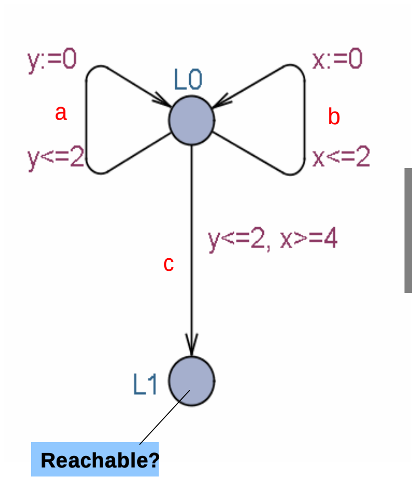
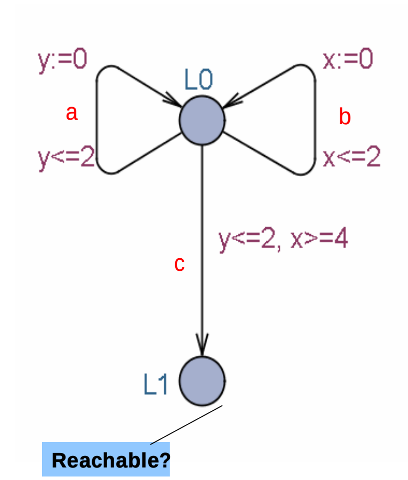
Decidability ?

