# Model Checking II

## pro Timed Automata

Jiří Vyskočil

2011

# Region Automaton

- Region Automaton (regionový automat)
  - Navržen Alurem a Dillem [AD94,AD91]
  - zobecňuje TA tak, že může nabývat pouze konečného množství stavů
  - Používá se v mnoha rozhodovacích výsledcích

- Problém dosažitelnosti (reachability)
  - Chceme ověřit zda je zadaná pozice v daném TA dosažitelná z počátečního stavu.

- Problém rozhodnutelnosti (decidability)
  - Chceme zjistit, zda existuje algoritmus, který umí pro libovolný TA $A$ a pozici $p$ rozhodnout, zda je $p$ dosažitelná v $A$ či nikoliv.

# Region Automaton – popis

- povolené tvary podmínek (constraints)

  Nechť $\mathbb{C}$ je množina proměnných typu *clock* a nechť $\Psi(\mathbb{C})$ je definováno následující gramatikou:

  $$\varphi := \varphi \wedge \varphi \mid \neg \varphi \mid x \leq n \mid x < n$$

  kde $x, y \in \mathbb{C}$, $n \in \mathbb{N}$

  Oproti standardní definici TA zde nejsou tzv. diagonální podmínky: $x - y \leq m \mid x - y < m$ pro $m \in \mathbb{Z}$

- konečný řídící graf

  TA $(Loc, l_0, \Sigma, E, Inv)$ má konečnou množinu pozic $Loc$ a konečnou množinu hran $E$.

- nekonečný přechodový systém

  Časový přechodový systém TTS (Timed Transition System) $(S, s_0, R)$ pro výše popsaný TA obsahuje nekonečnou množinu stavů a nekonečné množství přechodů.

# Region Automaton – popis

- redukce na konečný počet stavů

  Uvažujme TA $(\mathrm{Loc}, l_0, \Sigma, E, \mathrm{Inv})$ s TTS $(S, s_0, R)$

  Nyní definujeme relaci ekvivalence $\approx$ nad ohodnocením hodin takové, že platí:

  - Pro všechny stavy $(l,v),(l',v') \in S$ splňující $(l,v) \approx (l',v')$ platí, že libovolná pozice $l_f$ je dosažitelná z $(l,v)$, právě když je dosažitelná z $(l',v')$.
  - Počet tříd ekvivalence nad $S/\approx$ je konečný.

- problémy
  - Jak zvolit takovou relaci ekvivalence?
  - Jak reprezentovat třídy ekvivalence?

# Region Automaton – ≈

- 1. pozorování

  Všechny hodiny se porovnávají s celočíselnými hodnotami

- =>

  Třídy ekvivalence ≈ bude rozdělovat celočíselná mřížka podle ohodnocení hodin. Definice by vypadala následovně:

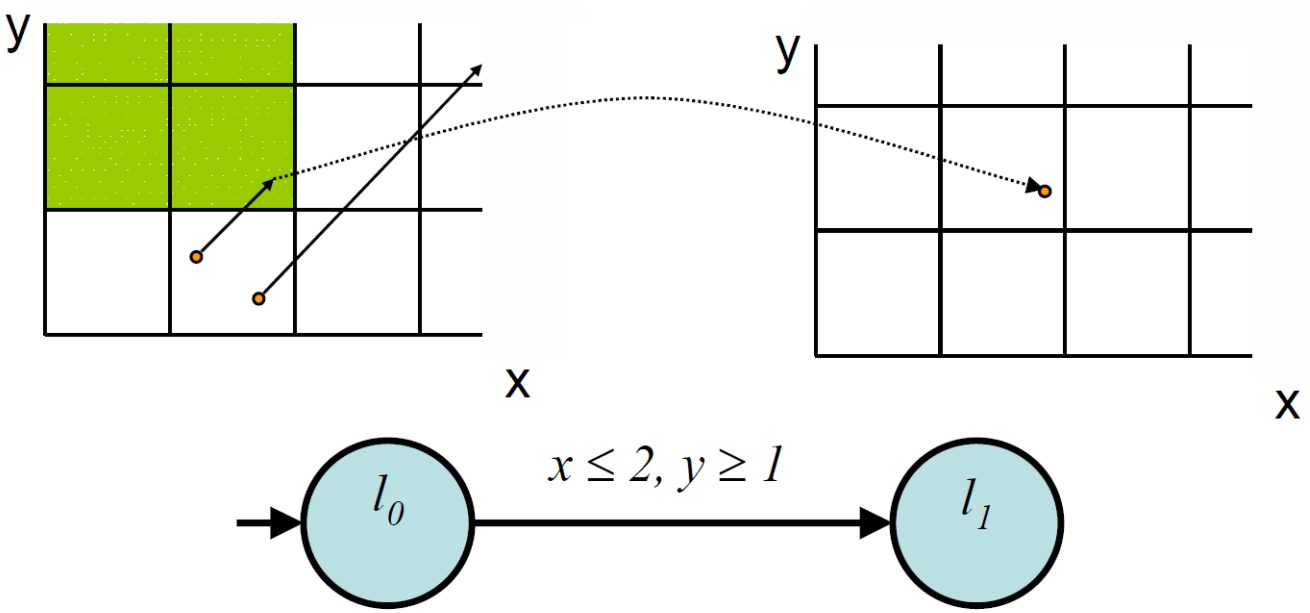
$(l,v) \approx (l',v')$ právě když ( $l = l'$ a $\forall x \in \mathbb{C}$ platí $\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$ )

