

Étude des logiques déontique et temporelle pour la disponibilité

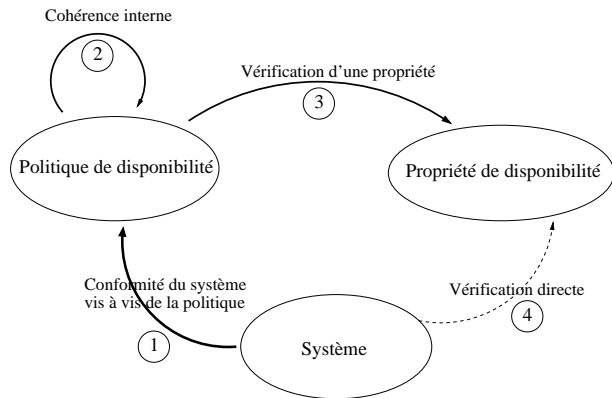
Institut de Recherche en Informatique de Toulouse

Julien Brunel, Jean-Paul Bodeveix, Mamoun Filali-Amine

22 septembre 2006 / Projet DISPO

- 1 Introduction
- 2 Combinaison des langages temporel et déontique
 - Temps arborescent
 - Temps linéaire
 - Opérateur d'obligation avec délai
- 3 Définition de propriétés d'une politique
 - Cohérence d'une politique
 - Système et respect d'une politique
 - Produit de logiques
- 4 Exemple
 - Description de l'exemple
 - Respect de la politique
- 5 Perspectives

Problématique



Différents aspects

- Spécifier une politique
 - ▷ Temps arborescent/linéaire
 - ▷ Actions / événements
 - ▷ Interaction entre les deux dimensions (déontique et temporelle)
 - Respect de la politique par un système
 - ▷ vérifier
 - ▷ contraindre
- ⇒ Utilisation des produits de logiques

Plan

- 1 Introduction
- 2 **Combinaison des langages temporel et déontique**
 - **Temps arborescent**
 - Temps linéaire
 - Opérateur d'obligation avec délai
- 3 Définition de propriétés d'une politique
 - Cohérence d'une politique
 - Système et respect d'une politique
 - Produit de logiques
- 4 Exemple
 - Description de l'exemple
 - Respect de la politique
- 5 Perspectives

SED-CTL*

Syntaxe

$$\Phi ::= p \in Prop \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid A\Pi \mid O\Phi$$

$$\Pi ::= \Phi \mid a \in \mathcal{E} \mid \neg\Pi \mid \Pi_1 \wedge \Pi_2 \mid \Pi_1 \mathcal{U}^+ \Pi_2$$

Sémantique

- Basé sur une structure de Kripke
- 2 relations d'accessibilité (déontique et temporelle)
 - ⇒ La relation déontique porte
 - sur les états (instants) ou
 - sur les modèles temporels

Plan

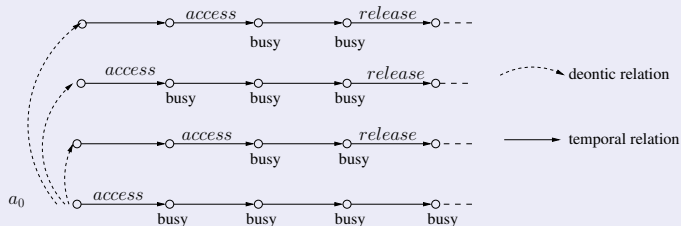
- 1 Introduction
- 2 **Combinaison des langages temporel et déontique**
 - Temps arborescent
 - **Temps linéaire**
 - Opérateur d'obligation avec délai
- 3 Définition de propriétés d'une politique
 - Cohérence d'une politique
 - Système et respect d'une politique
 - Produit de logiques
- 4 Exemple
 - Description de l'exemple
 - Respect de la politique
- 5 Perspectives

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



Propriétés non intuitives

S'il est obligatoire de satisfaire φ avant un délai k , l'obligation se propage tant que φ n'est pas satisfaite.

$$\not\models \mathbf{O}(F_{\leq k}\varphi) \wedge \neg\varphi \Rightarrow \mathbf{X}\mathbf{O}(F_{\leq k-1}\varphi)$$

