Modeling and Analysis of Hybrid Systems

Algorithmic analysis for linear hybrid systems

Prof. Dr. Erika Ábrahám

Informatik 2 - Theory of Hybrid Systems
RWTH Aachen University

SS 2013

Literature

Alur et al.: The algorithmic analysis of hybrid systems

Theoretical Computer Science, 138(1):3–34, 1995

0

$2x+y$

- A linear term e over a set $Var = \{x_1, \ldots, x_n\}$ of variables is a linear combination $\boxed{\sum_{i=1}^{n} c_i x_i}$ of variables $x_i \in Var$ with integer (rational) coefficients c_i, $i = 1, \ldots, n$.
- A linear constraint t over Var is an (in)equality $e_1 \sim e_2$ with $\sim \in \{>, \geq, =, \leq, <\}$ between linear terms e_1, e_2 over Var. $2x+y \leq 0$
- A hybrid automaton is time-deterministic iff for every location $l \in Loc$ and every valuation $\nu \in V$ there is exactly one activity $f \in Act(l)$ with $f(0) = \nu$. The activity f, then, is denoted by $f_l[\nu]$, its component for $x \in Var$ by $f_l^x[\nu]$.

$\dot{x} = 2 \qquad x(t) = x(0) + 2t$

Linear hybrid automata

Linear hybrid automata are time-deterministic hybrid automata whose definitions contain linear terms, only.

- Activities $Act(l)$ are given as sets of differential equations $\dot{x} = k_x$, one for each variable $x \in Var$, with k_x an integer (rational) constant:

$$f_l^x[\nu](t) = \nu(x) + \boxed{k_x} \cdot t.$$

- Invariants $Inv(l)$ are defined by conjunctions ψ of linear constraints over Var:

$$\nu \in Inv(l) \quad \textit{iff} \quad \nu \models \psi$$

- For all edges, the transision relation μ is defined by a guarded set of nondeterministic assignments:

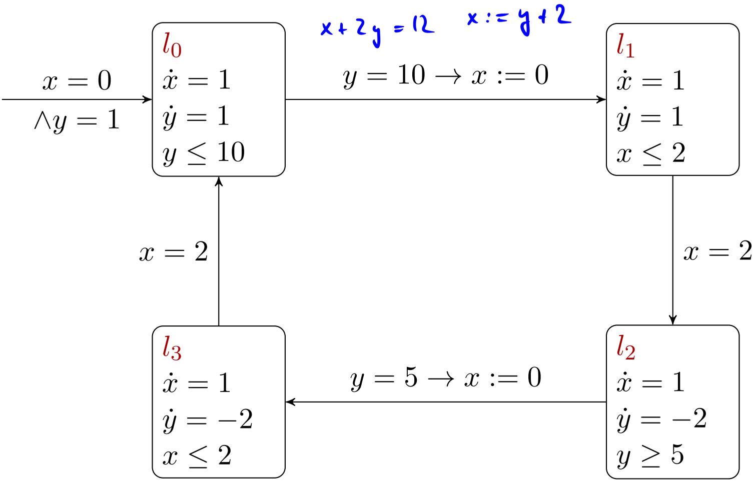
$x := [2y, z]$

$$\psi \Rightarrow \{x := [\alpha_x, \beta_x] \mid x \in Var\},$$

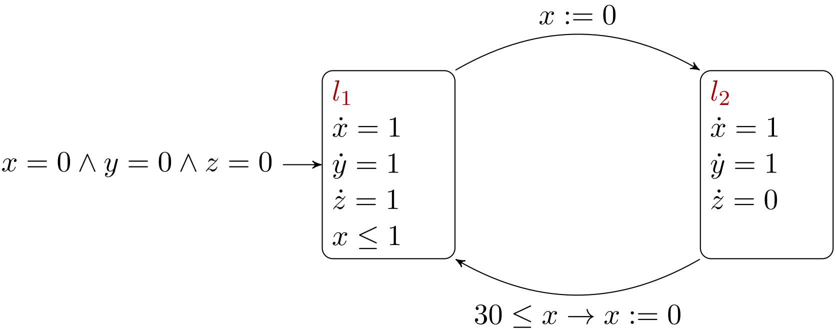
where the quard ψ is a conjunction of linear constraints and α_x, β_x are linear terms:

$$(\nu, \nu') \in \mu \quad \textit{iff} \quad \nu \models \psi \wedge \forall x \in Var.\ \nu(\alpha_x) \leq \nu'(x) \leq \nu(\beta_x).$$

