

Logique déontique, logique temporelle, spécification de la disponibilité

Julien Brunel

Institut de Recherche en Informatique de Toulouse

23 septembre 2005 / Projet DISPO

Plan

- 1 Logique déontique-temporelle
 - Exprimer des politiques
 - Quelle logique
- 2 Vers une logique d'action étendue
 - Rappels
 - Langage plus simple
- 3 Vérification
 - Consistence et non violation
- 4 Conclusion & Perspectives
- 5 Collaboration avec Hervé

Plan

- 1 Logique déontique-temporelle
 - Exprimer des politiques
 - Quelle logique
- 2 Vers une logique d'action étendue
 - Rappels
 - Langage plus simple
- 3 Vérification
 - Consistence et non violation
- 4 Conclusion & Perspectives
- 5 Collaboration avec Hervé

Politiques de disponibilité

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

$$A\Box (demande(s_1, r) \wedge \neg utilise(s_2, r) \Rightarrow \mathbf{P} utilise(s_1, r))$$

- Lorsque s_2 libère la ressource, s_1 a la permission de l'utiliser pendant 4 unités de temps.

$$A\Box (libere(s_2, r) \Rightarrow A\Box_{\leq 4} \mathbf{P}(utilise(s_1, r)))$$

- 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.

$$A\Box (demande(s_i, r) \wedge \mathbf{P} utilise(s_1, r) \Rightarrow \mathbf{O}_{\leq 10} utilise(s_1, r))$$

Politiques de disponibilité

Raisonner sur la violation

Si j'utilise la ressource sans permission, alors sanction

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

Plan

- 1 Logique déontique-temporelle
 - Exprimer des politiques
 - **Quelle logique**
- 2 Vers une logique d'action étendue
 - Rappels
 - Langage plus simple
- 3 Vérification
 - Consistence et non violation
- 4 Conclusion & Perspectives
- 5 Collaboration avec Hervé

CTL + déontique

Logique choisie

$\phi, \psi ::= p \in Prop \mid \neg\phi \mid \phi \wedge \psi \mid AX\phi \mid A(\phi \mathcal{U} \psi) \mid E(\phi \mathcal{U} \psi) \mid \mathbf{O}(\phi)$
où $Prop$ est l'ensemble des propositions atomiques.

Modèles

Modèle de CTL + relation déontique (qui donne sa sémantique à \mathbf{O})

Lien déontique-temporel

Quelles propriétés relient obligation et temps ?

“Axiomatique”

$\forall \phi$

$$(1) \text{ AX } \mathbf{O}(\phi) \Leftrightarrow \mathbf{O}(\text{AX } \phi)$$

$$(2) \text{ AX } \mathbf{P}(\phi) \Leftrightarrow \mathbf{P}(\text{AX } \phi)$$

Modèles

- (1) est traduit par une contrainte sur les modèles (analogie avec du raffinement)
- la deuxième contrainte sur les modèles est plus forte que (2)

Plan

- 1 Logique déontique-temporelle
 - Exprimer des politiques
 - Quelle logique
- 2 **Vers une logique d'action étendue**
 - **Rappels**
 - Langage plus simple
- 3 Vérification
 - Consistence et non violation
- 4 Conclusion & Perspectives
- 5 Collaboration avec Hervé

États, actions

États, actions

Nécessité d'utiliser

- des états : *utilise, oisif*
- des actions : *libere, accede*

Obligations

Il faut distinguer

- l'obligation d'être $O(\phi)$
- l'obligation de faire $O(\alpha)$

Logiques temporelles d'action

Extension de *CTL*

- Etend la logique temporelle avec des actions atomiques.
- *ATCTL* est une extension de *TCTL*. Le \mathcal{U} est indexé par une action atomique (on autorise le “ou” et le “not” sur les actions, mais pas la séquence).
- *ATCTL* se réduit à *TCTL*

Extension de *LTL*

- Une action est un langage régulier (plus expressif)
- *DLTL* est une extension de *LTL*. Le \mathcal{U} est indexé par une action.
- Expressivité de S1S.