Deux pistes explorées

- Définir un opérateur dédié à l'obligation avec délai
- Changer la sémantique pour augmenter l'interaction entre les faits et les obligations

Plan

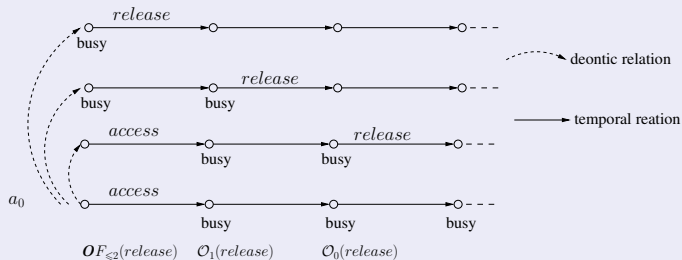
- 1 Introduction
- 2 **Combinaison des langages temporel et déontique**
 - Temps arborescent
 - Temps linéaire
 - **Opérateur d'obligation avec délai**
- 3 Définition de propriétés d'une politique
 - Cohérence d'une politique
 - Système et respect d'une politique
 - Produit de logiques
- 4 Exemple
 - Description de l'exemple
 - Respect de la politique
- 5 Perspectives

Opérateur d'obligation avec délai

Sémantique

$$\begin{aligned}
 (i, w) \models \mathcal{O}_{\leq k}(\varphi) \quad \text{ssi} \quad & \exists k' \in \mathbb{N} & (i - k', w) & \models \mathbf{OF}_{\leq k+k'} \varphi \\
 & \text{et} & (i - k', w) & \not\models \mathbf{OF}_{\leq k+k'-1} \varphi \\
 & \text{et} \quad \forall i - k' \leq j < i & (j, w) & \models \mathbf{P}\varphi \Rightarrow \neg \varphi
 \end{aligned}$$

Illustration



Propriétés de l'obligation avec délai

Propagation lors du non respect

$$\models \mathcal{O}_{\leq k}(\varphi) \wedge \neg\varphi \Rightarrow X\mathcal{O}_{\leq k-1}(\varphi)$$

Propagation lors d'une interdiction

$$\models \mathcal{O}_{\leq k}(\varphi) \wedge \mathbf{O}\neg\varphi \Rightarrow X\mathcal{O}_{\leq k-1}(\varphi)$$

Commutativité avec X

$$\models \mathcal{O}_{\leq k}(X\varphi) \Leftrightarrow X\mathcal{O}_{\leq k}(\varphi)$$

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

$$G (\text{request}_1 \wedge \neg \text{busy}_2 \Rightarrow \mathbf{P} \text{ busy}_1)$$

- Si s_i utilise la ressource sans permission, alors sanction

$$G (\text{busy}_i \wedge \mathbf{I}(\text{busy}_i) \Rightarrow \text{sanction})$$

- 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.

$$G (\text{request}_i \wedge \mathbf{P} \text{ busy}_i \Rightarrow \mathcal{O}_{\leq 10} \text{ busy}_i)$$

Plan

- 1 Introduction
- 2 Combinaison des langages temporel et déontique
 - Temps arborescent
 - Temps linéaire
 - Opérateur d'obligation avec délai
- 3 **Définition de propriétés d'une politique**
 - **Cohérence d'une politique**
 - Système et respect d'une politique
 - Produit de logiques
- 4 Exemple
 - Description de l'exemple
 - Respect de la politique
- 5 Perspectives

Cohérence d'une politique

- Une politique est modélisée par une formule *Policy*.
- La politique est cohérente ssi *Policy* est satisfiable.