Water-level monitor



Leaking gas burner



Reminder: Semantics of hybrid automata

$$\frac{(l,a,\mu,l') \in Edge \quad (\nu,\nu') \in \mu \quad \nu' \in Inv(l')}{(l,\nu) \xrightarrow{a} (l',\nu')} \; \texttt{Rule}_{\texttt{Discrete}}$$

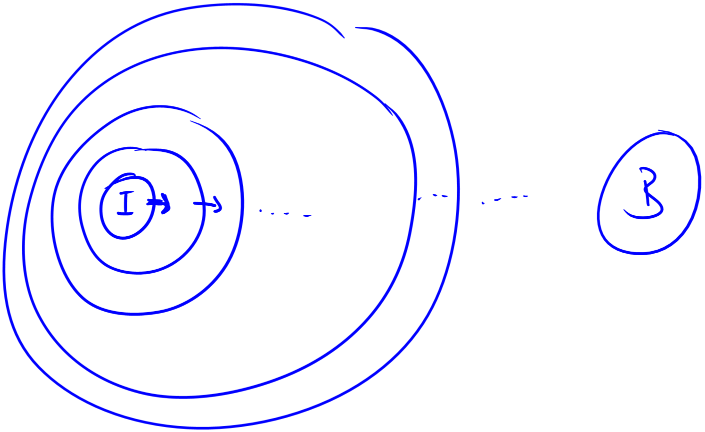
$$\frac{\begin{array}{c} f \in Act(l) \quad f(0) = \nu \quad f(t) = \nu' \\ t \geq 0 \quad \forall 0 \leq t' \leq t. f(t') \in Inv(l) \end{array}}{(l,\nu) \xrightarrow{t} (l,\nu')} \; \texttt{Rule}_{\texttt{Time}}$$

Time-deterministic systems

For linear hybrid automata we can rewrite the time-step rule to:

$$\frac{\nu' = f_l[\nu](t) \quad \nu' \in Inv(l)}{(l,\nu) \xrightarrow{t} (l,\nu')} \; \texttt{Rule}_{\texttt{Time}}$$

Forward analysis



I
B

- Given a region $I \subseteq \Sigma$, the reachable region $(I \mapsto^*) \subseteq \Sigma$ of I is the set of all states that are reachable from states in I:

$$\sigma \in (I \mapsto^*) \quad \textit{iff} \quad \exists \sigma' \in I.\ \sigma' \to^* \sigma.$$

- Given a region $I \subseteq \Sigma$, the reachable region $(I \mapsto^*) \subseteq \Sigma$ of I is the set of all states that are reachable from states in I:

$$\sigma \in (I \mapsto^*) \quad \textit{iff} \quad \exists \sigma' \in I.\ \sigma' \to^* \sigma.$$

- Our goal is to compute the reachable region of a set I of initial states.
- More specifically, we want to check whether the reachable region intersects with a set of bad (unsafe) states.