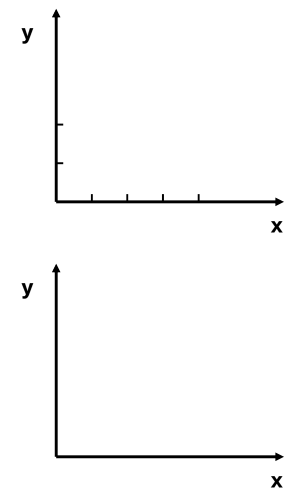


OBSTACLE: Uncountably infinite state space

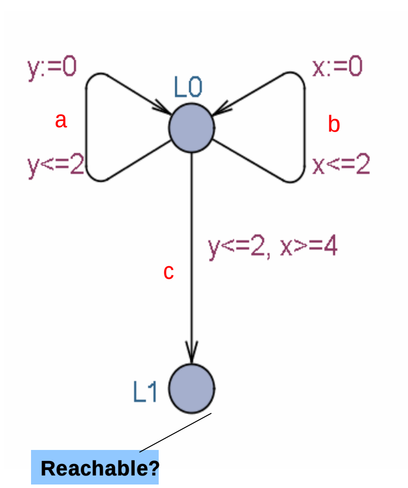
Stable Quotient



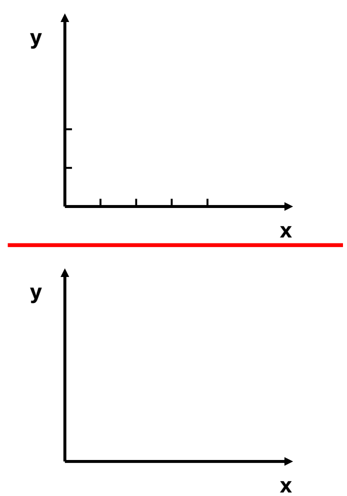
Partitioning



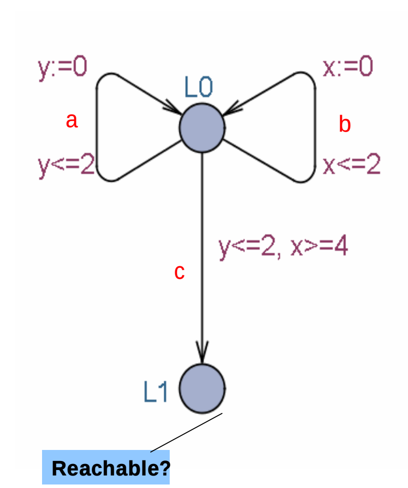
Stable Quotient



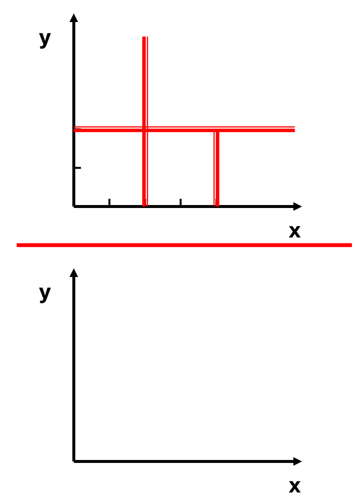
Partitioning



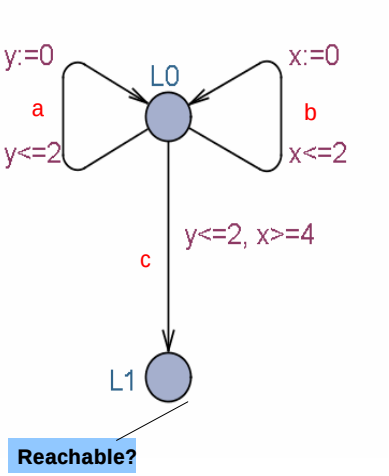
Stable Quotient



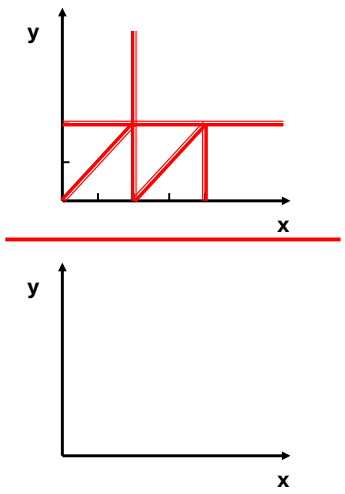
Partitioning



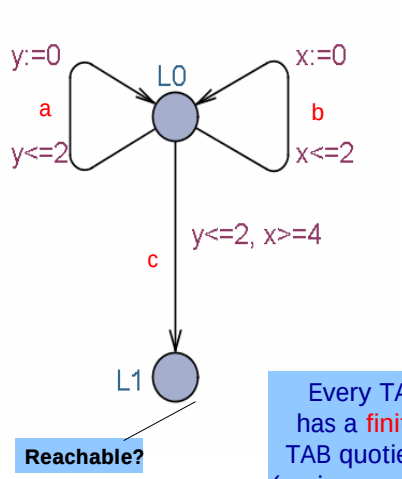
Stable Quotient



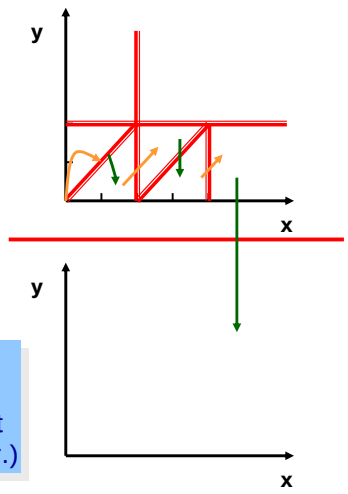
Partitioning



Stable Quotient



Partitioning



Every TA has a finite TAB quotient (region-constr.)

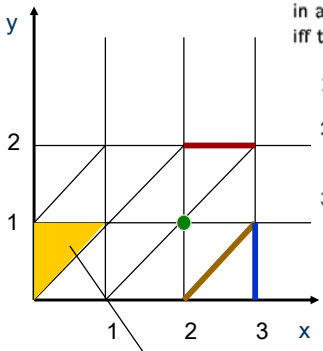
Region Equivalence

For each clock x let c_x be the largest integer with which x is compared in any guard or invariant of A. u and u' are *region equivalent*, $u \cong u'$ iff the following holds:

1. For all $x \in C$, either $\lfloor u(x) \rfloor = \lfloor u'(x) \rfloor$ or $u(x), u'(x) > c_x$;
2. For all $x, y \in C$ with $u(x) \leq c_x$ and $u(y) \leq c_y$, $fr(u(x)) \leq fr(u(y))$ iff $fr(u'(x)) \leq fr(u'(y))$;
3. For all $x \in C$ with $u(x) \leq c_x$, $fr(u(x)) = 0$ iff $fr(u'(x)) = 0$.

Regions

Finite Partitioning of State Space



For each clock x let c_x be the largest integer with which x is compared in any guard or invariant of A. u and u' are region equivalent, $u \cong u'$ iff the following holds:

1. For all $x \in C$, either $\lfloor u(x) \rfloor = \lfloor u'(x) \rfloor$ or $u(x), u'(x) > c_x$;
2. For all $x, y \in C$ with $u(x) \leq c_x$ and $u(y) \leq c_y$, $fr(u(x)) \leq fr(u(y))$ iff $fr(u'(x)) \leq fr(u'(y))$;
3. For all $x \in C$ with $u(x) \leq c_x$, $fr(u(x)) = 0$ iff $fr(u'(x)) = 0$.