Logique dynamique

Langage sur les actions

- ensemble d'actions atomiques $\mathcal{A} = \{a, b \dots\}$
- ensemble d'actions
 $\Sigma_{action} \ni \alpha, \beta \stackrel{def}{=} a \mid \neg\alpha \mid \alpha + \beta \mid \alpha; \beta \mid \alpha^*$

Opérateurs de la logique dynamique

$\langle \alpha \rangle \phi$ Il existe un état accessible en exécutant α qui satisfait ϕ .
 $[\alpha] \phi$ Tous les états accessibles en exécutant α satisfont ϕ

Modèle déontique dynamique obtenu en mai

Langage

$Prop$ propositions atomiques

\mathcal{A} et $\Sigma_{actions}$ actions resp. atomiques et complexes

$E \phi$ $U^\alpha \psi$, $A \phi$ $U^\alpha \psi$, $O(\phi)$.

Modèle

- W ensemble d'états
- $\nu : W \rightarrow 2^{Prop}$ valuation
- $R_o \subseteq W \times W$ relation déontique
- $\delta \subseteq W \times \mathcal{A} \times W$ relation de transition

Opérateurs supplémentaires (en mai)

Quelques opérateurs dynamiques temporels

$$E\langle\alpha\rangle\phi \stackrel{def}{=} E \top U^\alpha \phi$$

$$A\langle\alpha\rangle\phi \stackrel{def}{=} A \top U^\alpha \phi$$

$$E[\alpha]\phi \stackrel{def}{=} \neg E\langle\alpha\rangle\neg\phi$$

$$A[\alpha]\phi \stackrel{def}{=} \neg A\langle\alpha\rangle\neg\phi$$

$$E\Diamond\alpha \stackrel{def}{=} E \top U^{\Diamond\alpha} \top$$

$$A\Diamond\alpha \stackrel{def}{=} A \top U^{\Diamond\alpha} \top$$

$$\Diamond\alpha \stackrel{def}{=} \mathcal{A}^*; \alpha$$

Opérateurs déontiques

$$\mathcal{O}(\alpha) \stackrel{def}{=} \mathbf{O}(A \top U^\alpha \top)$$

obligation de faire α

$$\mathcal{I}(\alpha) \stackrel{def}{=} \mathbf{I}(E \top U^\alpha \top)$$

interdiction de faire α

$$\mathcal{P}(\alpha) \stackrel{def}{=} \neg\mathcal{I}(\alpha)$$

permission de faire α

Plan

- 1 Logique déontique-temporelle
 - Exprimer des politiques
 - Quelle logique
- 2 Vers une logique d'action étendue
 - Rappels
 - **Langage plus simple**
- 3 Vérification
 - Consistence et non violation
- 4 Conclusion & Perspectives
- 5 Collaboration avec Hervé

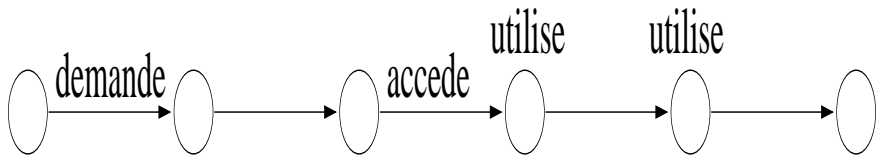
Langage déontique d'action

Syntaxe plus simple

- langage d'actions : a , $\neg\alpha$, $\alpha + \beta$ (pas de séquence d'actions)
- On place les actions et les propositions au même niveau dans la syntaxe (idée de Clarke, avec un temps linéaire)
- Pas de différence syntaxique obligation de faire / obligation d'être

La formule α signifie alors “je vais exécuter α au coup suivant”.

Illustration du Formalisme de Clarke



$$\square((\textit{demande} \wedge \neg \textit{utilise}) \Rightarrow \diamond \textit{accede})$$

Deux choix possibles

- Se baser sur *CTL**
 - Distinction entre formules de chemin et formules d'état
 - Interprétation naturelle des actions
 - Trop complexe, problème de disponibilité des outils de décision
- Se limiter à *CTL*
 - Interprétation moins naturelle
 - Langage plus simple
 - Plus efficace, outils connus, mais moins expressif

CTL* déontique

On distingue les formules d'état et de chemin

Formules d'état :

$\Phi ::= Prop \mid \neg\Phi \mid \Phi_1 \wedge \Phi_2 \mid A\phi \mid O\Phi$

Formules de chemin :

$\Pi ::= \Phi \mid a \in \Sigma_{action} \mid \neg\Pi \mid \Pi_1 \wedge \Pi_2 \mid \Pi_1 \mathcal{U} \Pi_2 \mid \Pi_1 \mathcal{U}_{\leq k} \Pi_2 \mid X\Pi$