One-step reachability under time steps:

- We define the forward time closure $\boxed{\mathcal{T}_l^+(P)}$ of $P \subseteq V$ at $l \in Loc$ as the set of valuations reachable from P by letting time progress:

$$\mathcal{T}_l^+(P) = \{ \underline{v} \in V \mid \underbrace{\quad}_{\exists v' \in P.\ \exists t \in \mathbb{R}.\ t \geq 0 \wedge} f_l[v'](t) = v \ \wedge\ v \in Inv(l) \} \qquad f_l[v]$$

One-step reachability under time steps:

- We define the forward time closure $\mathcal{T}_l^+(P)$ of $P \subseteq V$ at $l \in Loc$ as the set of valuations reachable from P by letting time progress:

$$\nu' \in \mathcal{T}_l^+(P) \quad \mathit{iff} \quad \exists \nu \in P.\ \exists t \in \mathbb{R}^{\geq 0}.\ \nu' = f_l[\nu](t) \wedge \nu' \in Inv(l).$$

- Extension to regions $R = \cup_{l \in Loc}(l, R_l)$, $R_l \subseteq V$ for each $l \in Loc$:

$$\mathcal{T}^+(R) = \cup_{l \in Loc}(l, \mathcal{T}_l^+(R_l)).$$

One-step reachability under time steps:

- We define the forward time closure $\mathcal{T}_l^+(P)$ of $P \subseteq V$ at $l \in Loc$ as the set of valuations reachable from P by letting time progress:

$$\nu' \in \mathcal{T}_l^+(P) \quad \textit{iff} \quad \exists \nu \in P.\, \exists t \in \mathbb{R}^{\geq 0}.\, \nu' = f_l[\nu](t) \wedge \nu' \in Inv(l).$$

- Extension to regions $R = \cup_{l \in Loc}(l, R_l)$, $R_l \subseteq V$ for each $l \in Loc$:

$$\mathcal{T}^+(R) = \cup_{l \in Loc}(l, \mathcal{T}_l^+(R_l)).$$

One-step reachability under discrete steps:

- We define the postcondition $\mathcal{D}_e^+(P)$ of P with respect to an edge $e = (l, a, \mu, l')$ as the set of valuations reachable from P by e:

$$\mathcal{D}_e^+(P) = \{ \nu \in V \mid \exists \nu' \in P.\ (\nu', \nu) \in \mu \wedge \nu \in Inv(l') \}$$

One-step reachability under time steps:

- We define the forward time closure $\mathcal{T}_l^+(P)$ of $P \subseteq V$ at $l \in Loc$ as the set of valuations reachable from P by letting time progress:

$$\nu' \in \mathcal{T}_l^+(P) \quad \textit{iff} \quad \exists \nu \in P.\ \exists t \in \mathbb{R}^{\geq 0}.\ \nu' = f_l[\nu](t) \wedge \nu' \in Inv(l).$$

- Extension to regions $R = \cup_{l \in Loc}(l, R_l)$, $R_l \subseteq V$ for each $l \in Loc$:

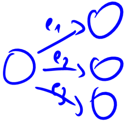
$$\mathcal{T}^+(R) = \cup_{l \in Loc}(l, \mathcal{T}_l^+(R_l)).$$

One-step reachability under discrete steps:

- We define the postcondition $\mathcal{D}_e^+(P)$ of P with respect to an edge $e = (l, a, \mu, l')$ as the set of valuations reachable from P by e:

$$\nu' \in \mathcal{D}_e^+(P) \quad \textit{iff} \quad \exists \nu \in P.\ (\nu, \nu') \in \mu \wedge \nu' \in Inv(l').$$

- Extension to regions $R = \cup_{l \in Loc}(l, R_l)$:



$$\mathcal{D}^+(R) = \cup_{e=(l,a,\mu,l') \in Edge}(l', \mathcal{D}_e^+(R_l)).$$

Linearity of reachable sets

Lemma

For all linear hybrid automata, if $P \subseteq V$ is a linear set of valuations, then for all $l \in Loc$ and $e \in Edge$, both $\mathcal{T}_l^+(P)$ and $\mathcal{D}_e^+(P)$ are linear sets of valuations.

$(\mathbb{R}, +, <, 0, 1)$

Linearity of reachable sets

Lemma

For all linear hybrid automata, if $P \subseteq V$ is a linear set of valuations, then for all $l \in Loc$ and $e \in Edge$, both $\mathcal{T}_l^+(P)$ and $\mathcal{D}_e^+(P)$ are linear sets of valuations.

