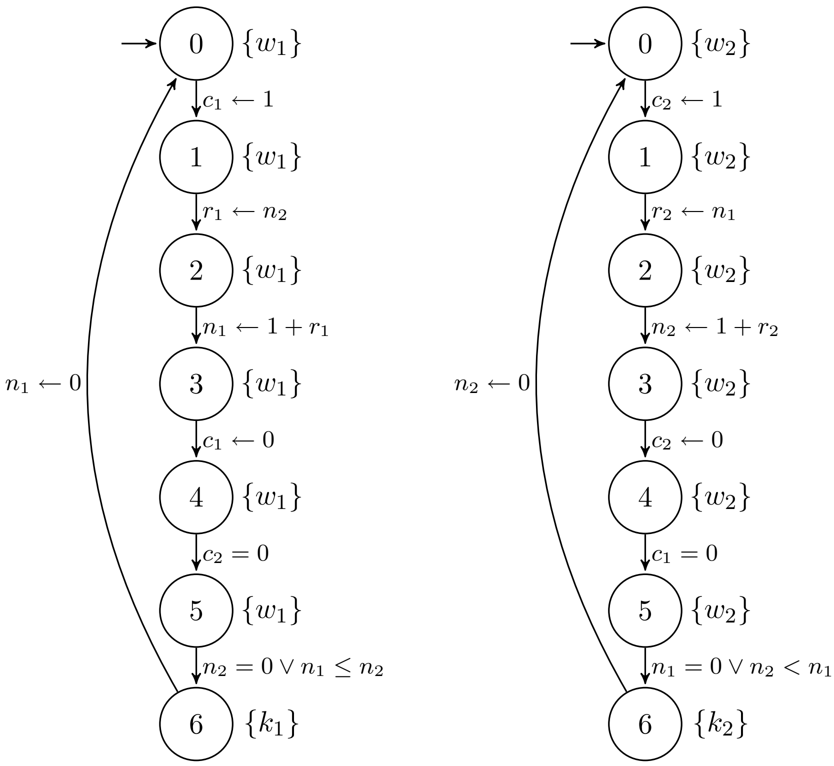
TD 14 : Simulation

1 Algorithme de la boulangerie

On cherche à établir la correction d'un algorithme d'exclusion mutuelle dû à Lamport. L'algorithme considère en général N processus P_i avec chacun trois variables entières n_i, c_i et r_i ; nous étudions ici le cas $N = 2$.

Chaque processus est soit en train d'attendre son tour (proposition atomique w_i, dans les états 0 à 5), soit en section critique (proposition atomique k_i, dans l'état 6). L'algorithme est représenté par le produit asynchrone des deux systèmes de transition suivants :



Le but de l'exercice est de donner un système abstrait fini bisimilaire à ce produit asynchrone.

1. Montrer que le système est infini.
2. Montrer qu'il existe au moins une assignation de variables $a = (c_1, r_1, n_1, c_2, r_2, n_2)$ tels que l'état $(4, 5, a)$ soit bisimilaire à l'état $(5, 4, a)$. Est-ce qu'il existe une telle assignation *accessible* dans le système ?
3. Montrer que les propositions $c_i \neq 0$ et $n_i \neq 0$ peuvent être exprimées seulement à l'aide de l'état de contrôle q_i.

4. Calculer le quotient de ce système par la bisimulation la plus large peut être difficile à réaliser à la main. On va se contenter de chercher une bisimulation qui raffine la partition qui préserve seulement les états de contrôle.
   Donner une condition sur les assignations a et a' pour que $(5, 5, a)$ soit bisimilaire à $(5, 5, a')$. Peut-on trouver une condition qui contraigne aussi peu que possible les valeurs des assignations ? Exploiter cette idée pour raffiner la partition initiale.

