[II.2409] Méthodes formelles
Introduction au *Model Checking*

Matthieu Manceny

1 Modélisation

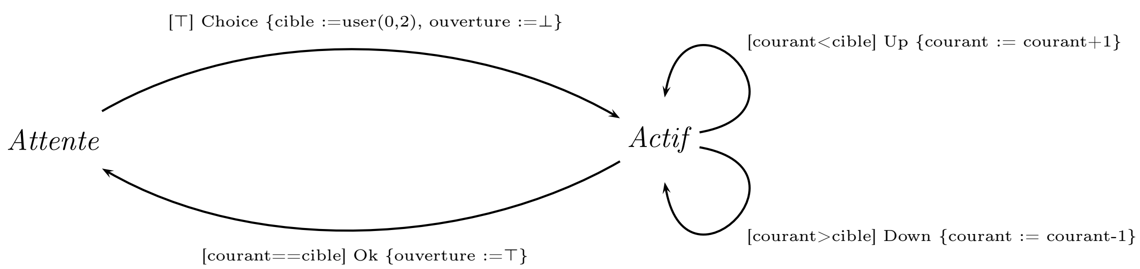
Exercice 1 (Ascenceur)
Le système de contrôle d'un ascenseur (pour 3 étages) est défini de la manière suivante.
- Le contrôleur garde en mémoire l'étage courant et l'étage cible.
- En mode actif, quand l'étage cible est atteint, les portes s'ouvrent et le contrôleur passe en mode attente.
- En mode actif, quand l'étage cible est plus élevé que l'étage courant, le contrôleur fait s'élever l'ascenseur.
- En mode actif, quand l'étage cible est moins élevé que l'étage courant, le contrôleur fait descendre l'ascenseur.
- En mode attente, il se peut que quelqu'un entre dans l'ascenseur et choisisse un nouvel étage cible. L'ascenseur ferme alors les portes et redevient actif.
- Initialement, l'ascenseur est à l'étage 0 et en mode attente.

Questions.

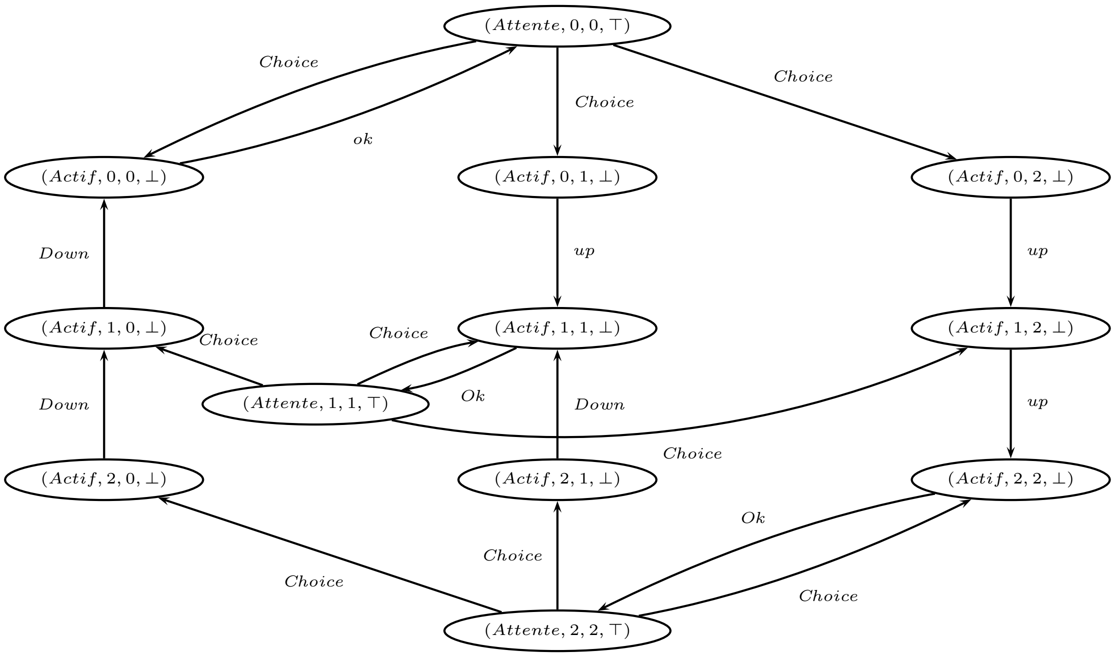
1. Proposez une machine à états modélisant le contrôle de l'ascenseur.
2. Définissez et dessinez le système de transitions correspondant (en vous limitant aux configurations accessibles depuis l'état initial).

