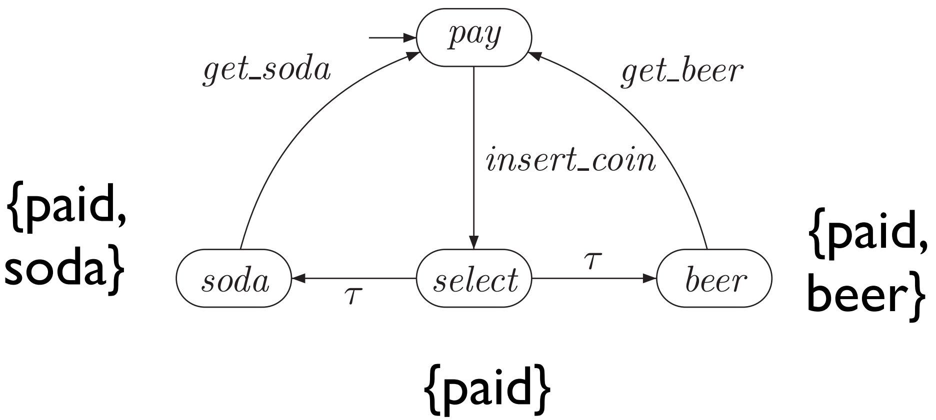
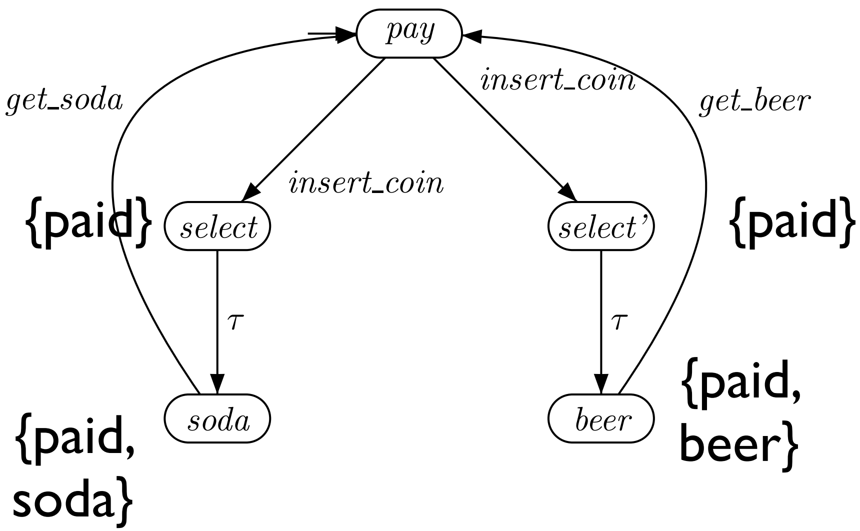
# 2.3 CTL

# Exprimer la possibilité

- La propriété «à chaque fois que *paid* est vérifié, il est possible d'obtenir une bière» n'est pas exprimable en LTL!



