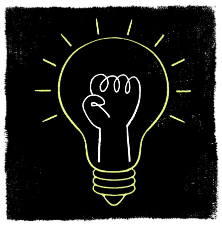
Model-checking de CTL

F. Laroussinie.

Nov. 2021

UE Modélisation & Spécification



Algorithme de Model-checking pour CTL

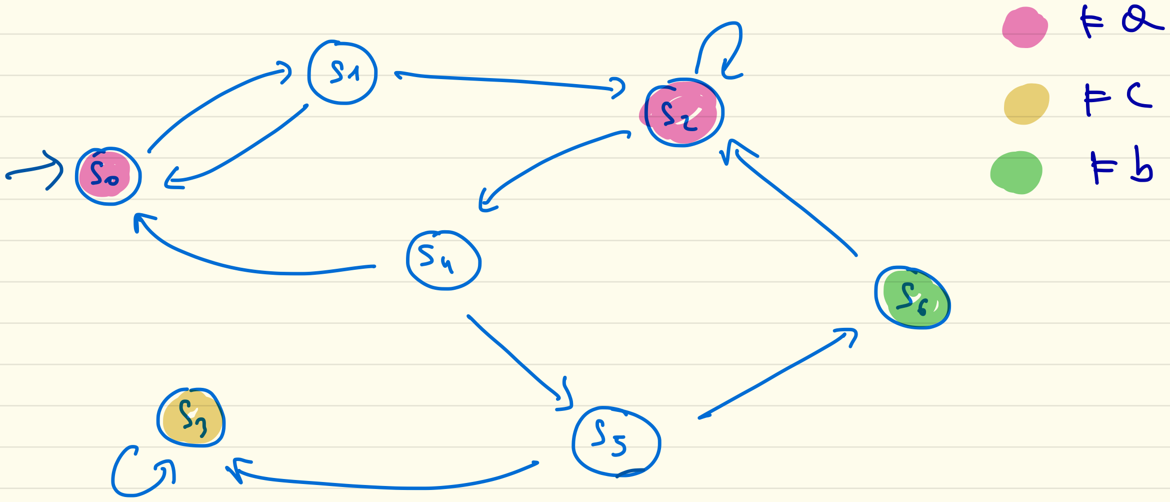
Input : un STE $\mathcal{S} = (Q, Act, \to, q_{init}, AP, \ell)$
+ une formule $\varphi \in CTL$

Output : oui ssi $\mathcal{S}, q_{init} \models \varphi$

idée de l'algo: indiquer pour chaque sous-formule de φ les états où elle est vraie.

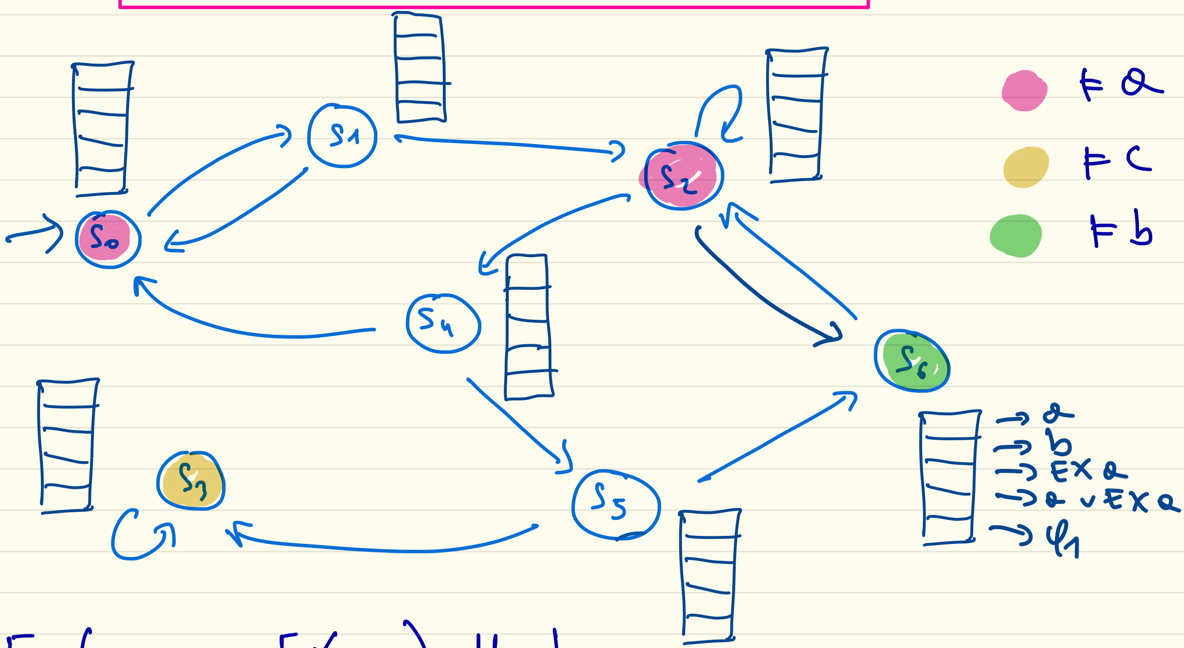
$\varphi \to \underbrace{SF(\varphi)}_{\text{sous-formule}}$ $[\ \varphi \in SF(\varphi)\ ]$