Correction.

1. *Les variables sont* `courant: int[0..2]`, `cible: int[0..2]` *et* `ouverture: Bool`. *L'action* `user(0,2)` *renvoie un entier compris entre 0 et 2. À l'état initial : état de contrôle Attente, (cible, courant, ouverture) = (0,0,$\top$)*



2. *Les états du système de transitions suivant sont de la forme (état de contrôle, courant, cible, ouverture).*



2 Logique temporelle

Exercice 2 (Pour débuter en douceur)
Quelques questions simples sur les connecteurs temporels (regardez la définition formelle).

1. $\mathbf{F}p$ est-il vrai si p vrai tout de suite dans l'état courant ?
2. $\mathbf{G}p$ est-il vrai si p faux dans l'état courant et vrai partout ailleurs ?
3. $p\mathbf{U}q$ est-il vrai si p faux et q vrai dans l'état courant ?
4. $p\mathbf{U}q$ est-il vrai si q est toujours faux, et p toujours vrai ?

Correction.

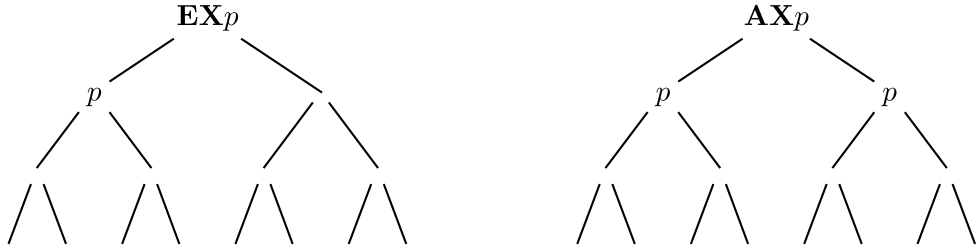
1. Oui

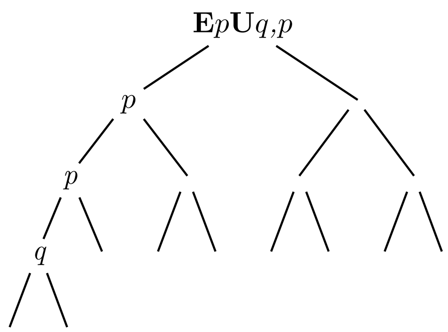
2. Non

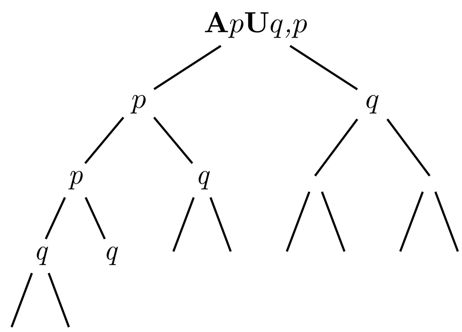
3. Oui

4. Non

Exercice 3 (Dépliages)
Dessinez des dépliages sur lesquels vous illustrerez les propriétés $\mathbf{EX}p$, $\mathbf{AX}p$, $\mathbf{E}p\mathbf{U}q$, $\mathbf{A}p\mathbf{U}q$.
Correction.







Exercice 4 (Du langage naturel à la logique temporelle)
Exprimer en CTL* les propriétés suivantes.

1. « Tous les états satisfont p. »
2. « On peut atteindre p par un chemin où q est toujours vrai. »
3. « Quelque soit l'état, on finit par aller à un état où p vrai. »
4. « Quelque soit l'état, on peut aller à un état où p vrai. »
5. « Absence de deadlock. »

Correction.