Exemples d'incohérence dans une politique

$$Op \wedge Ip$$

$$Pp \wedge Ip$$

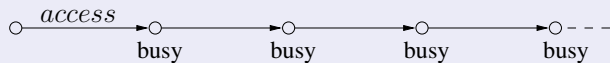
$$O_{\leq k} p \wedge O(G_{\leq k} \neg p)$$

Plan

- 1 Introduction
- 2 Combinaison des langages temporel et déontique
 - Temps arborescent
 - Temps linéaire
 - Opérateur d'obligation avec délai
- 3 **Définition de propriétés d'une politique**
 - Cohérence d'une politique
 - **Système et respect d'une politique**
 - Produit de logiques
- 4 Exemple
 - Description de l'exemple
 - Respect de la politique
- 5 Perspectives

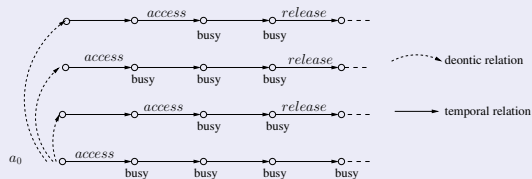
Le système

Ensemble de traces états/événements

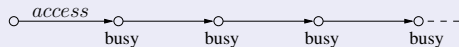


Extension déontique

Trace état/événement déontique



Trace état/événement



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

Respect d'une politique

Une trace temporelle respecte une politique

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

$\Rightarrow \tau^*$ est constructible si *SED-LTL* est décidable.

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.

$$\mathbf{System}_{/Policy} \stackrel{def}{=} \{ \tau \in \mathbf{System} / \tau \models_{resp} \mathbf{Policy} \}$$

Propriétés

Commutativité du diagramme introductif

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

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

Lien entre φ_{System} et $System$

- φ_{System} : SE-LTL-formule modélisant le système
- $System$: ensemble des traces qui satisfont φ_{System}

$\varphi_{System} \wedge Policy$ satisfiable

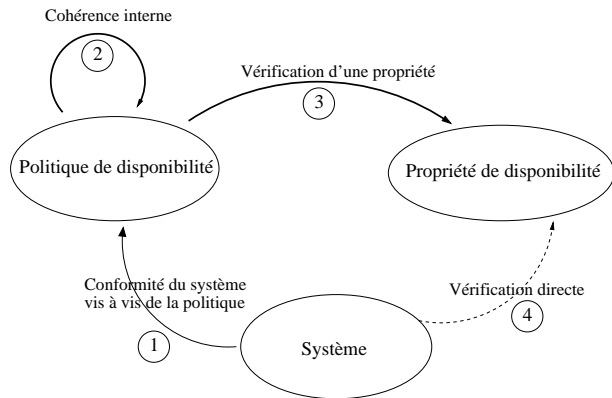
\Leftrightarrow

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

Plan

- 1 Introduction
- 2 Combinaison des langages temporel et déontique
 - Temps arborescent
 - Temps linéaire
 - Opérateur d'obligation avec délai
- 3 Définition de propriétés d'une politique**
 - Cohérence d'une politique
 - Système et respect d'une politique
 - Produit de logiques**
- 4 Exemple
 - Description de l'exemple
 - Respect de la politique
- 5 Perspectives

Techniques de vérification



Produit

Logique modale L_1 (pour nous *SELTL*)

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

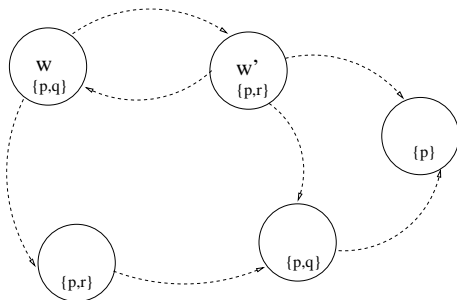
Logique modale L_2 (pour nous *SDL*)

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

Langage de $L_1 \times L_2$

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

Logiques modales



Sémantique de $\Box\varphi$

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

Logiques produits

Structures de Kripke

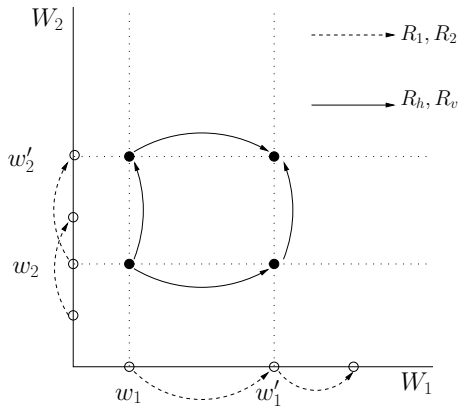
$F_1 = (W_1, R_1)$ et $F_2 = (W_2, R_2)$ 2 structures de Kripke.

