

Automates communicants (2)

Plusieurs approches pour vérifier
des CFM :

- ① abstraction : un seul type de messages $\rightarrow$ canaux = compteurs sans test à 0 $\leadsto$ RdP
- ② canaux avec pertes (Lossy CFM)

$\leadsto$ on rajoute des transitions

$$(s, w) \xrightarrow{\Sigma} (s, w'),$$

$$\forall w' \sqsubseteq w$$

(w' sous-mot de w :

$$ab \sqsubseteq bbaa, \quad bb \not\sqsubseteq aaba)$$

Lossy CFM : cas particulier des systèmes bien structurés
(WSTS : well-structured transition systems)

Th L'accessibilité des lang. CFM
est décidable (complexité très
élevée : non primitif-réc.)

Par contre, les pbs. suivants
restent indécidables :

- configurations bornées
- accessibilité répétée
- LTL, CTL

③ Model-checking avec logiques
d'ordre partiel, bornes sur
les canaux.

D'abord : spécifications séquentielles

A CFM, $\Sigma = \{ p!q(m), p?q(m') : \dots \}$

$L(A) = \{ a_1 a_2 \dots \in \Sigma^* \cup \Sigma^\omega :$

$(s_0, \varepsilon) \xrightarrow{a_1} (s_1, w_1) \xrightarrow{a_2} \dots \}$

eLTL : extended LTL

$\varphi ::= \text{tt} \mid a \mid X\varphi \mid X_{\text{msg}} \varphi \mid$

$\varphi \cup \varphi \mid \varphi \vee \varphi \mid \neg \varphi$

$(u, i) \models X_{\text{msg}} \varphi \quad \text{si}$

$u(i) = p!q(m)$ et il ex.

$j > i$, $u(j) = q?p(m)$,

$u(j)$ = reception qui correspond
à l'envoi $u(i)$,

et $(u, j) \models \varphi$

Prop. Model-checking de ω -LTL sur les langages des CFM est indécidable.

Réduction de PCP (pb. de correspondance de Post)

$$(u_1, v_1), \dots, (u_k, v_k) \in A^* \times A^*$$

On cherche une séquence d'indices $i_1, i_2, \dots \in \{1, \dots, k\}$

$$\text{tq.} \quad u_{i_1} \dots u_{i_m} = v_{i_1} \dots v_{i_m}$$

On note $p!q(u)$, $u \in A^*$:

la séquence $p!q(u_1) p!q(u_2) \dots p!q(u_n)$

$$u = u_1 \dots u_n, \quad u_i \in A$$

On va coder l'existence d'une solution à une instance de PCP $(u_1, v_1), \dots, (u_k, v_k)$ par une formule de eLTL.

Processus : p, q, r, s

Canaux : $(p, q), (r, s)$

Content messages : $A \cup \{1, \dots, k\} \cup \{\$ \}$

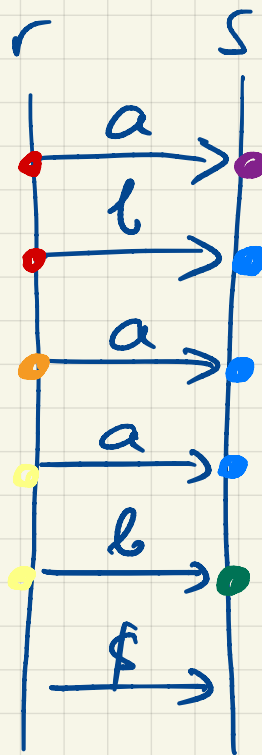
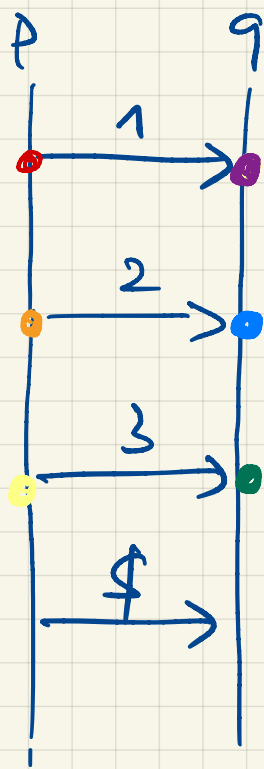
$$\left(\bigcup_{1 \leq i \leq k} p!q(i) \ r!s(u_i) \right)^+ p!q(\$) \ r!s(\$)$$