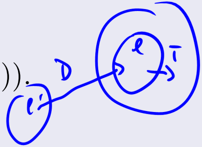
Lemma

Let $I \subseteq \bigcup_{l \in Loc}(l, Inv(l))$ be a region of the linear hybrid automaton A. The reachable region $(I, \mapsto^*) = \cup_{l \in Loc}(l, R_l)$ is the least fixpoint of the equation

$$\Rightarrow \quad X = \mathcal{T}^+(I \cup \mathcal{D}^+(X))$$

or, equivalently, for all locations $l \in Loc$, the set R_l of valuations is the least fixpoint of the set of equations

$$\Rightarrow \quad X_l = \mathcal{T}_l^+(\underline{I_l} \cup \bigcup_{e=(l',a,\mu,l) \in Edge} \mathcal{T}_l^+(\mathcal{D}_e^+(X_{l'}))).$$



$$\cancel{T^+(T^+(X))}$$

$$
\begin{aligned}
& \underline{X} \\
= \; & \underline{\mathcal{T}^+(I \cup \mathcal{D}^+(X))} \\
= \; & \mathcal{T}^+(I) \cup \mathcal{T}^+(\mathcal{D}^+(\underline{X})) \\
= \; & \mathcal{T}^+(I) \cup \mathcal{T}^+(\mathcal{D}^+(\underline{\mathcal{T}^+(I \cup \mathcal{D}^+(X))})) \\
= \; & \mathcal{T}^+(I) \cup \mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(I))) \cup \mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(\mathcal{D}^+(\underline{X})))) \\
= \; & \mathcal{T}^+(I) \cup \mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(I))) \cup \mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(\mathcal{D}^+(\underline{\mathcal{T}^+(I \cup \mathcal{D}^+(X))})))) \\
= \; & \mathcal{T}^+(I) \cup \mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(I))) \cup \mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(I))))) \cup \\
& \mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(\mathcal{D}^+(\mathcal{T}^+(\mathcal{D}^+(X)))))) \ldots
\end{aligned}
$$

State set representation and the computation of the forward reachability

$$\{ v \in V \mid \boxed{Q_1 x_1 . \ \ldots \ Q_n x_n . \ LE(Var \cup Var')} \}$$

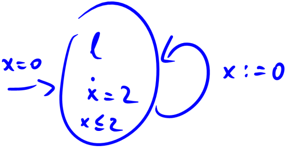
Formulas

$\cup \rightarrow \vee$

$\cap \rightarrow \wedge$

$x \in P \rightarrow P(x)$

$P = \emptyset \,? \rightarrow$ Prusat ?



$P_0(x):\ x=0$

$P_1(x):\ \underline{\exists x'.\ \exists t.\ x'=0 \wedge t\geq 0 \wedge x = x'+2t \wedge x\leq 2}$

$$P_2(x)\ \exists x''\ \big(\underbrace{\exists x'.\ \exists t.\ x'=0 \wedge t\geq 0 \wedge x''=x'+2t \wedge x''\leq 2}_{P_1(x'')\ \sim\ x'' \in P_1}\big)$$

$\wedge\ x=0\ \wedge\ x\leq 2$

$$P_3(x):\ \exists x'''\ \exists t.\ P_1(x''') \wedge t\geq 0 \wedge x = x'''+2t \wedge x\leq 2$$

$B:\ \boxed{x>2}$

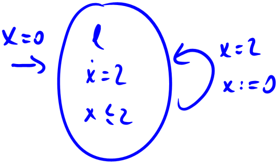
$P_1(x):\ \underline{0\leq x\leq 2}$

$2z \leq x$

$x \leq 2u+w$

$2x \leq 2u+w$

$$\begin{array}{ccccc} l_1 \leq & & \leq u_1 & & l_1 \leq u_1 \\ \vdots & x & \vdots & \rightsquigarrow & l_1 \leq u_2 \\ l_n \leq & & \leq u_m & & \vdots \\ & & & & l_n \leq u_m \end{array}$$