# Region Automaton – ≈

- Hypotéza:

  $(l,v) \approx (l',v')$ právě když ( $l = l'$ a $\forall x \in \mathbb{C}$ platí $\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$ )

- Příklad:




- Požadavek z definice relace ≈

  $(l,v) \approx (l',v')$ právě když ($l_f$ je dosažitelná z $(l,v) \Leftrightarrow l_f$ je dosažitelná z $(l',v')$).

# Region Automaton – $\approx$

- 2. pozorování

  Potřebujeme rozlišovat mezi ohodnocením nad a pod diagonálami.

- =>

  Třídy ekvivalence $\approx$ bude rozdělovat celočíselná mřížka podle ohodnocení hodin a každá buňka v této mřížce bude rozdělena podle své diagonály (diagonála je dána rovnicí $frac(v(x))=frac(v(y))$).

  Definice by vypadala následovně:

$(l,v) \approx (l',v')$ právě když :

- $l = l'$
- $\forall x \in \mathbb{C}$ platí $\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$
- $\forall x,y \in \mathbb{C}$ platí $frac(v(x)) \leq frac(v(y)) \Leftrightarrow frac(v'(x)) \leq frac(v'(y))$

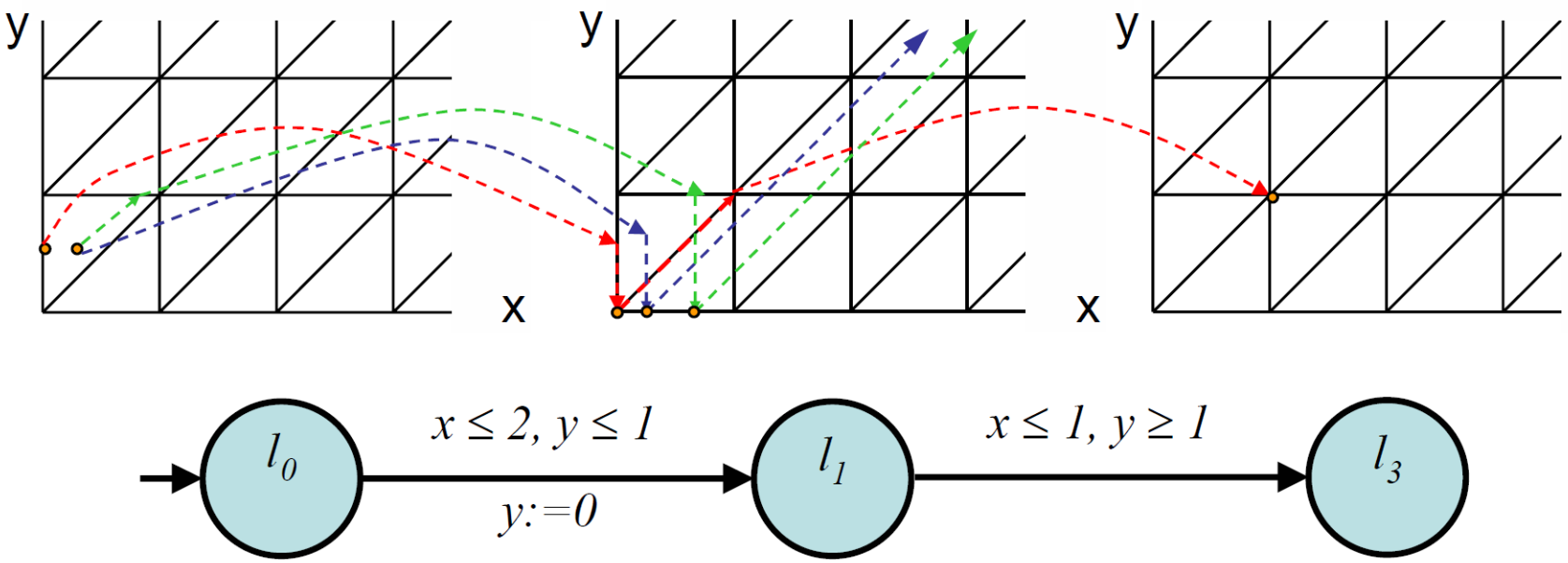
# Region Automaton – ≈

- Hypotéza:

  $(l,v) \approx (l',v')$ právě když $(l = l'$ a $\forall x \in \mathbb{C}$ platí $\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$ a

  $\forall x,y \in \mathbb{C}$ platí $frac(v(x)) \leq frac(v(y)) \Leftrightarrow frac(v'(x)) \leq frac(v'(y)))$

- Příklad:




- Požadavek z definice relace ≈

$(l,v) \approx (l',v')$ právě když ($l_f$ je dosažitelná z $(l,v) \Leftrightarrow l_f$ je dosažitelná z $(l',v')$).

