Exigences, réglementations et contraintes

Laurence Cholvy	Christophe Garion
ONERA Toulouse	SUPAERO
2 av. Édouard Belin	10 av. Édouard Belin
31055 Toulouse Cedex 4	31055 Toulouse Cedex 4
cholvy@cert.fr	garion@supaero.fr

Résumé

Cet article s'intéresse à la modélisation des exigences et à l'expression de leur compatibilité avec une réglementation et des contraintes du domaine. Nous nous plaçons dans le cas où les exigences sont ordonnées selon un ordre de priorité. Le problème est alors de déterminer, parmi les exigences ordonnées de l'agent, les plus préférées qui sont compatibles avec la réglementation et avec les contraintes du domaine. Pour cela, nous proposons de modéliser les exigences, les réglementations et les contraintes dans un cadre formel unique, une logique de préférences conditionnelles. Le choix d'un formalisme unique nous permet de donner une caractérisation simple des meilleures exigences compatibles avec la réglementation et les contraintes.

mot-clés *: logiques modales, cohérence, logique déontique, représentation de préférences.*

1 Introduction

Dans le contexte de la conception et fabrication d'un système, qu'il soit logiciel ou matériel, les exigences expriment des propriétés qu'un agent attend de ce système [FGH+94], [HN98]. Dès l'expression des exigences, il convient de prendre en compte les réglementations en vigueur, qui énoncent ce qui est permis, interdit ou obligatoire relativement au système à construire. Il convient également de prendre en compte les contraintes du domaine qui expriment les contraintes physiques, les lois du domaine et qui reflètent ce qui est possible dans ce domaine. En effet, avant de lancer la conception puis la fabrication du système, il faut s'assurer que les propriétés exprimées par les exigences émises à son sujet ne caractérisent pas un système qu'il sera impossible de construire ou bien un système qui violera une réglementation. C'est cette caractéristique des exigences que nous appelons ici compatibilité vis à vis des réglementations et des contraintes.

Pour plus de généralité, nous supposons qu'un agent peut ordonner en fonction de leur priorité les exigences qu'il émet.

Bien que dans un contexte réel, les exigences sont émises en général par plusieurs agents, cet article ne considère qu'un unique agent émetteur d'exigences, et ce pour respecter la taille requise des articles.

Dans ce travail, nous montrons comment l'utilisation d'un unique formalisme (la logique de préférences conditionelles de Boutilier [Bou94b]) pour modéliser les exigences d'un agent, les réglementations et les contraintes du domaine permet de définir la compatibilité des exigences au regard des contraintes et des réglementations, et aussi de déterminer les exigences préférées compatibles avec ces contraintes et ces réglementations.

Cet article est organisé comme suit. Dans la section 2, nous décrivons rapidement la logique de préférences conditionnelles. L'utilisation de cette logique pour modéliser les exigences, les réglementations et les contraintes du domaine est décrite dans les sections 3, 4 et 5. Le problème de la compatibilité des exigences vis à vis des réglementations et des contraintes est formalisé dans la section 6. Un exemple est traité dans la section 7. La section 8 conclut cet article.

2 Rappel : la logique CO

La logique CO est une logique de préférences conditionnelles développée par Craig Boutilier [Bou94b, Bou94a].

2.1 Sémantique de CO

Boutilier considère un langage propositionnel bimodal L_B constitué d'un langage propositionnel classique $PROP$ muni des connecteurs $\neg$, $\vee$, $\wedge$ et $\rightarrow$ et de deux opérateurs modaux $\Box$ et $\overleftarrow{\Box}$.

La sémantique de CO est caractérisée par des modèles de Kripke $\langle W, \leq, val\rangle$ où :

- W est un ensemble de mondes possibles ;
- $\leq$ est un préordre total sur W : c'est donc une relation sur W^2 qui est réflexive et transitive. Si w et w' sont deux mondes de W, alors $w \leq w'$ signifie que w est au moins autant préféré que w' ;
- val est une fonction de valuation sur W[1]. On notera classiquement $||\varphi|| = val(\varphi)$ (cf. [Che80]).

Définition 1 *Soit $\mathcal{M} = \langle W, \leq, val\rangle$ un CO-modèle et $w \in W$. La valeur de vérité d'une formule φ de L_B dans w par rapport à $\mathcal{M}$ est définie par :*

- $\mathcal{M} \models_w \varphi$ *ssi* $w \in val(\varphi)$ *pour* φ *formule bien formée de* $PROP$ *;*
- $\mathcal{M} \models_w \neg\varphi$ *ssi* $\mathcal{M} \not\models_w \varphi$ *;*
- $\mathcal{M} \models_w \varphi \vee \psi$ *ssi* $\mathcal{M} \models_w \varphi$ *ou* $\mathcal{M} \models_w \psi$ *;*
- $\mathcal{M} \models_w \Box\varphi$ *ssi* $\forall w' \in W$ *tel que* $w' \leq w$ *alors* $\mathcal{M} \models_{w'} \varphi$ *;*
- $\mathcal{M} \models_w \overleftarrow{\Box}\, \varphi$ *ssi* $\forall w' \in W$ *tel que* $w' \not\leq w$ *alors* $\mathcal{M} \models_{w'} \varphi$.

[1] I.e. $val : PROP \rightarrow 2^{\mathcal{W}}$ et val vérifie $val(\neg\varphi) = \mathcal{W} - val(\varphi)$ et $val(\varphi_1 \wedge \varphi_2) = val(\varphi_1) \cap val(\varphi_2)$.