$B : x > 2$

$$P_0(x) = x = 0$$

$$P_1(x) = \exists x'.\ \exists t.\ x' = 0 \wedge t \geq 0 \wedge x = x' + 2t \wedge x \leq 2$$

$$t = \frac{x - x'}{2}$$

$$= \exists x'\ \ x' = 0 \wedge x - x' \geq 0 \wedge x \leq 2$$

$$= x \geq 0 \wedge x \leq 2 \equiv 0 \leq x \leq 2$$

$$P_2(x) = \exists x'.\ P_1(x') \wedge x' = 2 \wedge x = 0 \wedge x \leq 2$$

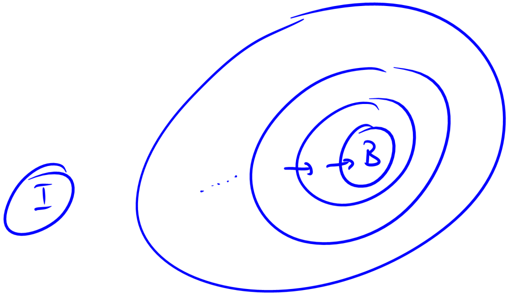
$$= \exists x'.\ 0 \leq x' \wedge x' \leq 2 \wedge x' = 2 \wedge x = 0 \wedge x \leq 2$$

$$= 0 \leq 2 \wedge 2 \leq 2 \wedge x = 0 \wedge x \leq 2$$

$$= x = 0$$

$$P_2(x) \rightarrow \left(P_0(x) \vee P_1(x)\right)$$

Backward analysis


I
B

- We define the backward time closure $\mathcal{T}_l^-(P)$ of $P \subseteq V$ at $l \in Loc$ as the set of valuations from which it is possible to reach a valuation in P by letting time progress:

- We define the backward time closure $\mathcal{T}_l^-(P)$ of $P \subseteq V$ at $l \in Loc$ as the set of valuations from which it is possible to reach a valuation in P by letting time progress:

$$\nu' \in \mathcal{T}_l^-(P) \quad \textit{iff} \quad \exists \nu \in P.\ \exists t \in \mathbb{R}^{\geq 0}.\ \nu = f_l[\nu'](t) \wedge \nu' \in Inv(l).$$

- Extension to regions $R = \cup_{l \in Loc}(l, R_l)$:

$$\mathcal{T}^-(R) = \cup_{l \in Loc}(l, \mathcal{T}_l^-(R_l)).$$

B: $\nu' \rightarrow \nu \in P$

F: $\exists \nu' \in P\ \nu' \rightarrow \nu$

- We define the precondition $\mathcal{D}_e^-(P)$ of P with respect to an edge $e = (l, a, \mu, l')$ as the set of valuations from which it is possible to reach a valuation from P by e:

$\nu' \in D_e^-(P)$ iff $\exists \nu \in P.\ (\nu', \nu) \in \mu \wedge Inv(l) \ni \nu'$

- We define the backward time closure $\mathcal{T}_l^-(P)$ of $P \subseteq V$ at $l \in Loc$ as the set of valuations from which it is possible to reach a valuation in P by letting time progress:

$$\nu' \in \mathcal{T}_l^-(P) \quad \textit{iff} \quad \exists \nu \in P.\ \exists t \in \mathbb{R}^{\geq 0}.\ \nu = f_l[\nu'](t) \wedge \nu' \in Inv(l).$$

- Extension to regions $R = \cup_{l \in Loc}(l, R_l)$:

$$\mathcal{T}^-(R) = \cup_{l \in Loc}(l, \mathcal{T}_l^-(R_l)).$$

- We define the precondition $\mathcal{D}_e^-(P)$ of P with respect to an edge $e = (l, a, \mu, l')$ as the set of valuations from which it is possible to reach a valuation from P by e:

$$\nu' \in \mathcal{D}_e^-(P) \quad \textit{iff} \quad \exists \nu \in P.\ (\nu', \nu) \in \mu \wedge \nu' \in Inv(l).$$