# Region Automaton – ≈

- 3. pozorování

  Potřebujeme rozlišovat mezi pokud je ohodnocením hodin celé číslo nebo ne.

- =>
  - Třídy ekvivalence ≈ bude rozdělovat celočíselná mřížka podle ohodnocení hodin.
  - každá buňka v této mřížce bude rozdělena podle své diagonály (diagonála je dána rovnicí $frac(v(x))=frac(v(y))$).
  - Každá buňka bude rozdělena na vrcholy, hrany a plochy.

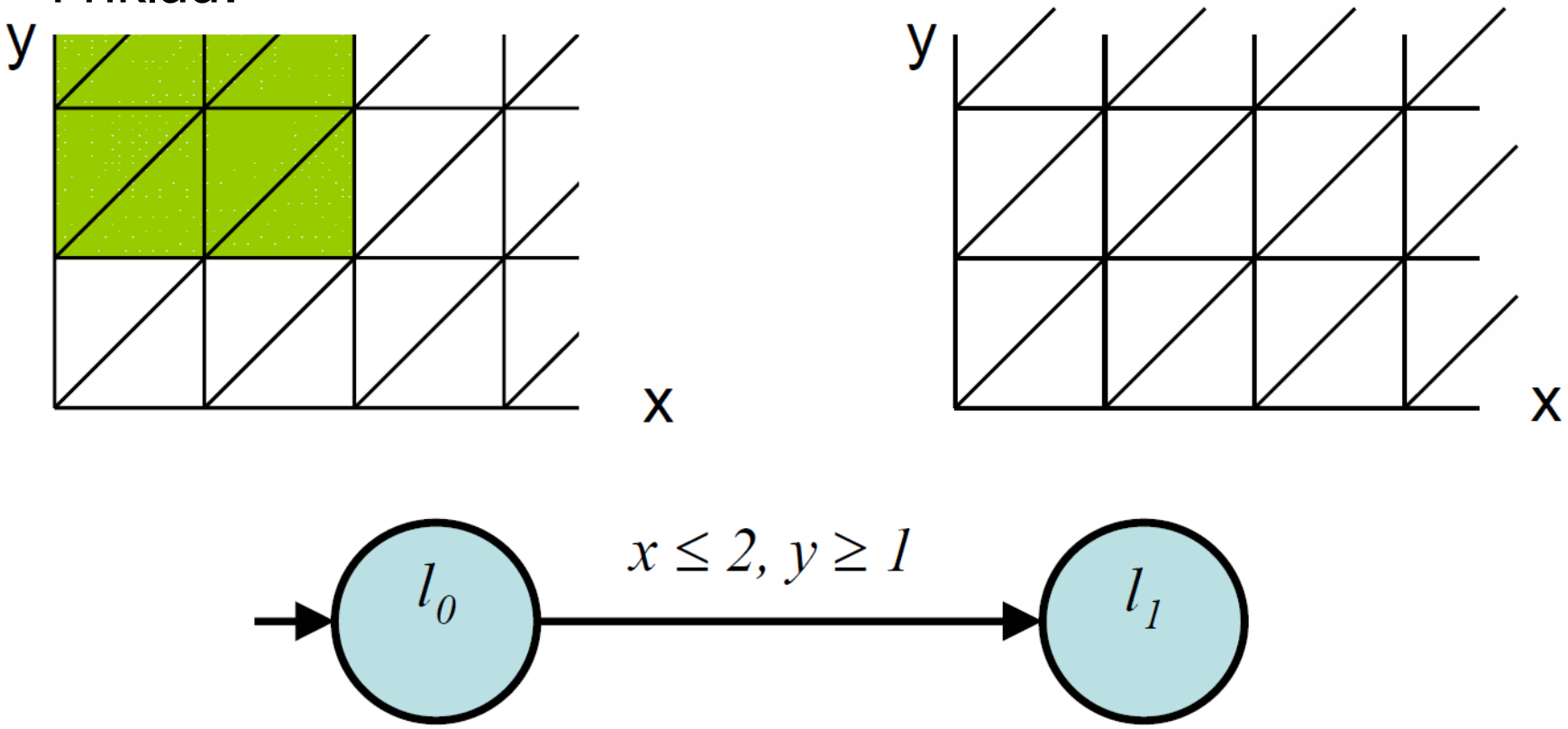
  Definice bude vypadat následovně:

$(l,v) \approx (l',v')$ právě když :

- $l = l'$
- $\forall x \in \mathbb{C}$ platí $\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$
- $\forall x,y \in \mathbb{C}$ platí $frac(v(x)) \leq frac(v(y)) \Leftrightarrow frac(v'(x)) \leq frac(v'(y))$
- $\forall x,y \in \mathbb{C}$ platí $frac(v(x)) = frac(v(y)) \Leftrightarrow frac(v'(x)) = frac(v'(y))$
- $\forall x \in \mathbb{C}$ platí $frac(v(x)) = 0 \Leftrightarrow frac(v'(x)) = 0$

# Region Automaton – ≈

- Příklad:




- Požadavky z definice relace ≈
  - $(l,v) \approx (l',v')$ právě když ($l_f$ je dosažitelná z $(l,v) \Leftrightarrow l_f$ je dosažitelná z $(l',v')$).
  - Počet tříd ekvivalence nad $S/\approx$ je konečný.