$\Box\varphi$ est vraie dans w signifie « φ est vraie dans tous les mondes au moins autant préférés que w ». $\overleftarrow{\Box}\ \varphi$ est vraie dans w ssi φ est vraie dans tous les mondes moins préférés que w. Comme d'habitude, les opérateurs duaux $\Diamond$ et $\overleftarrow{\Diamond}$ sont définis par : $\Diamond\varphi \equiv \neg\Box\neg\varphi$ et $\overleftarrow{\Diamond}\ \varphi \equiv \neg\ \overleftarrow{\Box}\ \neg\varphi$. $\overleftrightarrow{\Box}\ \varphi \equiv \Box\varphi\wedge\ \overleftarrow{\Box}\ \varphi$ et $\overleftrightarrow{\Diamond}\ \varphi \equiv \Diamond\varphi\wedge\ \overleftarrow{\Diamond}\ \varphi$ correspondent respectivement aux opérateurs modaux classiques de nécessité et de possibilité (cf. [Che80]).

Par exemple, la figure 1 montre un CO-modèle $\mathcal{M}$ tel que $\mathcal{M} \models \overleftrightarrow{\Box}\ \alpha$ (car tous les mondes satisfont α) et $\mathcal{M} \models_{w_2} \Box\beta$ (car tous les mondes au moins autant préférés que w_2 satisfont β).

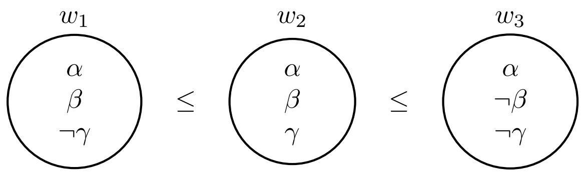

FIG. 1: Un CO-modèle particulier

Enfin, la notion de conséquence est définie par :

Définition 2 *Soit $\Sigma = \{\varphi_1, \ldots, \varphi_n\}$ un ensemble de formules de CO. Une formule ψ est une conséquence de Σ, noté $\Sigma \models \psi$ ssi pour tout CO-modèle $\mathcal{M}$, $\mathcal{M} \models \bigwedge_{i\in\{1,\ldots,n\}} \varphi_i \ \Rightarrow\ \mathcal{M} \models \psi$.*

2.2 Expression de préférences conditionnelles dans CO

Selon Boutilier, les préférences sont des formules du type $I(\beta|\alpha)$ qui signifient que « idéalement si α est vraie, alors β est vraie ». Formellement, l'opérateur I est défini par :

$$I(\beta|\alpha) \equiv_{def} \overleftrightarrow{\Box}\ \neg\alpha \vee \overleftrightarrow{\Diamond}\ (\alpha \wedge (\Box\alpha \rightarrow \beta))$$

Ainsi, si l'on considère un CO-modèle $\mathcal{M}$, $I(\beta|\alpha)$ sera satisfaite dans $\mathcal{M}$ ssi :

- soit α n'est vraie dans aucun monde de W ;
- soit il existe un monde w qui satisfait α et tel que tous les mondes au moins autant préférés à W satisfont $\alpha \rightarrow \beta$.

Cette définition traduit bien la signification intuitive en terme d'idéalité donnée à la formule $I(\beta|\alpha)$. $I(\beta)$ sera un raccourci d'écriture pour $I(\beta|\top)$. De même, on notera la notion duale de *tolérance* par $T(\beta|\alpha) \equiv_{def} \neg I(\neg\beta|\alpha)$.

3 Représentation d'exigences

3.1 Rappels : notion de position

Partant des travaux de Cholvy et Hunter [CH], nous considérons que les exigences d'un agent sont des formules propositionelles (d'un langage donné $PROP$), sur lesquelles l'agent exprime un ordre de priorité. La donnée des exigences est donc la donnée d'un tuple, appelé "position" de l'agent, dont la définition formelle est la suivante :

Définition 3 *Soit a un agent. On appelle* position *de l'agent a un tuple de formules propositionnelles d'un langage donné, $PROP$, $\Gamma_a = [\alpha_1, \ldots, \alpha_n]$ telle que $\{\alpha_1, ...\alpha_n\}$ soit consistant. Chaque α_i est une exigence de l'agent a. De plus α_i précéde α_j dans le tuple Γ_a ssi l'agent a considère α_i comme étant prioritaire par rapport à α_j.*

Pour Cholvy et Hunter, la signification intuitive d'une position $[\alpha_1, \alpha_2]$ est la suivante : pour l'agent, l'objet à concevoir doit satisfaire en priorité $\alpha_1 \wedge \alpha_2$; mais, si cela n'est pas possible (du fait de la réglementation et du fait des contraintes), alors l'objet doit satisfaire $\alpha_1 \wedge \neg\alpha_2$; si cela n'est toujours pas possible, alors l'objet doit satisfaire $\neg\alpha_1 \neg\alpha_2$; enfin, dans le pire des cas, l'objet doit satisfaire $\neg\alpha_1 \wedge \neg\alpha_2$. Plus formellement, Cholvy et Hunter ont montré qu'une position $[\alpha_1, ..., \alpha_n]$ induit un préordre sur les mondes possibles défini par l'ordre lexicographique sur l'ensemble $\{\| \beta_1 \wedge ... \wedge \beta_n \| : \beta_i \in \{\alpha_i, \neg\alpha_i\}\} - \emptyset$.

