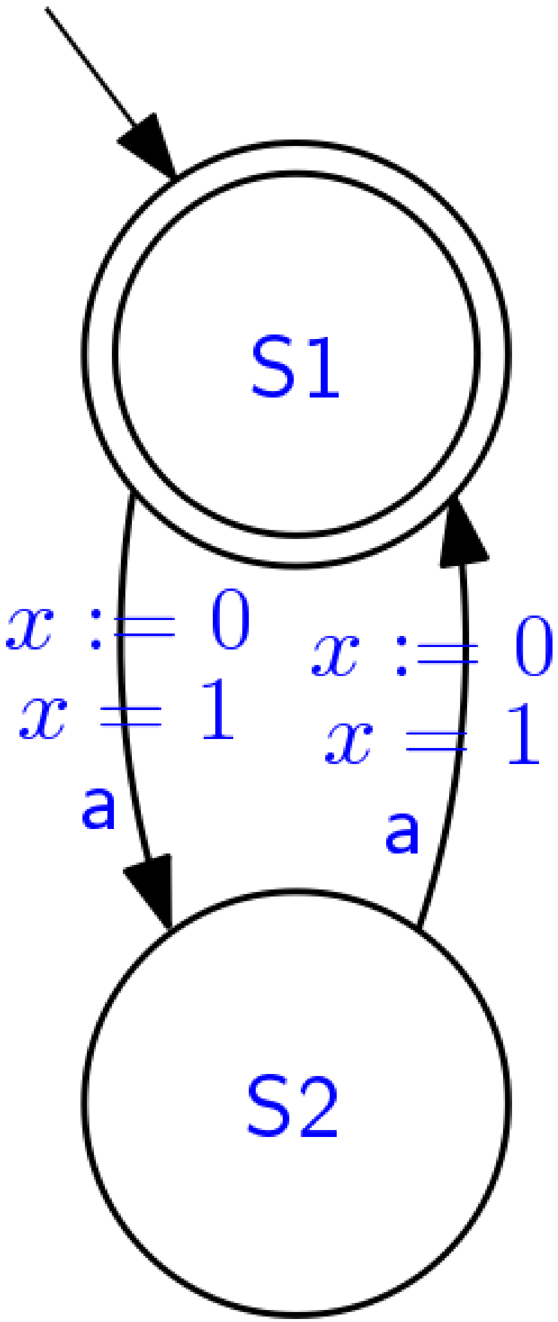
Software Verification
Exercise class:
Real Time Systems

Carlo A. Furia

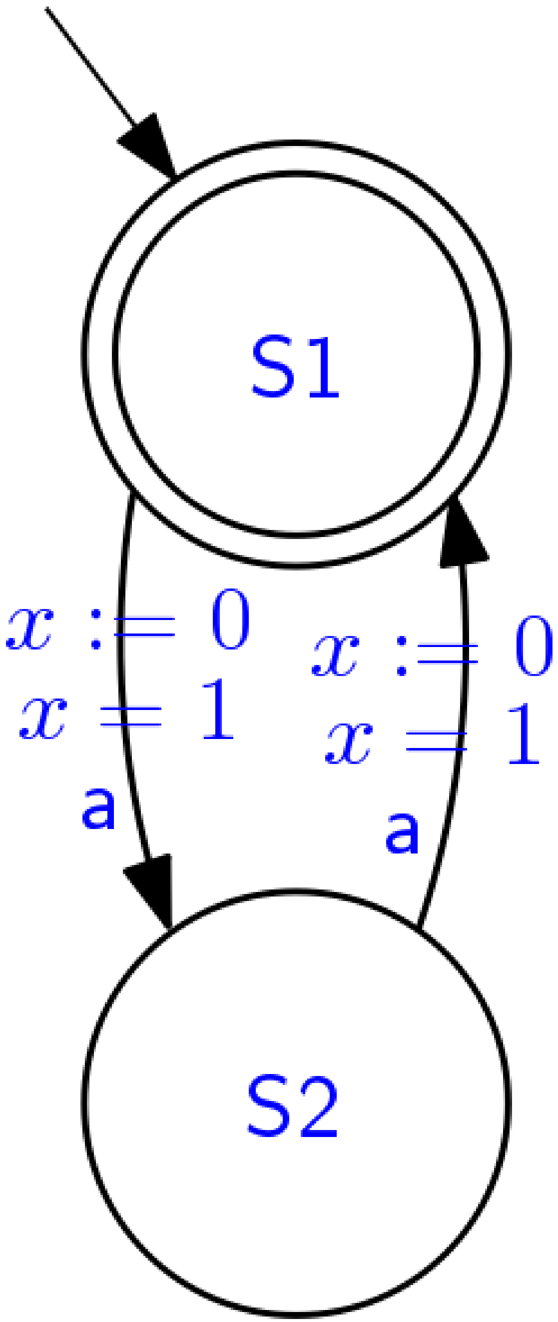
Exercises:
Does the property hold?

Does the property hold?



[] a

Does the property hold?

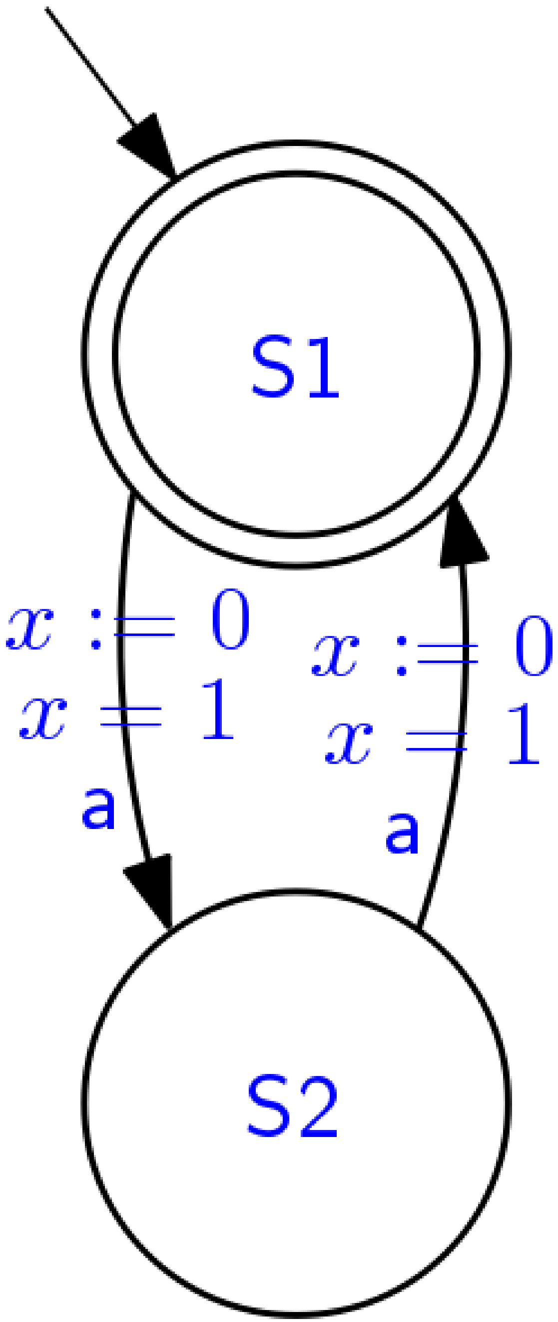


[] a

Yes:

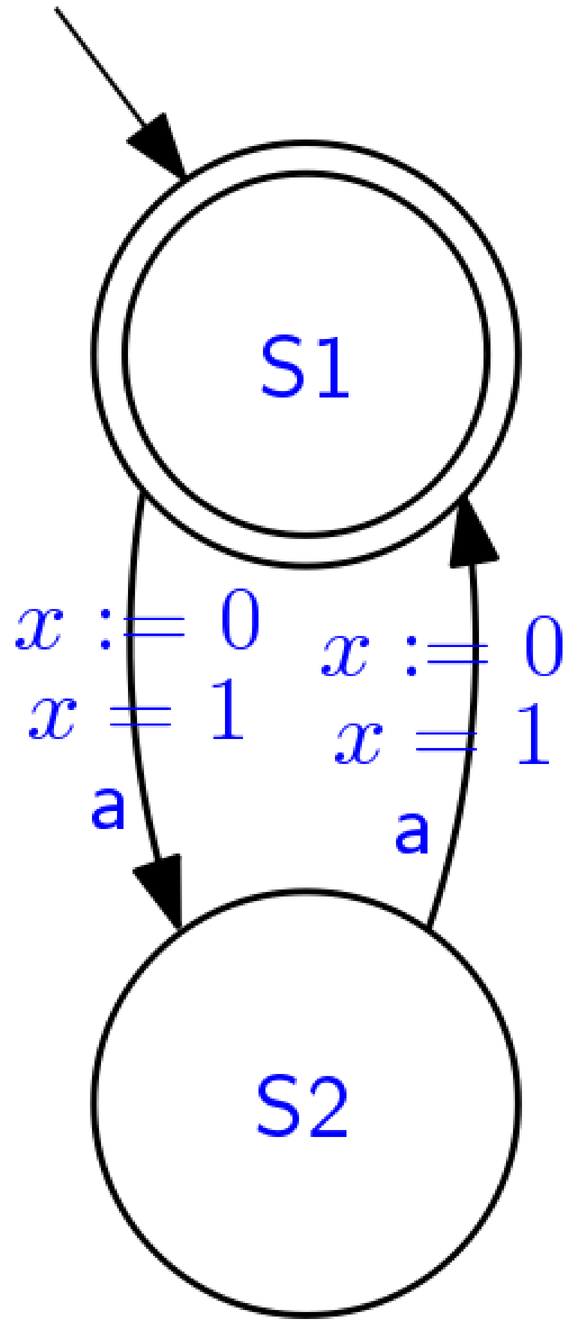
- it simply means that a holds at every position in the word (if any)

Does the property hold?



[] (<>=1 a)

Does the property hold?

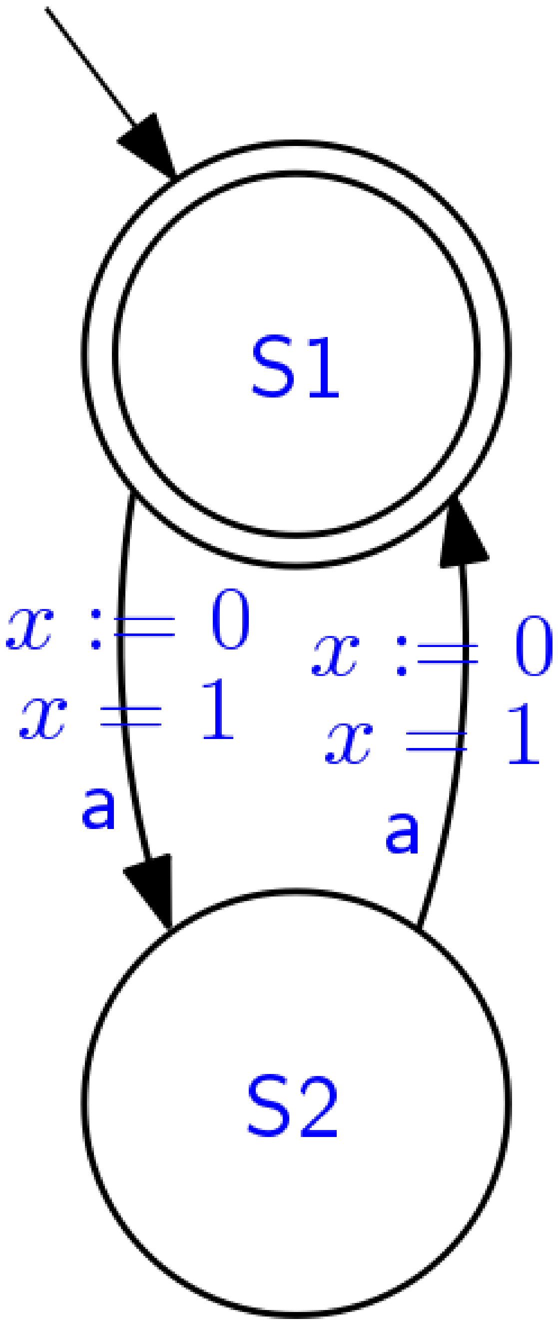


[] (<>=1 a)

No:

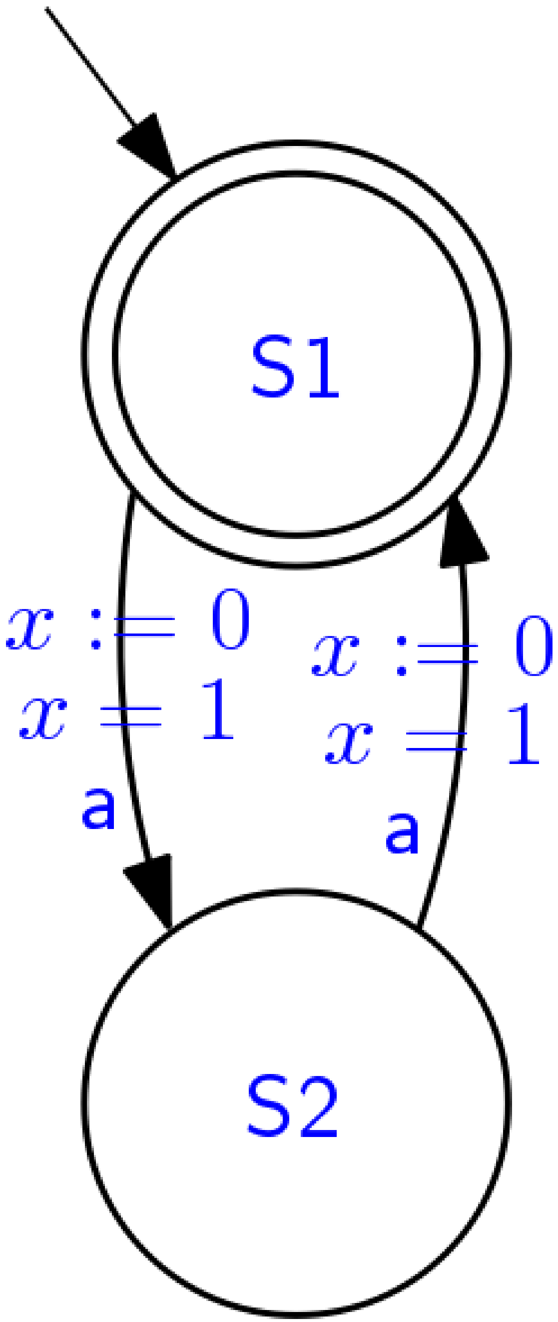
- this requires that there is always a future position, 1 time unit in the future, where a holds
- but this is not the case in the last position of any (non-empty) timed word

Does the property hold?



[] ([]=1 a)

Does the property hold?

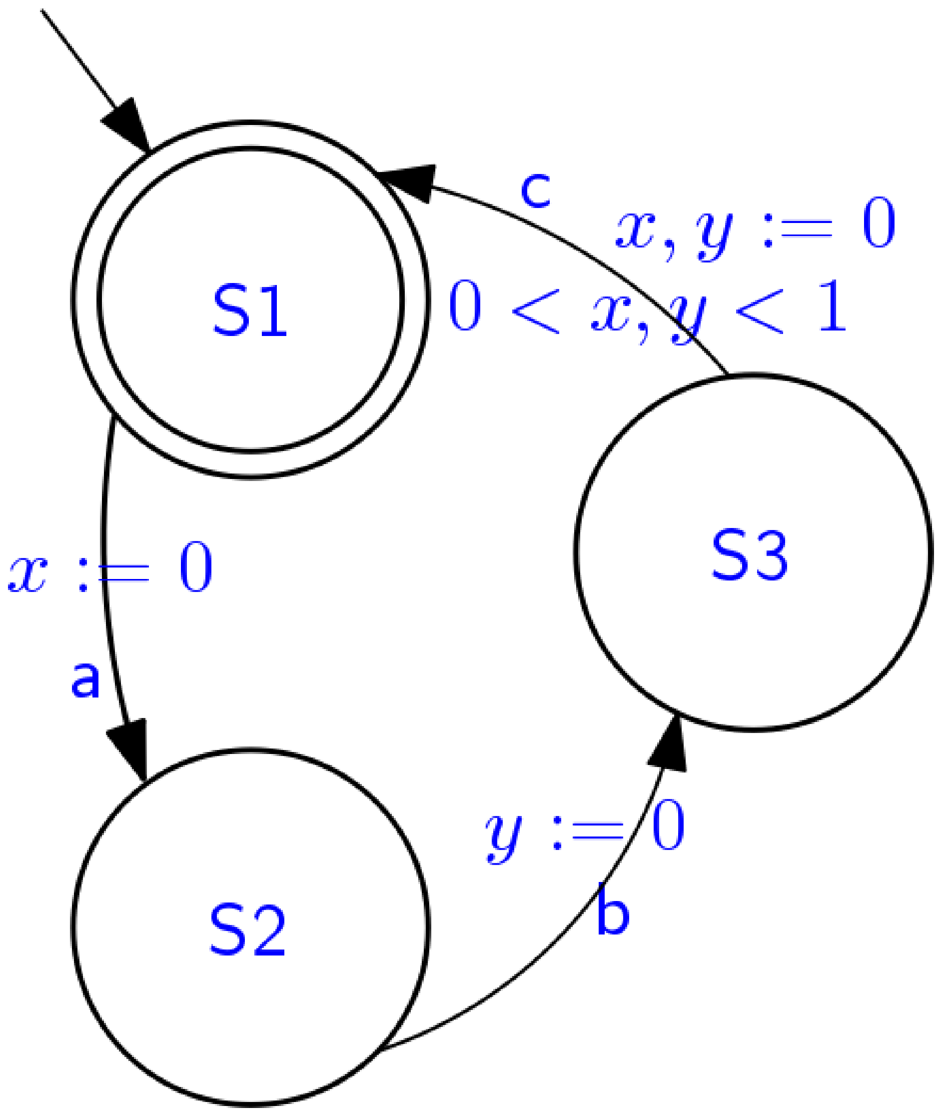


[] ([]=1 a)

Yes:

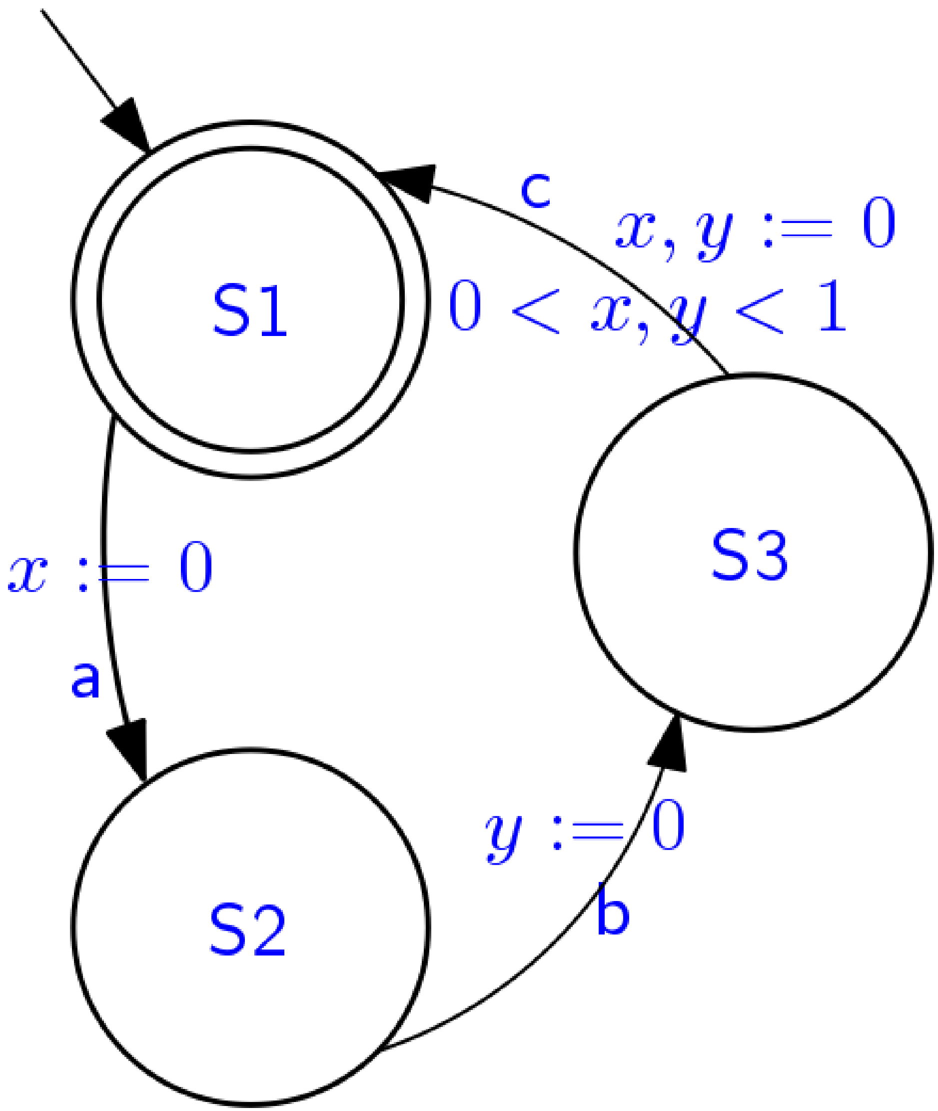
- the formula just requires that there if there is a future position 1 time unit in the future, then a holds there
- the automaton accepts only a's every time unit, hence the property is satisfied by any word accepted by the automaton

Does the property hold?



[] (a ⇒ <>(0,1) c)

Does the property hold?

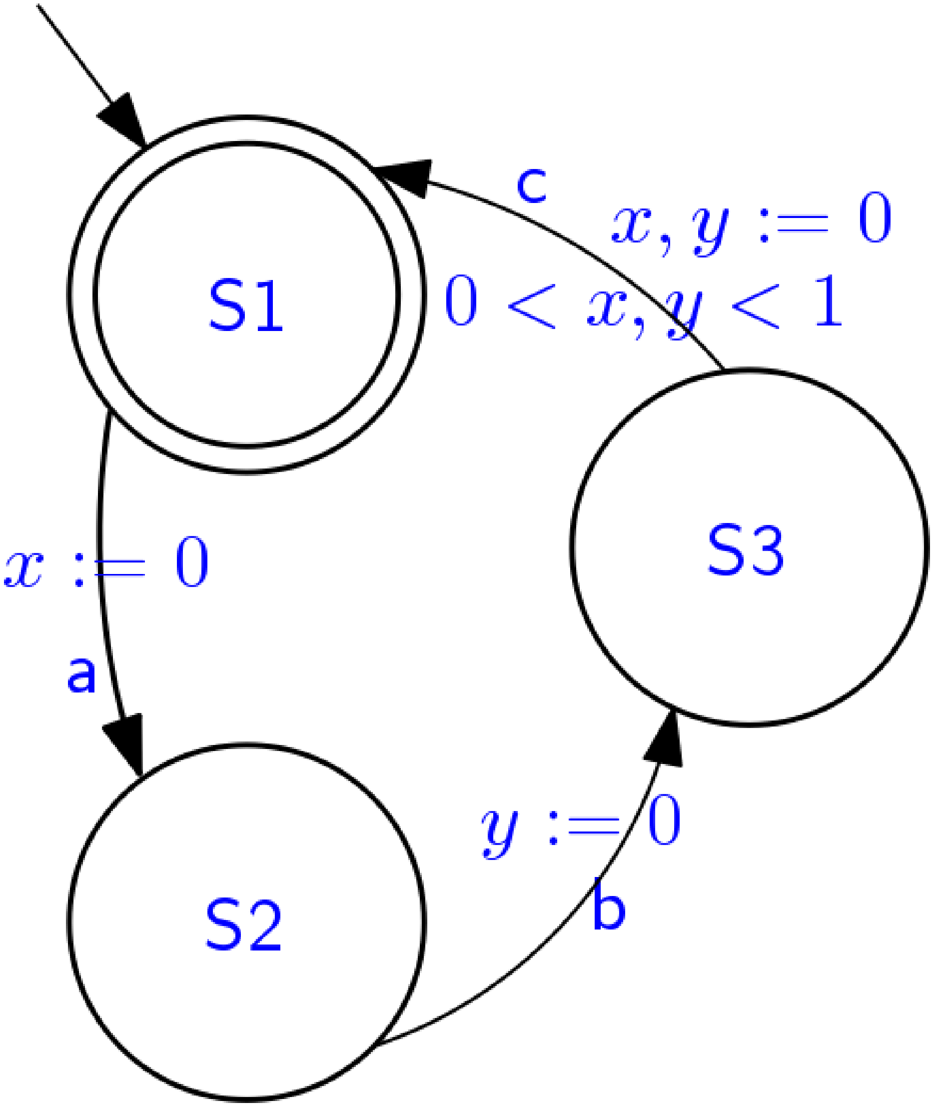


[] (a ⇒ <>(0,1) c)

Yes:

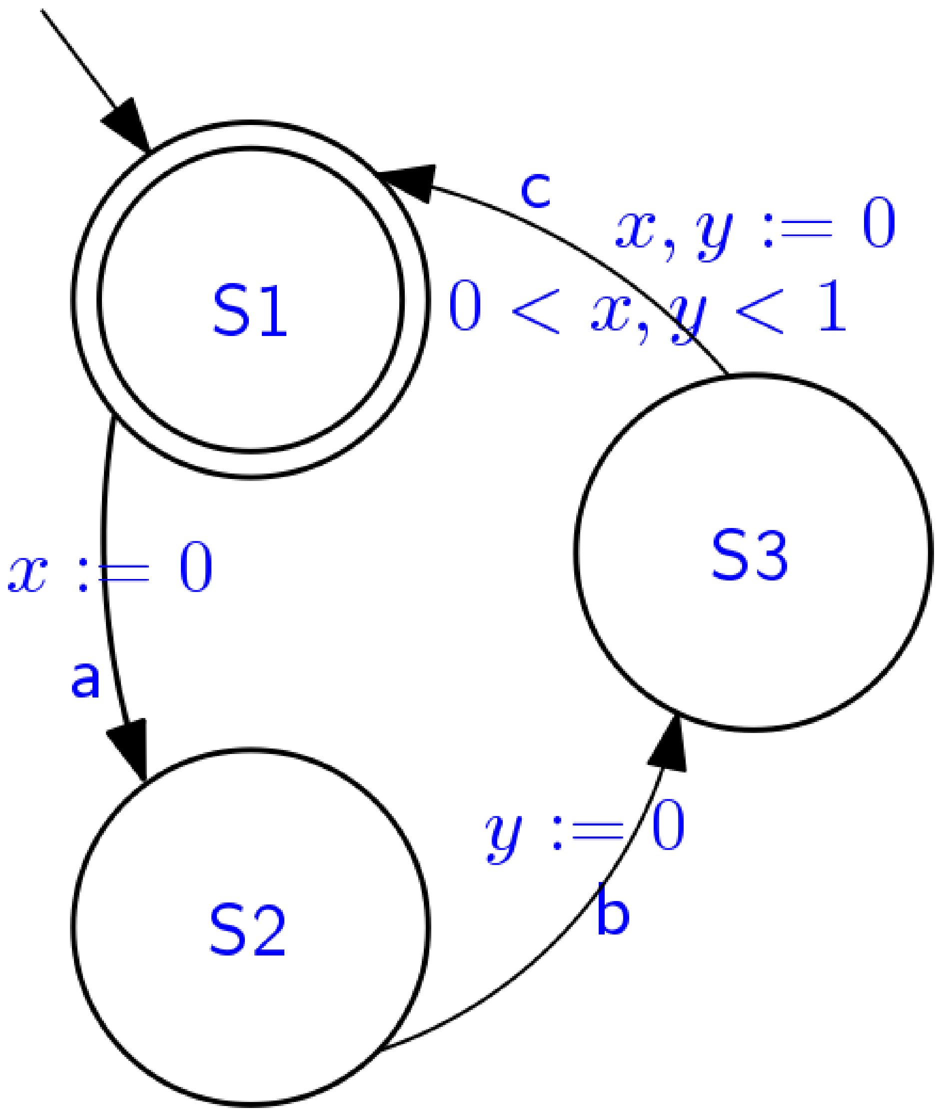
- clock x is reset upon reading a
- after that, it is checked upon reading c
- the constraint requires that x is in the range (0,1)

Does the property hold?



[] (a ⇒ <>(0,1) b)

Does the property hold?



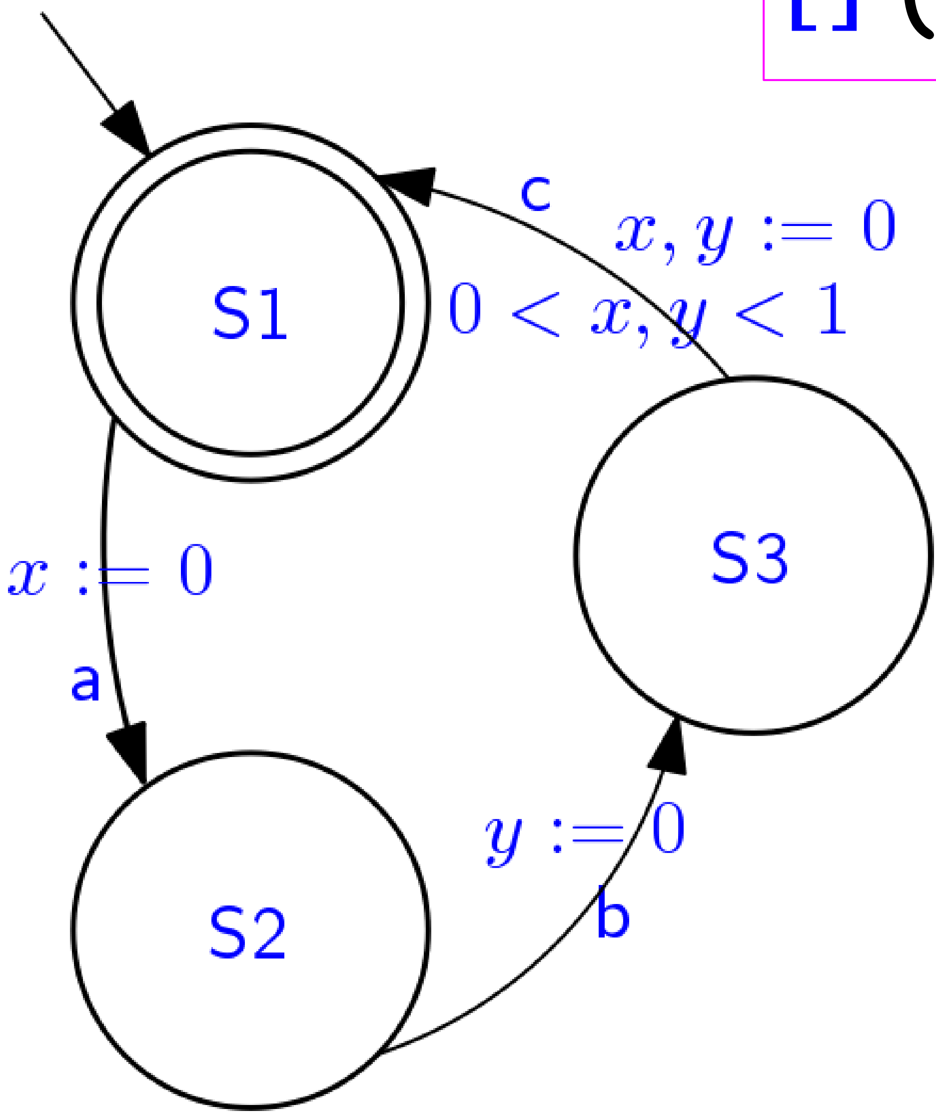
$[\,]\,(a \Rightarrow \langle\rangle(0,1)\; b)$

Yes:

- clock x is reset upon reading a; after that, it is checked upon reading c, which is always preceded by a reading of b
- if b occurs later than or exactly after 1 time unit since the reading of b, the same occurs for the reading of c
- in this case the constraint on x would be violated

