Automates temporisés

Partie 1: Définitions

Motivation

- Les automates temporisés constituent un des modèle de systèmes réactifs à temps continu proposé par Alur et Dill en 1991.
- Temps continu vs temps discret.
  - Résultat de Brzozowsky et Seger: le problème de l'atteignabilité pour les circuits asynchrones avec délais bornés est non soluble si le temps est supposé discret.
  - Discrétiser le temps conduit souvent à une explosion combinatoire.
- Il existe plusieurs modèles à temps continu, mais les automates temporisés se sont imposés.

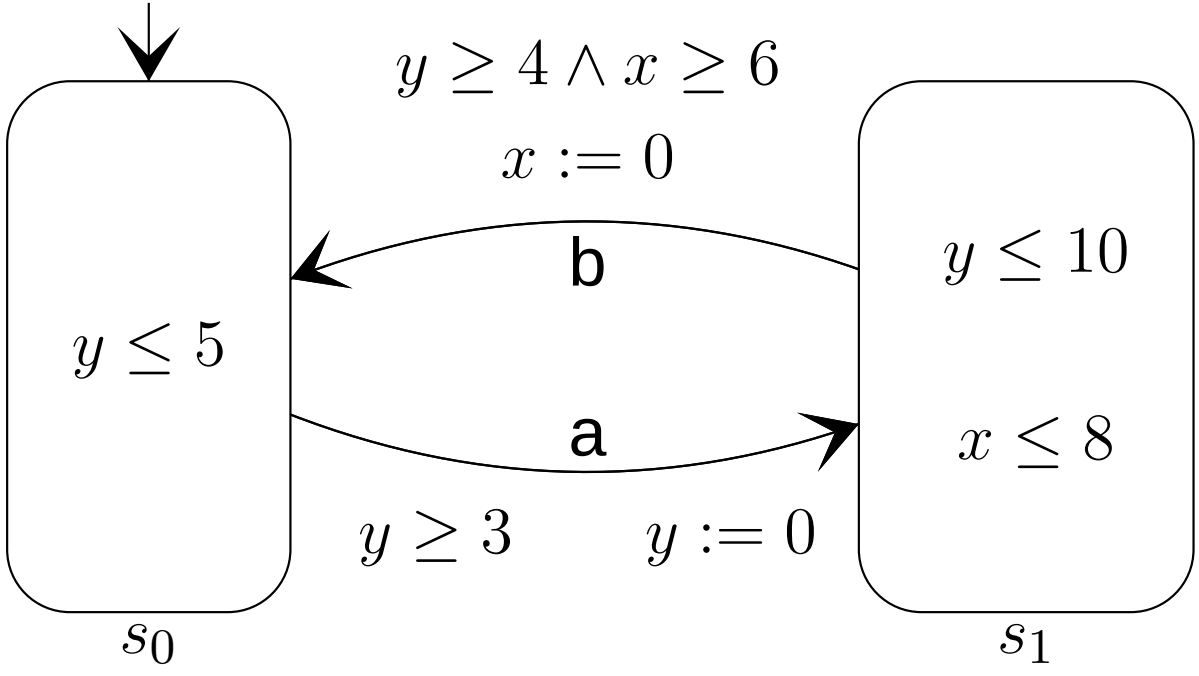
Automate temporisé: présentation

Un automate temporisé est un automate avec des *horloges*, c'est-à-dire des variables à valeurs réelles, positives ou nulles.

- Chaque automate possède un nombre fini de *places* (locations).
- Les transitions entre places sont instantanées.
- Dans chaque place, le temps peut s'écouler: à tout instant, la valeur d'une horloge x est le temps écoulé depuis la dernière mise à 0 de x.
- Les transitions entre places sont conditionnées par des contraintes sur les horloges, appelés *gardes*, et peuvent remettre certaines horloges à 0.
- A chaque place est associée une contrainte sur les horloges, appelée *invariant*.

Exemple

- Un automate temporisé simple:



Quelques trajectoires

- Quelques 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. $(s0,0,0) \longrightarrow^{3.2} (s0,3.2,3.2) \longrightarrow^{a} (s1,3.2,0) \longrightarrow^{4.1}$
     $(s1,7.3,4.1) \longrightarrow^{b} (s0,0,4.1) \longrightarrow^{0.1}$
     $(s0,0.1,4.2) \longrightarrow^{a} (s1,0.1,0)\ldots$
  3. $\ldots$

Déf. formelle: contraintes d'horloges

- Un horloge x est une variable à valeur dans $IR^{\geq 0}$, l'ensemble des réels positifs ou nuls.
- Soit X un ensemble fini d'horloges. L'ensemble $\mathcal{C}(X)$ des contraintes d'horloges est défini par la grammaire

$$true|x < c|x \leq c|x > c|x \geq c|\phi_1 \wedge \phi_2$$

où $x \in X$ est une horloge, $c \in \mathbb{Q}$ est un rationnel, ϕ_1,ϕ_2 sont des contraintes d'horloges.

Définition formelle

- Un automate temporisé est $A = (\Sigma, S, S_0, X, I, T)$ avec
  1. Σ un alphabet fini.
  2. S un ensemble fini de places (locations).
  3. $S_0 \subset S$ un ensemble de places initiales.
  4. X un ensemble fini de variables (horloges).
  5. $I : S \to \mathcal{C}(X)$ des invariants de places.
  6. $T \subset S \times \Sigma \times \mathcal{C}(X) \times 2^X \times S$ un ensemble de transitions d'actions.
     Chaque $e =< s, a, \varphi, \lambda, s' > \in T$ correspond à une transition entre la place s et la place s', gardée par la contrainte φ, étiquetée par la lettre a, et qui remet les variables de $\lambda \subset X$ à 0.

Hypothèses

- Hypothèses.
  1. Dans cet exposé, on suppose les automates temporisés non Zénon.

     I.e. il n'est pas possible d'effectuer un nombre non-fini de transitions en un temps borné.
  2. On suppose que le temps peut toujours progresser.

     I.e. dans chaque place, l'invariant n'a pas de borne supérieure, ou il existe une transition d'action que l'on peut prendre avant d'atteindre la borne supérieure de l'invariant.

Modèle d'un automate temporisé

Un automate temporisé A s'interprète comme le système de transition étiqueté avec un ensemble d'états infini $\tau(A) = (\Sigma, Q, Q_0, R)$ avec

1. Q, l'ensemble des états, est constitué des couples (s, v). $s \in S$ donne la place, et v est une valuation des horloges. (Une *valuation d'horloges* est une fonction $X \to I\!R^{\geq 0}$, c'est à dire une fonction qui associe à chaque horloge sa valeur.)
2. $Q_0 \subset Q$, l'ensemble des états initiaux est constitué des couples (s, v) avec $s \in S_0$ et $v(x) = 0$ pour tout $x \in V$. (autrement dit, on part d'une place de S_0 avec toutes les variables à 0).
3. R, la relation de transition est décrite dans les transparents suivants.

La relation R

Définitions. Soit v une valuation d'horloges.
(autrement dit, une fonction qui associe à chaque variable sa valeur.)

- Soit $\lambda \subset X$. On note $v[\lambda := 0]$ la valuation telle que

$$v[\lambda := 0](x) = \begin{cases} 0 & \text{si } x \in \lambda, \\ v(x) & \text{sinon.} \end{cases}$$

  (autrement dit, $v[\lambda := 0]$ est ce que l'on obtient en remettant les variables de $\lambda \subset X$ à 0.)

- Soit $d \in IR^{\geq 0}$. On note $v + d$ la valuation telle que $v + d(x) = v(x) + d$ pour tout $x \in X$.
  (autrement dit, $v + d$ est ce qu'on obtient en ajoutant d à toutes les variables.)