# Region Automaton – ≈

- 4. pozorování

  Hodnota hodin je irelevantní jakmile přesáhne největší konstantu z podmínek.

- =>
  - Třídy ekvivalence $\approx$ bude rozdělovat celočíselná mřížka podle ohodnocení hodin.
  - každá buňka v této mřížce bude rozdělena podle své diagonály (diagonála je dána rovnicí $frac(v(x))=frac(v(y))$).
  - Každá buňka bude rozdělena na vrcholy, hrany a plochy .
  - Tvorbu částí omezíme největší konstantou v podmínkách (stráže a invarianty) .

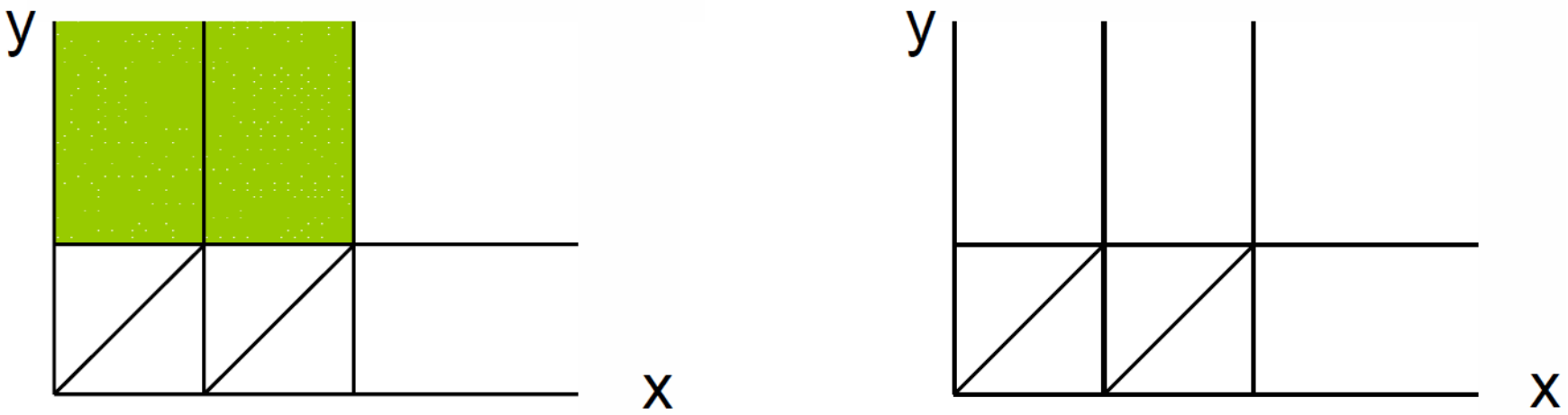
  Definice bude vypadat následovně:

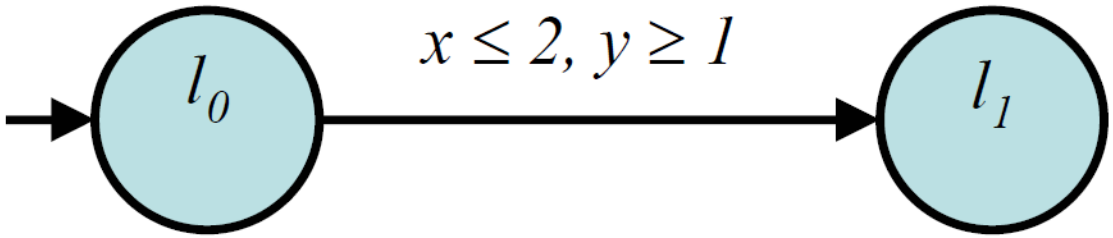
$(l,v) \approx (l',v')$ právě když :

- $l = l'$
- $\forall x \in \mathbb{C}$ platí $v(x) \leq c_x \Rightarrow \lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$
- $\forall x,y \in \mathbb{C}$ platí $(v(x) \leq c_x \vee v(y) \leq c_y) \Rightarrow frac(v(x)) \leq frac(v(y)) \Leftrightarrow frac(v'(x)) \leq frac(v'(y))$
- $\forall x,y \in \mathbb{C}$ platí $(v(x) \leq c_x \vee v(y) \leq c_y) \Rightarrow frac(v(x)) = frac(v(y)) \Leftrightarrow frac(v'(x)) = frac(v'(y))$
- $\forall x \in \mathbb{C}$ platí $v(x) \leq c_x \Rightarrow frac(v(x)) = 0 \Leftrightarrow frac(v'(x)) = 0$

# Region Automaton – ≈

- Příklad:




- Požadavky pro Region Automaton
  - $(l,v) \approx (l',v')$ právě když ($l_f$ je dosažitelná z $(l,v) \Leftrightarrow l_f$ je dosažitelná z $(l',v')$).
  - Počet tříd ekvivalence nad $S/\approx$ je konečný.
  - Dosažitelnost pro TA je rozhodnutelná.