Notation 1 *Dans la suite de l'article, comme nous ne considérons qu'un seul agent, pour alléger les notions nous omettrons de rappeler l'identifiant de l'agent en indice.*

Exemple 1 *Soit un agent X qui désire acheter une maison. X voudrait que la maison ne soit pas proche d'une station de métro (à cause de la gêne provoquée par le bruit) ou qu'elle soit bien insonorisée ; il voudrait également que si la maison n'est pas proche du centre ville, alors elle soit proche d'une station de métro. La première exigence est prioritaire pour X, par rapport à la deuxième. On considère un langage propositionnel contenant les variables I (la maison est insonorisée), M (la maison est proche d'une station de métro) et C (la maison est proche du centre ville), alors on peut exprimer l'ensemble des exigences de l'agent par la position : $\Gamma = [\neg M \vee I, \neg C \rightarrow M]$. Ceci signifie que X voudrait que sa maison vérifie $\neg M \vee I$ et $\neg C \rightarrow M$. Mais si ce n'est pas possible (à cause des contraintes du domaine ou de la réglementation), il préférerait que la maison vérifie $\neg M \vee I$ et ne vérifie pas $\neg C \rightarrow M$. Si ce n'est toujours pas possible, il accepte que la maison satisfasse $\neg C \rightarrow M$ et ne satisfasse pas $\neg M \vee I$. Enfin, dans le pire des cas, il accepte que la maison ne satisfasse ni $\neg C \rightarrow M$ ni $\neg M \vee I$. Cette position est associée au pré-ordre sur les mondes possibles suivant :*

$$||(\neg M \vee I) \wedge (C \vee M)|| \leq ||(\neg M \vee I) \wedge (\neg C \wedge \neg M)|| \leq ||(M \wedge \neg I) \wedge (C \vee M)|| \leq ||(M \wedge \neg I) \wedge (\neg C \wedge \neg M)||$$

Ainsi, les mondes qui satisfont $(\neg M \vee I) \wedge (C \vee M)$ *sont plus préférés que les mondes qui satisfont* $(\neg M \vee I) \wedge (\neg C \wedge \neg M)$*, lesquels sont eux-mêmes plus préférés aux mondes qui satisfont* $(M \wedge \neg I) \wedge (C \vee M)$*, lesquels sont eux-mêmes plus préférés aux mondes qui satisfont* $(M \wedge \neg I) \wedge (\neg C \wedge \neg M)$*.*

3.2 Modélisation des exigences dans la logique CO

Dans ce paragraphe, notre objectif est de montrer que toute position peut s'exprimer par des formules de CO. Pour cela, nous allons dans un premier temps construire les formules associées à chaque « cluster » de mondes ordonnés selon le préordre correspondant à une position.

Définition 4 *Soit* $\{\alpha_1, \ldots, \alpha_n\}$ *un ensemble cohérent de formules propositionnelles. Soit* $f_{[\alpha_1,\ldots,\alpha_n]} : N \rightarrow PROP$ *la fonction qui associe à un entier* $i \in \{0, \ldots, 2^n - 1\}$ *la formule propositionnelle* $\alpha_1(i) \wedge \ldots \wedge \alpha_n(i)$ *de la façon suivante :*

- *i est décomposé en* $i = \sum_{k=0}^{n-1} c_k(i) * 2^{n-1-k}$ *avec* $\forall k \in \{0, \ldots, n-1\}$ $c_k(i) = 0$ *ou* $c_k(i) = 1$ *;*
- $\forall k \in \{1, \ldots, n\}$ $\alpha_k(i) = \begin{cases} \alpha_k & si\ c_{k-1}(i) = 0 \\ \neg\alpha_k & si\ c_{k-1}(i) = 1 \end{cases}$

Exemple 2 *Dans le cas de l'exemple 1, on obtient :*

$$\begin{array}{lcl} f_\Gamma(0) & = & (I \vee \neg M) \wedge (M \vee C) \\ f_\Gamma(1) & = & (I \vee \neg M) \wedge \neg(M \vee C) \equiv \neg M \wedge \neg C \wedge I \\ f_\Gamma(2) & = & \neg(I \vee \neg M) \wedge (M \vee C) \equiv \neg I \wedge M \wedge C \\ f_\Gamma(3) & = & \neg(I \vee \neg M) \wedge \neg(M \vee C) \equiv \perp \end{array}$$

On restreint maintenant la fonction f pour n'obtenir que des propositions satisfaisables :

Définition 5 *Soit* $\{i_0, \ldots, i_m\} \subset \{0, \ldots, 2^n - 1\}$ *l'ensemble des entiers tels que* $\forall j \in \{i_0, \ldots, i_m\}$ $f_\Gamma(j)$ $est\ satisfaisable.$ f'_Γ *est construite de telle façon que* $\forall j \in \{0, \ldots, m\}$ $f'_\Gamma(j) = f_\Gamma(i_j)$

Exemple 3 *En reprenant l'exemple 2, on obtient :*

$$\begin{array}{lcl} f'_\Gamma(0) & = & (I \vee \neg M) \wedge (M \vee C) \\ f'_\Gamma(1) & = & (I \vee \neg M) \wedge \neg(M \vee C) \equiv \neg M \wedge \neg C \wedge I \\ f'_\Gamma(2) & = & \neg(I \vee \neg M) \wedge (M \vee C) \equiv \neg I \wedge M \wedge C \end{array}$$

On voit que la fonction f' permet de trouver les « clusters » de mondes ordonnés selon le préordre sur les mondes correspondant à la position de l'agent, soit $||f'_\Gamma(0)|| \leq ||f'_\Gamma(1)|| \leq ||f'_\Gamma(2)||$.

