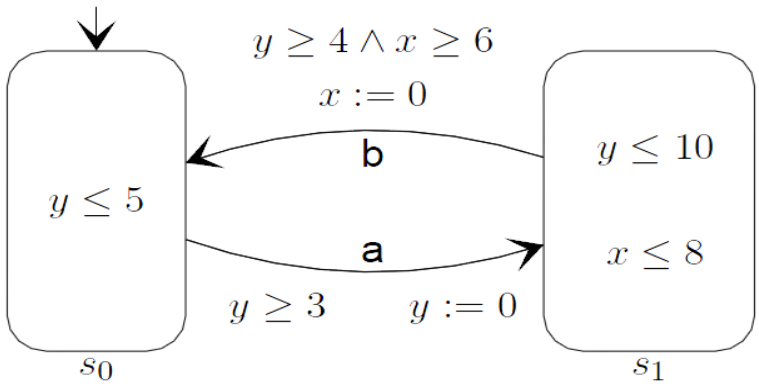
# SERIE 1 (CORRECTION)

**Cours :** Vérification formelle
**Filière/Classe :** 3ème ING
**Filière :** embarqué

## Exercice 1 :

Soit l'automate temporisé T suivant :




1. Définir formellement T.
2. Donner 2 trajectoires de T.

## Correction

1. T ==<Q,E,$s_0$,H,I,T> :
   - $Q = \{s_0, s_1\}$.
   - $E = \{a, b\}$.
   - $H = \{x, y\}$
   - $I$ : Q →C(H) associe à chaque état un invariant.
     $I(s_0) = y \leq 5$ , $I(s_1) = y \leq 10 \wedge x \leq 8$
   - $T \subseteq Q \times C(H) \times E \times 2^H \times Q = \{( s_0, y \geq 3, a, y, s_1), ( s_1, y \geq 4 \wedge x \geq 6, a, x, s_0)\}$.

2. Voici 2 trajectoires :

1. $(s0, 0, 0) \longrightarrow^{3} (s0, 3, 3) \longrightarrow^{a} (s1, 3, 0) \longrightarrow^{4}$
   $(s1, 7, 4) \longrightarrow^{b} (s0, 0, 4) \longrightarrow^{1} (s0, 1, 5) \longrightarrow^{a}$
   $(s1, 1, 0) \ldots$
2. $(s0, 0, 0) \longrightarrow^{3.2} (s0, 3.2, 3.2) \longrightarrow^{a} (s1, 3.2, 0) \longrightarrow^{4.1}$
   $(s1, 7.3, 4.1) \longrightarrow^{b} (s0, 0, 4.1) \longrightarrow^{0.1}$
   $(s0, 0.1, 4.2) \longrightarrow^{a} (s1, 0.1, 0) \ldots$

$(s0,0,0) \xrightarrow{a,3} (s1,3,0) \xrightarrow{b,7} (s0,0,4)$

**Exercice 2 :**

On considère un tunnel étroit qui ne permet le passage que d'un seul train à la fois. Deux trains circulent sur cette ligne.

Afin d'assurer la sécurité des voyageurs, chaque train peut échanger des signaux avec un médiateur qui assure le trafic dans le tunnel. Ces signaux sont de trois types :

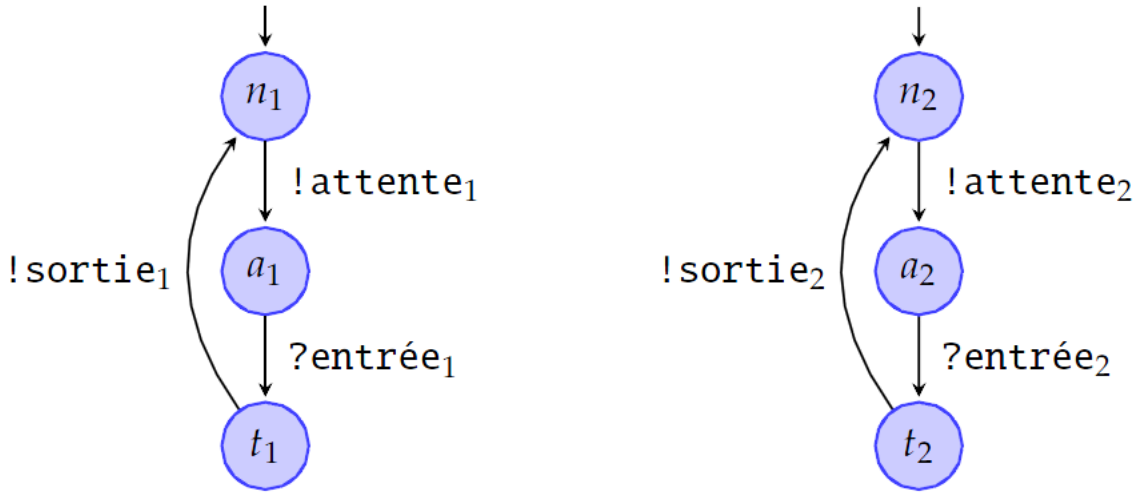
- attente : le train veut traverser le tunnel et attend une autorisation,
- entrée : le train obtient l'autorisation d'entrer dans le tunnel,
- sortie : le train sort du tunnel.

