

# Modèles réactifs

Louis MUSSAT  
ClearSy

7 juillet 2008

Ce document est l'ébauche d'une méthode de construction de *modèles réactifs* avec la méthode B événementielle. Ces modèles représentent un *environnement* en évolution et un *système* qui observe cet environnement aux moyens de capteurs et qui réagit aux faits observés. Certaines de ces réactions aboutissent à la mise en action d'effecteurs, ce qui permet au système (c'est en général sa raison d'être) de contrôler l'évolution de l'environnement.

Rappelons que selon la méthode B événementielle, un modèle est (principalement) constitué de *variables*, d'*événements* et d'*invariants* (les premières sont modifiées par les deuxièmes dans le respect des troisièmes). Une des difficultés est de mêler ces constituants dont certains représentent des quantités ou des événements de la réalité modélisée et d'autres des variables ou des actions du système : par exemple, peut-on et comment utiliser des variables de l'environnement dans les gardes d'un événement du système ? Plus généralement, quelles sont les règles à respecter ?

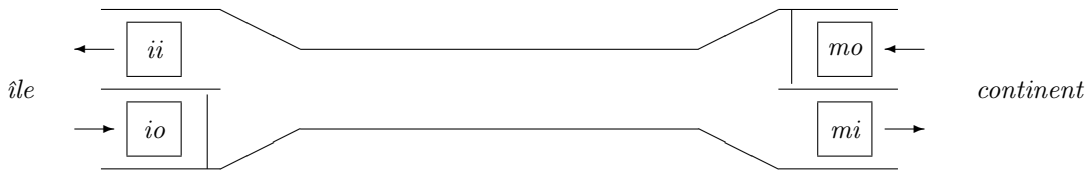
Pour essayer de les dégager, nous reprenons l'exemple du contrôle de voitures : un pont relie une île au continent ; il s'agit de limiter le nombre de voitures présentes sur l'île et de réguler l'accès au pont pour que la circulation y soit en sens unique alterné. (Plusieurs solutions à ce problème sont disponibles sur Internet.)

Dans notre approche, on commence par représenter les quantités physiques de l'environnement et les événements qui les modifient. Puis on introduit les capteurs qui permettent au système de se construire une représentation du monde réel. Enfin on spécifie les actions du système.

## 1 Le problème

Une île est reliée au continent par un pont. Il est large d'une seule voie, sauf à chaque extrémité où deux voies à sens unique forment une entrée et une sortie. Ces entrées et sorties sont chacune munies d'un capteur capable de détecter la présence d'une voiture. Deux barrières permettent de fermer les entrées.

Le schéma ci-dessous résume cette description (les carrés libellés *mo*, *ii*, *io* et *mi* sont les capteurs ; les flèches indiquent les sens de circulation) :



En supposant que les conducteurs respectent les sens uniques et ne font ni arrêt ni marche arrière ni demi-tour sur le pont, il s'agit de spécifier le système qui ouvre et ferme les barrières, de façon à :

- limiter le nombre de voitures sur l'île ;
- limiter le nombre de voitures sur le pont ;
- éviter que des voitures soient bloquées sur l'île ;
- éviter que des voitures soient bloquées sur le pont ;
- empêcher la circulation simultanée dans les deux sens sur le pont.

(Le problème de l'île stipule que «le nombre de voitures sur le l'île et le pont est limité», ce que je traduit par une limite pour chaque nombre. Les solutions publiées limitent la somme.)

## 2 Une solution

### 2.1 Première phase : l'environnement

Lors de cette première phase on modélise l'environnement grâce à des invariants et événements portant sur des quantités physiques. Ces invariants et événements sont observables dans le monde *réel*, ils forment la *physique* du problème.

On spécifie aussi la *finalité* du système en termes de ces quantités physiques, par exemple en stipulant (sous la forme d'un invariant) que le nombre réel de voitures présentes sur l'île ne dépasse jamais une certaine constante. À ce stade, les événements de l'environnement respectent ces contraintes grâce à des gardes portant sur ces quantités physiques. Par exemple, pour qu'une voiture s'engage sur le pont en direction de l'île, il faut que le nombre de voitures présentes sur l'île n'ait pas atteint sa limite. Lors des phases suivantes, ces gardes devront être remplacées par d'autres portant sur des éléments du système modifiant l'environnement (par exemple une barrière pilotée par le système). On ne peut en effet demander aux conducteurs de compter eux-mêmes le nombre de voitures présentes sur l'île !