Nous allons maintenant construire à partir des formules données par f' un ensemble de formules de CO dont les modèles correspondront au préordre précédent.

Définition 6 *On note :* $\alpha <_E \beta \equiv_{def} \overleftrightarrow{\Diamond} (\alpha \wedge \overleftarrow{\Box} \neg\alpha \wedge \Box\neg\beta)$

Définition 7 *Soit* $\Gamma = [\alpha_1, \ldots, \alpha_n]$ *la position de l'agent. Cette position est représentée par l'ensemble de formules de CO noté* Γ^{CO} *défini par :*

$$\Gamma^{CO} \;=\; \bigcup_{i \in \{0,\ldots,m-1\}} \{f'_\Gamma(i) <_E f'_\Gamma(i+1))\}$$

Définition 8 *On dira que* $\alpha <_\Gamma \beta$ *ssi* $\Gamma^{CO} \models \alpha <_E \beta$.

Théorème 1 $<_\Gamma$ *est une relation d'ordre sur les formules propositionnelles de* $PROP$.

Preuve: La démonstration se fait en trois points :

- $<_\Gamma$ est une relation irréflexive
  La démonstration est aisée : supposons que $<_\Gamma$ ne soit pas une relation irréflexive, alors il existe deux propositions α et β telles que $\alpha <_\Gamma \beta$ et $\alpha \equiv \beta$ (au sens logique). On a donc $\Gamma^{CO} \models \overleftrightarrow{\Diamond} (\alpha \wedge \overleftarrow{\Box} \neg\alpha \wedge \Box\neg\beta)$. Comme $\alpha \equiv \beta$, on a donc $\Gamma^{CO} \models \overleftrightarrow{\Diamond} (\alpha \wedge \overleftarrow{\Box} \neg\alpha \wedge \Box\neg\alpha)$.
  Soit $M = \langle W, \leq, val \rangle$ un modèle de Γ^{CO}. Il existe un monde w_0 de W tel que $M, w_0 \models \alpha \wedge \Box\neg\alpha$, donc en particulier $M, w_0 \models \alpha \wedge \neg\alpha$ ce qui est impossible.
- $<_\Gamma$ est une relation antisymétrique
  Supposons que $<_\Gamma$ soit une relation symétrique, alors il existe deux propositions α et β telles que $\Gamma^{CO} \models \alpha < \beta$ et $\Gamma \models \beta < \alpha$. Soit $M = \langle W, \leq, val \rangle$ un modèle de Γ^{CO}. On a :

  1. $\exists w_\alpha$ tel que $M, w_\alpha \models \alpha \wedge \Box\neg\beta$
  2. $\exists w_\beta$ tel que $M, w_\beta \models \beta \wedge \Box\neg\alpha$

  Supposons que $w_\alpha \leq w_\beta$, alors dans ce cas, $M, w_\alpha \models \alpha \wedge \neg\alpha$, ce qui est impossible. La démonstration est identique pour le cas $w_\beta \leq w_\alpha$.
- $<_\Gamma$ est une relation transitive
  Soient α, β et γ trois propositions telles que $\Gamma^{CO} \models \alpha < \beta$ et $\Gamma^{CO} \models \beta < \gamma$. On a donc $\alpha <_\Gamma \beta$ et $\beta <_\Gamma \gamma$.
  Soit $M = \langle W, \leq, val \rangle$ un modèle de Γ. On a :

  1. $\exists w_\alpha$ tel que $M, w_\alpha \models \alpha \wedge \Box\neg\beta \wedge \overleftarrow{\Box} \neg\alpha$
  2. $\exists w_\beta$ tel que $M, w_\beta \models \beta \wedge \Box\neg\gamma \wedge \overleftarrow{\Box} \neg\beta$

  Supposons que $w_\beta \leq w_\alpha$, alors on a $M, w_\beta \models \beta \wedge \neg\beta$ car $M, w_\alpha \models \Box\neg\beta$, donc $w_\alpha \leq w_\beta$.
  Comme $M, w_\beta \models \Box\neg\gamma$, $M, w_\alpha \models \Box\neg\gamma$. Donc $M, w_\alpha \models \alpha \wedge \Box\neg\gamma \wedge \overleftarrow{\Box} \neg\alpha$, donc $\Gamma^{CO} \models \alpha < \gamma$.

$\blacksquare$

Théorème 2 *Soit* $\Gamma = [\alpha_1, \ldots, \alpha_n]$ *la position de l'agent. Les CO-modèles* $\langle W, \leq, val\rangle$ *de* Γ^{CO} *sont tels que :* $\|f'_\Gamma(0)\| \leq \ldots \leq \|f'_\Gamma(m)\|$.

Preuve: Soit $\Gamma = [\alpha_1, \ldots, \alpha_n]$ la position de l'agent. Soit $M = \langle W, \leq, val\rangle$ un modèle de Γ^{CO}. Soit $j \in \{0, \ldots, m-1\}$, on note w_j le monde de W tel que $M, w_j \models f'_\Gamma(j) \wedge \overleftarrow{\Box} \neg f'_\Gamma(j) \wedge \Box\neg f'_\Gamma(j+1)$.

Démontrons dans un premier temps que $\forall j \in \{1, \ldots, m-1\}\ w_{j-1} \leq w_j$. Soit $j \in \{0, \ldots, m-1\}$, alors $M, w_{j-1} \models \Box\neg f'_\Gamma(j)$. Or $M, w_j \models f'_\Gamma(j)$ donc $w_{j-1} \leq w_j$.