Chaque signal est indexé par le numéro du train concerné.

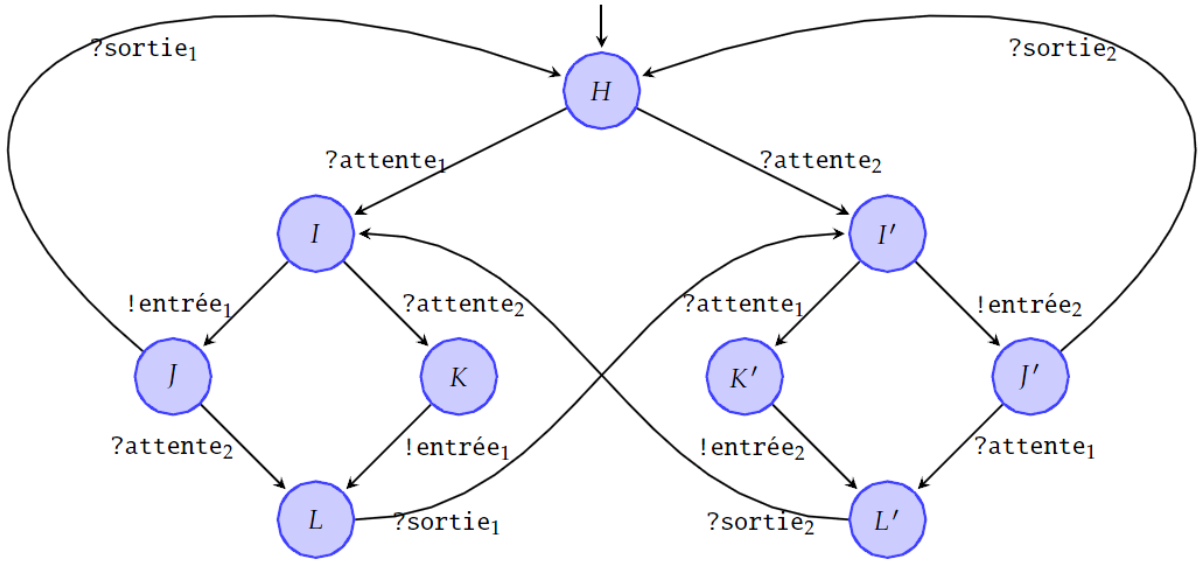
1. Modéliser le comportement des deux trains sachant qu'ils sont synchronisés par émission de message (signaux).
2. Modéliser le comportement du médiateur.
3. Dans le système global, obtenu par le produit synchronisé des 3 automates, quelles-sont les transitions de ce système ? Dessiner-le.

**Correction**

1.