- Extension to regions $R = \cup_{l \in Loc}(l, R_l)$:

$$\mathcal{D}^-(R) = \cup_{e=(l',a,\mu,l) \in Edge}(l', \mathcal{D}_e^-(R_l)).$$

- Given a region $R \subseteq \bigcup_{l \in Loc}(l, Inv(l))$, the initial region $(\mapsto^* R) \subseteq \Sigma$ of R is the set of all states from which a state in R is reachable:

$$\sigma \in (\mapsto^* R) \quad \textit{iff} \quad \exists \sigma' \in R.\ \sigma \to^* \sigma'.$$

Lemma

For all linear hybrid automata, if $P \subseteq V$ is a linear set of valuations, then for all $l \in Loc$ and $e \in Edge$, both $\mathcal{T}_l^-(P)$ and $\mathcal{D}_e^-(P)$ are linear sets of valuations.

Lemma

For all linear hybrid automata, if $P \subseteq V$ is a linear set of valuations, then for all $l \in Loc$ and $e \in Edge$, both $\mathcal{T}_l^-(P)$ and $\mathcal{D}_e^-(P)$ are linear sets of valuations.

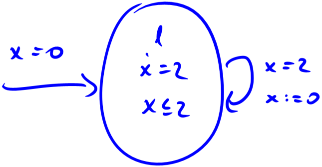
Lemma

Let $R = \cup_{l \in Loc}(l, R_l)$ be a region of the linear hybrid automaton A. The initial region $I = \cup_{l \in Loc}(l, I_l)$ is the least fixpoint of the equation

$$\Rightarrow \quad X = \mathcal{T}^-(R \cup \mathcal{D}^-(X))$$

or, equivalently, for all locations $l \in Loc$, the set I_l of valuations is the least fixpoint of the set of equations

$$\Rightarrow \quad X_l = \mathcal{T}_l^-(R_l \cup \bigcup_{e=(l,a,\mu,l') \in Edge} \mathcal{D}_e^-(X_{l'})).$$



$I: x=0$

$x \to x' \in P_0$

$P_0(x) = x \geq 2 \wedge x \leq 2 = x=2$

$P_1(x) = \exists t \exists x'.\ \underbrace{x'=2}_{P_0(x')} \wedge t \geq 0 \wedge \boxed{x' = x + 2t} \wedge \underset{x \leq 2}{}$

$= \exists t.\ t \geq 0 \wedge 2 = x + 2t \wedge x \leq 2$

$t = \frac{2-x}{2}$

$= \frac{2-x}{2} \geq 0 \wedge x \leq 2$

$= 2 \geq x \wedge x \leq 2$

$= x \leq 2$

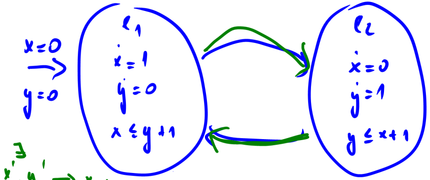
$P_2(x) = \exists x'.\ x' \leq 2 \wedge x'=0 \wedge x=2 \wedge x \leq 2$

$= 0 \leq 2 \wedge x=2$

$P_2(x) \to P_0(x) \vee P_1(x)$

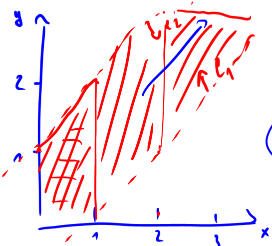
$(P_0 \vee P_1) \wedge I = (x=2 \vee x \leq 2) \wedge x=0$