Produit $F_1 \times F_2$

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

Vérification

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

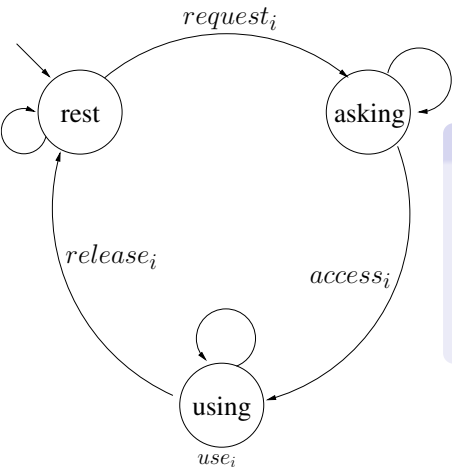
Applications

- Cohérence d'une politique
- ⇒ Satisfiabilité de la formule *Policy*
- La politique garantit un propriété temporelle φ
- ⇒ Validité de *Policy* $\Rightarrow \varphi$
- Le système peut être contraint par la politique
- ⇒ Satisfiabilité de $\varphi_{System} \wedge Policy$

Plan

- 1 Introduction
- 2 Combinaison des langages temporel et déontique
 - Temps arborescent
 - Temps linéaire
 - Opérateur d'obligation avec délai
- 3 Définition de propriétés d'une politique
 - Cohérence d'une politique
 - Système et respect d'une politique
 - Produit de logiques
- 4 **Exemple**
 - **Description de l'exemple**
 - Respect de la politique
- 5 Perspectives

Le système, un ordonnanceur générique



Contraintes de l'ordonnanceur :

- Exclusion mutuelle :
 $G\neg(use_1 \wedge use_2)$
- Traitement des demandes :
 $G(request_1 \vee request_2 \Rightarrow F(access_1 \vee access_2))$

La politique

Les deux utilisateurs ont la permission d'utiliser la ressource à l'initialisation, et au moins jusqu'à leur premier accès.

$P_{use_i} U_{access_i}$ (règle 1)

Si un utilisateur reste 6 unités de temps sans utiliser la ressource, il a la permission d'y accéder

$G(G_{\leq 6} \neg use_i \Rightarrow F_{=6} P_{access_i})$ (règle 2)

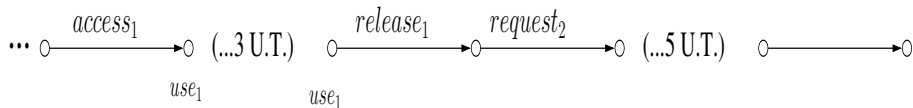
Les utilisateurs ont l'obligation de libérer la ressource au plus tard 5 unités de temps après y avoir accéder.

$G(access_i \Rightarrow O_{\leq 5} release_i)$ (règle 3)

Plan

- 1 Introduction
- 2 Combinaison des langages temporel et déontique
 - Temps arborescent
 - Temps linéaire
 - Opérateur d'obligation avec délai
- 3 Définition de propriétés d'une politique
 - Cohérence d'une politique
 - Système et respect d'une politique
 - Produit de logiques
- 4 **Exemple**
 - Description de l'exemple
 - **Respect de la politique**
- 5 Perspectives

Respect de la politique ?



Politique

$$G(\text{request}_i \wedge \mathbf{P}use_i \Rightarrow \mathcal{O}_{\leq 5} \text{access}_i)$$

$$G(\mathbf{O} \text{access}_i \Rightarrow \text{access}_i)$$

+ règles 1,2,3

Le comportement ci-dessus ne respecte pas la politique

Perspectives

- Démontrer formellement la décidabilité de *SED-LTL*
- Étendre la procédure de décision à \mathcal{O}_k
- Et pour *SED-CLT** ?
- Extension aux agents (utilisation de *ATL*)