Systèmes temporisés (suite)

MI045 – Modélisation et Représentation des Connaissances

Mathieu Sassolas
mathieu.sassolas@lip6.fr

Université Pierre et Marie Curie

6 mai 2010

Plan du cours

Besoin de modélisation modulaire

- Des parties plus petites sont plus facilement modélisables par l'homme.
- Modélisation de différentes parties par différents acteurs.
- Vérification plus simple de chaque modèle.
- Un processus de modélisation itératif.

Intuition

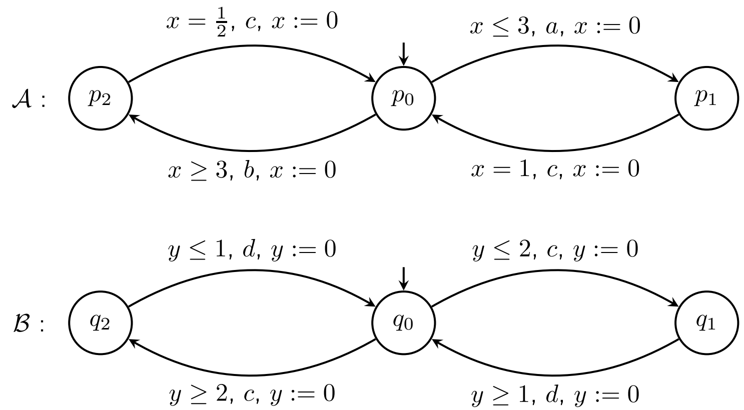
- Synchronisation sur certaines actions
- Les autres actions sont indépendantes les unes des autres
- Les horloges restent indépendentes
- Toutes les horloges gardent la même pente

Définition

Si $\mathcal{A}_1 = \langle Q_1, q_1^i, \Sigma_1, X_1, \Delta_1, Inv_1\rangle$ et $\mathcal{A}_2 = \langle Q_2, q_2^i, \Sigma_2, X_2, \Delta_2, Inv_2\rangle$ sont des automates temporisés avec $X_1 \cap X_2 = \emptyset$, la synchronisation de $\mathcal{A}_1$ et $\mathcal{A}_2$ est l'automate temporisé $\mathcal{A}_1||\mathcal{A}_2 = \langle Q, q^i, \Sigma, X, \Delta, Inv\rangle$ où

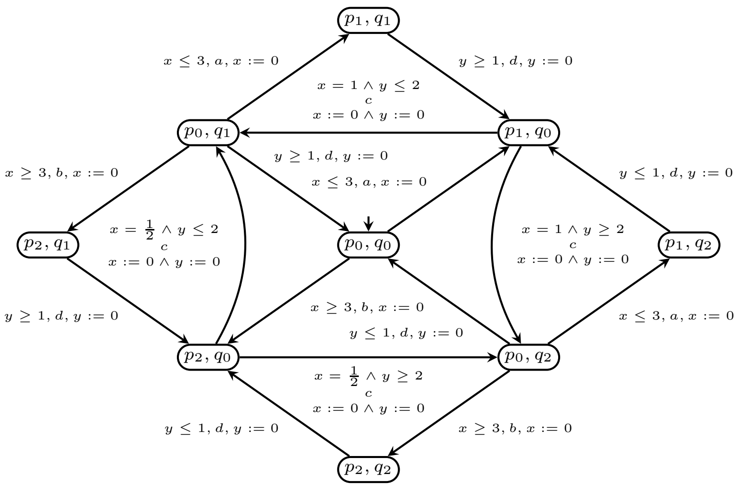
- $Q = Q_1 \times Q_2$
- $q^i = (q_1^i, q_2^i)$
- $\Sigma = \Sigma_1 \cup \Sigma_2$
- $X = X_1 \cup X_2$
- Supposons que $(q_1, g_1, a_1, r_1, q_1') \in \Delta_1$ et $(q_2, g_2, a_2, r_2, q_2') \in \Delta_2$.
  - si $a_1 = a_2 = a \in \Sigma_1 \cap \Sigma_2$, on se synchronise : $((q_1, q_2), g_1 \wedge g_2, a, r_1 \cup r_2, (q_1', q_2')) \in \Delta$
  - si $a_1 \in \Sigma_1 \setminus \Sigma_2$, seul $\mathcal{A}_1$ évolue : $((q_1, q_2), g_1, a_1, r_1, (q_1', q_2)) \in \Delta$
  - si $a_2 \in \Sigma_2 \setminus \Sigma_1$, seul $\mathcal{A}_2$ évolue : $((q_1, q_2), g_2, a_2, r_2, (q_1, q_2')) \in \Delta$
- $\forall (q_1, q_2) \in Q_1 \times Q_2,\ Inv(q_1, q_2) = Inv_1(q_1) \wedge Inv_2(q_2)$

Exemple – Automates originaux



$\hookrightarrow$ Synchronisation sur c.