En revanche, d'autres gardes de ces événements expriment des contraintes physiques, liées à la réalité, qui peuvent légitimement être conservées : par exemple pour qu'une voiture quitte l'île il faut que le nombre de voitures sur l'île ne soit pas nul.

Cette phase peut être réalisée en plusieurs étapes de raffinement, mais ce n'est pas le cas pour la solution présentée ici : tout l'environnement est décrit dans le modèle initial.

MODEL <i>car</i>	VARIABLES	INVARIANTS		INITIALISATIONS
CONSTANTS	$A$	$MO \in \{0, 1\}$	$\omega$ $A \leq e$	$A := 0$
	$B$	$II \in \{0, 1\}$	$\omega$ $B \leq d$	$B := 0$
$d$	$C$	$IO \in \{0, 1\}$	$\omega$ $C \leq e$	$C := 0$
$e$	$MO$	$MI \in \{0, 1\}$	$\omega$ $A = 0 \vee C = 0$	$MO := 0$
	$II$	$II \leq A$	$\omega$ $A + B \leq d$	$II := 0$
AXIOMS	$IO$	$IO \leq B$		$IO := 0$
	$MI$	$MI \leq C$		$MI := 0$
$0 < d$				
$0 < e$				

Les variables  $A$  et  $C$  représentent respectivement le nombre réel de voitures circulant sur le pont en direction de l'île et le nombre réel de voitures circulant sur le pont en direction du continent ; la variable  $B$  représente le nombre réel de voitures présentes sur l'île.

Les variables  $MO$ ,  $II$ ,  $IO$  et  $MI$  comptent le nombre réel de voitures présentes aux entrées et sorties du pont. Ce sont ces voitures qui seront détectées par les capteurs introduits dans le raffinement suivant. Ces capteurs ne peuvent que détecter la présence de voitures, mais pas donner leur nombre. Comme on veut compter les voitures présentes sur le pont et sur l'île, on impose qu'une seule voiture puisse être dans chacune des zones surveillées par les capteurs. Cela induit des contraintes sur la taille de ces zones.

Les six premiers invariants sont en rapport avec la physique du problème. L'invariant  $MO \in \{0, 1\}$  indique qu'une voiture au plus peut se trouver à l'entrée du pont située sur le continent ; les trois invariants suivants ont un sens similaire. L'invariant  $II \leq A$  indique qu'une voiture s'apprêtant à gagner l'île (c'est à dire présente à la sortie du pont menant à l'île) circule sur le pont en direction de l'île ; les invariants  $IO \leq B$  et  $MI \leq C$  ont un sens similaire. Ces prédicats reflètent la position des zones où seront placés les capteurs.

Les cinq derniers invariants sont marqués d'un  $\omega$  pour indiquer qu'ils sont en rapport avec la finalité du système en cours de développement : les invariants  $A \leq e$ ,  $B \leq d$  et  $C \leq e$  stipulent que le système devra limiter le nombre de voitures sur le pont et sur l'île ; l'invariant  $A = 0 \vee C = 0$  stipule que le système devra empêcher la circulation simultanée dans les deux sens sur le pont ; l'invariant  $A + B \leq d$  stipule que le système devra empêcher que des voitures s'engagent sur le pont sans qu'elles puissent gagner l'île.

EVENTS				
<i>ML_PRE_OUT</i>	<i>IL_PRE_IN</i>	<i>IL_PRE_OUT</i>	<i>ML_PRE_IN</i>	
WHEN	WHEN	WHEN	WHEN	
$MO = 0$	$II = 0$	$IO = 0$	$MI = 0$	
	$0 < A$	$0 < B$	$0 < C$	
THEN	THEN	THEN	THEN	
$MO := 1$	$II := 1$	$IO := 1$	$MI := 1$	
END	END	END	END	
<i>ML_OUT</i>	<i>IL_IN</i>	<i>IL_OUT</i>	<i>ML_IN</i>	
WHEN	WHEN	WHEN	WHEN	
$MO = 1$	$II = 1$	$IO = 1$	$MI = 1$	
$A < e$	$B < d$	$C < e$		
$C = 0$		$A = 0$		
$A + B < d$				
THEN	THEN	THEN	THEN	
$MO := 0$	$II := 0$	$IO := 0$	$MI := 0$	
$A := A + 1$	$A := A - 1$	$B := B - 1$		
	$B := B + 1$	$C := C + 1$	$C := C - 1$	
END	END	END	END	
			END	

L'événement *ML\_PRE\_OUT* survient quand une voiture s'apprête à quitter le continent en se plaçant à l'entrée du pont. L'événement *ML\_OUT* survient quand une voiture s'engage sur le pont en direction de l'île. Les autres événements ont un sens similaire. Tous ces événements surviennent dans la réalité.