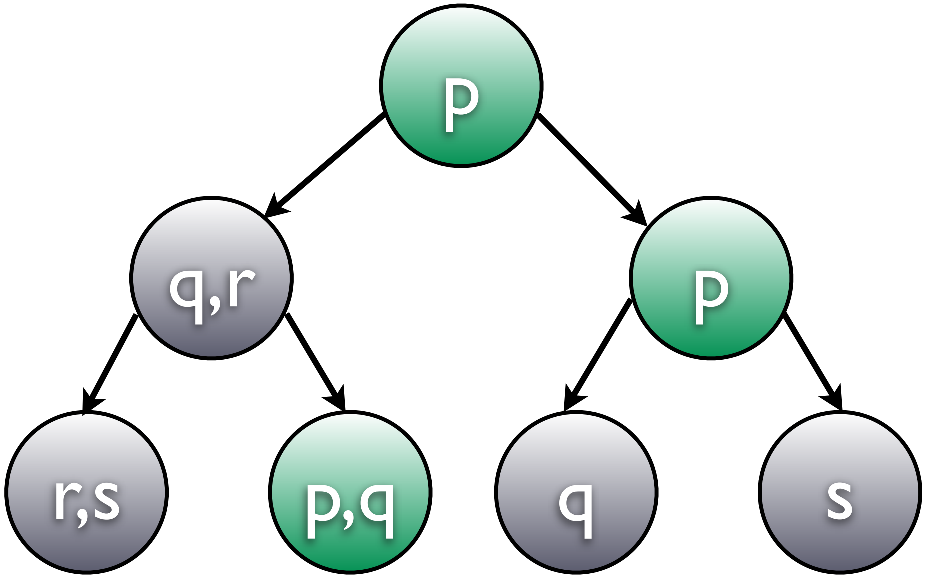

Les deux systèmes vérifient les mêmes propriétés LTL!!

# Computational Tree Logic : CTL

[Clarke, Emerson 81]

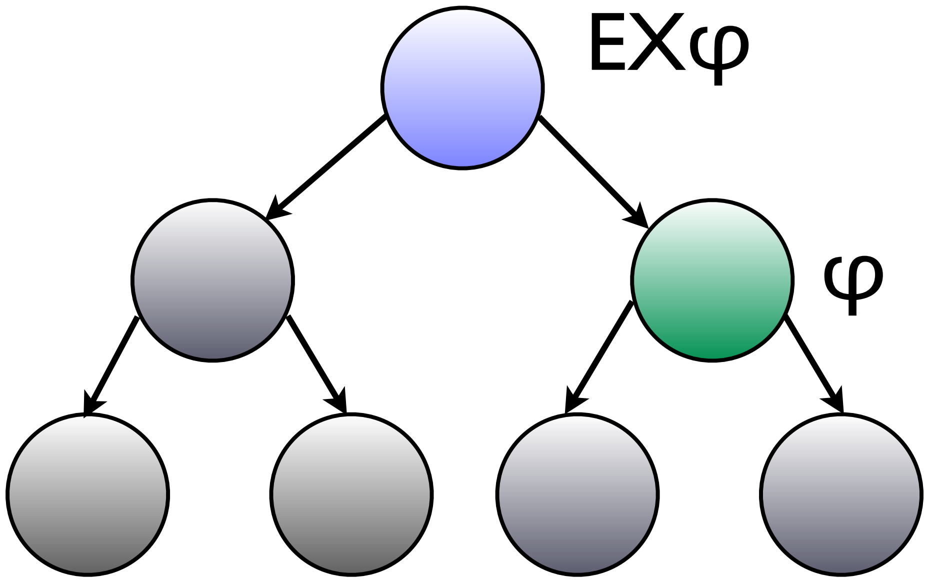
- Modèle des formules : état de l'arbre d'exécutions infini.
- $M,s \models \varphi$ ssi la formule $\varphi$ est vérifiée à l'état s de la structure de Kripke M.
- On note $S(\varphi)$ l'ensemble des états s t.q. $M,s \models \varphi$
- Ajout de quantificateurs sur les chemins dans l'arbre : E et A.
- Défini inductivement sur la formule.

