Méthodes Formelles Approche Probabiliste

Arnaud Sangnier

IRIF - Université de Paris

Cours 5

Méthodes Formelles Approche Probabiliste

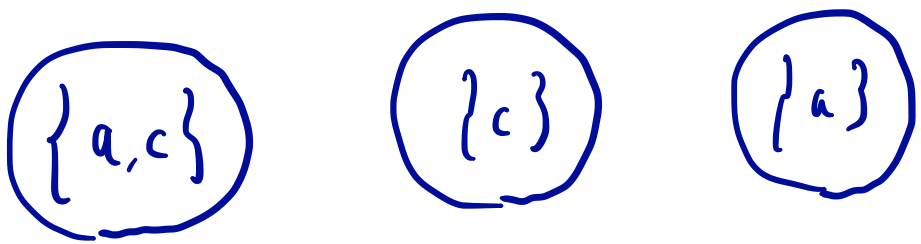
Arnaud Sangnier

IRIF - Université de Paris

Cours 5

Logique Temporelle Linéaire (LTL)

- La logique LTL permet de décrire les traces d'un système de transitions
- Une formule de LTL permet donc de décrire un sous-ensemble de $(2^{PA})^{\omega}$
- Une formule de LTL permet de parler d'un état particulier, par exemple si $PA = \{a, b, c\}$, alors la formule $(a \wedge \neg b) \vee c$ décrit les états ou soit l'on trouve la proposition a mais pas b, soit l'on a c ($\wedge$ veut dire 'ET', $\vee$ veut dire 'OU' et $\neg$ veut dire 'NON').
- Exemple d'états vérifiant $(a \wedge \neg b) \vee c$:



Syntaxe

- Dans la logique LTL on va s'autoriser à se déplacer le long d'une trace.
- On a pour cela deux opérateurs temporels :
  1. $\mathtt{X}\phi$ veut dire "Next ϕ" pour dire que l'on regarde si l'état suivant dans la trace vérifie ϕ
  2. $\phi_1 \mathtt{U} \phi_2$ veut dire "ϕ_1 Until ϕ_2", une propriété ϕ_1 reste vraie jusqu'à ce que l'on atteigne un état où ϕ_2 est vraie (et un tel état est atteint).