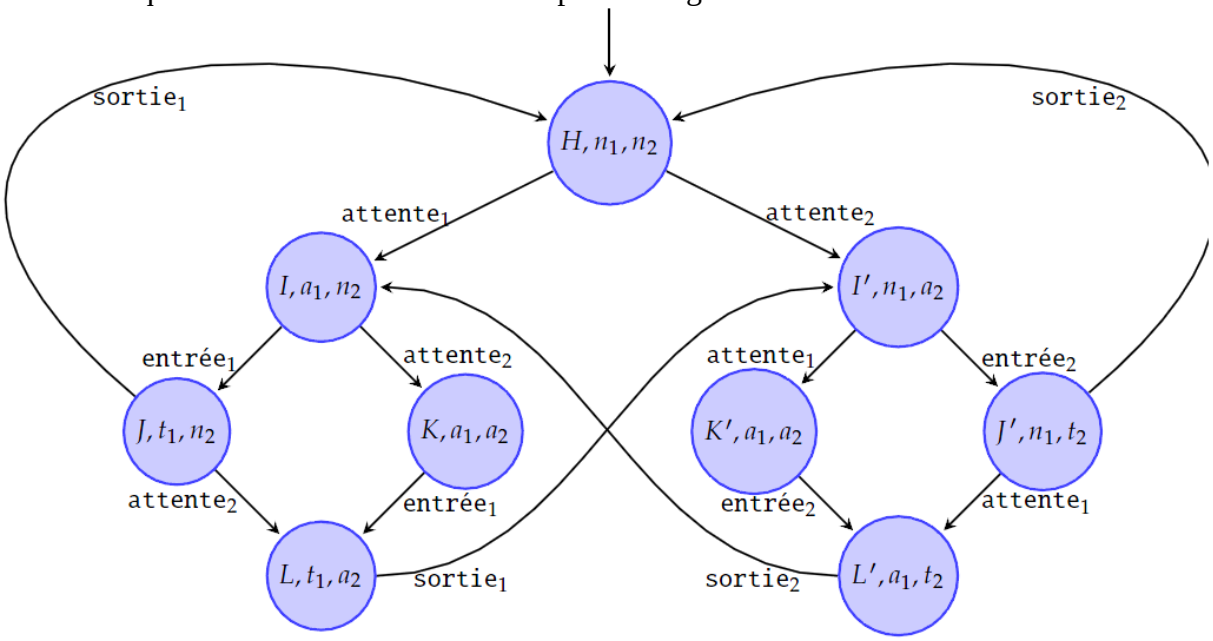



2.




3. Pour modéliser le système global, on réalise un produit synchrone des trois automates.
Un produit synchrone est un produit d'automates pour lequel on ne considère qu'un certain type de transitions.

Dans le cas présent, on réalise une synchronisation par messages et on se limite donc aux transitions qui contiennent à la fois ?x et !x pour un signal x donné.



**Exercice 3**

Nous aimerions modéliser un distributeur d'argent simplifié dans lequel le client récupère toujours la même somme d'argent fixée d'emblée. Ci-dessous les opérations possibles :

- Un client insère sa carte,
- ensuite il saisit son code,
- le distributeur peut ou bien valider le code ou bien le refuser,
- si le code est bon le client récupère directement sa carte puis son argent.
- si le code n'est pas bon, le distributeur lui donne une autre chance de saisir son code (il peut essayer 3 fois de suites) sinon, à la fin du troisième essai, le distributeur garde la carte du client sans informer celui-ci.

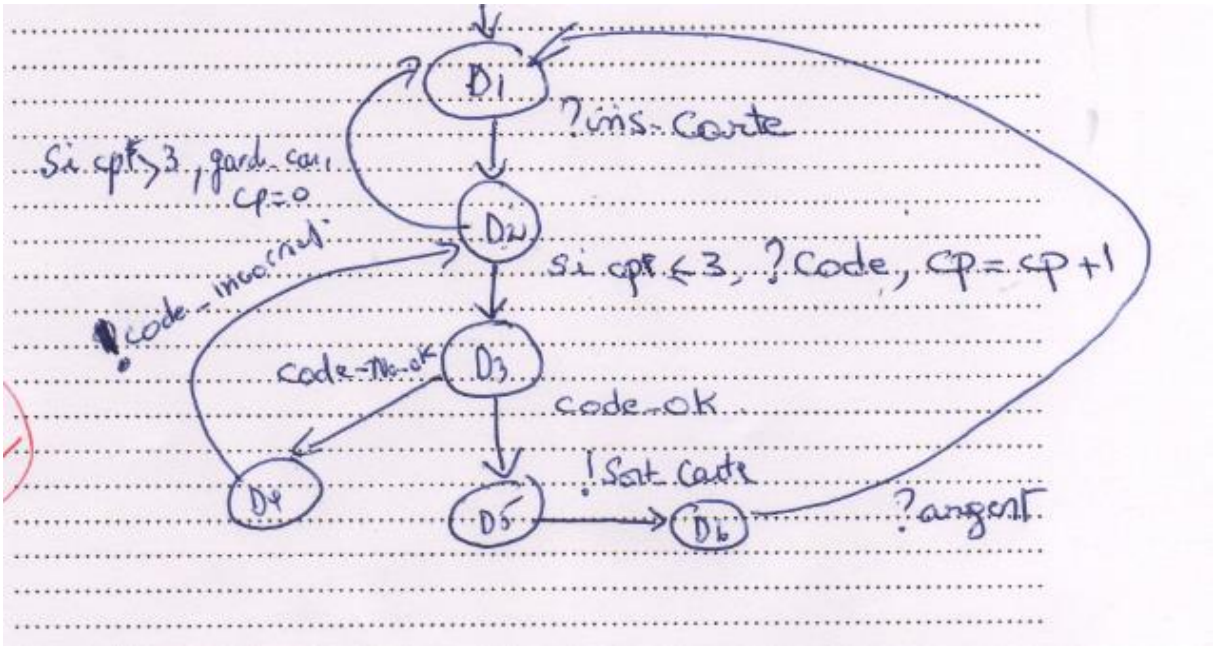
Sachez que le but de l'exercice est de synchroniser les deux processus Client et Distributeur par envoie/réception de message et qu'il peut y avoir des actions d'envoie/réception et d'autres internes aux processus.