Algorithme de Model-checking pour CTL



$$\varphi_1 = E\,(a \lor EX\,a)\;\mathcal{U}\;b$$

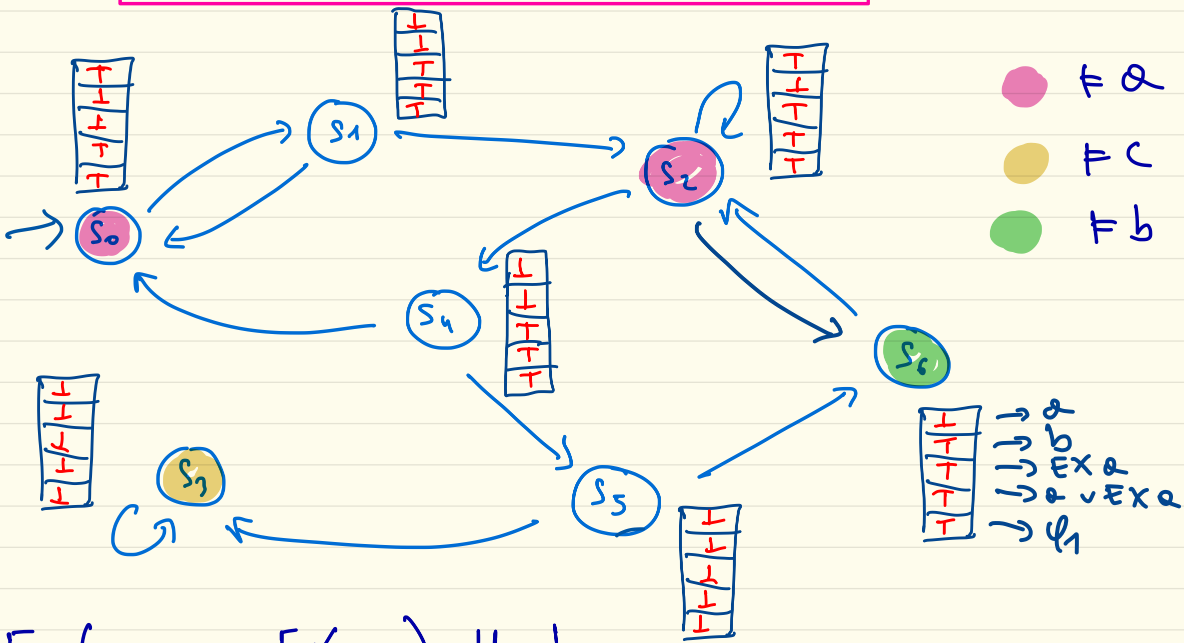
Algorithme de Model-checking pour CTL



$$\varphi_1 = E\,(a \lor EX\,a)\;\mathcal{U}\;b$$

Sous-formules de φ_1 : $\{a,\ b,\ EX\,a,\ a \lor EX\,a,\ \varphi_1\}$

Algorithme de Model-checking pour CTL



$\varphi_1 = E\,(a \vee EX\, a)\ U\ b$

Sous. formules de φ_1 : $\{a,\ b,\ EX\,a,\ a \vee EX\,a,\ \varphi_1\}$

Algorithme de Model-checking pour CTL

procédure Marquage(φ) :