$= x=0$



$\exists\; x',y' \to x,y$

$x = y+2$



$x \ge 0 \wedge y \ge 0 \wedge$

$-1 \le x-y \le 1$

$R^1_0 = x=0 \wedge y=0 \wedge x \le y+1$

$R^1_1 = \exists x',y',t.\ R^1_0(x',y') \wedge t \ge 0 \wedge f^x_{\ell_1}(x',y') = x \wedge$

(x,y) $\quad f^y_{\ell_1}(x',y') = y \wedge \mathrm{Inv}(\ell_1)(x,y)$

$= \exists x',y',t.\ x'=0 \wedge y'=0 \wedge t \ge 0 \wedge x = x'+t \wedge$

$y = y' \wedge x \le y+1$

$= \exists t.\ t \ge 0 \wedge x=t \wedge y=0 \wedge x \le y+1$

$= x \ge 0 \wedge y=0 \wedge x \le y+1$

$R^1_2 = \exists x',y'.\ R^2_1(x',y') \wedge \ldots = \text{false}$

$R^1_3 = \text{false}$

$R^2_0 = \text{false}$

$R^2_1 = \exists x',y',t.\ \text{false} \wedge \ldots\ldots = \text{false}$

$R^2_2 = \exists x',y'.\ \underbrace{x' \ge 0 \wedge y'=0 \wedge x' \le y'+1}_{R^1_1(x',y')} \wedge x = x' \wedge$

$y = y' \wedge y \le x+1$

$= x \ge 0 \wedge y=0 \wedge x \le y+1 \wedge y \le x+1$

$R^2_3 = \exists x',y',t.\ x' \ge 0 \wedge y'=0 \wedge x' \le y'+1 \wedge y' \le x'+1$

$\wedge\ x = x' \wedge y = y'+t \wedge y \le x+1 \wedge t \ge 0$

$= \exists t.\ x \ge 0 \wedge y-t=0 \wedge x \le y-t+1 \wedge y-t \le x+1$

$\wedge\ y \le x+1 \wedge t \ge 0$

$= x \ge 0 \wedge x \le 1 \wedge 0 \le x+1 \wedge y \le x+1 \wedge y \ge 0$

$= 0 \le x \le 1 \wedge y \ge 0 \wedge y \le x+1$

$R_3^1 = \text{false}$

$R_3^2 = 0 \le x \le 1 \wedge 0 \le y \wedge y \le x+1$

$R_4^1 = \exists x', y'.\ 0 \le x' \le 1 \wedge 0 \le y' \wedge y' \le x+1 \wedge$
$\underline{x = x'} \wedge \underline{y = y'} \wedge x \le y+1$

$= \underline{0 \le x \le 1 \wedge 0 \le y} \wedge \underline{y \le x+1} \wedge \underline{x \le y+1}$

$R_4^2 = \text{false}$

$R_5^2 = \text{false}$

$R_5^1 = \exists x', y', t.\ 0 \le x' \le 1 \wedge 0 \le y' \wedge y' \le x'+1 \wedge x' \le y'+1 \wedge t \ge 0 \wedge \underline{x = x'+t} \wedge \underline{y = y'} \wedge x \le y+1$

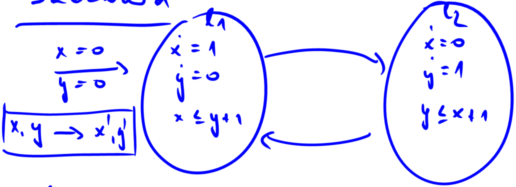
$= \exists t.\ 0 \le x - t \le 1 \wedge 0 \le y \wedge y \le x - t + 1 \wedge x - t \le y+1 \wedge t \ge 0 \wedge x \le y+1$

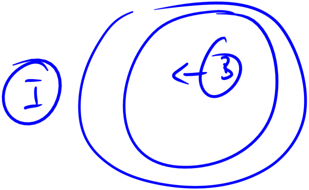
$= \exists t.\ \underset{u}{t \le x} \wedge \underset{l}{x-1 \le t} \wedge \underline{0 \le y} \wedge \underset{u}{t \le x-y+1} \wedge \underset{l}{x-y-1 \le t} \wedge \underset{l}{t \ge 0} \wedge \underline{x \le y+1}$