1. $\mathbf{AG}p$
2. *Deux possibilités suivant le sens donné à la phrase : soit* $\mathbf{E}(\mathbf{F}p \wedge \mathbf{G}q)$, *soit* $\mathbf{E}(q\mathbf{U}p)$
3. $\mathbf{AGAF}p$
4. $\mathbf{AGEF}p$
5. $\mathbf{AGEX}\top$

Exercice 5 (Autres connecteurs)
On s'intéresse à quelques connecteurs additionnels utiles.

1. Définir formellement la relation $\models$ pour les connecteurs suivants.
   (a) $\varphi\mathbf{W}\psi$ (weak until) : signifie que φ est vraie jusqu'à ce que ψ soit vraie, mais ψ n'est pas forcément vraie à un moment. Dans ce cas, φ reste vraie tout le long du chemin.
   (b) $\mathbf{F}^{\infty}\varphi$ (infiniment souvent) : φ est infiniment vraie au long de l'exécution.
   (c) $\mathbf{G}^{\infty}\varphi$ (presque toujours) : à partir d'un moment donné, φ est toujours vraie.
   (d) $\varphi\mathbf{U}_{\leq k}\psi$ (bounded until) : φ vraie jusqu'à ce que ψ soit vraie, et ψ est vraie avant au plus k observations.
   (e) $\varphi\mathbf{R}\psi$ (release) : ψ est vraie jusqu'à (et inclus) le premier état où φ est vraie, et φ n'est pas forcément vraie un jour.
2. Faire le lien entre ces connecteurs et les anciens.
   (a) Exprimer $\mathbf{W}$, $\mathbf{F}^{\infty}$, $\mathbf{G}^{\infty}$, $\mathbf{U}_{\leq k}$, $\mathbf{R}$ par des connecteurs basiques de LTL (pour $\mathbf{U}_{\leq k}$ juste avec $\mathbf{X}$).
   (b) Exprimer $\mathbf{U}$ uniquement avec $\mathbf{W}$.

Correction.

1. *(a)* $\sigma \models \varphi\mathbf{W}\psi$ *ssi (il existe* $k \geq 0$ *tel que* $\sigma^k \models \psi$ *et pour tout* $0 \leq j < k$, $\sigma^j \models \varphi$*) ou (pour tout* $k \geq 0$, $\sigma^k \models \varphi$*)*
   (b) $\sigma \models \mathbf{F}^{\infty}\varphi$ *ssi pour tout* $k \geq 0$, *il existe* $j \geq k$ *tel que* $\sigma^j \models \varphi$
   (c) $\sigma \models \mathbf{G}^{\infty}\varphi$ *ssi il existe* $k \geq 0$ *tel que pour tout* $j \geq k$ *on a* $\sigma^j \models \varphi$
   (d) $\sigma \models \varphi\mathbf{U}_{\leq k}\psi$ *ssi il existe* $0 \leq i \leq k$ *tel que* $\sigma^i \models \psi$ *et pour tout* $0 \leq j < i$, $\sigma^j \models \varphi$

(e) $\sigma \models \varphi \mathbf{R} \psi$ *ssi (il existe* $k \geq 0$ *tel que* $\sigma^k \models \varphi$ *et pour tout* $0 \leq j \leq k$, $\sigma^j \models \varphi$*) ou (pour tout* $k \geq 0$, $\sigma^k \models \psi$*)*