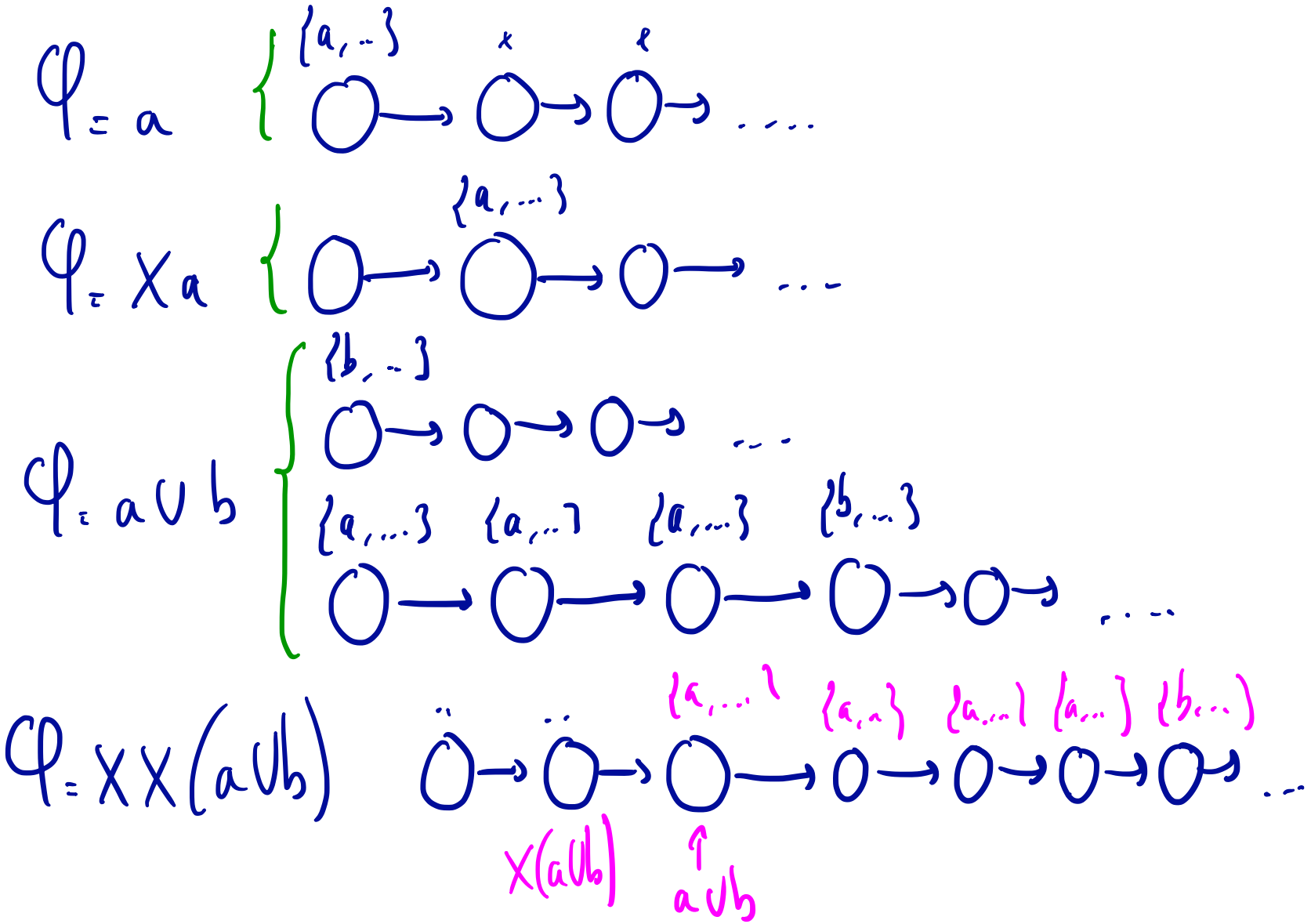
Syntaxe de LTL

$$\phi ::= \top \mid a \mid \phi \wedge \phi \mid \neg\phi \mid \mathtt{X}\phi \mid \phi \mathtt{U} \phi$$

où $a \in PA$

- Une formule de LTL reconnaît des séquences dans $(2^{PA})^\omega$ et étant donnée une telle séquence elle se "déplace dessus" pour vérifier certaines choses

Exemple



Sémantique

$\sigma_i \subseteq PA$

- Soit $\sigma = \sigma_0\sigma_1\sigma_2 \ldots$ in $(2^{PA})^\omega$. Pour $i \in \mathbb{N}$, on note $\sigma[i...]$ la séquence infinie $\sigma_i\sigma_{i+1}\sigma_{i+2} \ldots$.
- Soit ϕ une formule de LTL, on définite la relation $\sigma \models \phi$ de façon inductive:

$\sigma \models \top$		est toujours vraie
$\sigma \models a$	$\Leftrightarrow$	$a \in \sigma_0$
$\sigma \models \phi_1 \wedge \phi_2$	$\Leftrightarrow$	$\sigma \models \phi_1$ et $\sigma \models \phi_2$
$\sigma \models \neg\phi$	$\Leftrightarrow$	$\sigma \not\models \phi$
$\sigma \models \mathrm{X}\phi$	$\Leftrightarrow$	$\sigma[1..] \models \phi$
$\sigma \models \phi_1 \mathrm{U} \phi_2$	$\Leftrightarrow$	$\exists j \in \mathbb{N}.\sigma[j..] \models \phi_2$ et $\forall 0 \leq i < j.\sigma[i..] \models \phi_1$

- On note $Seq(\phi) = \{\sigma \in (2^{PA})^\omega \mid \sigma \models \phi\}$

↳ $Seq(\phi) \subseteq (2^{PA})^\omega$ → $Seq(\phi)$ est une propriété temporelle linéaire

Raccourcis et formules classiques

On a les raccourcis suivants :

- $\phi_1 \vee \phi_2$ équivaut à $\neg(\neg\phi_1 \wedge \neg\phi_2)$
- $\phi_1 \rightarrow \phi_2$ équivaut à $\neg\phi_1 \vee \phi_2$
- $\mathtt{F}\phi$ équivaut à $\top\mathtt{U}\phi$ (Un jour on a ϕ)
- $\mathtt{G}\phi$ équivaut à $\neg(\mathtt{F}\neg\phi)$ (On a toujours ϕ)

Quelques formules usuelles en plus :

- $\mathtt{GF}\phi$: ϕ est vraie infiniment souvent
- $\mathtt{FG}\phi$: un jour ϕ devient toujours vraie

Exemples

- Systèmes avec deux processus qui veulent entrer en section critique et $PA = \{crit1, crit2\}$
  - Les deux processus ne sont jamais en même temps en section critique : $\mathtt{G}(\neg crit1 \vee \neg crit2)$
  - Chaque processus accède infiniment souvent à sa section critique : $\mathtt{GF}(crit1) \wedge \mathtt{GF}(crit2)$
  - **Attention :** C'est différent de $\mathtt{GF}(crit1 \wedge crit2)$
- Systèmes avec un feu de circulation $PA = \{V, O, R\}$
  - Quand il est rouge, le feu ne peut pas être vert directement au coup suivant : $\mathtt{G}(R \rightarrow (\neg \mathtt{X} V))$
  - Quand il est rouge, le feu devient orange au bout d'un moment après avoir été tout le temps rouge avant, puis il devient vert au bout d'un moment et entre temps il est resté orange : $\mathtt{G}(R \rightarrow (R \mathtt{U} (O \wedge \mathtt{X}(O \mathtt{U} V))))$