Soit $j \in \{0, \ldots, m_a - 1\}$, deux cas se présentent :

- soit $j \neq 0$ et alors dans ce cas $M, w_j \models f'_\Gamma(j) \wedge \overleftarrow{\Box} \neg f'_\Gamma(j)$. Donc $\forall w \in \|f'_\Gamma(j)\|\ w \leq w_j$.
  De plus, $M, w_{j-1} \models \Box\neg f'_\Gamma(j)$, donc $\forall w \in \|f'_\Gamma(j)\|\ w_{j-1} \leq w$.
  Comme $\forall j \in \{1, \ldots, m-1\}\ w_{j-1} \leq w_j$, on peut écrire que $M, w_{j-1} \models \bigwedge_{l \in \{0,\ldots,j-1\}} \overleftarrow{\Box} \neg f'_\Gamma(l)$ et que $M, w_j \models \bigwedge_{l \in \{j+1,\ldots,m\}} \Box\neg f'_\Gamma(l)$. Donc pour tout $w \in W$, si $w \leq w_j$ et $w_{j-1} \leq w$, $M, w \models \bigwedge_{\substack{l \in \{0,\ldots,m\} \\ l \neq j}} \neg f'_{\Gamma_a}(l)$.
  Soit $w \in W$ tel que $w \leq w_j$ et $w_{j-1} \leq w$. Si pour tout $l \in \{0, \ldots, m\}$, on écrit $f'_\Gamma(l) = \alpha_1(l) \wedge \ldots \wedge \alpha_n(l)$, alors $\forall l \in \{1, \ldots, m\}\ l \neq j \Rightarrow M, w \models \neg\alpha_1(l) \vee \ldots \vee \neg\alpha_n(l)$.
  Or par construction de f'_Γ, $\forall l \in \{1, \ldots, m\}\ l \neq j \Rightarrow \exists l_j \in \{1, \ldots n\}$ tq $\alpha_{l_j}(l) \equiv \neg\alpha_{l_j}(j)$.
  Donc comme $\forall l \in \{1, \ldots, m\}\ l \neq j \Rightarrow M, w \models \neg\alpha_1(l) \vee \ldots \vee \alpha_n(l)$, $M, w \models \alpha_1(j) \wedge \ldots \wedge \alpha_n(j)$. Donc $M, w \models f'_\Gamma(j)$.
  Les modèles de $f'_\Gamma(j)$ sont donc les mondes $w \in W$ tel que $w \leq w_j$ et $w_{j-1} \leq w$.
- soit $j = 0$, $M, w_0 \models f'_\Gamma(0) \wedge \overleftarrow{\Box} \neg f'_\Gamma(0)$ donc $\forall w \in \|f'_\Gamma(0)\|$, $w \leq w_0$.
  De plus, on peut écrire que $M, w_0 \models \bigwedge_{l \in \{1,\ldots,m\}} \Box\neg f'_\Gamma(l)$ donc d'après ce qui précéde, $\forall w \in W$, $w \leq w_0 \Rightarrow M, w \models f'_\Gamma(0)$.

Enfin, $M, w_{m-1} \models \Box\neg f'_\Gamma(m)$ donc $\forall w \in \|f'_\Gamma(m)\|\ w_{m-1} \leq w$. De plus, $M, w_{m-1} \models \bigwedge_{l \in \{0,\ldots,m-1\}} \overleftarrow{\Box} \neg f'_\Gamma(l)$, donc $\forall w \in W\ w_{m-1} \leq w \Rightarrow M, w \models f'_\Gamma(m)$.

■

On remarquera donc que l'encodage dans *CO* de la position de l'agent nous permet de retrouver un ordre sur les mondes possibles identiques à celui établi par Cholvy et Hunter.

Exemple 4 *Reprenons l'exemple 1. On a* $\Gamma = [\neg M \vee I, \neg C \rightarrow M]$. *On a donc* $\Gamma^{CO} = \{(I \vee \neg M) \wedge (M \vee C) < \neg M \wedge \neg C \wedge I, \neg M \wedge \neg C \wedge I < \neg I \wedge M \wedge C\}$.

Nous avons donc montré dans cette section, que tout ensemble ordonné d'exigences (cad toute position) pouvait être modélisé par un ensemble de formules de *CO*.

Nous allons, dans la section suivante, nous intéresser aux réglementations.

4 Représentation de phrases normatives avec *CO*

Dans [CG01, CG02a, Gar02], nous avons montré comment modéliser des phrases normatives à l'aide de la logique *CO*, qu'il s'agisse de simples obligations, permissions ou interdictions (comme par exemple, *il est interdit de construire en zone non constructible* , *il est permis de peindre les volets en vert*) ou qu'il s'agisse de phrases normatives plus complexes telles les normes avec exceptions (comme par exemple *il est interdit de peindre les volets en couleur, sauf si la maison ne se trouve pas proche d'un batiment historique*) ou les Contrary-to-Duties (comme par exemple *il est interdit de peindre les volets en couleur ; mais si les volets sont peints en couleur, alors ils doivent l'être dans un ton clair*).

