il a l'obligation de l'utiliser avant 10 unités de temps.

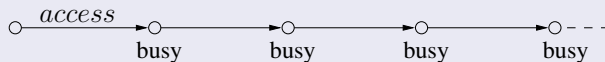
$$A\Box (request_i \wedge \mathbf{P} busy_i \Rightarrow \mathcal{O}_{10} busy_i)$$

Plan

- 1 Introduction
- 2 **Formalisation de la problématique**
 - Spécification d'une politique avec *SED-LTL*
 - **Système et respect d'une politique**
- 3 Produit de logiques
 - Concept pour l'expression de deux modalités
 - Sémantique du produit
- 4 Perspectives

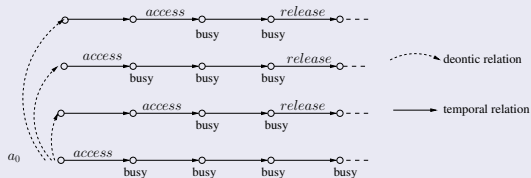
Le système

Ensemble de traces états/événements

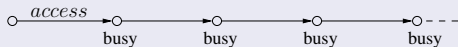


Extension déontique

Trace état/événement déontique



Trace état/événement



$$\bar{\tau} \stackrel{\text{def}}{=} \{ \tau^* \mid \tau^* \text{ est une extension déontique de } \tau \}$$

Respect d'une politique

Une trace temporelle respecte une politique

$\tau \models_{resp} Policy$ ssi $\exists \tau^* \in \bar{\tau}$ telle que $\tau^* \models_{SED LTL} Policy$

Le système respecte une politique

$System \models_{resp} Policy$ ssi $\forall \tau \in System \tau \models_{resp} Policy$

Système contraint par la politique

Système contraint

Définition : ensemble des traces (temporelles) du système qui “respectent” la politique.

$$\mathit{System}_{/Policy} \stackrel{\text{def}}{=} \{ \tau \in \mathit{System} \mid \tau \models_{\text{resp}} \mathit{Policy} \}$$

Propriétés

Commutativité du diagramme introductif

Si $System \models_{resp} Policy$ et $\models_{SEDLTL} Policy \Rightarrow \varphi$ Alors

$$System \models_{SELTL} \varphi$$

Lien entre $System_f$ et $System$

- $System_f$: *SE-LTL*-formule modélisant le système
- $System$: ensemble des traces qui satisfont $System_f$

$System_f \wedge Policy$ satisfiable

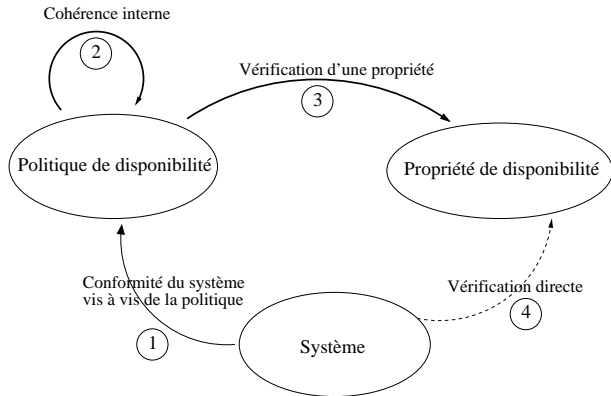
\Leftrightarrow

$System$ peut être contraint par $Policy$ ($System_{/Policy} \neq \emptyset$)

Plan

- 1 Introduction
- 2 Formalisation de la problématique
 - Spécification d'une politique avec *SED-LTL*
 - Système et respect d'une politique
- 3 Produit de logiques**
 - **Concept pour l'expression de deux modalités**
 - Sémantique du produit
- 4 Perspectives

Besoin d'un outil



Produit

Logique modale L_1 (pour nous *SELTL*)

$$\varphi ::= p \in P \mid \perp \mid \varphi \Rightarrow \varphi \mid \Box_1(\varphi)$$