- Soit $d \in IR^{\geq 0}$. On note $v - d$ la valuation telle que $v - d(x) = v(x) - d$ pour tout $x \in X$.
  (autrement dit,$v - d$ est ce qu'on obtient en supprimant d à toutes les variables.)

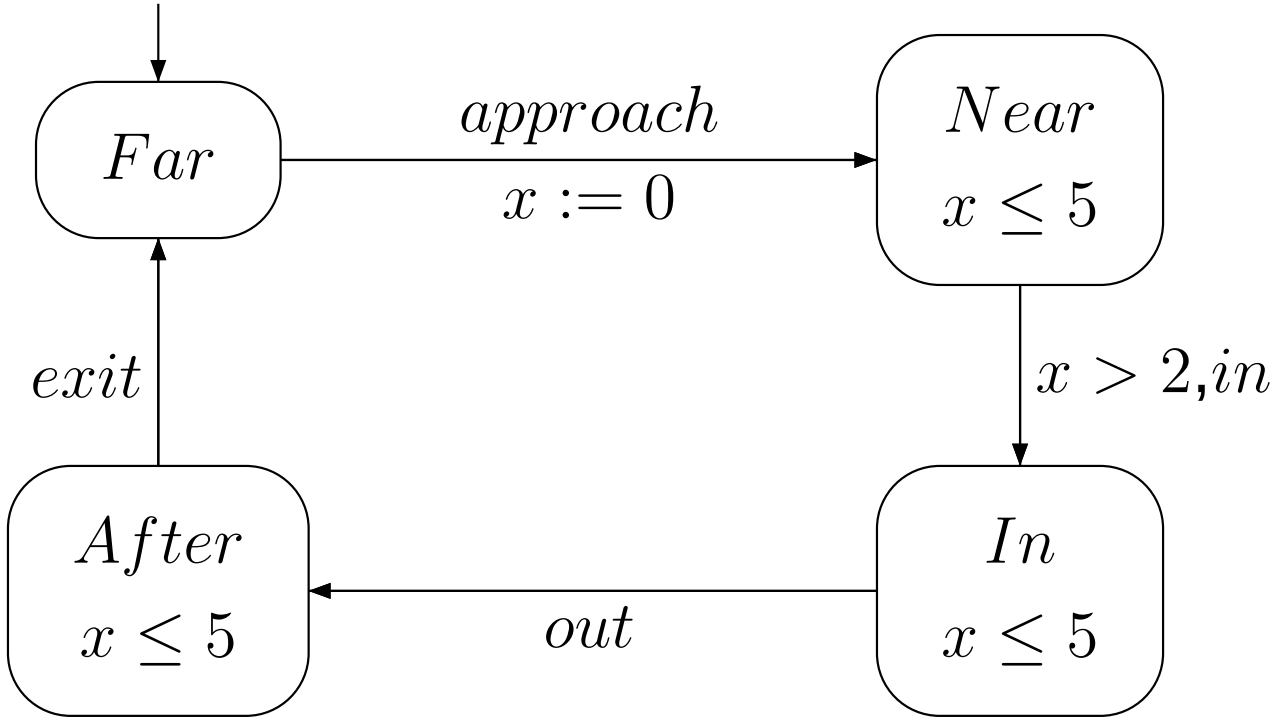
Relation R (suite)

- Principe: les transitions sont
  1. soit des transitions de temps,
  2. ou des transitions d'action.
- Transitions de temps: pour $d \in IR^{\geq 0}$, on note $(s, v) \longrightarrow^{d} (s, v')$ si $v' = v + d$ et pour tout $0 \leq e \leq d$, $v + e$ vérifie la contrainte $I(s)$.
- Transitions d'action: pour $a \in \Sigma$, on note $(s, v) \longrightarrow^{a} (s', v')$ s'il existe $< s, a, \varphi, \lambda, s' > \in T$ tel que
  1. v satisfait φ,
  2. $v' = v[\lambda := 0]$.

- La relation R est définie par: $(s,v)R(s',v')$ ssi il existe un $d \in IR^{\geq 0}$, un $a \in \Sigma$, et un état intermédiaire (s'',v'') , tels que $(s,v) \longrightarrow^{d} (s'',v'') \longrightarrow^{a} (s',v')$.
- On note $(s,v) \Rightarrow^{a} (s',v')$ ssi $(s,v)R(s',v')$.

Modélisation d'un train / barrière

Train:



Automates temporisés

Partie 2: Modélisation de systèmes

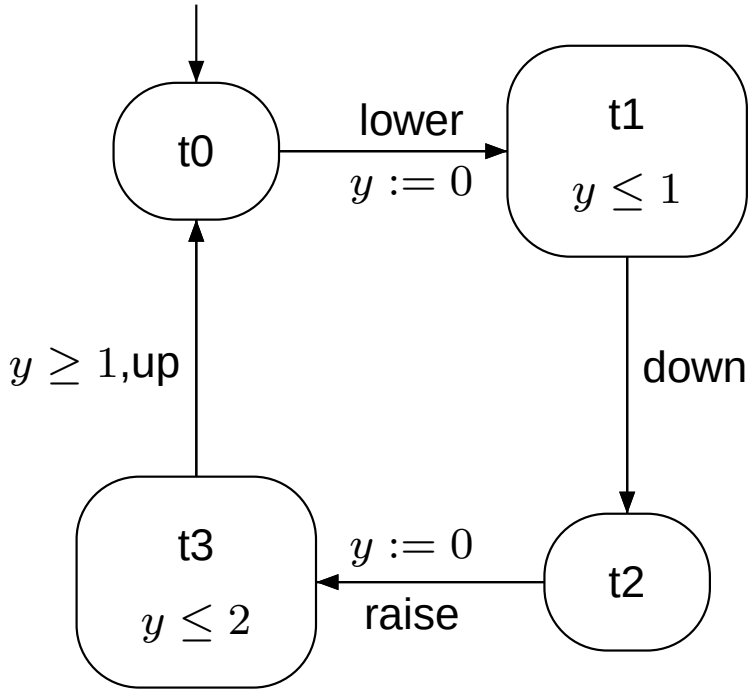
Modélisation avec des automates tem

Soient $A_1 = (\Sigma_1, S_1, S_0^1, X_1, I_1, T_1)$ et
$A_2 = (\Sigma_2, S_2, S_0^2, X_2, I_2, T_2)$ deux automates temporisés
avec $X_1 \cap X_2 = \emptyset$.
Alors $A_1 \| A_2$ est l'automate temporisé
$(\Sigma_1 \cup \Sigma_2, S_1 \times S_2, S_0^1 \times S_0^2, X_1 \cup X_2, I, T)$ avec

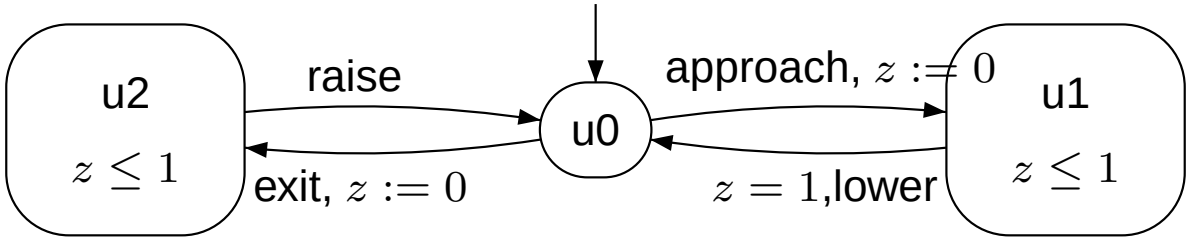
1. $I(s_1, s_2) = I_1(s_1) \wedge I_2(s_2)$
2. T est défini par:
   (a) pour $a \in \Sigma_1 \cap \Sigma_2$
   $< s_1, a, \varphi_1, \lambda_1, s_1' > \in T_1$ et $< s_2, a, \varphi_2, \lambda_2, s_2' > \in T_2$
   $\Rightarrow < (s_1, s_2), a, \varphi_1 \wedge \varphi_2, \lambda_1 \cup \lambda_2, (s_1', s_2') > \in T$,
   (b) pour $a \in \Sigma_1 - \Sigma_2$
   $< s, a, \varphi, \lambda, s' > \in T_1$ et $t \in S_2$
   $\Rightarrow < (s, t), a, \varphi, \lambda, (s', t) > \in T$,
   (c) symétriquement.