Les gardes marquées d'un  $\omega$  sont en rapport avec la finalité du système en cours de développement ; elles devront disparaître lors du développement du système.

On peut prouver que le modèle ne peut connaître d'interblocage, et qu'aucun des événements ne peut être en famine.

## 2.2 Deuxième phase : les capteurs

Au cours de cette phase on introduit les capteurs qui permettent au système de se construire une représentation du monde réel. Cette représentation accuse un léger retard sur la réalité, dû au temps de réaction des capteurs.

Cette phase peut être réalisée en plusieurs étapes, mais la solution présentée ici n'y consacre que le premier raffinement.

On introduit les variables du système : *mo*, *ii*, *io* et *mi* enregistrent le décompte des voitures que le système détecte dans les zones d'entrée et de sortie du pont ; *a*, *b* et *c* enregistrent le décompte des voitures que le système considère être sur le pont ou sur l'île. Toutes ces variables sont le reflet (imparfait) des quantités réelles qui portent le même nom en capitales.

REFINEMENT 01		INVARIANTS	
VARIABLES	$mo$	$mo \in \{0, 1\}$	$II \leq a$
	$ii$	$ii \in \{0, 1\}$	$IO \leq b$
$MO$	$io$	$io \in \{0, 1\}$	$MI \leq c$
$II$	$mi$	$mi \in \{0, 1\}$	$A = a - ii * (1 - II) + mo * (1 - MO)$
$IO$	$a$	$ii \leq a$	$B = b - io * (1 - IO) + ii * (1 - II)$
$MI$	$b$	$io \leq b$	$C = c - mi * (1 - MI) + io * (1 - IO)$
	$c$	$mi \leq c$	

Les six premiers invariants ne concernent que des variables du système ; ils sont dictés par le sens attribués à ces variables par le système et ne dépendent que de la manière dont le système remplit sa mission, pas de la physique du problème.

Par contre, les six derniers invariants mêlent les variables du système et celles de l'environnement : il faut impérativement les justifier au regard de la physique modélisée, sinon on court le risque de créer une limitation artificielle aux évolutions de l'environnement et ainsi d'obtenir un système remplissant sa mission par magie.

Nous justifions ci-dessous ceux qui portent sur  $a$  ; une propriété essentielle utilisée est que le temps de réaction des capteurs est inférieur au temps de parcours du pont par les véhicules. Cela induit une contrainte sur la qualité des capteurs, fonction de la longueur du pont et de la vitesse de déplacement des véhicules.

Le capteur situé sur le continent à l'entrée du pont est suffisamment rapide : une voiture ayant quitté le continent ne peut arriver à l'autre extrémité du pont et s'apprêter à gagner l'île avant d'avoir été décomptée par le système. Donc :

$$II \leq a$$

Une voiture quittant le continent pour aller vers l'île est comptée par le système avec un très léger retard : il se peut que dans la réalité la voiture se soit engagée sur le pont ( $MO = 0$ ) mais que le système ne l'ai pas encore détecté ( $mo = 1$ ). Cette hypothétique voiture est comptée par l'expression  $mo * (1 - MO)$  qui vaut 1 dans le cas considéré et 0 dans les autres cas. Symétriquement, une voiture détectée comme s'apprêtant à gagner l'île ( $ii = 1$ ) peut déjà y être dans la réalité ( $II = 0$ ). Cette hypothétique voiture est comptée par l'expression  $ii * (1 - II)$ .