# Region Automaton – symbolická sémantika

- Použijeme ekvivalenci nad hodinami pro definici konečného regionového automatu (finite region automaton)
- Nejprve definujeme regiony symbolicky:

  Nechť $\mathbb{C}$ je množina proměnných typu *clock* s maximální konstantou $c_x$ pro každé hodiny z $\mathbb{C}$. Region $H$ budeme reprezentovat jako trojici $H=(h,[\mathbb{C}_0,\ldots, \mathbb{C}_k], \mathbb{C}_>)$ kde

  - h: $\mathbb{C} \rightarrow \mathbb{N}^{|\mathbb{C}|}$ taková, že přiřazuje každým hodinám $x$ z $\mathbb{C}$ přirozené číslo $\leq c_x$,
  - $\mathbb{C}_0,\ldots, \mathbb{C}_k$ a $\mathbb{C}_>$ definují část prostoru nad množinou hodin.
  - $\mathbb{C}_0$ a $\mathbb{C}_>$ mohou být prázdné.

Nechť $\mathbb{H}$ je konečná množina všech možných $H$ získaných z množiny hodin $\mathbb{C}$ a maximálních konstant pro každé hodiny z $\mathbb{C}$.

# Region Automaton – symbolická sémantika

Ohodnocení hodin $v \in (h,[\mathbb{C}_0,\ldots,\mathbb{C}_k],\mathbb{C}_>)$ pokud:

- $\lfloor v(x) \rfloor = h(x)$ pro $x \notin \mathbb{C}_>$
- $\lfloor v(x) \rfloor > c_x$ pro $x \in \mathbb{C}_>$
- $frac(v(x)) = 0$ pro $x \in \mathbb{C}_0$
- $frac(v(x)) = frac(v(y))$ pro $x,y \in \mathbb{C}_i$
- $frac(v(x)) < frac(v(y))$ pro $x \in \mathbb{C}_i$ , $y \in \mathbb{C}_j$ kde $i<j$

Vztah mezi ohodnocením hodin a ekvivalencí $\approx$ :

- $v,v' \in (h,[\mathbb{C}_0,\ldots,\mathbb{C}_k],\mathbb{C}_>)$ implikuje $(l,v) \approx (l,v')$

# Region Automaton – symbolická sémantika

- Ještě zbývá definovat sémantiku operací nad regiony.