# CTL: syntaxe et sémantique



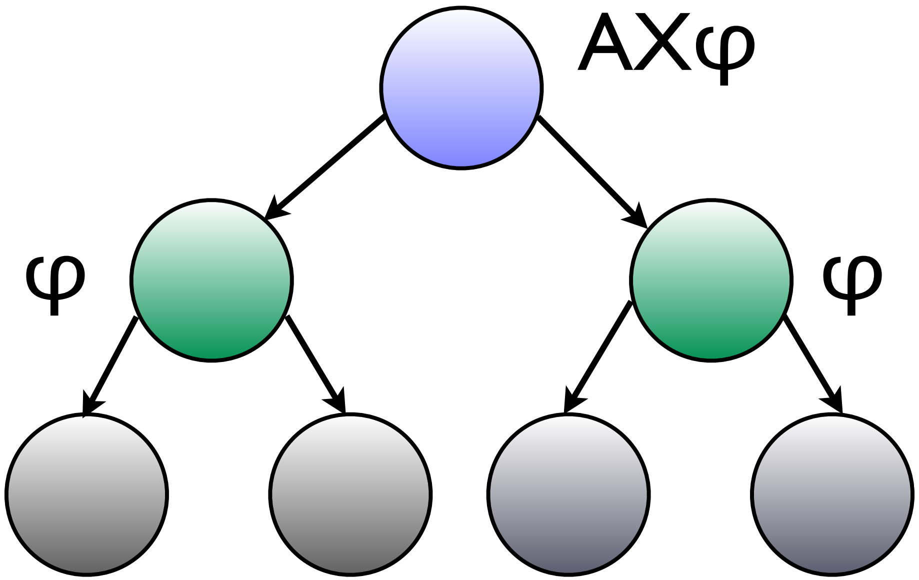

s ⊧ p ssi p∈l(s)