Exemple 1: Train || barrière || contrôl

Barrière:



Contrôleur:



Exemple 2

- Exemple: une zone de traitement, avec deux robots et des boites sur un tapis roulant.

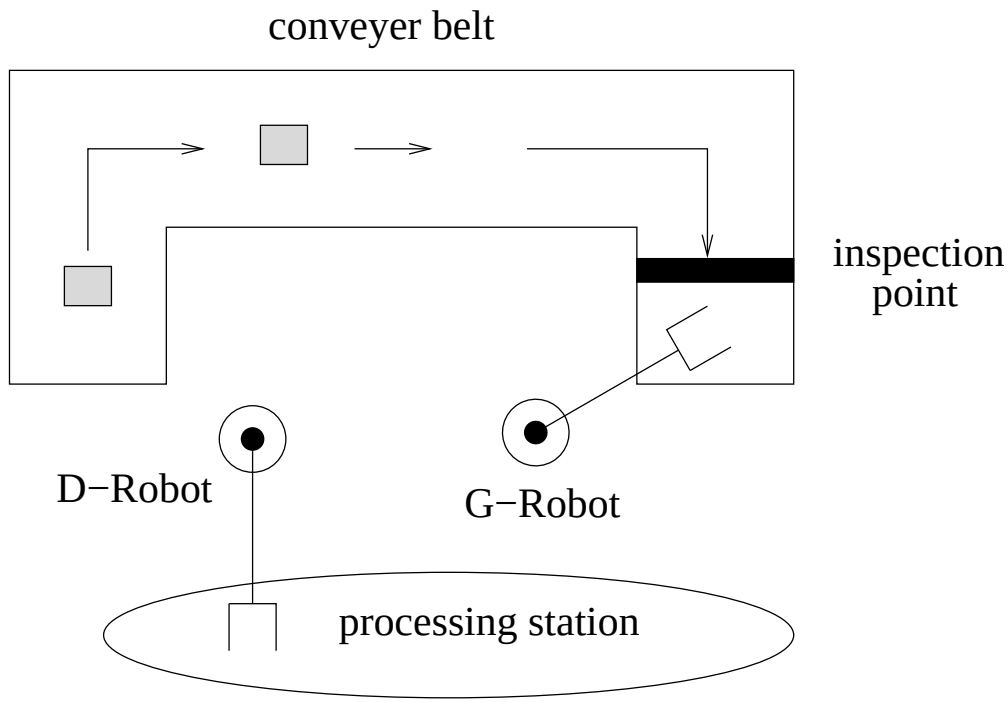
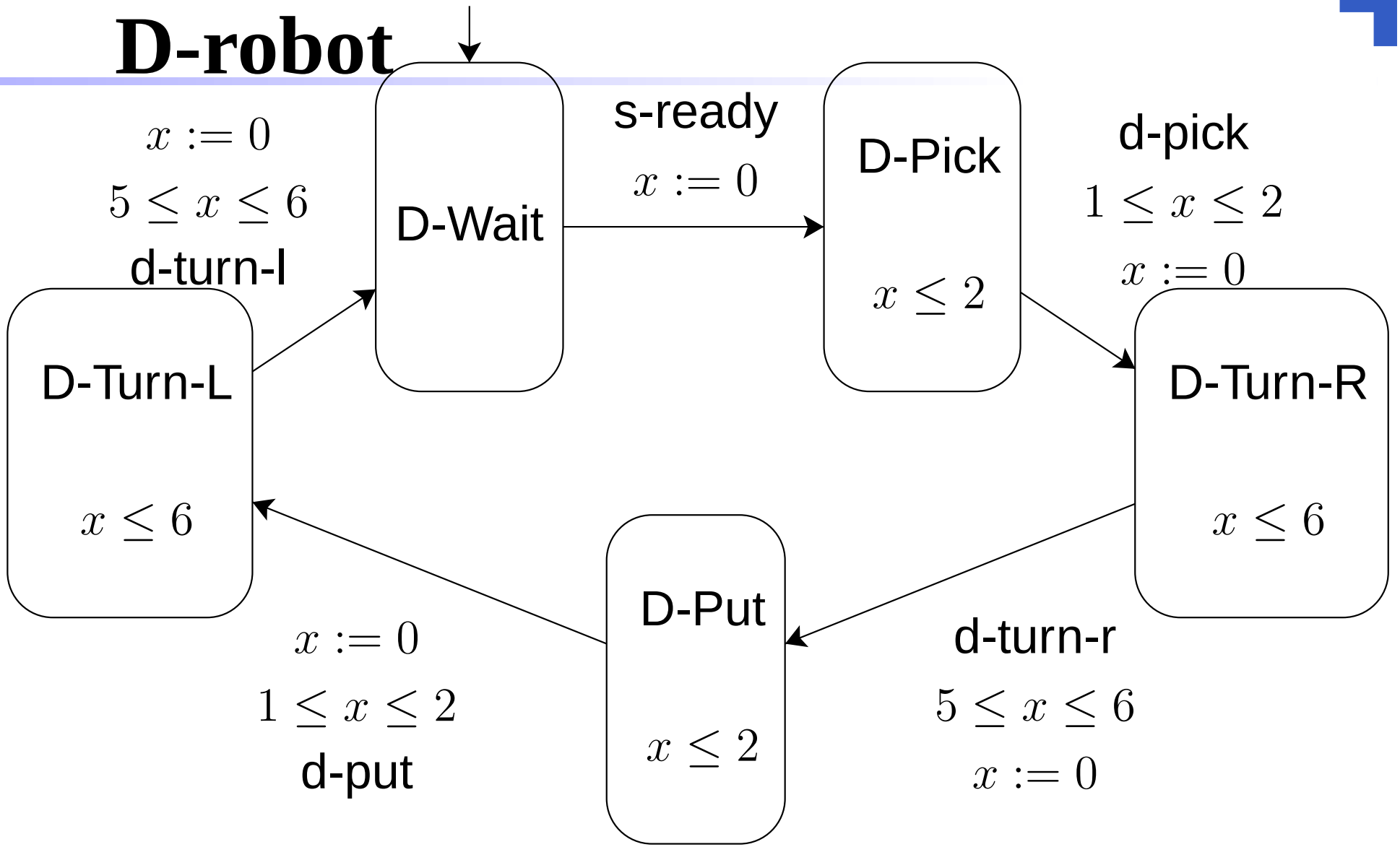
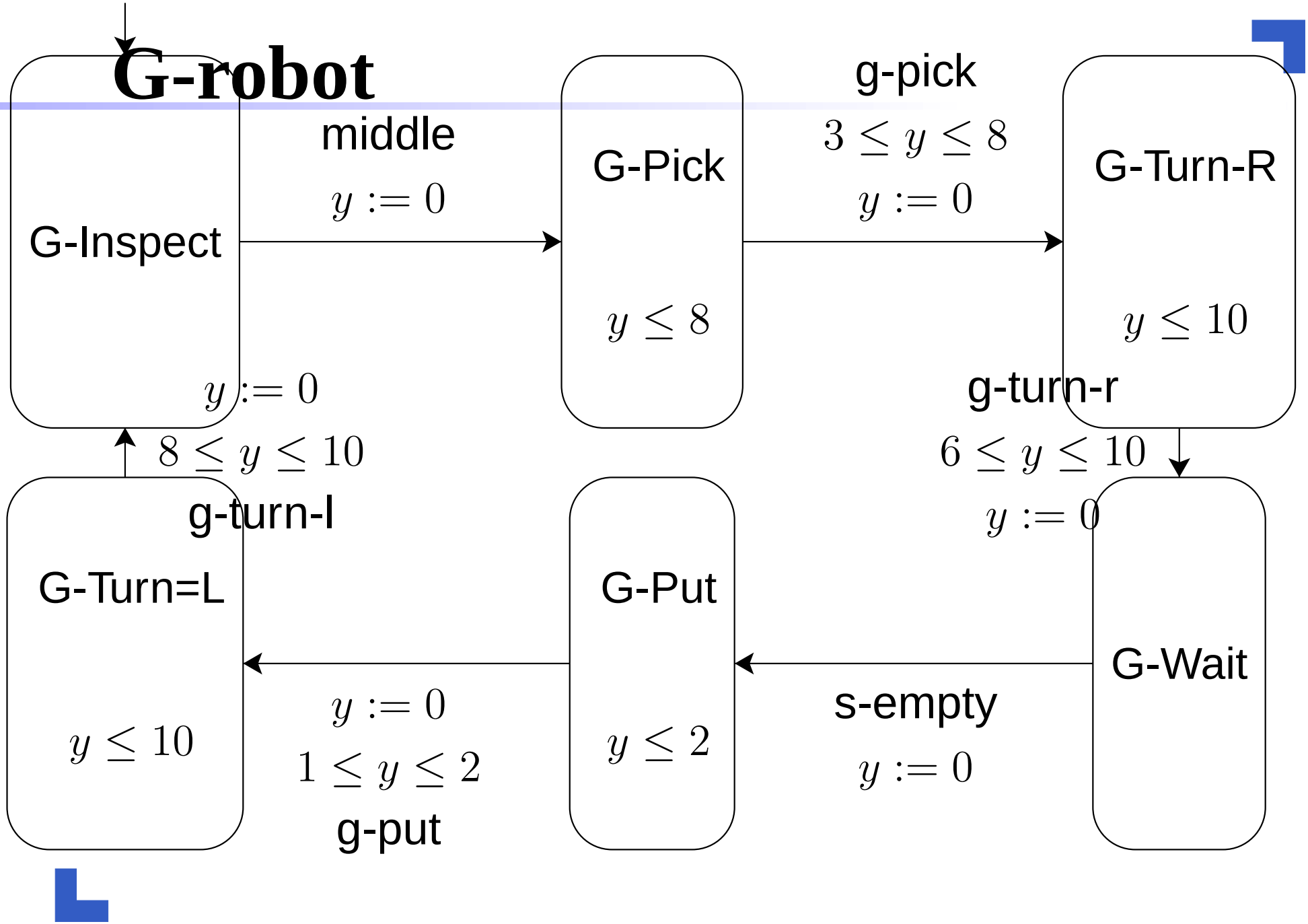