$$\left(\bigcup_{1 \leq i \leq k} q?p(i) \ s?r(v_i) \right)^+ q?p(\$) \ s?r(\$)$$

ex $\overset{1}{(a1, a)}, \overset{2}{(a, baa)}, \overset{3}{(ab, b)}$

$\begin{array}{c} a1 \quad a1 \\ a1 \quad ba1 \end{array}$
 $\begin{array}{ccc} 1 & 2 & 3 \end{array}$

solution PCP



en LTL :

- forme syntaxique correcte

$$\left[\bigvee_i p!q(i) \left(\bigvee_{a \in A} r!s(a) \right)^* \right]^+ p!q(\$) r!s(\$)$$

$$\left[\bigvee_i q?p(i) \left(\bigvee_a s?r(a) \right)^* \right]^+ q?p(\$) s?r(\$)$$

+ chaque $p!q(i)$ suivi par

$$r!s(ui) \left(\bigvee_j p!q(j) + r!s(\$) \right)$$

etc

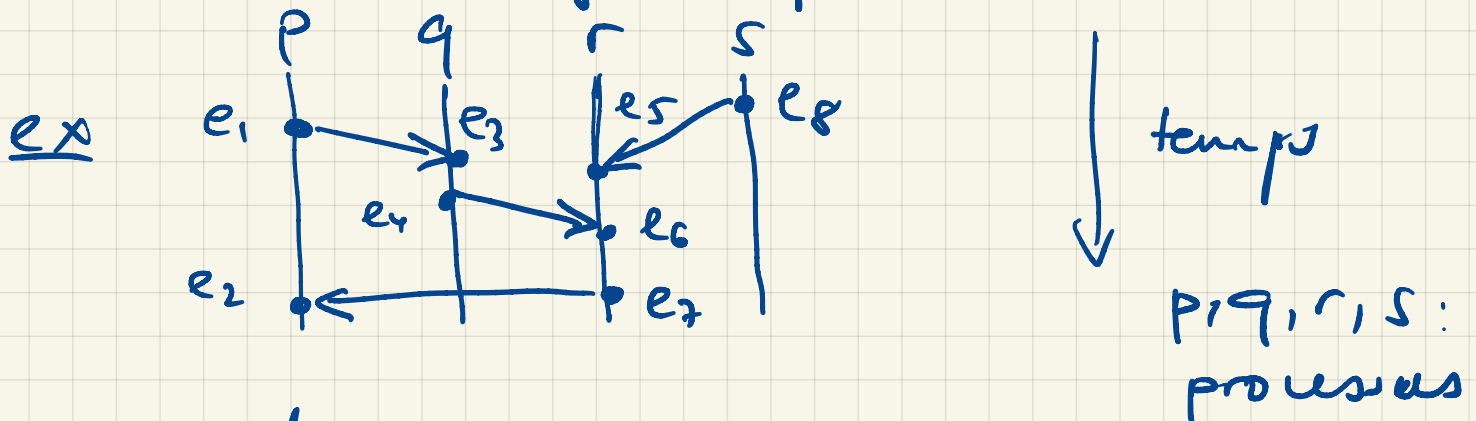
- chaque emission a une reception

e.g. $G(p!q(x) \rightarrow \exists m, y, t)$

- chaque réception a une émission ?
- pas nécessaire, car la formule est interprétée sur des exécutions de CFM
- FIFO ?
- même raison

Spécifications d'ordre partiel : MSC

MSC : message sequence chart



- events : $e_1, \dots, e_7$
- $P(e)$: processus de e

$$P(e_1) = P(e_2) = p, \quad P(e_3) = P(e_4) = q, \text{ etc}$$