Dans le tableau suivant, nous listons les traductions en formules de *CO* de ces différentes phrases normatives, sans rappeler en détail les choix qui nous ont amené à ces propositions ni les problèmes encore en suspens (pour cela, nous renvoyons le lecteur aux articles précédents).

il est obligatoire que α soit vraie	$I(\alpha)$
il est autorisé que α soit vraie	$T(\alpha) \equiv \neg I(\neg\alpha)$
il est interdit que α soit vraie	$I(\neg\alpha)$
il est normalement interdit que α mais si β est vraie, alors α est autorisé	$I(\neg\alpha) \wedge \neg I(\neg\alpha\|\beta)$
il est normalement interdit que α mais si β est vraie alors α est obligatoire	$I(\neg\alpha) \wedge I(\alpha\|\beta)$
Contrary-To-Duty : (RP) Il est interdit que α soit vraie (CTD) Mais si α est vraie, alors il est obligatoire que β soit vraie	 $I(\neg\alpha)$ $I(\beta\|\alpha)$

5 Représentation de contraintes du domaine avec *CO*

Les contraintes du domaine représentent les contraintes physiques ou les contraintes inhérentes au domaine de l'objet à concevoir. Elles représentent ce qui est nécessairement vrai dans le monde réel. Exprimer les contraintes du domaine en *CO* est aisé car il suffit de restreindre les mondes possibles à des mondes qui vérifient les contraintes du domaine. Ceci est exprimé par la définition suivante :

Définition 9 *Une contrainte du domaine du type « la proposition α est toujours vraie » est représentée par la formule de CO* $\overleftrightarrow{\Box}\alpha$.

Ainsi, la contrainte « les grandes maisons coûtent plus de 100 000 euros », peut être modélisée par la formule $\overleftrightarrow{\Box} G \rightarrow P\_100000$ (G représente le fait qu'une maison est grande et P_100000 qu'elle coûte plus de 100 000 euros). Les *CO*-modèles de cette formule sont tels que le monde $\{G, \neg P\_100000\}$ n'est pas un monde possible.

Définition 10 *Un ensemble de contraintes du domaine $\mathcal{C}$ est un ensemble cohérent de formules du type $\overleftrightarrow{\Box}\alpha$.*

6 Compatibilité des exigences vis à vis d'une réglementation et de contraintes du domaine

Pour vérifier la compatibilité d'un ensemble d'exigences avec une réglementation et des contraintes du domaine, il convient tout d'abord de vérifier que la réglementation est compatible avec les contraintes du domaine, ce qui signifie intuitivement que la réglementation n'oblige pas quelque chose qui est impossible, ou n'interdit pas quelque chose qui est nécessairement vrai.

6.1 Compatibilité d'une réglementation vis à vis des contraintes

Définition 11 *Soit $\mathcal{R}$ un ensemble de phrases normatives. $\mathcal{R}$ est compatible avec la contrainte du domaine $\overleftrightarrow{\Box}\varphi$ ssi $\forall\psi$ telle que $\psi \wedge \varphi$ est satisfaisable, alors $\mathcal{R} \models \neg I(\neg\varphi|\psi)$. $\mathcal{R}$ est compatible avec l'ensemble de contraintes du domaine $\mathcal{C} = \{\overleftrightarrow{\Box}\varphi_1, \ldots, \overleftrightarrow{\Box}\varphi_l\}$ ssi $\mathcal{R}$ est compatible avec $\overleftrightarrow{\Box}(\varphi_1 \wedge \ldots \wedge \varphi_l)$.*

Exemple 5 *Considérons la réglementation suivante : toute maison doit avoir une connexion EDF, mais si une maison n'a pas de connexion EDF, alors elle doit être pourvue d'un groupe électrogène. On modélise cette réglementation par l'ensemble $\{I(edf), I(groupe|\neg edf)\}$. Supposons que les contraintes du domaine nous indique qu'il est impossible que la maison soit pourvue d'un groupe électrogène. Dans ce cas, la réglementation n'est pas compatible avec les contraintes car il existe des cas prévus par la réglementation (le cas où une maison n'a pas de connexion EDF) où il est obligatoire de mettre un groupe électrogène, alors que c'est impossible.*

6.2 Etats tolérés par une réglementation

Définition 12 *Soit $\mathcal{R}$ une réglementation et $\mathcal{C}$ un ensemble de contraintes. On note*

$$T(\mathcal{R}, \mathcal{C}) = \bigvee_{R \models \neg I(\neg\phi) \quad et \quad C \models \overleftrightarrow{\Diamond}\phi} \phi$$

$T(\mathcal{R}, \mathcal{C})$ est une formule dont les modèles sont les états tolérés par la réglementation $\mathcal{R}$ sous les contraintes $\mathcal{C}$.

Le résultat suivante montre que l'ensemble des états tolérés par une réglementation compatible avec des contraintes n'est jamais vide.

Théorème 3 *Soit $\mathcal{R}$ une réglementation compatible vis à vis d'un ensemble de contraintes $\mathcal{C}$.* $\parallel T(\mathcal{R}, \mathcal{C}) \parallel \neq \emptyset$

Pour prouver ce théorème, il suffit de remarquer que si $\mathcal{R}$ est compatible avec $\mathcal{C} = \{\overleftrightarrow{\Box}\, \varphi_1, \ldots, \overleftrightarrow{\Box}\, \varphi_l\}$, alors $\varphi_1 \wedge \ldots \wedge \varphi_l$ est une disjonction de $T(\mathcal{R}, \mathcal{C})$.

