# Logique déontique, logique temporelle, spécification de la disponibilité

Julien Brunel

Institut de Recherche en Informatique de Toulouse

23 septembre 2005 / Projet DISPO

# Plan

# Plan

# Politiques de disponibilité

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

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

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

$$A\Box\,(\mathit{libere}(s_2, r) \Rightarrow A\Box_{\leqslant 4}\,\boldsymbol{P}(\mathit{utilise}(s_1, r)))$$

- 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.

$$A\Box\,(\mathit{demande}(s_i, r) \wedge \boldsymbol{P}\,\mathit{utilise}(s_1, r) \;\Rightarrow\; \boldsymbol{O}_{\leqslant 10}\,\mathit{utilise}(s_1, r))$$

# 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

# *CTL* + déontique

## Logique choisie

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

## Modèles

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

# Lien déontique-temporel

Quelles propriétés relient obligation et temps ?

## "Axiomatique"

$\forall \phi$

(1) $AX\ \boldsymbol{O}(\phi) \Leftrightarrow \boldsymbol{O}(AX\ \phi)$

(2) $AX\ \boldsymbol{P}(\phi) \Leftrightarrow \boldsymbol{P}(AX\ \phi)$

## 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

# États, actions

## États, actions

Nécessité d'utiliser

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

## Obligations

Il faut distinguer

- l'obligation d'être $\boldsymbol{O}(\phi)$
- l'obligation de faire $\mathcal{O}(\alpha)$

# 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

$<\alpha>\phi$ Il existe un état accessible en exécutant $\alpha$ qui satisfait $\phi$ .
$[\alpha]\phi$ Tous les états accessibles en exécutant $\alpha$ satisfont $\phi$

# Modèle déontique dynamique obtenu en mai

## Langage

*Prop* propositions atomiques
$\mathcal{A}$ et $\Sigma_{actions}$ actions resp. atomiques et complexes
$E\ \phi\ \mathcal{U}^{\alpha}\ \psi$ , $A\ \phi\ \mathcal{U}^{\alpha}\ \psi$ , $\boldsymbol{O}(\phi)$.

## 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

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

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

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

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

## Opérateurs déontiques

$\mathcal{O}(\alpha) \stackrel{def}{=} \boldsymbol{O}(A\top\mathcal{U}^{\alpha}\top)$ obligation de faire $\alpha$

$\mathcal{I}(\alpha) \stackrel{def}{=} \boldsymbol{I}(E\top\mathcal{U}^{\alpha}\top)$ interdiction de faire $\alpha$

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

# Plan

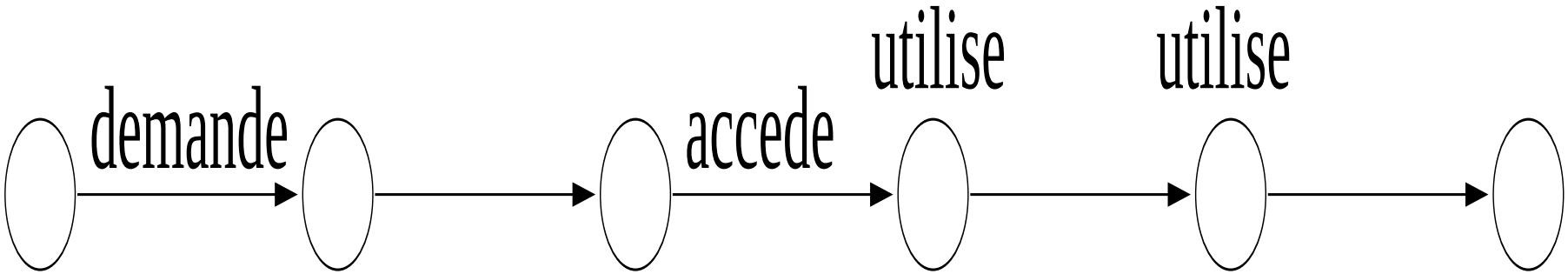
# Langage déontique d'action

## 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 $\alpha$ signifie alors "je vais exécuter $\alpha$ au coup suivant".