# CTL: syntaxe et sémantique



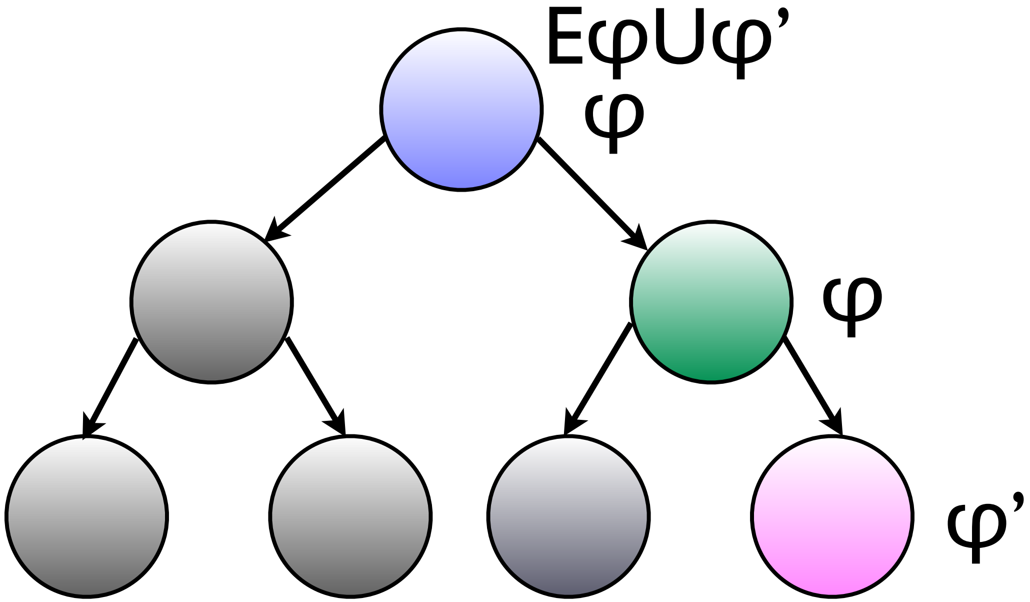

s ⊧ EXφ ssi il existe s', successeur de s t.q. s' ⊧φ

# CTL: syntaxe et sémantique




s ⊧ AXφ ssi pour tout s', successeur de s, s' ⊧φ

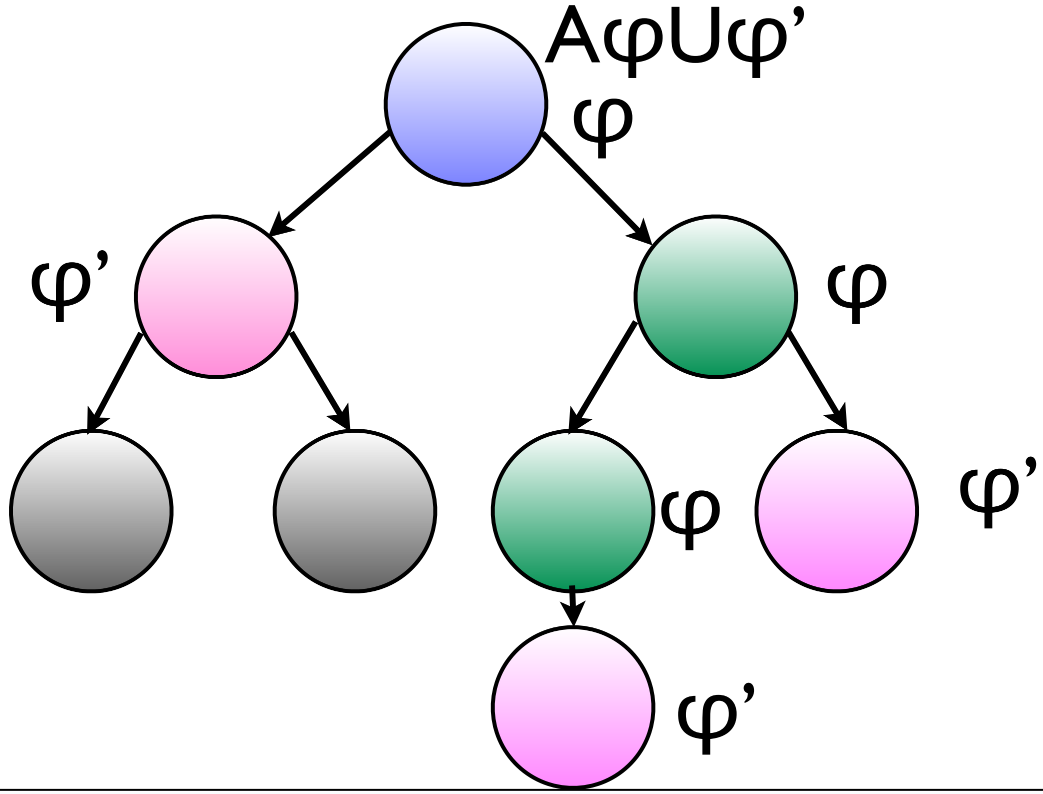
# CTL: syntaxe et sémantique




s ⊧ EφUφ' ssi il existe une exécution $s_0 s_1 \ldots s_k$ telle que $s_0=s$, $s_k \models \varphi'$ et pour tout $0 \leq i < k$, $s_i \models \varphi$.

# CTL: syntaxe et sémantique

’




s ⊧ AφUφ’ ssi pour toute exécution $s_0 s_1$… telle que $s_0$=s, ∃ k t.q. $s_k$ ⊧φ’ et pour tout $0 \leq i < k$, $s_i$ ⊧φ.

# CTL: syntaxe et sémantique

$\varphi ::= p \in AP \mid \neg\varphi \mid \varphi \vee \varphi$
$\mid EX\varphi \mid AX\varphi \mid E\varphi U\varphi \mid A\varphi U\varphi$

$s \models p$ ssi $p \in l(s)$

$s \models \neg\varphi$ ssi $s \not\models \varphi$

$s \models \varphi_1 \vee \varphi_2$ ssi $s \models \varphi_1$ ou $s \models \varphi_2$

$s \models EX\varphi$ ssi il existe s', successeur de s, t.q. $s' \models \varphi$

$s \models AX\varphi$ ssi s', pour tout s', successeur de s, $s' \models \varphi$

$s \models E\varphi_1 U\varphi_2$ ssi il existe une exécution $s_0 s_1 \ldots s_k$ tel que $s_0 = s$, $s_k \models \varphi_2$ et pour tout $0 \leq i \leq k$, $s_i \models \varphi_1$.

$s \models A\varphi_1 U\varphi_2$ ssi pour toute exécution $s_0 s_1 \ldots$ telle que $s_0 = s$, il existe k t.q. $s_k \models \varphi_2$ et pour tout $0 \leq i \leq k$, $s_i \models \varphi_1$.