6.3 Caractérisation des exigences compatibles avec la réglementation et les contraintes

Définition 13 *Soit Γ^{CO} les formules de CO qui expriment les exigences de l'agent. Soit $\mathcal{R}$ une réglementation et $\mathcal{C}$ un ensemble de contraintes du domaine comatibles. L'ensemble des meilleures exigences compatibles avec $\mathcal{R}$ et $\mathcal{C}$ est :* $\Gamma^{CO}_{min} = \{\varphi : \Gamma^{CO} \models I(\varphi | T(\mathcal{R}, \mathcal{C}))\}$

On détermine donc les meilleures exigences compatibles avec $\mathcal{R}$ et $\mathcal{C}$ en dérivant, à partir de Γ^{CO}, les formules qui sont vraies dans les mondes minimaux pour le préordre défini par Γ^{CO}, étant fixées les situations tolérées.

Théorème 4 Γ^{CO}_{min} *est non vide*[2].

Preuve: Supposons que Γ^{CO}_{min} soit vide (hormis les tautologies).
Soit $\mathcal{M} = \langle W, \leq, val \rangle$ un modèle de Γ^{CO}. Deux cas se présentent :

- soit $\mathcal{M} \models \neg T(\mathcal{R}, \mathcal{C})$ et alors $\mathcal{M} \models I(\varphi | T(\mathcal{R}, \mathcal{C}))$ pour n'importe quelle formule φ (on peut remarquer que ce cas n'arrive jamais, car $\bigvee_{i \in \{1,\ldots,m\}} f'(i) \equiv \top$ et $T(\mathcal{R}, \mathcal{C}) \neq \phi$).
- soit $\exists (w_o, \ldots, w_l) \in W^n$ tel que $\forall i \in \{1, \ldots, l\}$ $\mathcal{M}, w_i \models T(\mathcal{R}, \mathcal{C})$.
  Soit $J \subseteq \{1, \ldots, l\}$ tel que $\forall i \in J$ $\forall j \in \{1, \ldots, l\}$ $w_i \leq w_j$ (rappelons que d'après la construction de Γ^{CO} tous les mondes de W sont comparables deux à deux). Dans ce cas, comme $\mathcal{M}$ est un modèle de Γ^{CO}, il existe $i_0 \in \{1, \ldots, m\}$ tel que $\forall j \in J$ $w_j \in \|f'(i_0)\|$ (d'après la construction de Γ^{CO}).
  De plus, toujours d'après la construction de Γ^{CO}, quelque soit le modèle $\mathcal{M}$ de Γ^{CO}, i_0 est unique (i.e. les meilleurs $T(\mathcal{R}, \mathcal{C})$ sont toujours dans le même « cluster »).
  Comme tous les mondes de $\|f'(i_0)\|$ vérifient $f'(i_0)$, on peut écrire que $\Gamma^{CO} \models I(f'(i_0) | T(\mathcal{R}, \mathcal{C}))$.

■

On est donc toujours sûr de trouver un ensemble d'exigences qui soient compatibles avec les contraintes du domaine.

[2] On ne considère bien sûr pas les tautologies.

7 Exemple

Considérons un agent qui émet des exigences à propos de sa future maison. Il souhaiterait que la maison soit au centre ville ou proche d'une station de métro ; la maison ait des murs blancs ; la maison coûte moins de 100 000 euros et soit dans un quartier peu bruyant. La position de M. X respecte l'ordre des exigences ci-dessus.

Par ailleurs, les contraintes du domaine sont telles que si une maison est proche d'une station de métro, alors elle n'est pas dans un quartier peu bruyant ; si une maison est au centre ville, alors elle coûte plus de 100 000 euros.

Enfin la réglementation de la ville stipule que si une maison est au centre ville, alors ses murs ne doivent pas être peints en blanc.

On considère un langage propositionnel dont les lettres sont C (la maison est au centre ville), M (la maison est proche d'une station de métro), B (les murs de la maison sont blancs), L (la maison coûte moins de 100 000 euros), T (la maison est dans un quartier peu bruyant) et H (la maison est sous une ligne haute tension).

La position de l'agent, l'ensemble des contraintes du domaine et la réglementation s'écrivent respectivement :

$$\Gamma = [C \vee M, B, L \wedge T] \quad \mathcal{C} = \{\overleftrightarrow{\Box}(M \rightarrow \neg T), \overleftrightarrow{\Box}(C \rightarrow \neg L)\} \quad \mathcal{R} = \{I(\neg B|C)\}$$

Remarquons tout de suite que $\mathcal{C}$ est bien un ensemble cohérent de formules de CO et que $\mathcal{R}$ est bien compatible avec $\mathcal{C}$.

La position de l'agent est modélisée par l'ensemble de formules : $\Gamma^{CO} =$
$\{(C \vee M) \wedge B \wedge (L \wedge T) \ < \ (C \vee M) \wedge B \wedge (\neg L \vee \neg T)$
$(C \vee M) \wedge B \wedge (\neg L \vee \neg T) \ < \ (C \vee M) \wedge \neg B \wedge (L \wedge T)$
$(C \vee M) \wedge \neg B \wedge (L \wedge T) \ < \ (C \vee M) \wedge \neg B \wedge (\neg L \vee \neg T)$
$(C \vee M) \wedge \neg B \wedge (\neg L \vee \neg T) \ < \ (\neg C \wedge \neg M) \wedge B \wedge (L \wedge T)$
$(\neg C \wedge \neg M) \wedge B \wedge (L \wedge T) \ < \ (\neg C \wedge \neg M) \wedge B \wedge (\neg L \vee \neg T)$
$(\neg C \wedge \neg M) \wedge B \wedge (\neg L \vee \neg T) \ < \ (\neg C \wedge \neg M) \wedge \neg B \wedge (L \wedge T)$
$(\neg C \wedge \neg M) \wedge \neg B \wedge (L \wedge T) \ < \ (\neg C \wedge \neg M) \wedge \neg B \wedge (\neg L \vee \neg T)\}$

Considérons la formule la plus préférée, c'est à dire : $(C \vee M) \wedge B \wedge (L \wedge T)$. On peut vérifier que ses modèles ne sont pas des états tolérés, car ce ne sont pas des états possibles du fait des contraintes. En effet, $((C \vee M) \wedge (L \wedge T)) \wedge ((M \rightarrow \neg T) \wedge (C \rightarrow \neg L))$ est insatisfaisable.