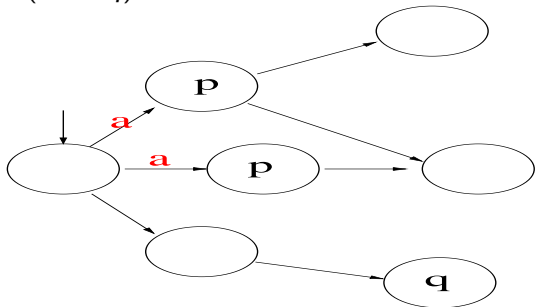
Opérateurs de logique dynamique

$[\alpha]\phi \stackrel{def}{=} A(\alpha \Rightarrow \phi)$

$\langle\alpha\rangle\phi \stackrel{def}{=} \neg[\alpha]\neg\phi$

Illustration de CTL^* déontique

$A(a \vee \diamond q)$



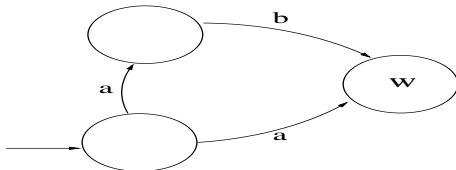
CTL déontique

Syntaxe

$\phi, \psi ::= p, \alpha, EX \phi, E \phi U \psi, A \phi U \psi, O(\phi)$

Sens de α : “**Je viens d’exécuter** α ”

Une formule s’interprète sur un couple (état, action par laquelle j’arrive à cet état)



$w, a \models a$
 $w, b \models \neg a$

Sémantique

$w, a \models p \in Prop$	$ssi \quad p \in \nu(w)$
$w, a \models \alpha \in \Sigma_{actions}$	$ssi \quad a \in \alpha$
$w, a \models AX \phi$	$ssi \quad \forall w', b \in W \times \mathcal{A}$ $\delta(w, b, w') \Rightarrow w', b \models \phi$
$w, a \models A(\phi \mathcal{U} \psi)$	$ssi \quad \forall \langle w_i, a_i \rangle_i$ chemin de \mathcal{M} partant de w $\exists i$ tel que $w_i, a_{i-1} \models \psi \wedge$ $\forall j < i \quad w_j, a_{j-1} \models \phi$
$w, a \models \mathbf{O}(\phi)$	$ssi \quad \forall w' \in W \quad wR_0 w'$ $\Rightarrow (\exists a \in \mathcal{A} \text{ tel que } w', a \models \phi)$

Plan

- 1 Logique déontique-temporelle
 - Exprimer des politiques
 - Quelle logique
- 2 Vers une logique d'action étendue
 - Rappels
 - Langage plus simple
- 3 Vérification**
 - Consistence et non violation**
- 4 Conclusion & Perspectives
- 5 Collaboration avec Hervé

Vérification de la consistance

Consistence de la politique

- Satisfiabilité d'une formule
⇒ méthode des tableaux
- Difficultés :
 - construire un modèle satisfaisant les contraintes (lien entre les relations déontique et temporelle)
 - s'assurer de la terminaison d'une telle construction

Vérification de la conformité

Point de départ

- Un système de transition *Systeme* représentant une modélisation du système informatique
- Une formule déontique temporelle *Politique* représentant la politique de disponibilité

Satisfiabilité

On doit construire un modèle (déontique temporel) $System_{mod}$ à partir de *Systeme* tel que

$$System_{mod} \models \phi \stackrel{def}{=} Politique \Rightarrow A\Box(O(p) \Rightarrow p)$$

pour un p bien choisi.

(idem avec $I(p) \Rightarrow \neg p$ et $p \Rightarrow P(p)$)

\Rightarrow Méthode des tableaux avec $\neg\phi$ en partant de *Systeme*

Conclusion & Perspectives

Conclusion

- Étude de la logique déontique
- Lien avec les logiques temporelle et dynamique
- Spécification de politiques de disponibilité

Perspectives

- Développement d'une méthode des tableaux pour l'extension de *CTL*
- Prise en compte d'agents
- Environnement de preuve pour notre formalisme

Collaboration avec Hervé

Etude de la disponibilité sur un système concret (un programme)

- Modélisation comportementale ?
- Prise en compte et évolution des obligations (test et mise à jour des obligations) ?
- Vérification de modèles :
Élimination des opérateurs déontiques (totale ou partielle)