An equivalence class (i.e. a *region*)
in fact there is only a *finite* number of regions!!

Logical Characterization of Regions

Each region may be represented by specifying

1. for every clock x a constraint from

$$\{x = c \mid c = 0, 1, \ldots, c_x\} \cup \{c - 1 < x < c \mid c = 1, \ldots, c_x\} \cup \{x > c_x\}$$

2. for every pair of clocks x, y such that $c-1 < x < c$ and $d-1 < y < d$ appears in 1., whether $fr(x)$ is $<$, $=$ or $>$ than $fr(y)$.

Theorem

The number of regions is $n! \cdot 2^n \cdot \prod_{x \in C}(2c_x + 2)$.

Stability of Regions

Lemma

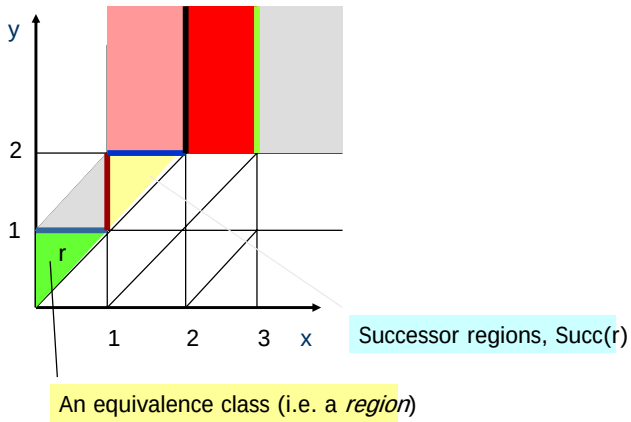
1. If $u \cong u'$ then $\forall d. \exists d'. u + d \cong u' + d'$;
2. If $u \cong u'$ then* $\forall g \in \mathcal{B}(X). u \models g \Leftrightarrow u' \models g$;
3. If $u \cong u'$ then $\forall r \subseteq C. u[r] \cong u'[r]$.

Theorem

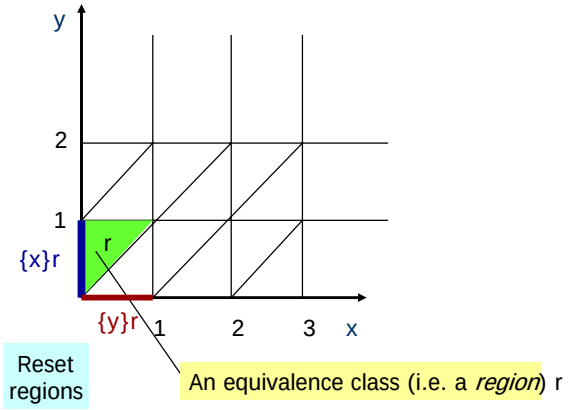
Let $(l, u) \cong (l', u')$ iff $l = l'$ and $u \cong u'$. Then $\cong$ is a TAB with respect to any set of goal locations G.

*Here $\cong$ and g should agree on the maximal constants.

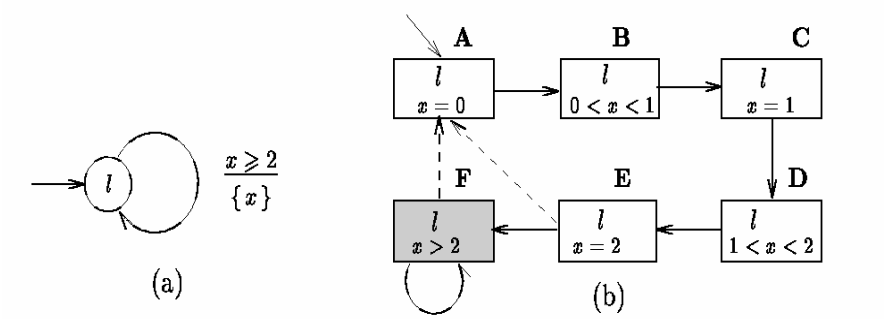
Regions
Successor Operation (wrt delay)