1. Modéliser le processus D (Distributeur) par une structure de Kripke. Indiquer l'état initial et les actions de ce dernier.
2. Modéliser le processus C (Client) par une structure de Kripke. Indiquer l'état initial et les actions de ce dernier.

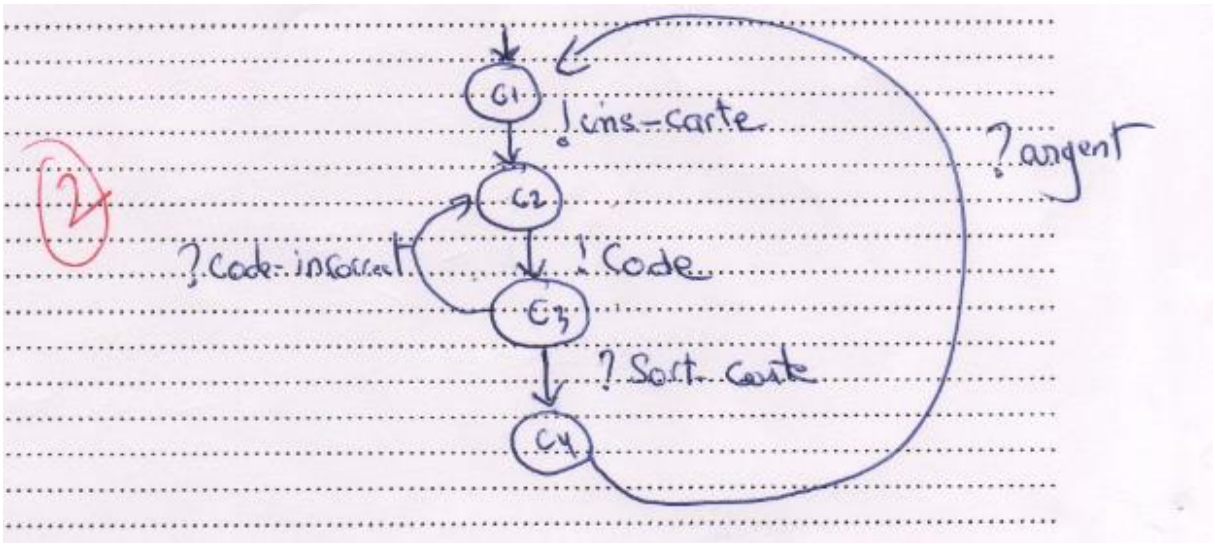
3. Synchroniser les deux processus par envoie/réception de messages.

**Correction :**

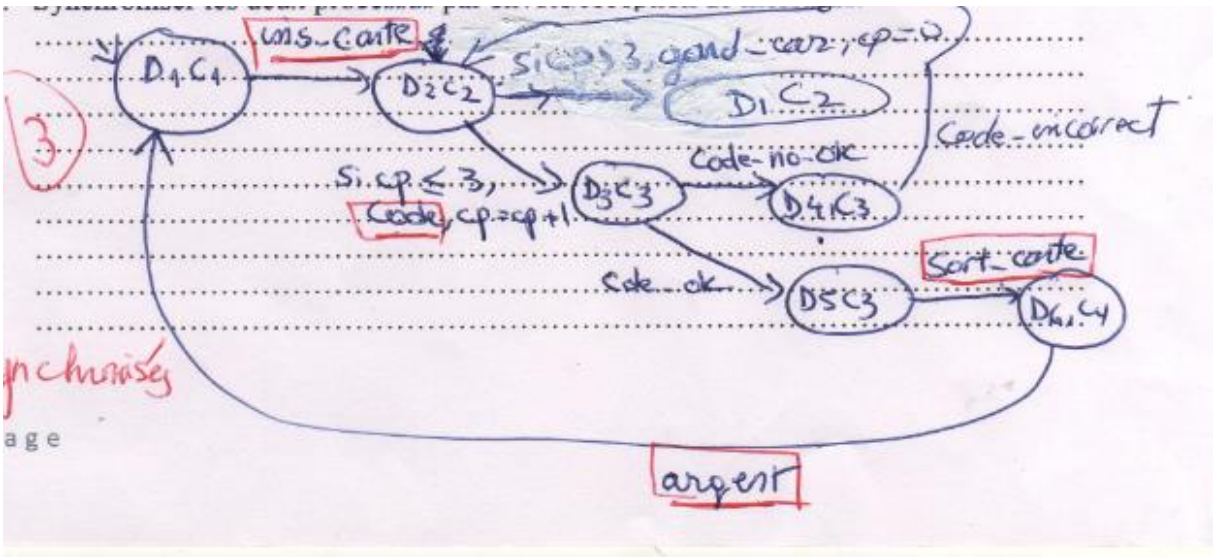
4. Modéliser le processus D (Distributeur) par une structure de Kripke. Indiquer l'état initial et les actions de ce dernier.