2. (a) $\varphi \mathbf{W} \psi \equiv (\varphi \mathbf{U} \psi) \vee \mathbf{G}\varphi$
   $\mathbf{F}^\infty \varphi \equiv \mathbf{GF}\varphi$
   $\mathbf{G}^\infty \varphi \equiv \mathbf{FG}\varphi$
   $\varphi \mathbf{U}_{\leq k} \psi \equiv \varphi \mathbf{U} \psi \wedge (\psi \vee \mathbf{X}\psi \vee \mathbf{XX}\psi \vee \ldots \vee \mathbf{X}^k\psi)$
   $\varphi \mathbf{U}_{\leq k} \psi \equiv \psi \vee (\varphi \wedge \mathbf{X}\psi) \vee \ldots \vee (\varphi \wedge \mathbf{X}\varphi \wedge \ldots \wedge \mathbf{X}^{k-1}\varphi \wedge \mathbf{X}^k\psi)$
   $\varphi \mathbf{R} \psi \equiv (\psi \mathbf{U}(\varphi \wedge \psi)) \vee \mathbf{G}\psi$
   (b) $\varphi \mathbf{U} \psi \equiv (\varphi \mathbf{W} \psi) \wedge \mathbf{F}\psi \equiv (\varphi \mathbf{W} \psi) \wedge \neg \mathbf{G} \neg \psi \equiv (\varphi \mathbf{W} \psi) \wedge \neg(\neg \psi \mathbf{W} \bot)$

Exercice 6 (De la logique temporelle au langage naturel)
Exprimer en langage naturel les propriétés suivantes.

1. $\mathbf{AG}(emission \Rightarrow \mathbf{F}reception)$
2. $\mathbf{AF}^\infty ok \Rightarrow \mathbf{G}(emission \Rightarrow \mathbf{F}reception)$

Correction.

1. *Une émission est toujours suivie d'une réception (quelque soit l'état, et quelque soit l'exécution suivie).*
2. *Pour toute exécution, si on a infiniment souvent "ok", alors une émission est toujours suivie d'une réception.*

Exercice 7 (CTL)
Les connecteurs CTL sont $\neg$, $\vee$, $\wedge$, $\mathbf{AX}$, $\mathbf{EX}$, $\mathbf{AF}$, $\mathbf{EF}$, $\mathbf{AG}$, $\mathbf{EG}$, $\mathbf{AU}$, $\mathbf{EU}$.

1. Montrer que $\top$, $\bot$, $\wedge$, $\neg$, $\mathbf{EX}$, $\mathbf{AU}$ et $\mathbf{EU}$ suffisent à exprimer les autres connecteurs CTL.
2. Même question avec $\top$, $\bot$, $\vee$, $\neg$, $\mathbf{EX}$, $\mathbf{EG}$ et $\mathbf{EU}$.

On pourra utiliser les relations suivantes :

$$\mathbf{X}\neg\varphi \equiv \neg\mathbf{X}\varphi \qquad \mathbf{G}\varphi \equiv \neg\mathbf{F}\neg\varphi \qquad \mathbf{F}\varphi \equiv \top\mathbf{U}\varphi \qquad \mathbf{A}\varphi \equiv \neg\mathbf{E}\neg\varphi$$

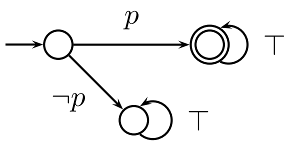
Correction.

1. $\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$
   $\mathbf{AX}\varphi \equiv \neg\mathbf{E}\neg\mathbf{X}\varphi \equiv \neg\mathbf{EX}\neg\varphi$
   $\mathbf{AF}\varphi \equiv \mathbf{A}\top\mathbf{U}\varphi$
   $\mathbf{EF}\varphi \equiv \mathbf{E}\top\mathbf{U}\varphi$
   $\mathbf{AG}\varphi \equiv \neg\mathbf{E}\neg\mathbf{G}\varphi \equiv \neg\mathbf{EF}\neg\varphi \equiv \neg\mathbf{E}\top\mathbf{U}\neg\varphi$
   $\mathbf{EG}\varphi \equiv \neg\mathbf{A}\neg\mathbf{G}\varphi \equiv \neg\mathbf{AF}\neg\varphi \equiv \neg\mathbf{A}\top\mathbf{U}\neg\varphi$
2. $\varphi \wedge \psi \equiv \neg(\neg\varphi \vee \neg\psi)$
   $\mathbf{AX}\varphi \equiv \neg\mathbf{E}\neg\mathbf{X}\varphi \equiv \neg\mathbf{EX}\neg\varphi$
   $\mathbf{AF}\varphi \equiv \neg\mathbf{E}\neg\mathbf{F}\varphi \equiv \neg\mathbf{EG}\neg\varphi$
   $\mathbf{EF}\varphi \equiv \mathbf{E}\top\mathbf{U}\varphi$
   $\mathbf{AG}\varphi \equiv \neg\mathbf{E}\neg\mathbf{G}\varphi \equiv \neg\mathbf{EF}\neg\varphi \equiv \neg\mathbf{E}\top\mathbf{U}\neg\varphi$
   $\mathbf{A}\varphi\mathbf{U}\psi \equiv \neg\mathbf{E}\neg(\varphi\mathbf{U}\psi) \equiv \neg\mathbf{E}[(\neg\psi\mathbf{U}\neg(\varphi \vee \psi)) \vee \mathbf{G}\neg\psi] \equiv \neg[\mathbf{E}(\neg\psi\mathbf{U}\neg(\varphi \vee \psi)) \vee \mathbf{EG}\neg\psi]$