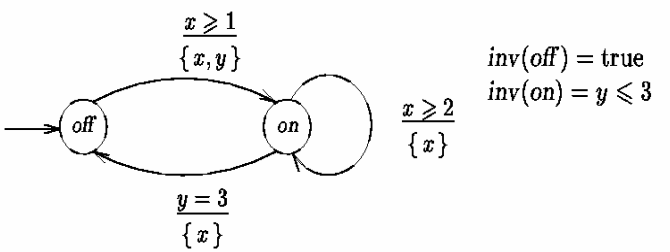
Regions
Reset Operation

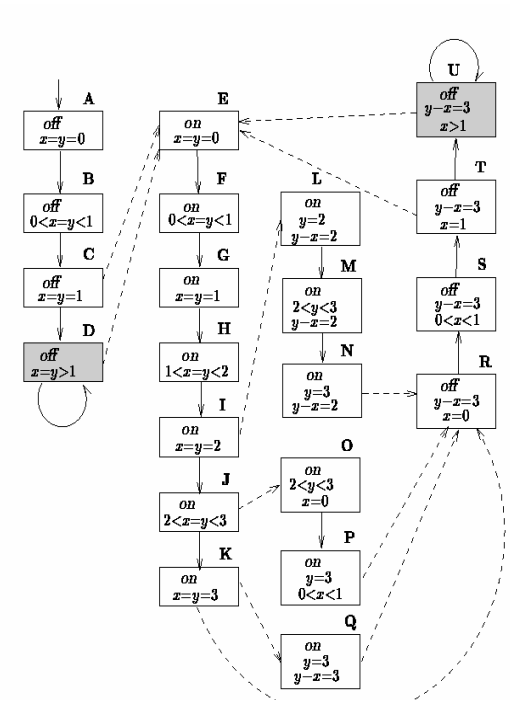


An Example Region Graph



Modified light switch





Reachable part of region graph

Properties

$AG(x \leq y)$

$AG(on \Rightarrow AF off)$

$AG(on \Rightarrow AF_{\leq 9} off)$

Hennessy Milner Logic

F ::=

p | X | [a]F | ⟨a⟩F | $F_1 \wedge F_2$ | $F_1 \vee F_2$

Atomic Prop

Recursion Variables

Action Modalities

Boolean Connectives

Timed HML

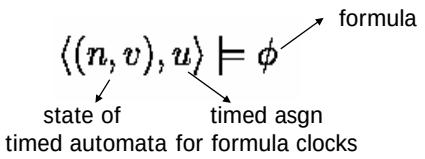
Larsen, Holmer, Wang'91
Larsen, Laroussine, Weise, 1995
Larsen, Pettersson, Wang, 1995

$$F ::= p \mid X \mid [a]F \mid \langle a \rangle F \mid F_1 \wedge F_2 \mid F_1 \vee F_2 \mid c \mid x \text{ in } F \mid \forall F \mid \exists F$$

Atomic Prop — **Recursion Variables** — **Action Modalities** — **Boolean Connectives** — **Formula Clock Constr** — **Formula Clock Reset** — **Delay Modalities**

$$c ::= x \sim n \mid x - y \sim n \qquad \sim \in \{\leq, <, =, >, \geq\}$$

Semantics



Semantics

$$\langle (n,v), u \rangle \models \langle a \rangle \phi \quad \text{iff} \quad \exists (n,v) \xrightarrow{a} (n',v'). \langle (n',v'), u \rangle \models \phi$$

$$\langle (n,v), u \rangle \models \exists \phi \quad \text{iff} \quad \exists d. \langle (n, v+d), u+d \rangle \models \phi \wedge Inv(n, v+d)$$

$$\langle (n,v), u \rangle \models x \text{ in } \phi \quad \text{iff} \quad \langle (n,v)u[x \mapsto 0] \rangle \models \phi$$

$$\langle (n,v), u \rangle \models x \sim n \quad \text{iff} \quad u(x) \sim n$$

$$\langle (n,v), u \rangle \models X \quad \text{iff} \quad \langle (n,v), u \rangle \models \phi_X \quad \text{where } X = \phi_X$$

Derived Operators

ϕ holds between l and u

$$x \text{ in } \exists (l \leq x \leq u \wedge \phi)$$

CHARACTERIZATION RESULT
Two TA's are timed bisimilar precisely when they satisfy the exact same THML formula

Invariantly

$$X =_\nu \phi \wedge \bigwedge_a [a]X \wedge \mathbb{W}X$$

Weak UNTIL

$$X =_\nu \phi_2 \vee (\phi_1 \wedge \bigwedge_a [a]X \wedge \mathbb{W}X)$$

Bounded UNTIL

$$x \text{ in } ((\phi_1 \wedge x \leq t) \text{UNTIL} \phi_2)$$