# Illustration du Formalisme de Clarke




$\Box((demande \wedge \neg utilise) \Rightarrow \Diamond accede)$

## 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 :

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

## Formules de chemin :

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

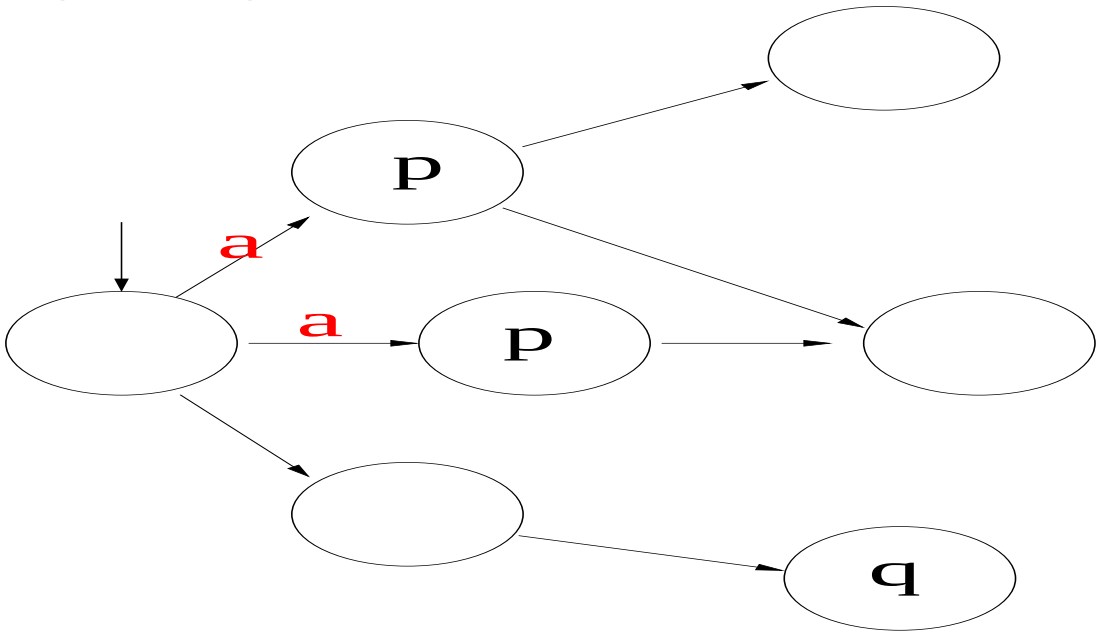
## Opérateurs de logique dynamique

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

$$<\alpha>\phi \stackrel{def}{=} \neg[\alpha]\neg\phi$$

# Illustration de $CTL^*$ déontique

$A(a \vee \Diamond q)$

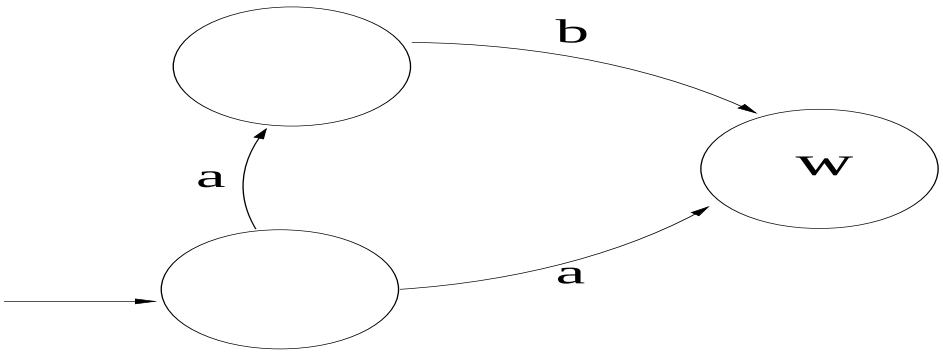


# *CTL* déontique

## Syntaxe

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

Sens de $\alpha$ : **"Je viens d'éxécuter $\alpha$"**
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

$$
\begin{array}{lll}
w, a \models p \in \mathit{Prop} & \mathit{ssi} & p \in \nu(w) \\
w, a \models \alpha \in \Sigma_{\mathit{actions}} & \mathit{ssi} & a \in \alpha \\
w, a \models \mathit{AX}\ \phi & \mathit{ssi} & \forall w', b \in W \times \mathcal{A} \\
 & & \delta(w, b, w') \Rightarrow w', b \models \phi \\
w, a \models A(\phi \mathcal{U} \psi) & \mathit{ssi} & \forall <w_i, a_i>_i \text{ chemin de } \mathcal{M} \text{ partant de } w \\
 & & \exists i \text{ tel que } w_i, a_{i-1} \models \psi \wedge \\
 & & \forall j < i\ w_i, a_{i-1} \models \phi \\
w, a \models \mathbf{O}(\phi) & \mathit{ssi} & \forall w' \in W\ wR_o w' \\
 & & \Rightarrow\ (\exists a \in \mathcal{A} \text{ tel que } w', a \models \phi)
\end{array}
$$

# Plan

# Vérification de la consistence

## Consistence de la politique

- Satisfiabilité d'une formule
  $\Rightarrow$ 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

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

pour un $p$ bien choisi.

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

$\Rightarrow$ 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) ?
- Vérifiaction de modèles :
  Élimination des opérateur déontiques (totale ou partielle)