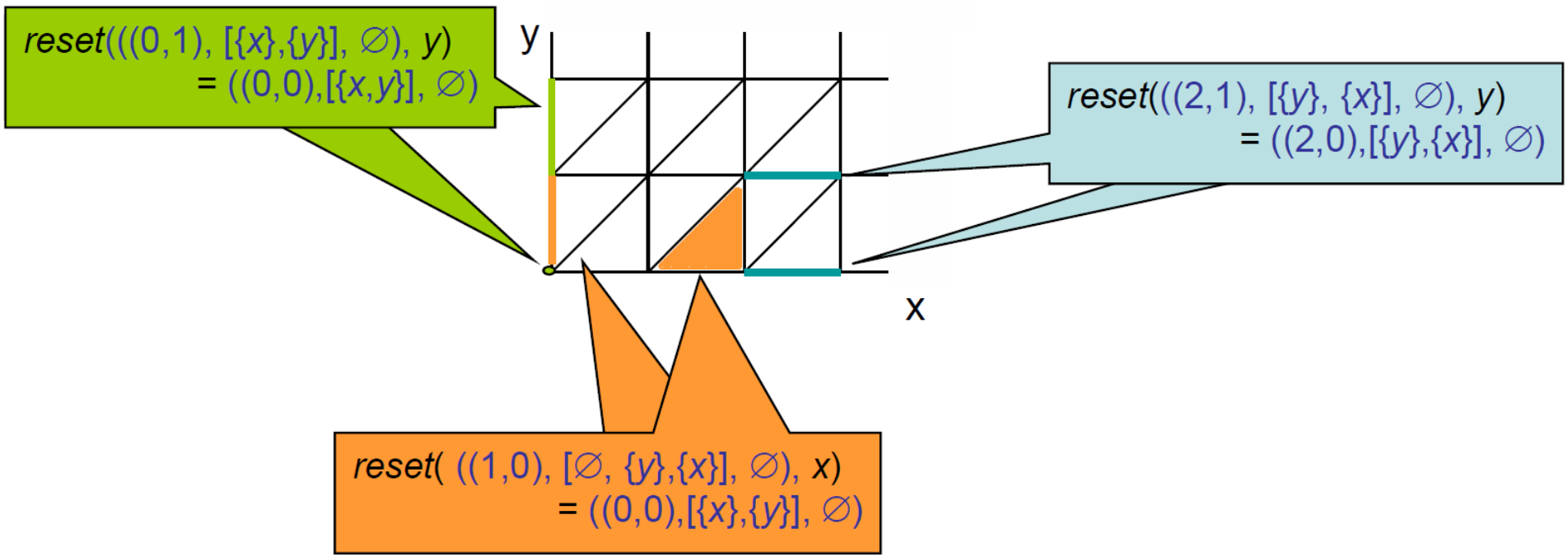
- **reset**

  Mějme region $H=(h,[\mathbb{C}_0,\ldots,\mathbb{C}_k],\mathbb{C}_>)$ a $x \in \mathbb{C}_i$
  - Jestliže $i = 0$ potom $reset(H,x) = (h',[\mathbb{C}_0,\ldots,\mathbb{C}_k],\mathbb{C}_>)$ kde $h' = h[x:=0]$
  - Jestliže $i > 0$ a $\mathbb{C}_i = \{x\}$ potom $reset(H,x) = (h',[\mathbb{C}'_0,\ldots,\mathbb{C}_{i-1},\mathbb{C}_{i+1},\ldots,\mathbb{C}_k],\mathbb{C}_>)$ kde $h' = h[x:=0]$ a $\mathbb{C}'_0 = \mathbb{C}_0 \cup \{x\}$
  - Jinak $reset(H,x) = (h',[\mathbb{C}'_0,\ldots,\mathbb{C}'_i,\ldots,\mathbb{C}_k],\mathbb{C}_>)$ kde $h' = h[x:=0]$, $\mathbb{C}'_i = \mathbb{C}_i \setminus \{x\}$ a $\mathbb{C}'_0 = \mathbb{C}_0 \cup \{x\}$ .

  Mějme region $H=(h,[\mathbb{C}_0,\ldots,\mathbb{C}_k],\mathbb{C}_>)$ a $x \in \mathbb{C}_>$
  - $reset(H,x) = (h',[\mathbb{C}'_0,\ldots,\mathbb{C}_k],\mathbb{C}'_>)$ kde $h' = h[x:=0]$, $\mathbb{C}'_> = \mathbb{C}_> \setminus \{x\}$ a $\mathbb{C}'_0 = \mathbb{C}_0 \cup \{x\}$ .

# Region Automaton – symbolická sémantika

- Příklad – **reset**



# Region Automaton – symbolická sémantika

## delay

Mějme region $H=(h,[\mathbb{C}_0,\ldots,\mathbb{C}_k],\mathbb{C}_>)$

- Jestliže $\mathbb{C}_0 \neq \emptyset$ potom

$$\text{delay}(H) = \begin{cases} (h,[\emptyset,\mathbb{C}'_0,\mathbb{C}_1,\ldots,\mathbb{C}_k],\mathbb{C}'_>) & \text{pro } \mathbb{C}'_0 \neq \emptyset \\ (h,[\emptyset,\mathbb{C}_1,\ldots,\mathbb{C}_k],\mathbb{C}'_>) & \text{pro } \mathbb{C}'_0 = \emptyset \end{cases}$$

kde $\mathbb{C}'_0 = \mathbb{C}_0 \setminus \{x \mid h(x)=c_x\}$ a $\mathbb{C}'_> = \mathbb{C}_> \cup \{x \mid h(x)=c_x\}$

- Jestliže $\mathbb{C}_0 = \emptyset$ a $k > 0$ potom

$\text{delay}(H) = (h',[\mathbb{C}_k,\mathbb{C}_1,\ldots,\mathbb{C}_{k-1}],\mathbb{C}_>)$

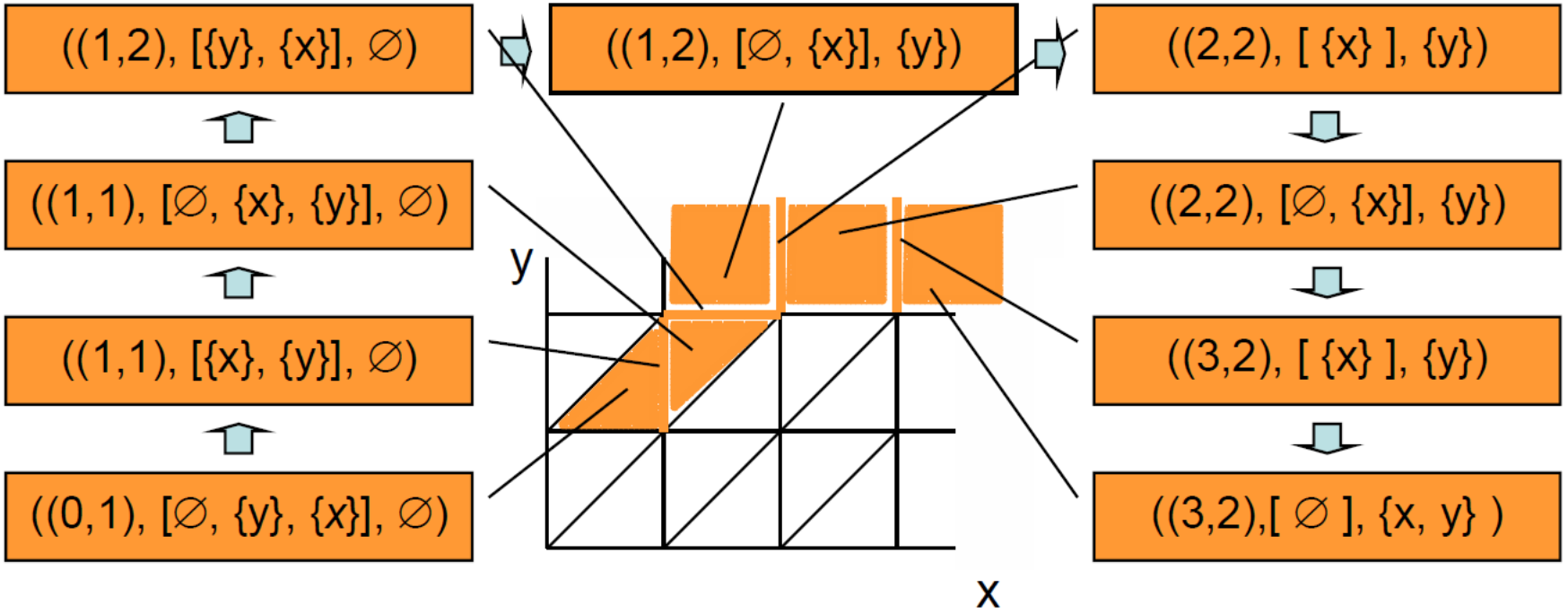
kde $h'(x) = h(x)+1$ pokud $x \in \mathbb{C}_k$, jinak $h'(x) = h(x)$