Figure 1: Une usine simple.

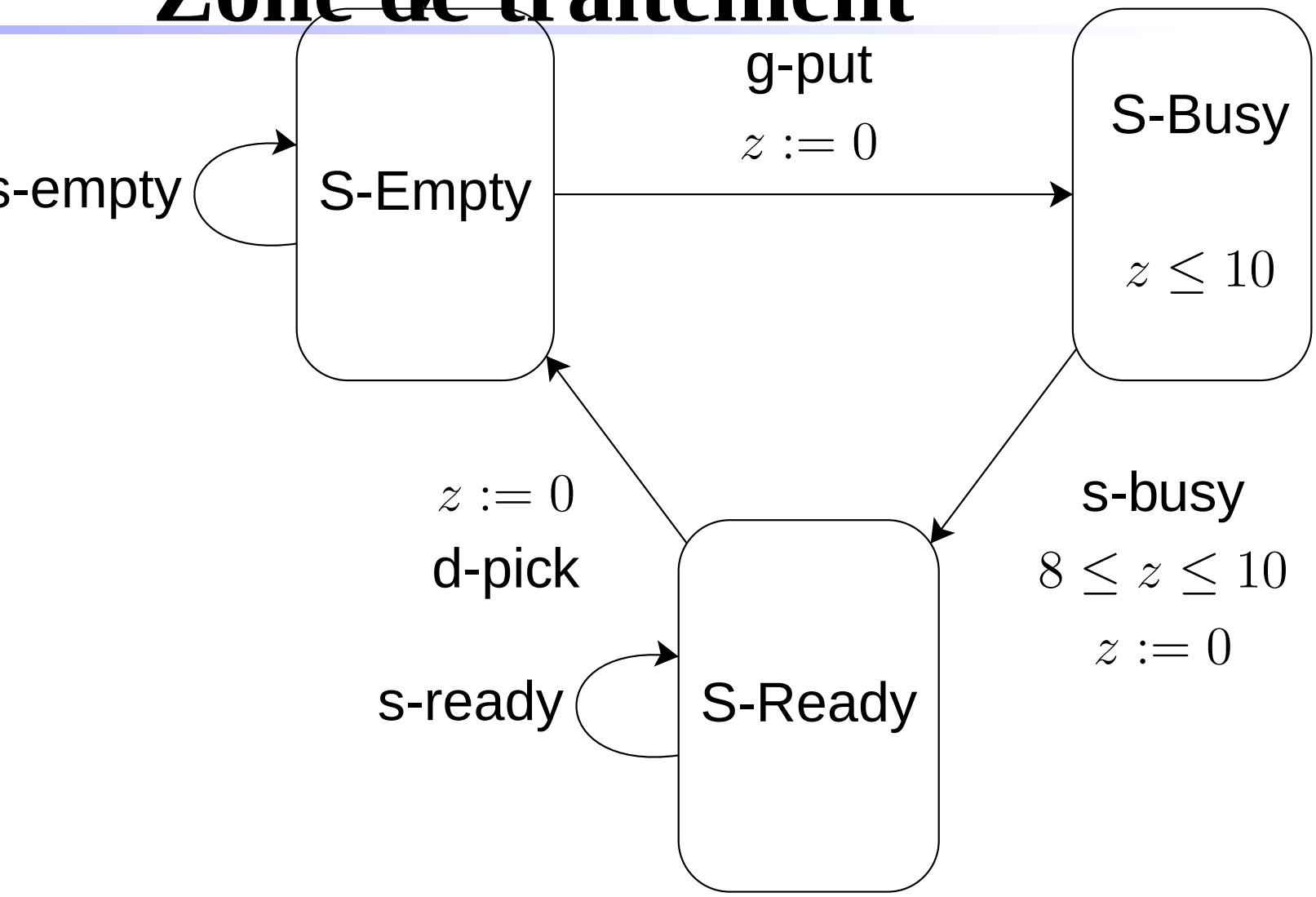
D-robot


D-Wait
s-ready
$x := 0$
D-Pick
$x \leq 2$
d-pick
$1 \leq x \leq 2$
$x := 0$
D-Turn-R
$x \leq 6$
d-turn-r
$5 \leq x \leq 6$
$x := 0$
D-Put
$x \leq 2$
$x := 0$
$1 \leq x \leq 2$
d-put
D-Turn-L
$x \leq 6$
$x := 0$
$5 \leq x \leq 6$
d-turn-l