cas 1 : $\varphi = p$

Pour tout $q \in Q$:
  Si $p \in \ell(q)$ Alors $q.\varphi := \top$
  Sinon $q.\varphi := \bot$

cas 2 : $\varphi = \neg \psi$

Marquage(ψ)
Pour tout $q \in Q$:
  $q.\varphi := \neg\ q.\psi$

cas 3 : $\varphi = \psi_1 \wedge \psi_2$

Marquage(ψ_1) , Marquage(ψ_2)
Pour tout $q \in Q$:
  $q.\varphi := q.\psi_1 \wedge q.\psi_2$

cas 3' : $\varphi = \psi_1 \vee \psi_2$

Marquage(ψ_1) , Marquage(ψ_2)
Pour tout $q \in Q$:
  $q.\varphi := q.\psi_1 \vee q.\psi_2$

Algorithme de Model-checking pour CTL

procédure Marquage(φ) (suite)

$AX\,\varphi \equiv \neg EX \neg \varphi$

cas 4 : $\varphi = EX\,\psi$

Marquage(ψ)
Pour tout $q \in Q$: $q.\varphi := \bot$
Pour toute $(q \to q')$:
Si $q'.\psi$ Alors $q.\varphi := \top$

$E\psi_1 \mathcal{U} \psi_2$?

$$E\psi_1 \mathcal{U} \psi_2 \equiv \psi_2 \vee (\psi_1 \wedge EX(E\psi_1 \mathcal{U} \psi_2))$$

Algorithme de Model-checking pour CTL

procédure Marquage(φ) (suite)

cas 5 : $\varphi = E\, \varphi_1 \,\mathcal{U}\, \varphi_2$

Marquage(φ_1), Marquage(φ_2)

Pour tout $q \in Q$:

$\quad q.\varphi := \bot$

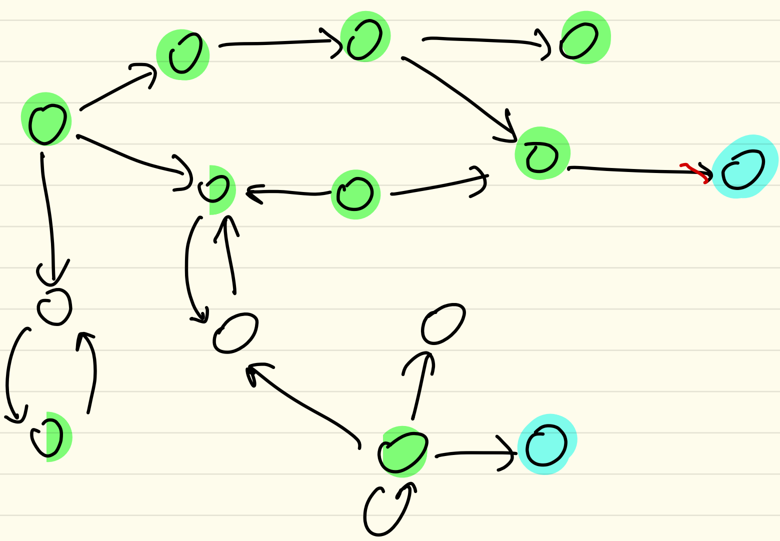
$L = \{\ \}$

Pour tout $q \in Q$: Si $q.\varphi_2$ Alors | $L := L + \{q\}$

$\qquad\qquad\qquad\qquad\qquad\qquad\quad$ | $q.\varphi := \top$

tant que $L \neq \emptyset$:

- piocher un q dans L $\qquad$ [... le retirer]
- Pour tout $(q' \to q)$:
  - Si $q'.\varphi_1 \wedge \neg q'.\varphi$ Alors
    - | $L := L + \{q'\}$
    - | $q'.\varphi := \top$



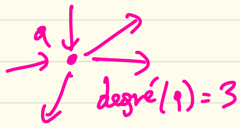
$\varphi = E\, a \,\mathcal{U}\, b$

$A \varphi_1 \mathcal{U} \varphi_2$?