- Jinak (pokud jsou všechny hodiny v $\mathbb{C}_>$)

$\text{delay}(H) = H$

# Region Automaton – symbolická sémantika

- Příklad – **delay**



# Region Automaton – symbolická sémantika

**Operační sémantika** pro *timed automaton (časový automat)* $A=(Loc, l_0, \Sigma, E, Inv)$ je definovaná pomocí časového přechodového systému TS(A) kde

- **množina stavů** $S = \{ (l,v) \mid l \in Loc, v \models Inv(l) \}$
- **počáteční stav** $s_0 = (l_0, \mathbf{0})$
- **relace přechodu** $R \subseteq S \times ( \Sigma \cup \mathbb{R}_{\geq 0} ) \times S$ která obsahuje následující možnosti
  - diskrétní přechody

    $(l,v) \xrightarrow{\sigma} (l',v')$ pokud existuje $(l,g,\sigma,r,l') \in E$ takové, že

    $v \models g$ a $v[r:=0] = v'$
  - časové přechody

    $(l,v) \xrightarrow{d} (l,v+d)$ pro $d \in \mathbb{R}_{\geq 0}$ pokud pro všechny $0 \leq d' \leq d$ platí

    $v + d' \models Inv(l)$

**=> Nekonečné množství stavů a přechodů!**

# Region Automaton – symbolická sémantika

**Symbolická regionová sémantika** pro *timed automaton* $A=(Loc, l_0, \Sigma, E, Inv)$ je definovaná pomocí časového přechodového systému RA(A) kde

- **množina stavů** $S = \{ (l,H) \mid l \in Loc, H \in \mathbb{H} \}$
- **počáteční stav** $s_0 = (l_0, (\mathbf{0},[\mathbb{C}],\emptyset))$
- **relace přechodu** $R \subseteq S \times ( \Sigma \cup \{\delta\} ) \times S$ která obsahuje následující možnosti
  - diskrétní přechody

    $(l,H) \xrightarrow{\sigma} (l',H')$ pokud existuje $(l,g,\sigma,r,l') \in E$ takové, že

    $H \models g$, $H' \models Inv(l')$ a $H'=reset(H,r)$
  - časové přechody

    $(l,H) \xrightarrow{\delta} (l,H')$ pokud platí $H' \models Inv(l)$ a $H'=delay(H)$

**=> Konečné množství stavů a přechodů!**

# Region Automaton – symbolická sémantika

- **Věta**

  Nechť $l$ je pozice a A je TA, potom
  $l$ je dosažitelná v TS(A), právě když je $l$ dosažitelná v RA(A).

- **Myšlenka důkazu**

  „=>"

  Ke každému běhu $(l_0,v_0)\ (\xrightarrow{d} \cup \xrightarrow{\sigma})^*\ (l,v)$ existuje

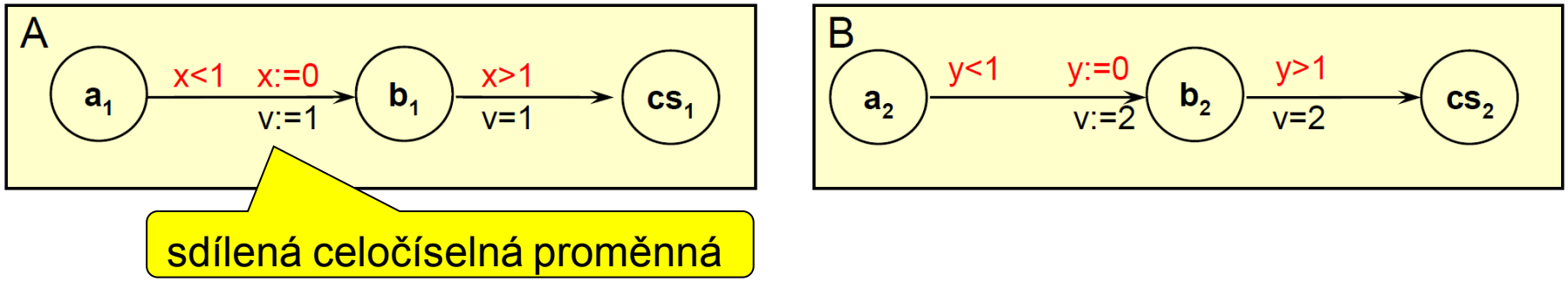
  symbolický běh $(l_0,H_0)\ (\xrightarrow{\delta} \cup \xrightarrow{\sigma})^*\ (l,H)$ pro $v \in H$