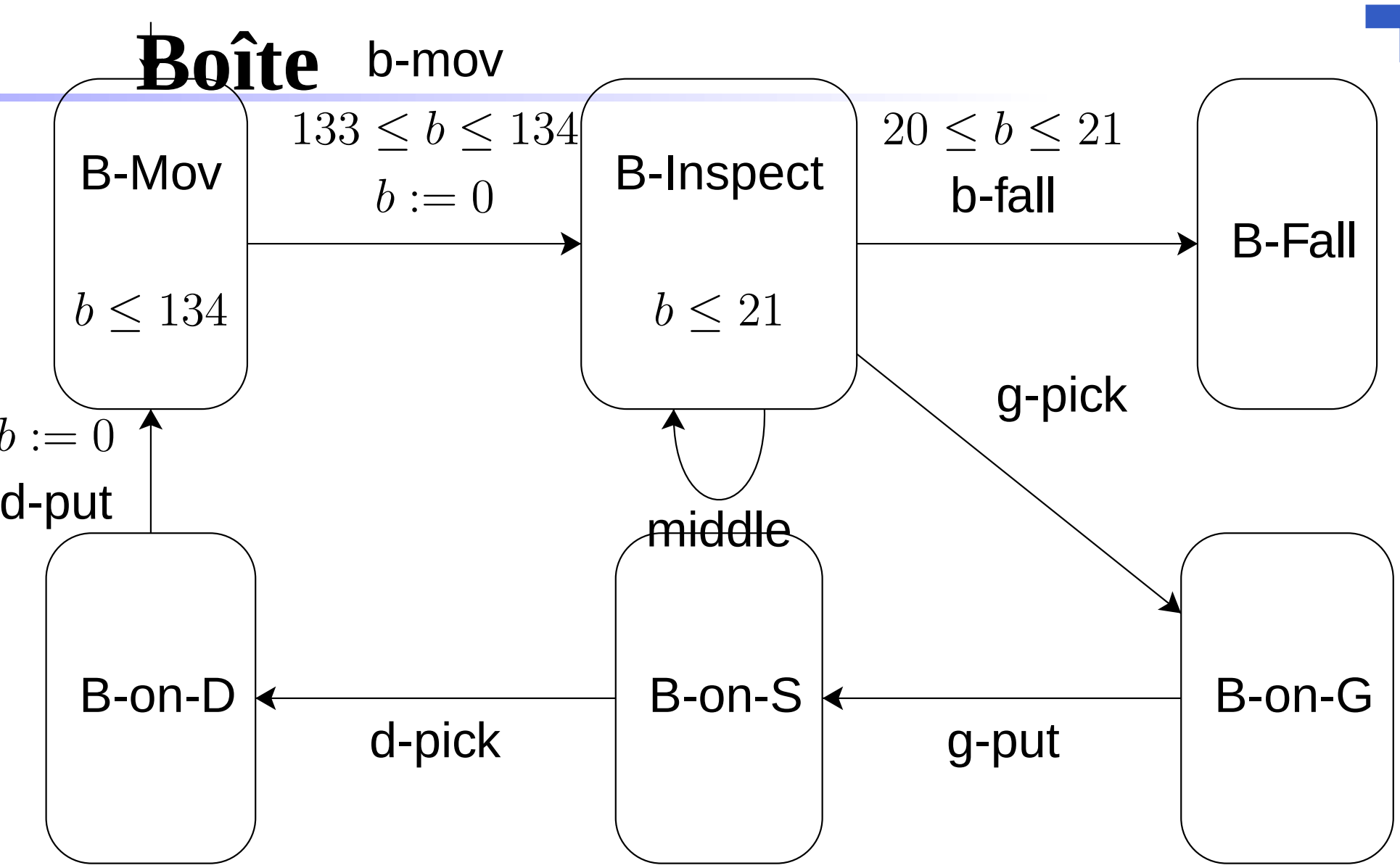
G-robot


G-Inspect
middle
$y := 0$
G-Pick
$y \leq 8$
g-pick
$3 \leq y \leq 8$
$y := 0$
G-Turn-R
$y \leq 10$
g-turn-r
$6 \leq y \leq 10$
$y := 0$
G-Wait
s-empty
$y := 0$
G-Put
$y \leq 2$
$y := 0$
$1 \leq y \leq 2$
g-put
G-Turn=L
$y \leq 10$
g-turn-l
$8 \leq y \leq 10$
$y := 0$

Zone de traitement



Boîte


b-mov
$133 \leq b \leq 134$
$b := 0$
B-Mov
$b \leq 134$
B-Inspect
$b \leq 21$
$20 \leq b \leq 21$
b-fall
B-Fall
g-pick
$b := 0$
d-put
middle
B-on-D
B-on-S
B-on-G
d-pick
g-put

Automates temporisés

Partie 3: Vérification

Problème de l'atteignabilité

Dans la suite on s'intéresse aux problèmes suivants:

- Problème de l'atteignabilité:
  1. Données:
     (a) A un automate temporisé,
     (b) $Q_f \subset Q$ un sous-ensemble d'états.
  2. Réponse: Oui s'il existe une trajectoire de A qui atteint Q_f, Non sinon.
- Problème du calcul des états atteignables:
  1. Données:
     (a) A un automate temporisé.
  2. Réponse: l'ensemble Q^R des états atteints par les trajectoires.

Remarque: si l'on sait résoudre le second, on sait résoudre le premier.

Il suffit de tester si $Q^R \cap Q_f \neq \emptyset$.

Remarque: ces problèmes ne sont pas triviaux car $\tau(A)$ a un nombre infini d'états.

Question

- Comment calculer les états atteignables par un automate temporisé?
- Solution.
  1. Étape 1: se ramener au cas où les constantes dans les contraintes d'horloges sont entières.
  2. Étape 2: considérer le quotient de $\tau(A)$ par une relation d'équivalence bien choisie.

Étape 1: supposer les constantes entiè

- Rappel: les contraintes d'horloges sont des conjonctions de contraintes du type $x \prec c$, avec $c \in \mathbb{Q}$, $\prec \in \{<, \leq, >, \geq\}$.
- Remarque:
  1. si on multiplie toutes les contraintes par une constante m,
  2. si on calcule les états atteignables de l'automate temporisé obtenu,
  3. et on divise le résultat par m,

  on obtient les états atteignables par l'automate temporisé initial.

- Conséquence: on peut supposer sans perte de généralité que l'ensemble $\mathcal{C}(X)$ des contraintes d'horloges est restreint à la grammaire

$$true|x < c|x \leq c|x > c|x \geq c|\phi_1 \wedge \phi_2$$

où $x \in X$ est une horloge, $c \in \mathbb{N}$ **est un entier**, ϕ_1,ϕ_2 sont des contraintes d'horloges.

Démonstration: considérer m comme le p.p.c.m. des dénominateurs des constantes.

- On suppose que c'est le cas dans la suite.

Étape 2: Remarques fondamentales

- Remarque 1. Deux états (s, v), (s, v') tels que v, v' ont même partie entière sur chaque horloge et tels que leurs parties fractionnaires sont dans le même ordre ont même comportement.
- Remarque 2. La valeur d'une horloge peut devenir très grande. Mais si une horloge n'est jamais comparée à une constante plus grande que c, alors la valeur de l'horloge n'a aucun effet sur le calcul de l'automate une fois qu'elle excède c.