$$A \varphi_1 \mathcal{U} \varphi_2 = \varphi_2 \vee \left(\varphi_1 \wedge AX \left(A \varphi_1 \mathcal{U} \varphi_2 \right) \right)$$

$$\boxed{\text{Algorithme de Model-checking pour CTL}}$$

procédure Marquage(φ) (suite)



cas 6 : $\varphi = A \psi_1 \mathcal{U} \psi_2$

```
Marquage(ψ1), Marquage(ψ2)
Pour tout q ∈ Q :
        q.nb := degré⁻(q) ,   q.φ := ⊥          (degré sortant)
L = {}
Pour tout q ∈ Q : Si q.ψ2 Alors | L := L + {q}
                                 | q.φ := ⊤
tant que L ≠ ∅ :
    . piocher un q dans L
    . Pour tout (q' → q) :
          q'.nb := q'.nb - 1
          Si (q'.nb == 0) ∧ (q'.ψ1) ∧ (¬ q'.φ) Alors :
                    | L := L + {q'}
                    | q'.φ := ⊤
```

Complexité ?

$S = (Q, Act, \rightarrow, q_{init}, AP, \ell)$

procédure Marquage (φ) :

cas 1 : $\varphi = p$ — $O(|Q|)$

```
Pour tout q ∈ Q :
    Si p ∈ ℓ(q)  Alors  q.φ := ⊤
    Sinon  q.φ := ⊥
```

cas 2 : $\varphi = \neg\psi$ — $O(|Q|)$

```
Marquage (ψ)
Pour tout q ∈ Q :
    q.φ := ¬ q.ψ
```

cas 3 : $\varphi = \psi_1 \wedge \psi_2$ — $O(|Q|)$

```
Marquage (ψ1) , Marquage (ψ2)
Pour tout q ∈ Q :
    q.φ := q.ψ1 ∧ q.ψ2
```

cas 4 : $\varphi = EX\psi$ — $O(|Q| + |\rightarrow|)$

```
Marquage (ψ)
Pour tout q ∈ Q :  q.φ := ⊥
Pour toute (q → q') :
    Si q'.ψ  Alors  q.φ := ⊤
```

cas 5 : $\varphi = E\psi_1 \mathcal{U} \psi_2$ — $O(|Q| + |\rightarrow|)$

```
Marquage (ψ1), Marquage (ψ2)
Pour tout q ∈ Q :
    q.φ := ⊥

L = { }
Pour tout q ∈ Q :  Si q.ψ2  Alors  | L := L + {q}
                                   | q.φ := ⊤
tant que L ≠ ∅ :
    . piocher un q dans L
    . Pour tout (q' → q) :
        Si q'.ψ1 ∧ ¬q'.φ  Alors
            | L := L + {q'}
            | q'.φ := ⊤
```

cas 6 : $\varphi = A\psi_1 \mathcal{U} \psi_2$ — idem.

```
Marquage (ψ1), Marquage (ψ2)
Pour tout q ∈ Q :
    q.nb := degré⁻(q) ,   q.φ := ⊥
L = { }
Pour tout q ∈ Q :  Si q.ψ2  Alors  | L := L + {q}
                                   | q.φ := ⊤
tant que L ≠ ∅ :
    . piocher un q dans L
    . Pour tout (q' → q) :
        q'.nb := q'.nb - 1
        Si (q'.nb == 0) ∧ (q'.ψ1) ∧ (¬ q'.φ) Alors :
            | L := L + {q'}
            | q'.φ := ⊤
```

Complexité

$S = (Q, Act, \rightarrow, q_{init}, AP, \ell)$

$|\varphi|$ = nb d'opérateurs + prop.

$$\begin{cases} |\varphi_1 \wedge \varphi_2| = |\varphi_1 \vee \varphi_2| = |E\varphi_1 \mathcal{U} \varphi_2| = |A\varphi_1 \mathcal{U} \varphi_2| = 1 + |\varphi_1| + |\varphi_2| \\ |\neg \varphi_1| = |EX\, \varphi_1| = |AX\, \varphi_1| = 1 + |\varphi_1| \\ |p| = 1 \end{cases}$$

La complexité de l'algo. de model-checking est donc en $O(|\varphi| \cdot |S|)$

$|S| = |Q| + |\rightarrow|$

↳ complexité polynomiale !

Rappel :

Pour LTL, le model-checking se ramène à tester si $\mathcal{A}_S \cap \mathcal{A}_{\neg\varphi} \stackrel{?}{=} \emptyset$

$\leadsto$ complexité en tps en $O(|S| \cdot 2^{|\varphi|})$

⚠

[le pb est PSPACE-complet]