Regardons maintenant les modèles de la formule juste un peu moins préférée, c'est à dire : $(C \vee M) \wedge B \wedge (\neg L \vee \neg T)$. On peut vérifier que certains de ses modèles ne sont pas des états tolérés : en particulier, les mondes vérifiant C ne sont pas tolérés car ils vérifient également B (or la réglementation interdit $C \wedge B$). Or les modèles de $(C \vee M) \wedge B \wedge (\neg L \vee \neg T)$ qui vérifient $\neg C$ vérifient également M. Cependant, parmi ceux là, seuls ceux qui vérifient $\neg T$ sont des états tolérés (du fait de la première contrainte). Les deux modèles de $(C \vee M) \wedge B \wedge (\neg L \vee \neg T)$ qui sont tolérés sont donc : $\{\neg C, M, B, \neg T, L\}$ et $\{\neg C, M, B, \neg T, \neg L\}$

La formule qui a ses deux mondes pour modèles est $M \wedge \neg C \wedge B \wedge \neg T$, et donc $\Gamma^{CO}_{min} = \{M \wedge \neg C \wedge B \wedge \neg T\}$.

Les meilleures exigences compatibles avec la réglementation et les contraintes sont donc les suivantes : la maison sera proche d'une station de métro, ne sera pas au centre ville, aura des murs blancs et ne sera pas dans un quartier tranquille. Cependant, rien n'empêche que la maison coûte moins de 100 000 euros.

8 Conclusion

Cet article a décrit comment utiliser une formalisme unique (la logique des préférences conditionnelles de Boutilier) pour modéliser des exigences, des contraintes du domaine et des réglementations.

En effet, nous avons montré que toute position (notion introduite par Cholvy et Hunter pour exprimer des exigences ordonnées par priorité) correspond à un ensemble de formules de CO. Nous avons également montré quelles sont les formules de CO qui expriment les contraintes du domaine. Et enfin, nous avons montré comment représenter par la logique CO des phrases normatives complexes, comme des règles avec exception ou des Contrary-to-Duties.

Traduire toutes ces notions dans une logique unique nous a permis de définir la notion de compatibilité entre une réglementation et les contraintes du domaine, puis la notion de meilleures exigences d'un agent, qui sont, rappelons-le, les exigences qui sont celles qu'il préfére parmi toutes celles qu'il a exprimées et qui sont compatibles avec les contraintes et la réglementation.

Comme il a été noté dans l'introduction, le processus d'ingénierie des exigences fait intervenir plusieurs participants (agents qui émettent des exigences). Une perspective de poursuite de ce travail serait donc d'étendre l'approche proposée pour prendre en compte plusieurs participants pouvant émettre des exigences contradictoires. L'utilisation d'une méthode de fusion d'exigences permettrait d'obtenir un seul ensemble cohérent d'exigences représentant un consensus entre les différents agents. Une ébauche de ce travail a été effectuée dans [CG02b].

Références

[Bou94a] C. Boutilier. Conditional logics of normality : a modal approach. *Artificial Intelligence*, 68(1) :87–154, 1994.

[Bou94b] C. Boutilier. Toward a logic for qualitative decision theory. In J. Doyle, E. Sandewall, and P. Torasso, editors, *Principles of Knowledge Representation and Reasoning (KR'94)*, pages 75–86. Morgan Kaufmann, 1994.

[CG01] L. Cholvy and C. Garion. An attempt to adapt a logic of conditional preferences for reasoning with contrary-to-duties. *Fundamenta Informaticae*, 48(2,3) :183–204, November 2001.

[CG02a] L. Cholvy and C. Garion. Collective obligations, commitments and individual obligations : a preliminary study. In J.F. Horty and A.J.I. Jones, editors, *Proceedings of the* 6^{th} *International Workshop* *on Deontic Logic In Computer Science (ΔEON'02)*, pages 55–71, Londres, May 2002.

[CG02b] L. Cholvy and C. Garion. Merging conflictual requirements with a majority approach. In *Proceedings of the International Workshop for High Assurance Systems (RHAS'02)*, Berlin, September 2002.

[CH] L. Cholvy and A. Hunter. Merging requirements from different agents. *Knowledge Based Systems.* A paraître.

[Che80] B.F. Chellas. *Modal logic. An introduction.* Cambridge University Press, 1980.

[FGH+94] A. Finkelstein, D. Gabbay, A. Hunter, J. Kramer, and B. Nuseibeh. Inconsistency handling in multi-perspective specifications. In *IEEE Transactions on Software Engineering*, volume 20, pages 569–578, August 1994.

[Gar02] C. Garion. *Apports de la logique mathématique en ingénierie des exigences.* PhD thesis, École Nationale Supérieure de l'Aéronautique et de l'Espace, 2002. In French.

[HN98] A. Hunter and B. Nuseibeh. Managing inconsistent specifications : Reasoning, analysis and action. *Transactions on Software Engineering and Methodology*, 7(4) :335–367, October 1998.