# CTL : macros

- $EF\varphi \equiv E\top U\varphi$
- $AF\varphi \equiv A\top U\varphi$
- $EG\varphi \equiv \neg AF\neg\varphi$
- $AG\varphi \equiv \neg EF\neg\varphi$

# CTL : Equivalences de formules

- $AX\varphi = \neg EX \neg \varphi$
- $A\varphi U \varphi' = \neg E \neg (\varphi U \varphi') = \neg E(G \neg \varphi' \vee \neg \varphi' U(\neg \varphi \wedge \neg \varphi')) = \neg EG \neg \varphi' \wedge \neg E(\neg \varphi' U(\neg \varphi \wedge \neg \varphi'))$

# CTL : Lois d'expansion

- $A\varphi U\varphi' = \varphi' \vee (\varphi \wedge AX(A\varphi U\varphi'))$
- $AF\varphi = \varphi \vee (AXAF\varphi)$
- $AG\varphi = \varphi \wedge AXAG\varphi$
- $E\varphi U\varphi' = \varphi' \vee (\varphi \wedge EXE(\varphi U\varphi'))$
- $EF\varphi = \varphi \vee EXEF\varphi$
- $EG\varphi = \varphi \wedge EXEG\varphi$

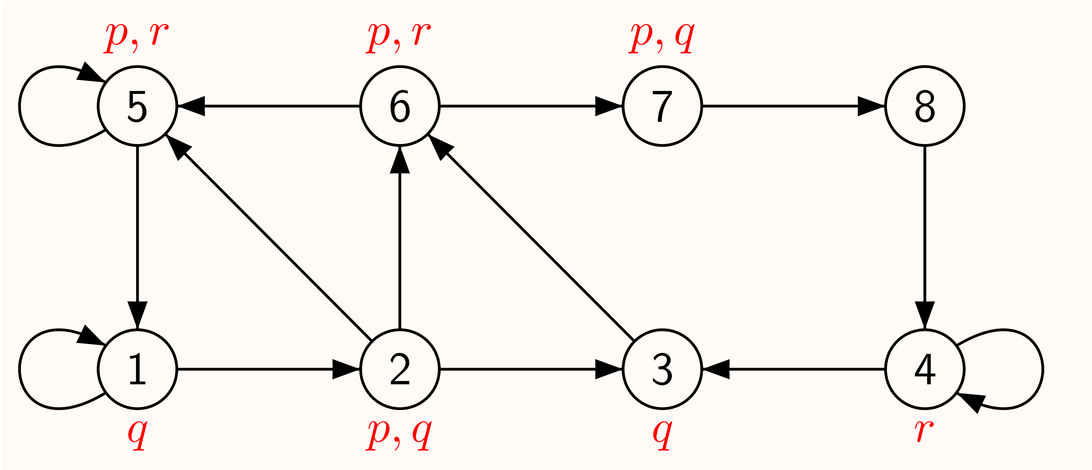
# CTL : lois distributives

- $AG(\varphi \wedge \varphi') = AG\varphi \wedge AG\varphi'$
- $EF(\varphi \vee \varphi') = EF\varphi \vee EF\varphi'$

# Exemples

- Accessibilité : EF(x=0)
- Invariance : AG¬(x=0)
- Vivacité : AGAF(active)

# Exercice




S(EXp)? S(AXp)?
S(EFp)? S(AFp)?
S(EqUr)?S(AqUr)?

# Exercice

- Toute fraude est susceptible d'être détectée un jour(AP={fraude, detect})
- Deux processus ne sont jamais en section critique en même temps (AP={crit1,crit2})
- Toute requête sera un jour satisfaite (AP = {requete, reponse})
- Le processus est activé infiniment souvent (AP= {active})
- Il est possible qu'à partir d'un moment, l'alarme sonne continuellement (AP= {alarm})
- La lumière finit toujours par s'éteindre (AP= {off})
- La lumière finit toujours par s'éteindre et la ventilation tourne tant que la lumière est allumée (AP= {ventilation,off})

# Comparaison LTL/CTL

- La formule CTL $AF(a \wedge EXa)$ n'est pas exprimable en LTL
- La formule LTL FG request → GF response n'est pas exprimable en CTL
- LTL et CTL incomparables!
- LTL et CTL inclus dans CTL*