Sémantique des raccourcis

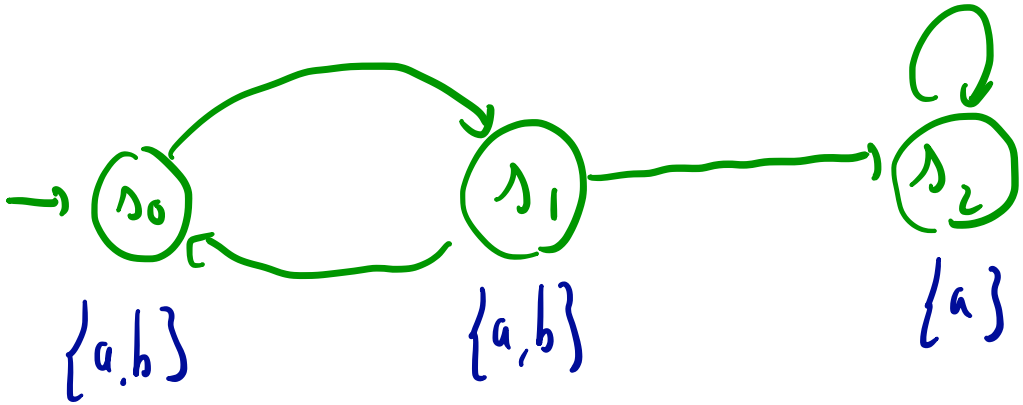
- Les raccourcis peuvent aussi être définis sémantiquement

$$\begin{array}{lcl}
\sigma \models \mathtt{F}\phi & \Leftrightarrow & \exists j \in \mathbb{N}.\sigma[j..] \models \phi \\
\sigma \models \mathtt{G}\phi & \Leftrightarrow & \forall j \in \mathbb{N}.\sigma[j..] \models \phi \\
\sigma \models \mathtt{GF}\phi & \Leftrightarrow & \forall j \in \mathbb{N}.\exists k \in \mathbb{N}.k \geq j \text{ et } \sigma[k..] \models \phi \\
\sigma \models \mathtt{FG}\phi & \Leftrightarrow & \exists j \in \mathbb{N}.\forall k \in \mathbb{N}.k \geq j \text{ implies } \sigma[k..] \models \phi
\end{array}$$

Model-checking

- Soit $ST = (S, \rightarrow, s_{in}, PA, L)$ un système de transitions et ϕ une formule de LTL.
- On dit que ST vérifie ϕ, noté $ST \models \phi$ si, et seulement si, $Traces(ST) \subseteq Seq(\phi)$.
- Comme LTL est clos par négation, on a $ST \models \phi$ si, et seulement si, $Traces(ST) \cap Seq(\neg\phi) = \emptyset$
- **Attention :** On n'a pas que si $ST \not\models \phi$ alors $ST \models \neg\phi$

Exemple



- $ST \models \mathtt{X}(a \wedge b)$
- $ST \models \mathtt{G}a$
- $ST \models \mathtt{G}(\neg b \rightarrow \mathtt{G}(a \wedge \neg b))$
- $ST \not\models b\mathtt{U}(a \wedge \neg b)$

Model-checking en pratique

- Si ϕ est une formule de LTL alors $Seq(\phi)$ est une propriété temporelle linéaire régulière
- Il existe donc un automate de Büchi A_ϕ tel que $\mathcal{L}_\omega(A_\phi) = Seq(\phi)$
- Du coup, $\neg\phi$ est aussi régulière et il existe un automate de Büchi $A_{\neg\phi}$ tel que $\mathcal{L}_\omega(A_{\neg\phi}) = Seq(\neg\phi) = (2^{PA})^\omega \setminus Seq(\phi)$
- Pour vérifier si $ST \models \phi$, on vérifie si $Traces(ST) \cap \mathcal{L}_\omega(A_{\neg\phi})$ est vide ou non en passant par le produit $ST \otimes A_{\neg\phi}$

Si $Traces(ST) \cap \mathcal{L}_\omega(A_{\neg\phi}) \neq \emptyset$ alors $ST \not\models \phi$

Si $Traces(ST) \cap \mathcal{L}_\omega(A_{\neg\phi}) = \emptyset$ alors $ST \models \phi$

Model-checking en pratique

- Si ϕ est une formule de LTL alors $Seq(\phi)$ est une propriété temporelle linéaire régulière
- Il existe donc un automate de Büchi A_ϕ tel que $\mathcal{L}_\omega(A_\phi) = Seq(\phi)$
- Du coup, $\neg\phi$ est aussi régulière et il existe un automate de Büchi $A_{\neg\phi}$ tel que $\mathcal{L}_\omega(A_{\neg\phi}) = Seq(\neg\phi) = (2^{PA})^\omega \setminus Seq(\phi)$
- Pour vérifier si $ST \models \phi$, on vérifie si $Traces(ST) \cap \mathcal{L}_\omega(A_{\neg\phi})$ est vide ou non en passant par le produit $ST \otimes A_{\neg\phi}$