Partition: Formalisation

- Définition: soit $x \in X$ un variable. On note c_x la plus grande constante à laquelle x est comparée.
- Notation: pour $t \in IR^{\geq 0}$,
  1. $fr(t)$ est la partie fractionnaire de t;
  2. $\lfloor t \rfloor$ est sa partie entière.

$$t = fr(t) + \lfloor t \rfloor$$

- Définition. on définit une relation d'équivalence $\simeq$ sur les valuations d'horloges.

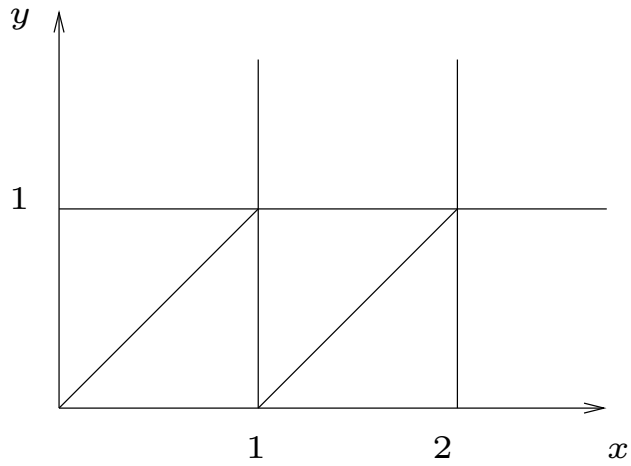
  Soient v, v' deux valuations d'horloges.
  $v \simeq v'$ ssi les trois conditions suivantes sont satisfaites:

  1. $\forall x \in X$,
     (a) soit $v(x) \geq c_x$ et $v'(x) \geq c_x$
     (b) ou $\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$;
  2. $\forall x, y \in X$ tels que $v(x) \leq c_x$ et $v(y) \leq c_y$
     $fr(v(x)) \leq fr(v(y))$ ssi $fr(v'(x)) \leq fr(v'(y))$;
  3. $\forall x \in X$ tels que $v(x) \leq c_x$
     $fr(v(x)) = 0$ ssi $fr(v'(x)) = 0$.

- Propriété: $\simeq$ est une relation d' équivalence sur les valuations d'horloges.

- Définitions:
  1. on appelle région une classe d'équivalence de $\simeq$;
  2. on note $[v]$ la région associée à la valuation d'horloges v.

Exercice: Représenter les classes d'équivalence pour $c_x = 2$ et $c_y = 1$.
Réponse:



- 6 régions réduites à un point: Exemple $(0, 1)$.
- 14 régions correspondantes à un segment ouvert: Exemple $0 < x = y < 1$.
- 8 régions ouvertes: Exemple $0 < x < y < 1$.

Résultats

- Prop: soient v_1, v_2 deux valuations d'horloges,
  φ une contrainte d'horloges,
  et $\lambda \subset X$.

  1. Si $v_1 \simeq v_2$ alors pour tout entier t, $v_1 + t \simeq v_2 + t$.
  2. Si $v_1 \simeq v_2$ alors pour tout $t_1 \in IR^{\geq 0}$ il existe $t_2 \in IR^{\geq 0}$ tel que $v_1 + t_1 \simeq v_2 + t_2$.
  3. Si $v_1 \simeq v_2$ alors v_1 satisfait φ ssi v_2 satisfait φ.
  4. Si $v_1 \simeq v_2$ alors $v_1[\lambda := 0] \simeq v_2[\lambda := 0]$.

- Prop: si $v_1 \simeq v_2$, et si $(s, v_1) \Rightarrow^a (s', v_1')$ alors il existe v_2' tel que $v_1' \simeq v_2'$ et $(s, v_2) \Rightarrow^a (s', v_2')$,

Résultats

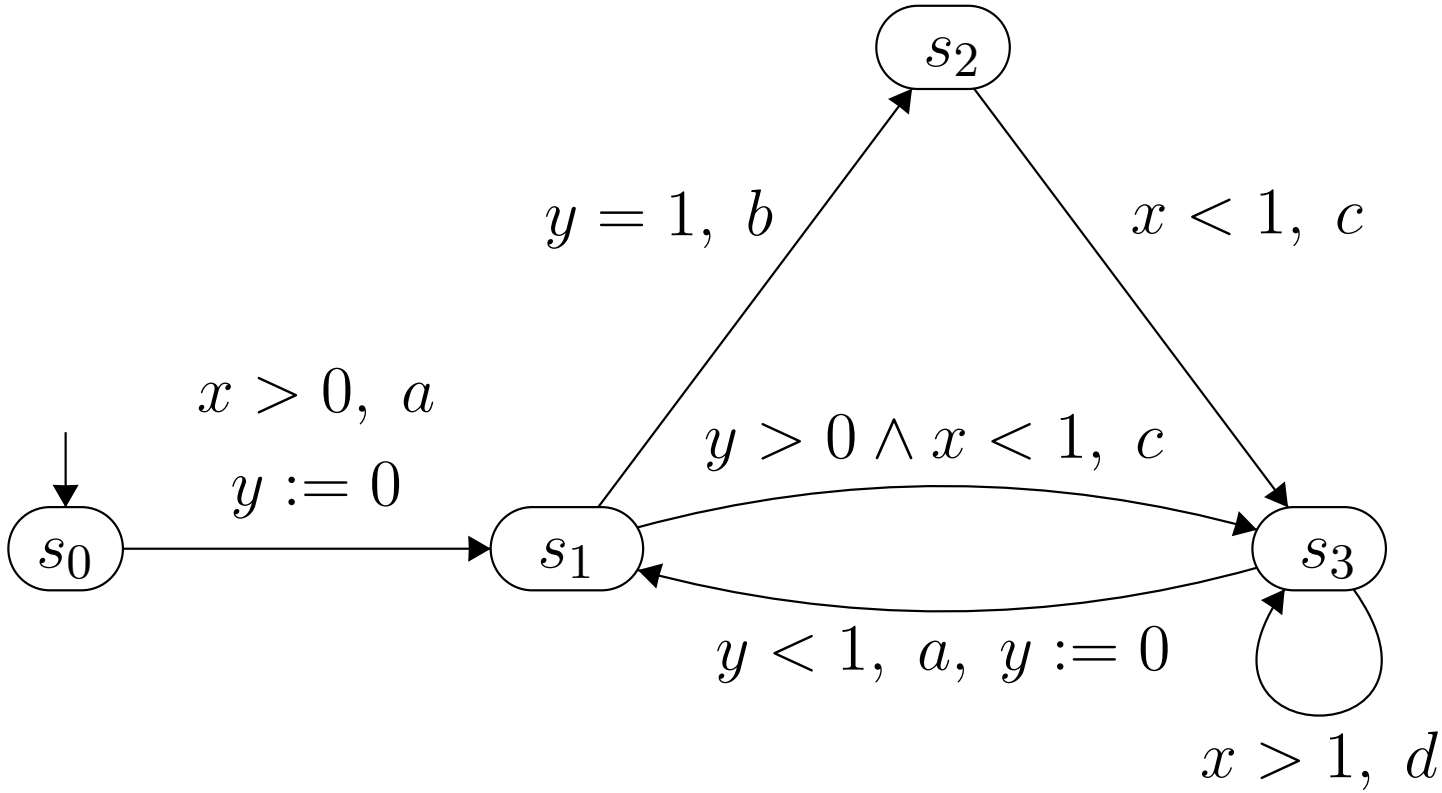
- Définition. On étend $\simeq$ à Q: on dit que $(s, v) \simeq (s', v')$ si $s = s'$ et $v \simeq v'$.
- Pour une classe d'équivalence σ de cette partition, on note $[\sigma]$ pour la partie de Q correspondante: i.e. $[\sigma] = \{s\} \times [v]$ pour $(s, v) \in \sigma$.
- Théorème:
  1. $\simeq$ est une partition stable sur les états de $\tau(A)$.
  2. $\tau(A)/\simeq$ et $\tau(A)$ sont deux structures de Kripke bissimilaires.
- Conséquence: le problème de l'atteignabilité (ou du calcul des états atteignables) sur A se ramène à celui sur $\tau(A)/\simeq$