Donc le nombre réel de voitures présentes sur le pont et se dirigeant vers l'île, à savoir  $A$ , vérifie

$$A = a - ii * (1 - II) + mo * (1 - MO)$$

Il est intéressant de tirer quelques conséquences de ces invariants. Par exemple on peut démontrer que

$$II + mo * (1 - MO) \leq A$$

En particulier, si une voiture vient de quitter le continent, elle est encore sur le pont, et ne peut avoir atteint l'autre extrémité :

$$(II = 1 \wedge MO = 0 \wedge mo = 1) \Rightarrow 2 \leq A$$

(Si une voiture s'apprête à gagner l'île et qu'une voiture vient de quitter le continent, c'est qu'il y a deux voitures sur le pont.)

On peut aussi démontrer que

$$a = 0 \quad \Rightarrow \quad A = mo * (1 - MO)$$

c'est à dire que si le système considère qu'aucune voiture ne circule sur le pont en direction de l'île, alors dans la réalité il ne peut y en avoir plus d'une, et le cas échéant elle vient tout juste de s'engager sur le pont, donc ne peut être présente à la sortie du pont menant à l'île (puisque le capteur est suffisamment rapide).

On peut ainsi renforcer la garde  $0 < A$  de l'événement  $IL\_PRE\_IN$  en la changeant pour  $0 < a$ , puisque dans la réalité cet événement ne peut survenir avant que le système soit au fait de la présence de voitures sur le pont. Cette modification n'est qu'un affinement de la modélisation de la réalité, correspondant à la prise en compte de la rapidité du capteur.

En remarquant que

$$mo * (1 - MO) = 0 \quad \Leftrightarrow \quad mo \leq MO$$

on obtient encore

$$A = 0 \quad \Leftrightarrow \quad a = ii \wedge II = 0 \wedge mo \leq MO$$

ce qui nous permet de réécrire la garde de l'événement  $IL\_OUT$ .

On peut donc éliminer dans ce raffinement la variable  $A$  et, par des raisonnements similaires, les variables  $B$  et  $C$ .

VARIANT	INITIALISATIONS	
$\text{card}(\{mo, MO\})$	$MO := 0$	$mo := 0$
$+ \text{card}(\{ii, II\})$	$II := 0$	$ii := 0$
$+ \text{card}(\{io, IO\})$	$IO := 0$	$io := 0$
$+ \text{card}(\{mi, MI\})$	$MI := 0$	$mi := 0$
		$a := 0$
		$b := 0$
		$c := 0$

EVENTS				
<i>ML_PRE_OUT</i>	<i>IL_PRE_IN</i>	<i>IL_PRE_OUT</i>	<i>ML_PRE_IN</i>	
WHEN	WHEN	WHEN	WHEN	
$MO = 0$	$II = 0$	$IO = 0$	$MI = 0$	
$mo = 0$	$ii = 0$	$io = 0$	$mi = 0$	
	$0 < a$	$0 < b$	$0 < c$	
THEN	THEN	THEN	THEN	
$MO := 1$	$II := 1$	$IO := 1$	$MI := 1$	
END	END	END	END	
<i>mo_1</i>	<i>ii_1</i>	<i>io_1</i>	<i>mi_1</i>	
WHEN	WHEN	WHEN	WHEN	
$MO = 1$	$II = 1$	$IO = 1$	$MI = 1$	
$mo = 0$	$ii = 0$	$io = 0$	$mi = 0$	
THEN	THEN	THEN	THEN	
$mo := 1$	$ii := 1$	$io := 1$	$mi := 1$	
END	END	END	END	
<i>ML_OUT</i>	<i>IL_IN</i>	<i>IL_OUT</i>	<i>ML_IN</i>	
WHEN	WHEN	WHEN	WHEN	
$MO = 1$	$II = 1$	$IO = 1$	$MI = 1$	
$mo = 1$	$ii = 1$	$io = 1$	$mi = 1$	
$a < e + ii * (1 - II)$		$c < e + mi * (1 - MI)$		
$c = mi$		$a = ii$		
$MI = 0$		$II = 0$		
$io \leq IO$		$mo \leq MO$		
$a + b < d$				
THEN	THEN	THEN	THEN	
$MO := 0$	$II := 0$	$IO := 0$	$MI := 0$	
END	END	END	END	
<i>mo_0</i>	<i>ii_0</i>	<i>io_0</i>	<i>mi_0</i>	
WHEN	WHEN	WHEN	WHEN	
$MO = 0$	$II = 0$	$IO = 0$	$MI = 0$	
$mo = 1$	$ii = 1$	$io = 1$	$mi = 1$	
THEN	THEN	THEN	THEN	
$mo := 0$	$ii := 0$	$io := 0$	$mi := 0$	
$a := a + 1$	$a := a - 1$	$b := b - 1$	$c := c - 1$	
	$b := b + 1$	$c := c + 1$		
END	END	END	END	END