  „<="

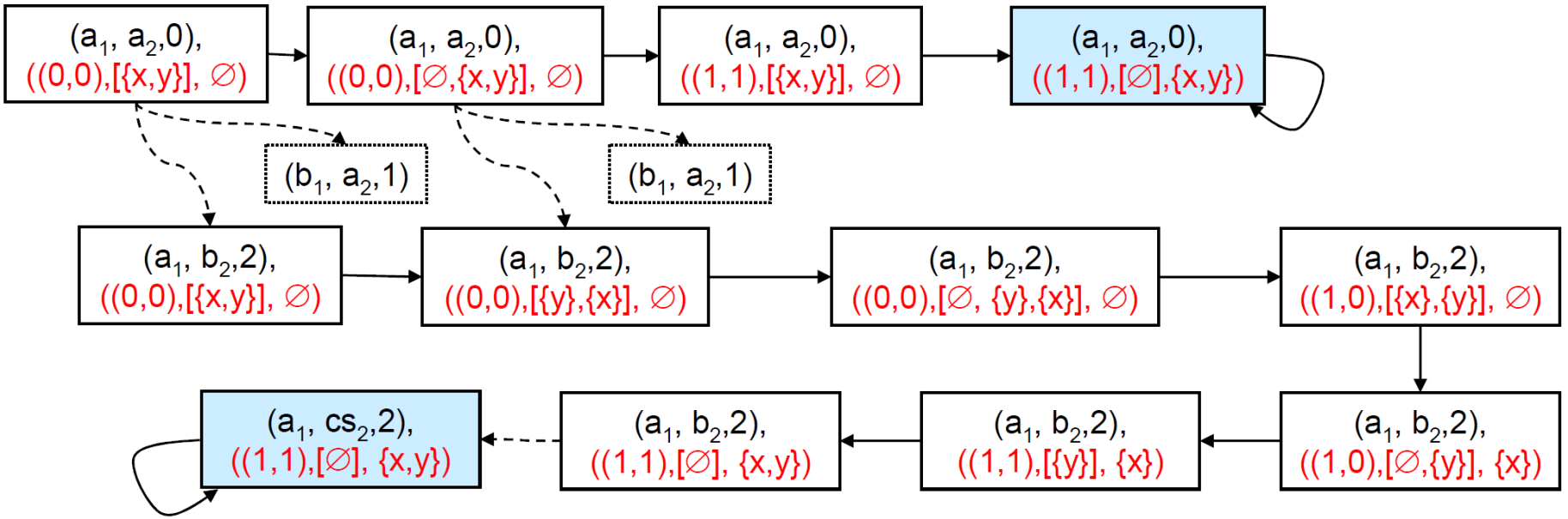
  Ke každému symbolickému běhu $(l_0,H_0)\ (\xrightarrow{\delta} \cup \xrightarrow{\sigma})^*\ (l,H)$

  existuje běh $(l_0,v_0)\ (\xrightarrow{d} \cup \xrightarrow{\sigma})^*\ (l,v)$ pro $v \in H$

# Region Automaton – příklad




Důkaz toho, že z A || B není dosažitelná kritická sekce v pozici ($cs_1$,$cs_2$).



# Model Checking

- **dopředná dosažitelnost** (forward reachability)
  - Začneme s počátečním stavem $(l_0, (\mathbf{0},[\mathbb{C}],\emptyset))$ RA
  - Prozkoumáme stavový prostor použitím relace přechodu dokud buď
    - nedosáhneme pevného bodu (fix-point) nebo
    - nedosáhneme cílovou pozici $l$.
  - Pro prozkoumávání můžeme použit DFS, BFS, randomizované DFS, ….
- **zpětná dosažitelnost** (backward reachability)
  - Začneme se všemi regiony v cílové pozici RA.
  - Prozkoumáme stavový prostor použitím inverzní relace přechodu dokud buď
    - nedosáhneme pevného bodu (fix-point) nebo
    - nedosáhneme počáteční pozici $(l_0, (\mathbf{0},[\mathbb{C}],\emptyset))$.

# Závěr

- problém dosažitelnosti TA je rozhodnutelný
- existuje konečná symbolická sémantika pro RA
- regionová konstrukce je užitečná k dokazování rozhodnutelnosti i dalších problémů

- dosažitelnost je lineární k velikosti RA
- velikost RA je
  - lineární k počtu pozic
  - exponenciální k počtu hodin a
  - exponenciální k maximální konstantě
- Problém dosažitelnosti je PSpace úplný
- **=> existují pokročilejší a efektivnější techniky pro řešení**