Résultats: suite

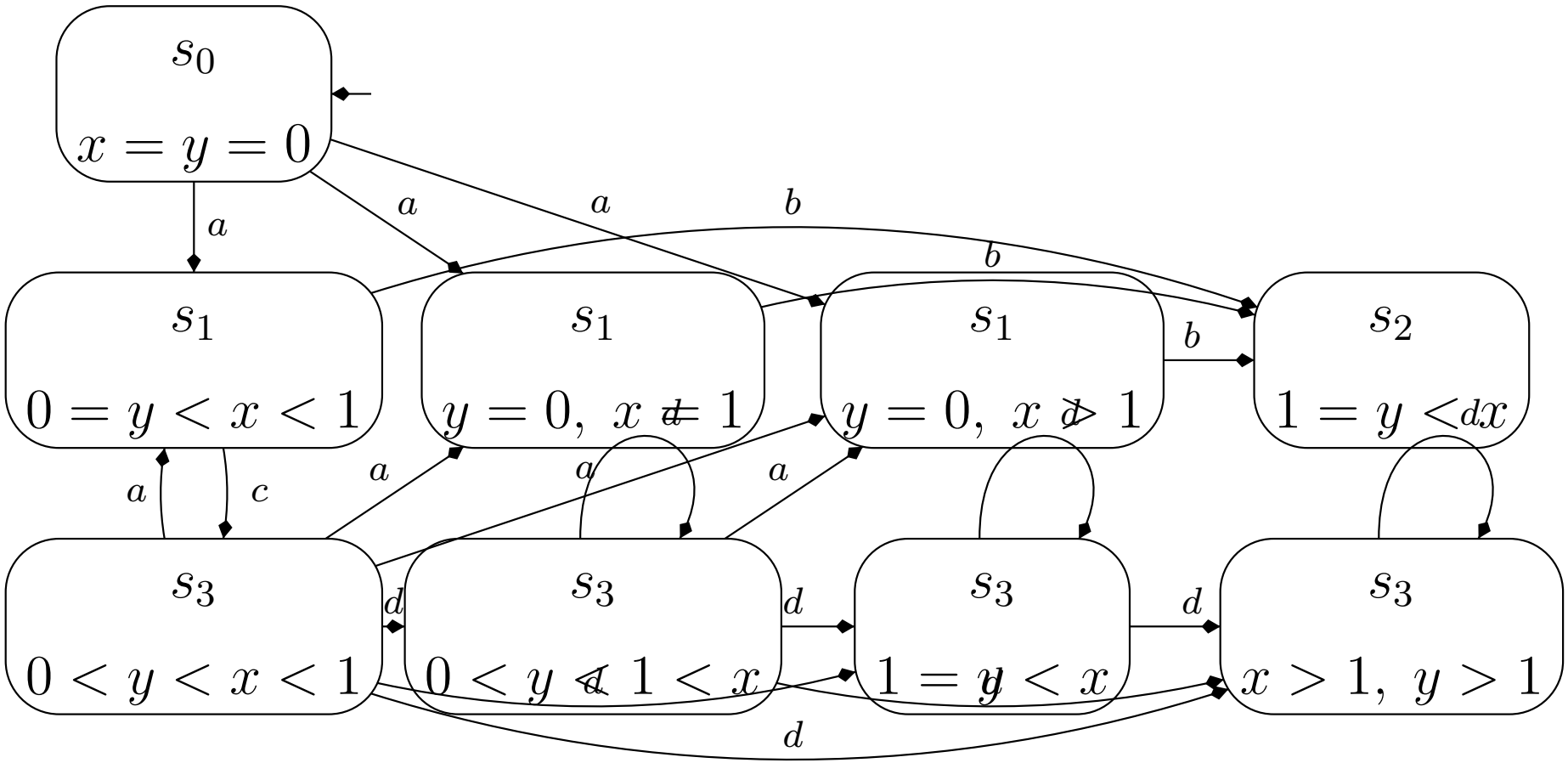
- Remarque: le nombre de classes d'équivalence (régions) de $\simeq$ est fini.
  Il est borné par $|Q||X|!2^{|X|}\Pi_{x\in X}(2c_x+2)$.
- $\tau(A)/\simeq$ est donc un système de transition *fini*: i.e. un automate fini appelé *automate des régions*.
- Conséquence: le problème de l'atteignabilité (ou du calcul des états atteignables) se ramène à un problème sur un automate fini: son automate des régions: si Q^R désigne l'ensemble des états atteignables de A, et Q'^R l'ensemble fini des états atteignables du graphe fini $\tau(A)/\simeq$, on a:

$$Q^R = \bigcup_{\sigma\in Q'^R} [\sigma].$$

Exemple: Automate Initial A_0.



Partie atteignable de l'automate des r



Automates temporisés

Partie 4: Graphe des zones

Problèmes d'implémentation

- Manipuler directement l'automate des régions est coûteux: il est fini mais a un nombre exponentiel de régions.
- Suite de ce cours: expliquer comment on peut faire pour ne pas manipuler des régions, mais des unions convexes de régions, i.e. des *zones*.

Zone d'horloge

- Définition: une zone d'horloges est une conjonction d'inégalités du type $true$, $x \prec c$, $c \prec x$, ou $x - y \prec c$. Forme générale:

$$x_0 = 0 \wedge \bigwedge_{0 \leq i \neq j \leq n} x_i - x_j \prec c_{i,j}.$$

- Définitions: soit φ une zone d'horloge.
  1. Soit $\lambda \subset X$. On note $\varphi[\lambda := 0] = \{v[\lambda := 0] | v \in \varphi\}$.
  2. Soit $d \in IR^{\geq 0}$. On note $\varphi + d = \{v + d | v \in \varphi\}$.
  3. Soit $d \in IR^{\geq 0}$. On note $\varphi - d = \{v - d | v \in \varphi\}$.

Propriété fondamentale

- Propriétés: si φ est une zone d'horloge avec x comme variable libre, alors $\exists x[\varphi]$ est (équivalent à) une zone d'horloge.

Preuve: découle d'un algorithme d'élimination des quantificateurs du type Fourrier-Motzkin.

Preuve sur l'exemple

$\varphi(x) = x \leq 2 \wedge y - x \leq 3 \wedge y \leq 2 \wedge z - x \leq 1 \wedge x - y \leq -2$.

$\exists x \varphi(x)$ ssi $\exists x(y - 3 \leq x \wedge z - 1 \leq x \wedge x \leq 2 \wedge x \leq -2 + y \wedge y \leq 2)$ ssi

$\exists x(y - 3 \leq x \wedge z - 1 \leq x \wedge x \leq 2 \wedge x \leq -2 + y) \wedge y \leq 2$. Or

$\exists x(y - 3 \leq x \wedge z - 1 \leq x \wedge x \leq 2 \wedge x \leq -2 + y)$ ssi

$max(y - 3, z - 1) \leq min(2, -2 + y)$ ssi

$y - 3 \leq min(2, -2 + y) \wedge z - 1 \leq min(2, -2 + y)$ ssi

$y - 3 \leq 2 \wedge y - 3 \leq -2 + y \wedge z - 1 \leq 2 \wedge z - 1 \leq -2 + y$ ssi

$y \leq 5 \wedge -3 \leq -2 \wedge z \leq 3 \wedge z - y \leq -1$ ssi $y \leq 5 \wedge z \leq 3 \wedge z - y \leq -1$.