Exemple – Composition



Accessibilité

Théorème ([Alur et Dill, 1990])

L'accessibilité d'un état de contrôle est décidable pour les automates temporisés.

Procédure de décision.

Donnée : un automate temporisé $\mathcal{A} = (X, Q, q_0, \Delta, Inv)$, avec domaine de temps $\mathbb{R}_{\geq 0}$ et un état de contrôle q_f

$\mathcal{T}_\mathcal{A} = (S, s_0, E)$ système de transition associé à $\mathcal{A}$ configurations : (q, v) $q \in Q$, $v \in \mathbb{R}_{\geq 0}^X$	$\xrightarrow{quotient}$	$\mathcal{K}_\mathcal{A}$ automate des régions de $\mathcal{A}$ états : $(q, [v])$ $q \in Q$, $[v]$ classe d'équivalence pour une relation $\sim$ sur $\mathbb{R}_{\geq 0}^X$

Construction d'un automate non temporisé $\mathcal{K}_\mathcal{A}$ tel que :
$\mathcal{A}$ a une exécution qui atteint (q_f, v_f) $\iff$ $\mathcal{K}_\mathcal{A}$ a une exécution qui atteint $(q_f, [v_f])$. □

Construction d'une relation quotient

Définition (Équivalence des régions)

La relation que l'on veut construire a les propriétés suivantes : Pour deux valuations équivalentes $v \sim v'$

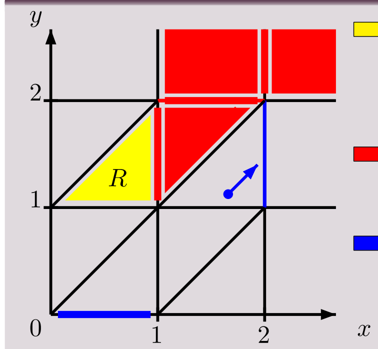
1. si une transition d'action $q \xrightarrow{g,a,r} q'$ est possible depuis v, alors la même transition est possible depuis v' et les valuations obtenues $v[r \mapsto 0]$ et $v'[r \mapsto 0]$ sont équivalentes,
2. si une transition de délai d est possible depuis v, alors une transition de délai d' est possible depuis v' et les valuations obtenues $v + d$ et $v' + d'$ sont équivalentes.

Remarques

- Cette relation est une bisimulation avec abstraction du temps entre les états de $\mathcal{T}_\mathcal{A} : Q \times \mathbb{R}^X_{\geq 0}$ et ceux de $\mathcal{K}_\mathcal{A} : Q \times \mathbb{R}^X_{\geq 0}/\sim$.
- Pour la première condition, il suffit de considérer les contraintes $x \bowtie k$, pour les horloges de X et les constantes $0 \leq k \leq m$, où m est la plus grande constante apparaissant dans les contraintes de $\mathcal{A}$.

Vue géométrique

Exemple (avec deux horloges x et y, pour $m = 2$)



Région R définie par
$I_x =]0;1[$, $I_y =]1;2[$
$frac(x) > frac(y)$

Successeur de R pour le temps
$I_x = [1;1]$, $I_y =]1;2[$

Successeur de R pour une action avec $y := 0$
$I_x =]0;1[$, $I_y = [0;0]$

- Compatibilité de valuations équivalentes avec les contraintes $x, y \bowtie k$
- Compatibilité de valuations équivalentes avec l'écoulement du temps

Construction de l'automate

Définition

Automate des régions $\mathcal{K}_\mathcal{A}$ pour l'automate temporisé $\mathcal{A} = (X, Q, q_0, \Delta, Inv)$, avec constante maximale m, quotient $\mathbb{R}^X_{\geq 0}/\sim$ noté $\mathcal{R}_{X,m}$.

- états $Q \times \mathcal{R}_{X,M}$
- transitions de délai (abstraites) : $(q, R) \xrightarrow{\leq} (q, succ(R))$
- transitions d'action : $(q, R) \xrightarrow{a} (q', R')$ s'il existe une transition $q \xrightarrow{g,a,r} q'$ de $\mathcal{A}$ avec $R \models g$ et $R' = R[r \mapsto 0]$

Remarque

La taille de $\mathcal{R}_{X,m}$ est en $\mathcal{O}(|X|! \cdot m^{|X|})$, à multiplier par $|\ Q\ |$.

Construction des configurations accessibles

Exemple