Logique modale L_2 (pour nous *SDL*)

$$\varphi ::= p \in P \mid \perp \mid \varphi \Rightarrow \varphi \mid \Box_2(\varphi)$$

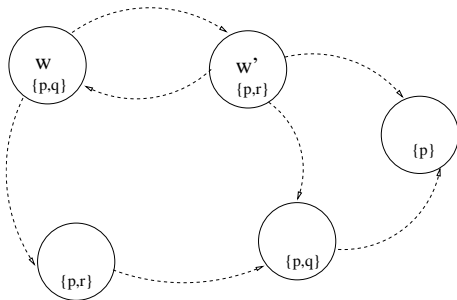
Langage de $L_1 \times L_2$

$$\varphi ::= p \in P \mid \perp \mid \varphi \Rightarrow \varphi \mid \Box_1(\varphi) \mid \Box_2(\varphi)$$

Plan

- 1 Introduction
- 2 Formalisation de la problématique
 - Spécification d'une politique avec *SED-LTL*
 - Système et respect d'une politique
- 3 **Produit de logiques****
 - Concept pour l'expression de deux modalités
 - Sémantique du produit**
- 4 Perspectives

Logiques modales



Sémantique de $\Box\varphi$

$$w \models \Box\varphi \quad \text{ssi} \quad \forall w' \quad (w, w') \in R \Rightarrow w' \models \varphi$$

Logiques produits

Structures de Kripke

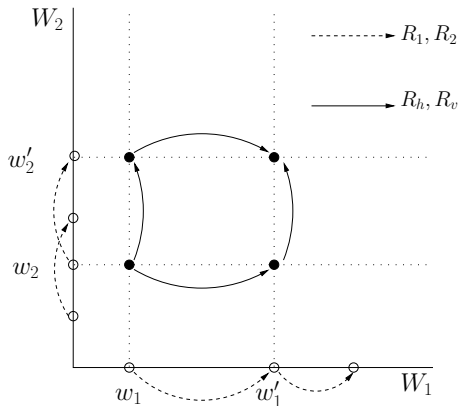
$F_1 = (W_1, R_1)$ et $F_2 = (W_2, R_2)$ 2 structures de Kripke.

Produit $F_1 \times F_2$

$F_1 \times F_2 \stackrel{\text{def}}{=} (W_1 \times W_2, R_h, R_v)$ où

- $(w_1, w_2)R_h(w'_1, w'_2)$ ssi $w_1 R_1 w'_1$ et $w_2 = w'_2$
- $(w_1, w_2)R_v(w'_1, w'_2)$ ssi $w_2 R_2 w'_2$ et $w_1 = w'_1$

Logiques produits(2)



Propriétés

• **Commutativité**

$$\Rightarrow \Box_1 \Box_2 p \Leftrightarrow \Box_2 \Box_1 p$$

• **Church Rosser**

$$\Rightarrow \Diamond_1 \Box_2 p \Rightarrow \Box_2 \Diamond_1 p$$

Logiques produits(3)

Propriétés sur les produits

- Pas de résultat général
- $K \times K$ décidable, propriété du modèle fini, complexité non élémentaire
- $LTL \times S4$ indécidable
- $LTL \times K$ décidable, pas la propriété du modèle fini, complexité non élémentaire

Cohérence interne

Propriétés de *SED-LTL*

SED-LTL est très proche du produit $KD \times LTL$.

- piste pour prouver la décidabilité de *SED-LTL*
- procédure de décision non élémentaire

Applications

- Cohérence d'une politique
- ⇒ Satisfiabilité de la formule *Policy*
- La politique garantit une propriété temporelle φ
- ⇒ Validité de *Policy* ⇒ φ

Perspectives

- Démontrer formellement la décidabilité de *SED-LTL*
- Étendre la procédure de décision à \mathcal{O}_k
- Cas d'étude