$= x-1 \le x \wedge x-1 \le x-y+1 \wedge x-y-1 \le x \wedge x-y-1 \le x-y+1 \wedge 0 \le x \wedge 0 \le x-y+1 \wedge$
$\wedge\ 0 \le y \wedge x \le y+1$

$= \underline{y \le 2 \wedge -1 \le y \wedge 0 \le x} \wedge \underline{y \le x+1} \wedge \underline{0 \le y} \wedge \underline{x \le y+1}$

Backward





$R_0^1 = x = y+2 \wedge x \le y+1 \equiv false$

$R_1^1 = false$

$R_2^1 = \exists x', y'.\ x'-y'-2 \ge 0 \wedge y' \le x'+1 \wedge x = x' \wedge y = y' \wedge$
$\quad x \le y+1$
$\quad = x-y-2 \ge 0 \wedge y \le x+1 \wedge x \le y+1$
$\quad = x-y \ge 2 \wedge x-y \ge -1 \wedge x-y \le 1$
$\quad = false$

$R_0^2 = x = y+2 \wedge y \le x+1 = x = y+2$

$R_1^2 = \exists x', y', t.\ x' = y'+2 \wedge t \ge 0 \wedge x = x'$
$\quad \wedge\ y+t = y' \wedge y \le x+1$
$\quad = \exists t.\ x = y+t+2 \wedge t \ge 0 \wedge y \le x+1$
$\quad = x-y-2 \ge 0 \wedge y \le x+1$

$R_2^2 = false$

$$R_0^1 = \underline{x \geq 0 \wedge y \geq 0 \wedge y \leq x+1 \wedge x \leq y+1} \qquad R_0^2 = R_0^1$$

$$R_1^1 = \exists x', y', t.\ x' \geq 0 \wedge y' \geq 0 \wedge y' \leq x'+1 \wedge x' \leq y'+1 \wedge$$

$$t \geq 0 \wedge \underline{x = x'+t} \wedge \underline{y = y'} \wedge x \leq y+1$$

$$= \exists t.\ x-t \geq 0 \wedge y \geq 0 \wedge y \leq x-t+1 \wedge x-t \leq y+1 \wedge$$

$$t \geq 0 \wedge x \leq y+1$$

$$= \exists t.\ \underset{u}{x \geq t} \wedge y \geq 0 \wedge \underset{u}{t \leq x-y+1} \wedge \underset{\underline{\ell}}{x-y-1 \leq t} \wedge$$

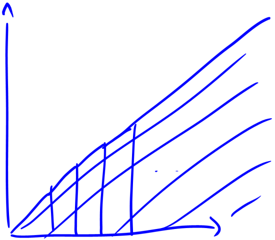
$$\underset{\underline{\ell}}{t \geq 0} \wedge x \leq y+1$$

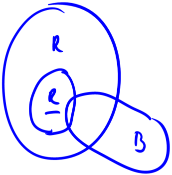
$$= x-y-1 \leq x \wedge x-y-1 \leq x-y+1 \wedge \underline{0 \leq x} \wedge 0 \leq x-y+1 \wedge$$

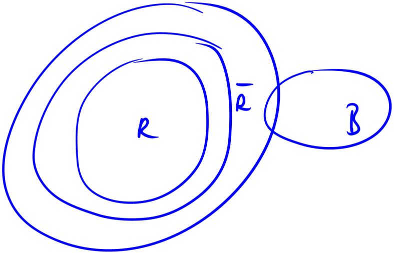
$$y \geq 0 \wedge x \leq y+1$$

$$= \underline{0 \leq x \wedge y \leq x+1 \wedge y \geq 0 \wedge x \leq y+1}$$

$$x = y+2$$




R
R̲
B


R̄
R
B