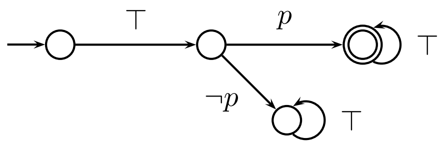
3 Automates de Büchi

Exercice 8 (Formules LTL classiques)
Transformez les propriétés de chemin suivantes en automates de Büchi sur l'alphabet $\{p, \neg p\} \times \{q, \neg q\}$: p, $\mathbf{X}p$, $\mathbf{F}p$, $\mathbf{G}p$, $p\mathbf{U}q$.
Correction.

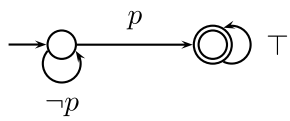
L'automate pour p



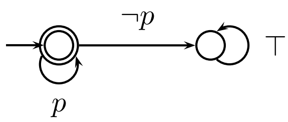
L'automate pour $\mathbf{X}p$



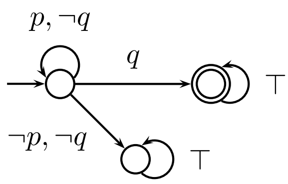
L'automate pour $\mathbf{F}p$



L'automate pour $\mathbf{G}p$



L'automate pour $p\mathbf{U}q$

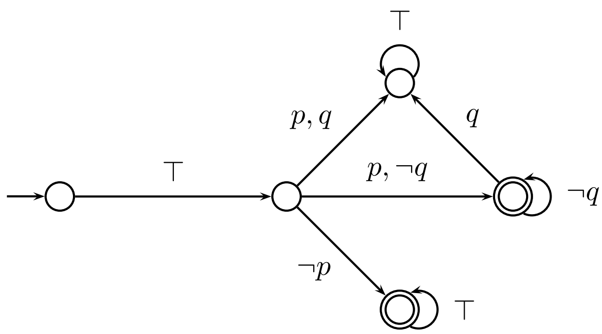


Exercice 9 (Formules LTL un peu plus compliquées)
Exprimer en LTL les propriétés suivantes, puis dessiner les automates de Büchi correspondants.

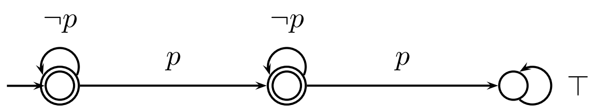
1. « À l'instant suivant, si p vrai alors q n'est jamais vrai. »
2. « p sera vrai au plus une fois. »
3. « p sera vrai exactement 2 fois. »

Correction.

1. $(\mathbf{X}p) \Rightarrow \mathbf{XG}\neg q$



2. $(\mathbf{G}\neg p) \vee (\neg p\mathbf{U}(p \wedge \mathbf{XG}\neg p))$



3. $\neg p\mathbf{U}(p \wedge \mathbf{X}(\neg p\mathbf{U}(p \wedge \mathbf{XG}\neg p)))$