2 Simulations

Soient $M_1 = \langle \mathrm{AP}, Q_1, I_1, T_1, l_1 \rangle$ et $M_2 = \langle \mathrm{AP}, Q_2, I_2, T_2, l_2 \rangle$ deux systèmes de transition. On appelle une *simulation* une relation R dans $Q_1 \times Q_2$ telle que si $q_1 \, R \, q_2$, alors

1. $l_1(q_1) = l_2(q_2)$,
2. $\forall q_1' \in T_1(q_1) \Rightarrow \exists q_2' \in T_2(q_2) \wedge q_1' \, R \, q_2'$.

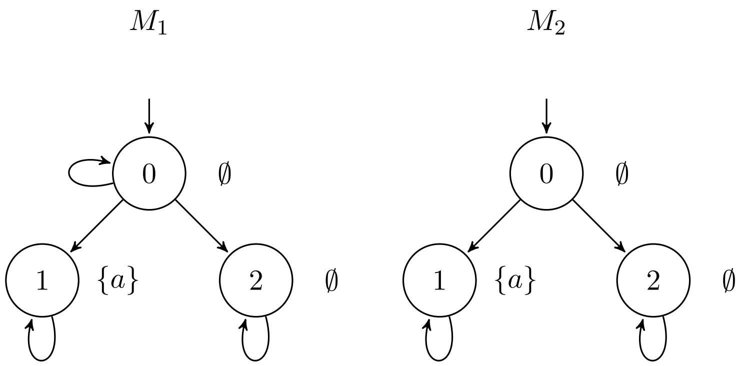
Une relation R est une simulation entre M_1 et M_2 si de plus, pour tout q_1 de I_1, il existe q_2 de I_2 tel que $q_1 \, R \, q_2$.

Un couple d'états (q_1, q_2) est *similaire*, noté $q_1 \preceq q_2$, si et seulement s'il existe une simulation R telle que $q_1 \, R \, q_2$. On généralise de même aux systèmes de transition. La relation $\preceq$ est un pré-ordre (elle est reflexive et transitive).

Deux états q_1 et q_2 sont équivalents modulo simulation, noté $q_1 \simeq q_2$, si $q_1 \preceq q_2$ et $q_2 \preceq q_1$.

2.1 Relation de simulation

On considère les deux systèmes de transition suivants :



1. Montrer que $M_2 \preceq M_1$.
2. Montrer que $M_1 \not\preceq M_2$: on peut le faire en fournissant une formule CTL existentielle φ telle que $M_1 \models \varphi$ mais $M_2 \not\models \varphi$.

Une formule CTL existentielle vérifie la syntaxe suivante :

$$\psi ::= \top \mid \bot \mid p \mid \neg p \mid \psi \wedge \psi \mid \psi \vee \psi \mid \mathsf{E}\varphi$$
$$\varphi ::= \mathsf{X}\psi \mid \psi \, \mathsf{U} \, \psi \mid \psi \, \mathsf{R} \, \psi$$

2.2 Systèmes AP-déterministes

Un système de transition $\langle \mathrm{AP}, Q, I, T, l \rangle$ est *AP-déterministe* si

1. pour tout ensemble $a \subseteq \mathrm{AP}$ de propositions atomiques, $|I \cap \{q \mid l(q) = a\}| \leq 1$, et
2. pour tout état q de Q, $(q, q_1) \in T$ et $(q, q_2) \in T$ avec $l(q_1) = l(q_2)$ impliquent $q_1 = q_2$.

Montrer que si deux systèmes de transition sont AP-déterministes, alors ils sont équivalents modulo bisimulation si et seulement s'ils sont équivalents modulo simulation : $M_1 \sim M_2$ ssi $M_1 \simeq M_2$.

2.3 Bisimulations

1. Montrer que $M_1 \sim M_2$ implique $M_1 \simeq M_2$.
2. Donner un exemple de deux systèmes M_1 et M_2 tels que $M_1 \simeq M_2$ mais $M_1 \not\sim M_2$.