On peut démontrer grâce aux invariants que les gardes de l'événement *ML\_OUT* (exceptée celle portant sur *mo*) de ce raffinement sont collectivement équivalents

à celles de sa version abstraite, c'est à dire :

$$\begin{aligned}
& MO = 1 \wedge a < e + ii * (1 - II) \wedge c = mi \wedge MI = 0 \wedge io \leq IO \wedge a + b < d \\
\Leftrightarrow & MO = 1 \wedge A < e \wedge C = 0 \wedge A + B < d
\end{aligned}$$

Noter que pour les événements réels, les gardes portant sur les capteurs traduisent la vitesse de ceux-ci relativement à la rapidité des modifications de l'environnement. Par exemple, une voiture ne peut s'engager sur le pont en direction de l'île (événement  $ML\_OUT$ ) avant d'avoir été détectée ( $mo = 1$ ).

D'autre part, les gardes des événements du système traduisent le bon fonctionnement des capteurs : ils enregistrent la réalité quand et seulement quand celle-ci change.

Le système est à ce stade un simple observateur, il n'introduit pas de contraintes sur le comportement (d'ailleurs parfait) des conducteurs.

### 2.3 Troisième phase : les actions

Au cours de cette phase on spécifie les actions du système. Pour simplifier, on considère que ces actions ont un effet immédiat sur l'environnement (par exemple dès que l'ordre est donné d'abaisser une barrière devant le pont, les voitures ne peuvent plus y accéder, comme si la barrière tombait brutalement). Sans cette simplification, il faudrait introduire une dernière phase pour traduire le délai s'écoulant entre la prise de décision d'actionner un effecteur et l'accomplissement de son travail.

Cette phase peut être réalisée en plusieurs étapes, mais la solution présentée ici n'y consacre que le second raffinement.

REFINEMENT 02	VARIABLES	INVARIANTS	INITIALISATIONS
SETS	$MO$	$ml\_br \in BARRIER$	$MO := 0$
	$II$	$il\_br \in BARRIER$	$II := 0$
$BARRIER$	$IO$	$ml\_br = up \Rightarrow a < e$	$IO := 0$
	$MI$	$ml\_br = up \Rightarrow c = 0$	$MI := 0$
CONSTANTS	$mo$	$ml\_br = up \Rightarrow a + b < d$	$mo := 0$
	$ii$	$il\_br = up \Rightarrow c < e$	$ii := 0$
$up$	$io$	$il\_br = up \Rightarrow a = 0$	$io := 0$
$down$	$mi$	$ml\_br = down \vee il\_br = down$	$mi := 0$
	$a$	$MO < mo \Rightarrow ml\_br = up$	$a := 0$
AXIOMS	$b$	$IO < io \Rightarrow il\_br = up$	$b := 0$
	$c$	$ml\_br = up \Rightarrow mo = 1$	$c := 0$
$BARRIER = \{up, down\}$	$ml\_br$	$il\_br = up \Rightarrow io = 1$	$ml\_br := down$
$up \neq down$	$il\_br$	$a \leq e$	$il\_br := down$
		$b \leq d$	
		$c \leq e$	
		VARIANT	
		$2 - \text{card}(\{ml\_br, il\_br\})$	

Les invariants

$$MO < mo \Rightarrow ml\_br = up$$

et

$$IO < io \Rightarrow il\_br = up$$

traduisent le bon comportement des conducteurs : s'ils viennent de s'engager sur le pont c'est que la barrière s'est ouverte devant eux. Ils signifient également que le système attend d'avoir détecté le départ de la voiture avant de baisser la barrière.