- Conséquences:
  - Soient φ, ψ deux zones d'horloges. Alors $\varphi \wedge \psi$ est une zone d'horloge.
  - Soit φ une zone d'horloge et $\lambda \subset X$. Alors $\varphi[\lambda := 0]$ est une zone d'horloge.

    Démonstration: Pour $\lambda = \{x\}$, $\varphi[x := 0] = \exists x[\varphi \wedge x = 0]$.

    Pour $\lambda = \{x_1, \ldots, x_k\}$,

    $\varphi[\lambda := 0] = (((\phi[x_1 := 0])[x_2 := 0]) \ldots [x_k := 0])$.

Opérateur $\Uparrow$

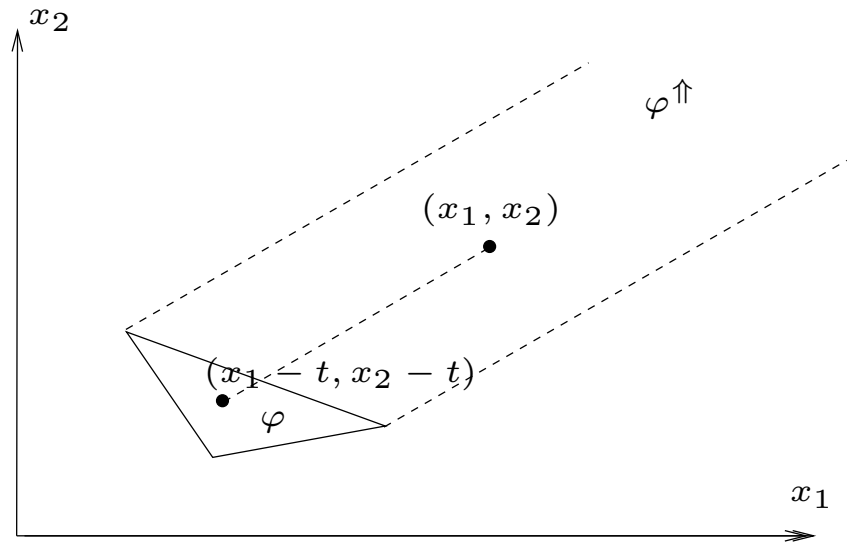
- Soit φ une zone d'horloge. Alors

$$\varphi^{\Uparrow} = \{v + t | v \in \varphi, t \in I\!R^{\geq 0}\}$$

est une zone d'horloge.

Démonstration: $\varphi^{\Uparrow} = \exists t \geq 0 \, (v - t \in \varphi) = \exists t \geq 0 \, v \in \varphi + t$.

- Illustration:



Utilisation

- Définition: soit $e = (s, a, \psi, \lambda, s') \in T$ une transition et φ une zone d'horloge.
  On note $succ(\varphi, e)$ l'ensemble des valuation d'horloges v' atteignables à partir d'une valuation $v \in \varphi$ en laissant le temps évoluer puis en prenant une transition d'action.
- Théorème:
  $succ(\varphi, e) = ((\varphi \wedge I(s))^{\Uparrow} \wedge I(s) \wedge \psi)[\lambda := 0]$.

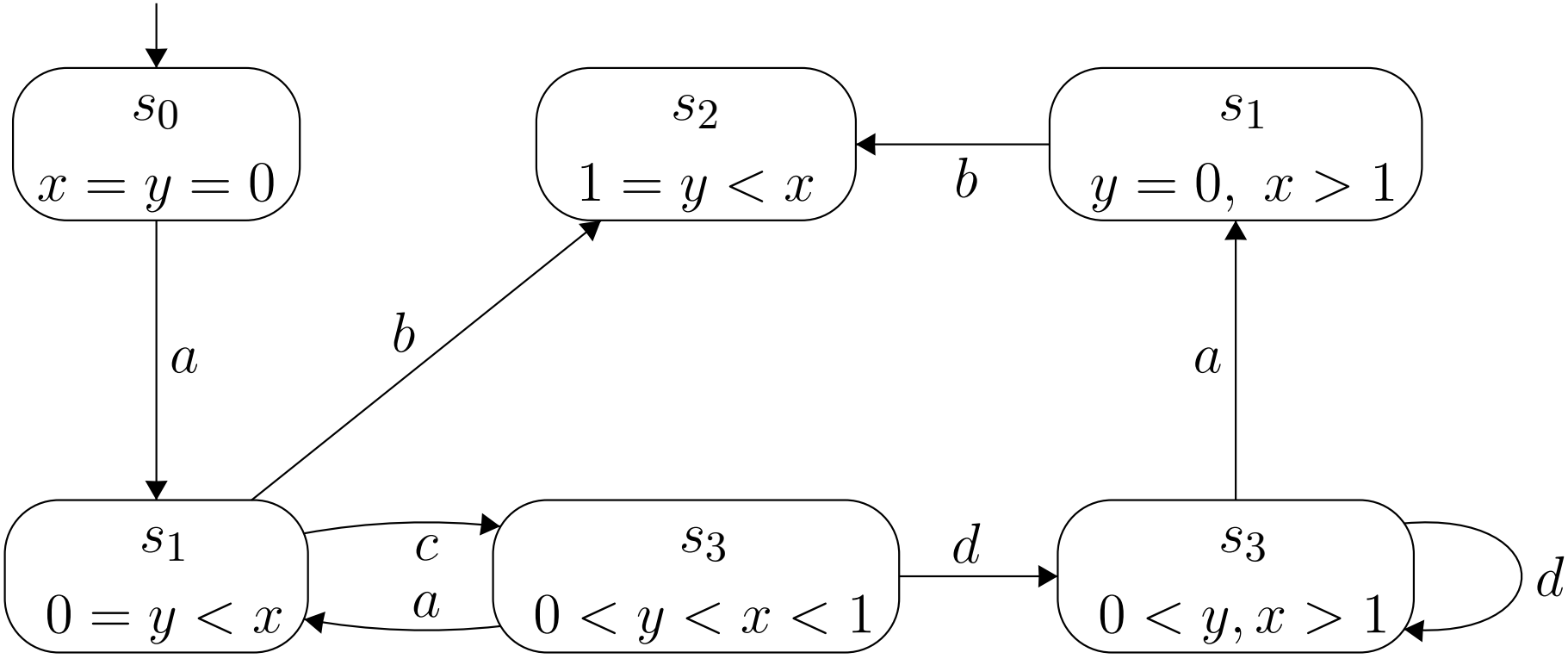
Utilisation (suite)

- Définition: on appelle *zone* un couple (s, φ) où $s \in S$ et φ est une zone d'horloge.
- Définition: le *graphe des zones* de A est le système de transition $Z(A) = (Q_Z, S_0^Z, R_Z)$ avec
  1. Q_Z, l'ensemble des états, est constitué des zones de A.
  2. S_0^Z, l'ensemble des zones initiales, est constitué des zones $(s, X = 0)$ avec $s \in S_0$.
  3. R_Z, la relation de transition, est définie par: $(s, \varphi) R_Z (s', \varphi')$ ssi $\varphi' = succ(\varphi, e)$ pour une certaine transition $e \in T$ entre s et s'.

- Conséquence: le problème de l'atteignabilité ou du calcul des états atteignables sur l'automate temporisé A se ramène à celui sur $Z(A)$.

Graphe des zones de l'automate A_0

(A_0 est défini dans le transparent 39)
(Seule la partie atteignable est représentée).



A comparer au graphe des régions du transparent 40.