5. 


Modéliser le processus C (Client) par une structure de Kripke. Indiquer l'état initial et les actions de ce dernier.



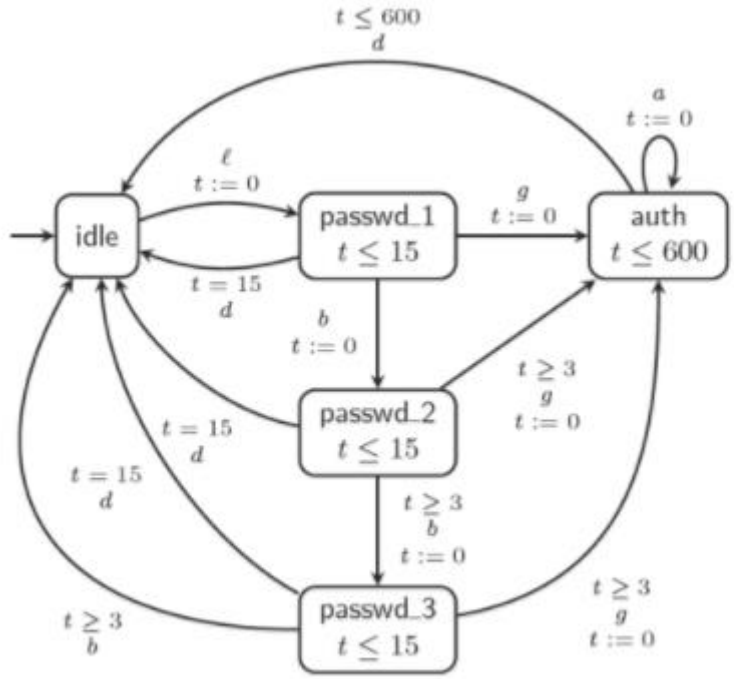

6. Synchroniser les deux processus par envoie/réception de messages. **2**




**Exercice 4**

Le but de cet exercice est de modéliser un système de web mail dans lequel un utilisateur se connecte en introduisant son login et mot de passe afin de réaliser des opérations divers.

1. Modéliser ce système par un automate approprié en prenant soin de donner sa définition formelle et la structure de Kripke schématisée, en respectant la spécification donnée ci-dessous.
    - L'utilisateur doit saisir son login.
    - Dès que le login saisi, l'utilisateur a 15 secondes pour saisir son mot de passe, sinon il sera déconnecté à l'instant *t = 15 secondes* (après déconnexion il peut bien sûr ensuite réessayer à nouveau).
    - Si le mot de passe a été saisi dans un délai ne dépassant pas 15 secondes, l'utilisateur a trois tentatives pour entrer un mot de passe correct, et à chaque fois dans un délai de 15 secondes. Au bout de ces trois tentatives, si le bon mot de passe n'est pas saisi, l'utilisateur sera déconnecté. Il est à noter, que si le mot de passe est incorrect, il ne peut essayer à nouveau qu'au bout de 3 secondes (après déconnexion il peut bien sûr ensuite réessayer à nouveau).
    - Si le bon mot de passe est saisi dans le délai fixé, l'utilisateur est authentifié et peut réaliser des opérations diverses.
    - Pendant cette connexion, l'utilisateur peut rester connecter tant qu'il réalise des opérations et peut aussi se déconnecter de son propre grès.
    - Cependant, s'il reste inactif pendant plus que 600 secondes, la session est perdue et l'utilisateur est déconnecté.




$\ell$ = login entré,

$g$ = mot de passe correct,

$b$ = mot de passe incorrect,

$a$ = actions diverses,

$d$ = déconnexion.