EVENTS				
<i>ML_PRE_OUT</i>	<i>IL_PRE_IN</i>	<i>IL_PRE_OUT</i>	<i>ML_PRE_IN</i>	
WHEN	WHEN	WHEN	WHEN	
MO = 0	II = 0	IO = 0	MI = 0	
mo = 0	ii = 0	io = 0	mi = 0	
	0 < a	0 < b	0 < c	
THEN	THEN	THEN	THEN	
MO := 1	II := 1	IO := 1	MI := 1	
END	END	END	END	
<i>mo_1</i>	<i>ii_1</i>	<i>io_1</i>	<i>mi_1</i>	
WHEN	WHEN	WHEN	WHEN	
MO = 1	II = 1	IO = 1	MI = 1	
mo = 0	ii = 0	io = 0	mi = 0	
THEN	THEN	THEN	THEN	
mo := 1	ii := 1	io := 1	mi := 1	
END	END	END	END	
<i>ML_OUT</i>	<i>IL_IN</i>	<i>IL_OUT</i>	<i>ML_IN</i>	
WHEN	WHEN	WHEN	WHEN	
MO = 1	II = 1	IO = 1	MI = 1	
mo = 1	ii = 1	io = 1	mi = 1	
ml_br = up		il_br = up		
THEN	THEN	THEN	THEN	
MO := 0	II := 0	IO := 0	MI := 0	
END	END	END	END	
<i>mo_0</i>	<i>ii_0</i>	<i>io_0</i>	<i>mi_0</i>	
WHEN	WHEN	WHEN	WHEN	
MO = 0	II = 0	IO = 0	MI = 0	
mo = 1	ii = 1	io = 1	mi = 1	
THEN	THEN	THEN	THEN	
mo := 0	ii := 0	io := 0	mi := 0	
a := a + 1	a := a - 1			
	b := b + 1	b := b - 1		
		c := c + 1		
ml_br := down		il_br := down	c := c - 1	
END	END	END	END	

Collectivement, les invariants montrent que le contrôle effectué par le système est plus strict que nécessaire. En effet, on a par exemple

$$A = 0 \quad \Leftrightarrow \quad a = ii \wedge II = 0 \wedge mo \leq MO$$

mais

$$il\_br = up \quad \Rightarrow \quad a = 0 \wedge mo \leq MO$$

Le conducteur qui veut quitter l'île (c'est l'événement  $IL\_OUT$ ) doit attendre que la barrière soit levée, alors que dans l'abstraction il peut le faire quand

$$a = 1 \wedge II < ii \wedge mo \leq MO$$

c'est à dire dès que la dernière voiture circulant vers l'île a quitté le pont, et avant qu'une autre voiture ne soit autorisée à quitter le continent.

Il ne reste plus qu'à écrire les événements de levée d'une barrière :

<pre> <i>ml_br_up</i> WHEN   <i>ml_br = down</i>   <i>il_br = down</i>   <i>mo = 1</i>   <i>a &lt; e</i>   <i>c = 0</i>   <i>a + b &lt; d</i> THEN   <i>ml_br := up</i> END </pre>	<pre> <i>il_br_up</i> WHEN   <i>il_br = down</i>   <i>ml_br = down</i>   <i>io = 1</i>   <i>c &lt; e</i>   <i>a = 0</i> THEN   <i>il_br := up</i> END </pre>
	<pre> END </pre>

### 3 Conclusion

En suivant une approche en trois phases (modélisation de l'environnement, modélisation des capteurs, modélisation des actions) nous avons présenté un système simple et apporté la preuve qu'il remplit sa mission. La première phase a permis la description de l'environnement physique du système; la seconde a permis de dégager les propriétés attendues des capteurs du système vis à vis de l'environnement; la troisième a permis de préciser la façon dont l'environnement doit réagir aux actions du système. Ces trois phases bien identifiées sont liées grâce au raffinement qui permet d'assurer la cohérence du tout.

Nous pensons que notre approche nous a aidé à surmonter cette difficulté de la construction d'un modèle réactif, que ce soit avec la méthode B événementielle ou une autre : à savoir la mise à jour et la justification rigoureuse (mais nécessairement informelle) des propriétés modélisant l'environnement. Bien entendu, l'explicitation de ces propriétés (surtout celles qui lient l'environnement

et le système) est le principal bénéfice de l'activité de modélisation, véritable «machine à poser des questions».

(Note : Une base de données pour *Rodin 0.8.2* est automatiquement produite à partir du source de ce document. Cette base contient (sous forme de THEOREMS) les obligations de preuve d'absence d'interblocage. Au total, on compte 211 obligations de preuve dont 28 sont prouvées interactivement.)