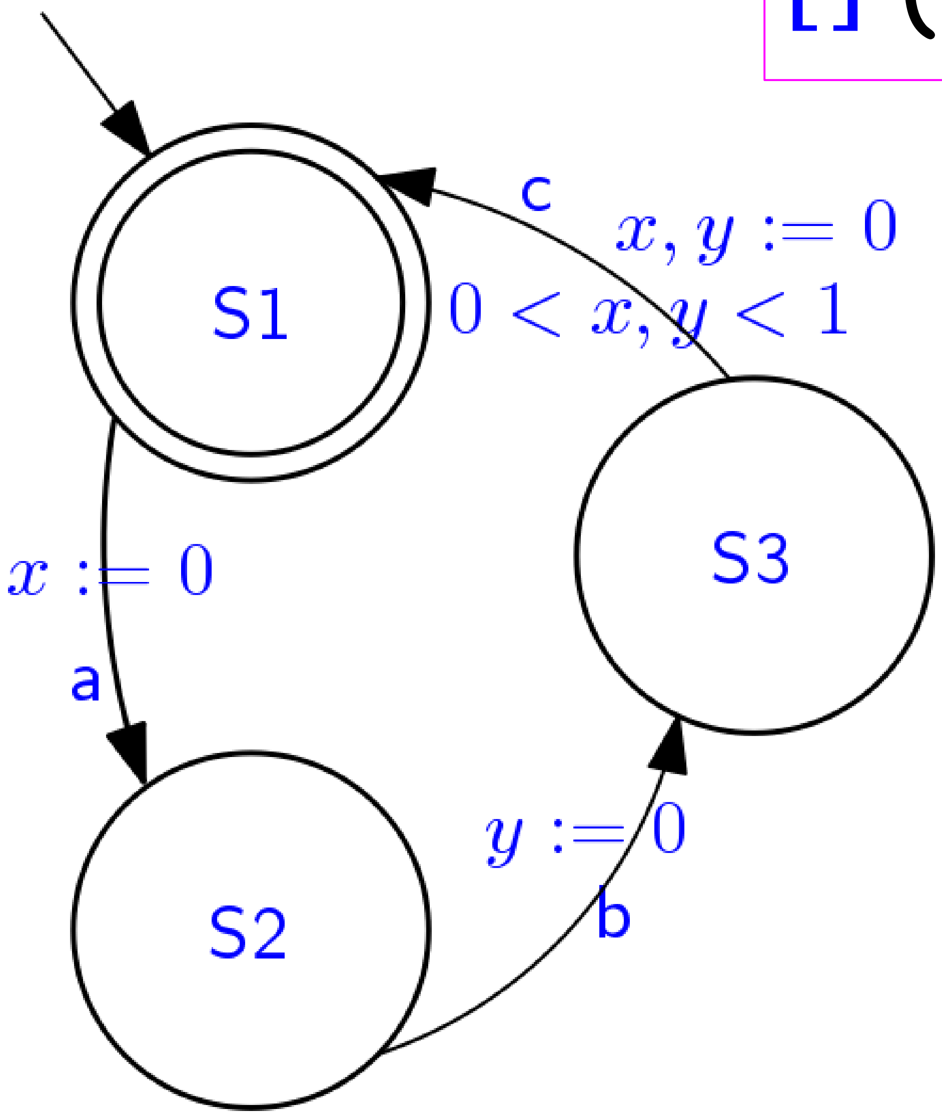
Does the property hold?

$$[\,]\,(\,a \Rightarrow (a \lor b)\ U(0,1)\ c)$$



Does the property hold?

$$[]\,(a \Rightarrow (a \vee b)\ U(0,1)\ c)$$

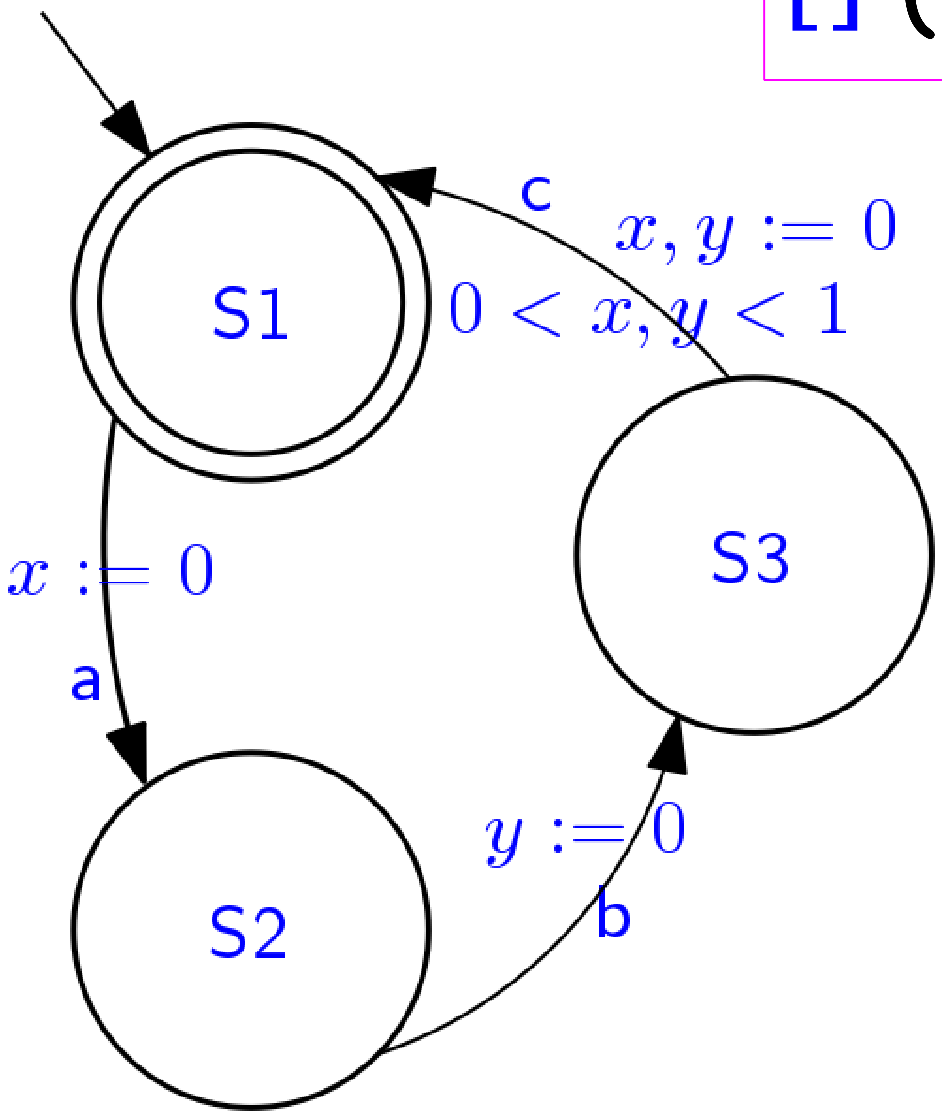


Yes:

- clock x is reset upon reading a
- after that there is one reading of b followed by a reading of c, which satisfies the sequence of events required by the until formula
- as far as timing is concerned, c must occur within interval of time (0,1) since a occurred because of the clock constraint $0 < x,y < 1$

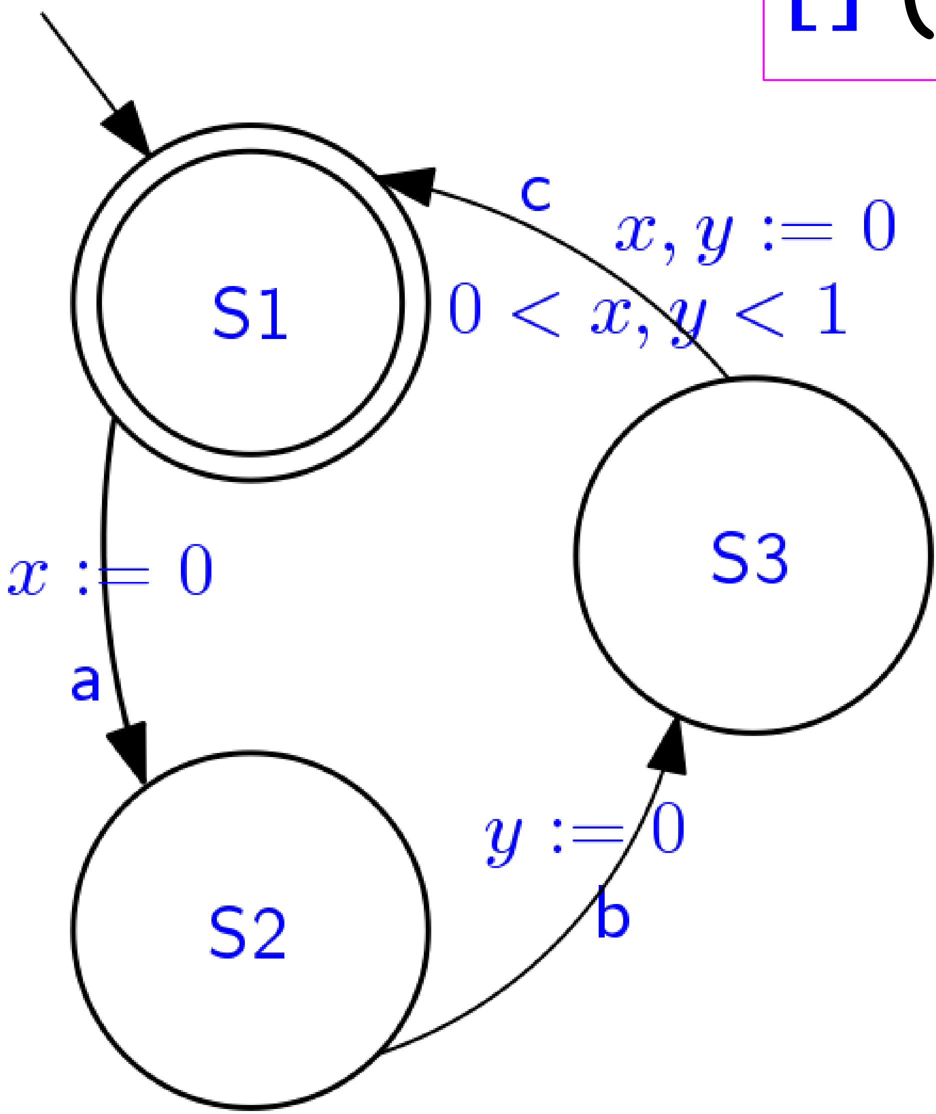
Does the property hold?

$$[\,]\,(\,a \Rightarrow (a \vee b)\ U(1,2)\ c)$$



Does the property hold?

$[]\ (\ a \Rightarrow (a \vee b)\ U(1,2)\ c)$

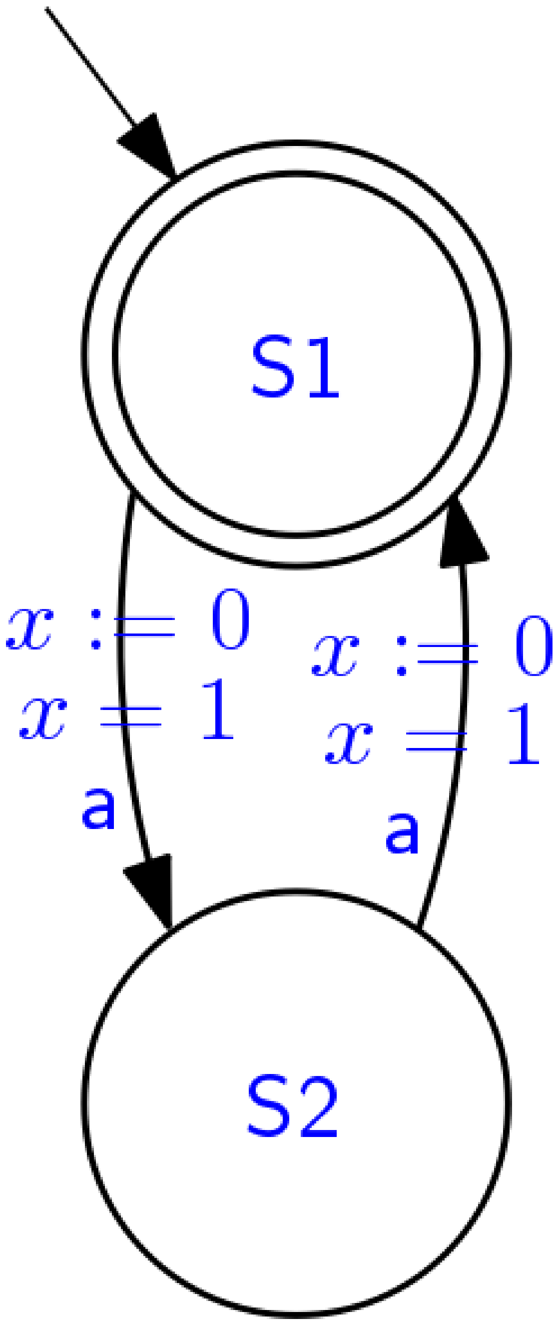


No:

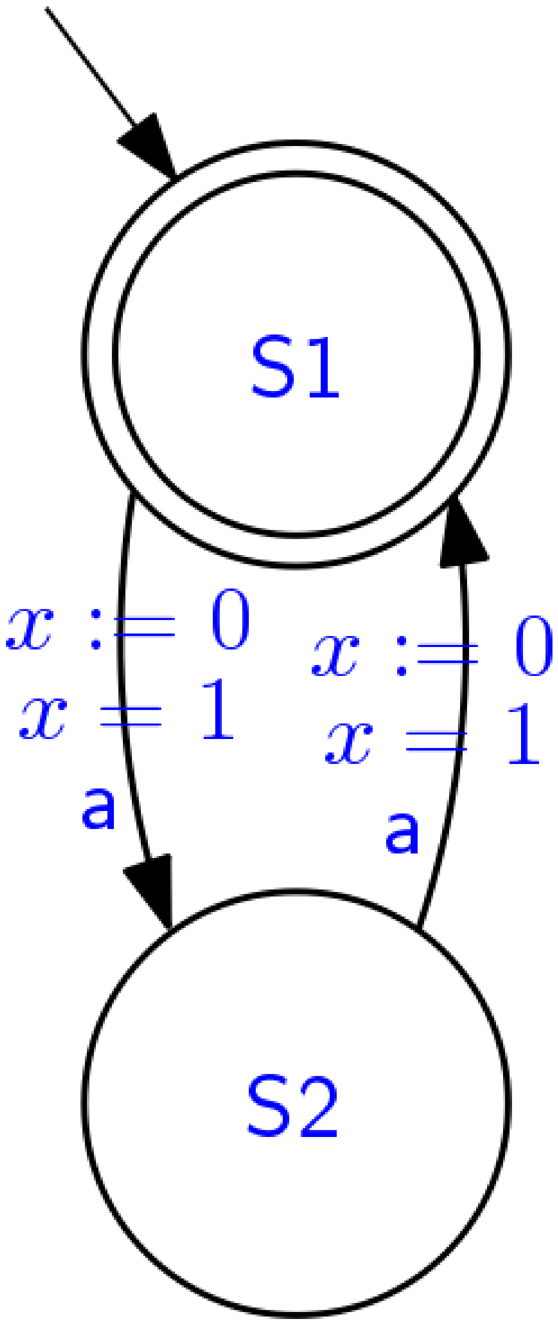
- if the "next" c is considered w.r.t when a occurs, it cannot happen in interval (1,2)
- if a successive occurrence of c is considered, it is preceded by at least another occurrence of c, which is not admitted by avb

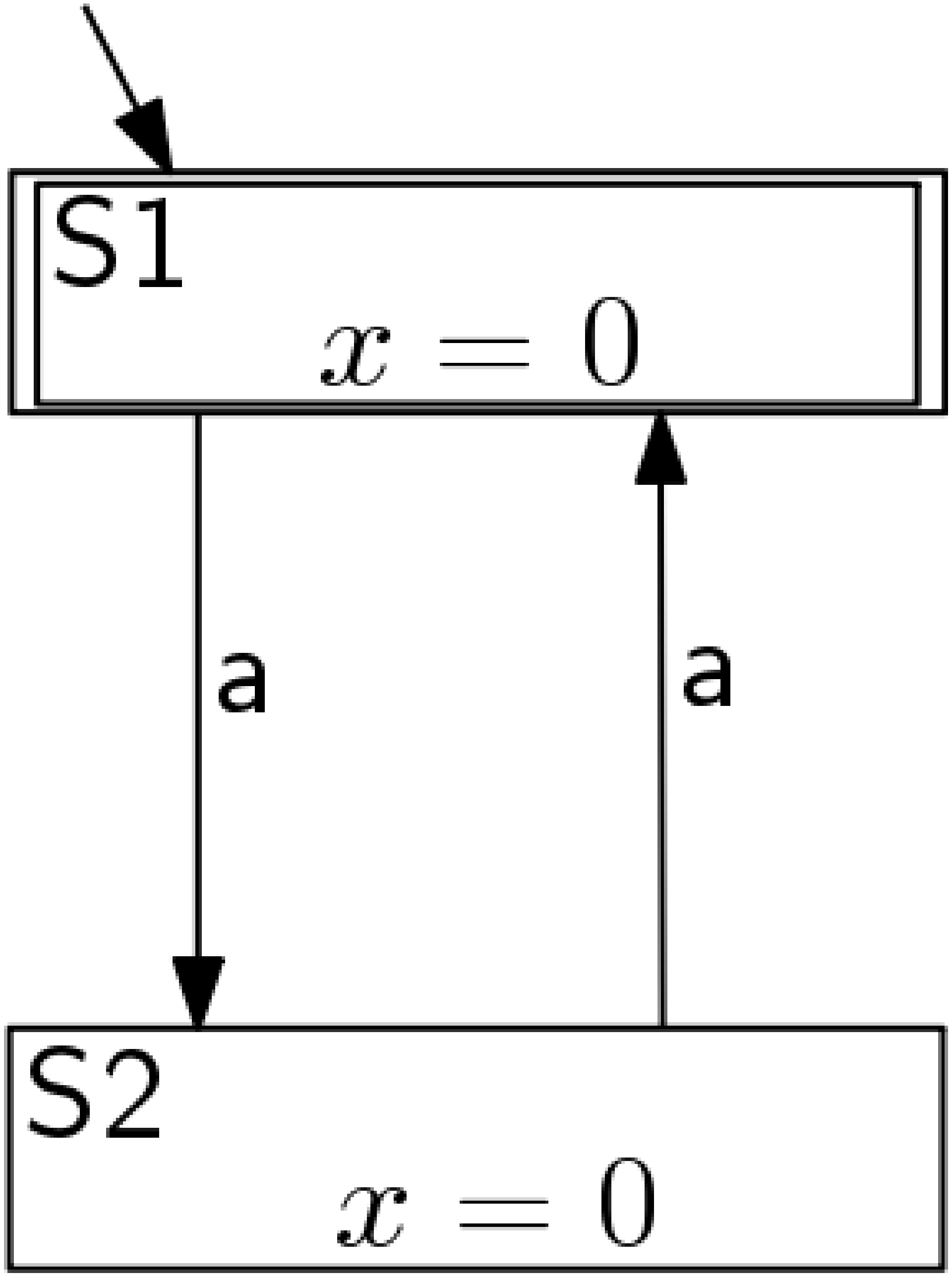
Exercises:
Region automaton construction

Build the region automaton for:

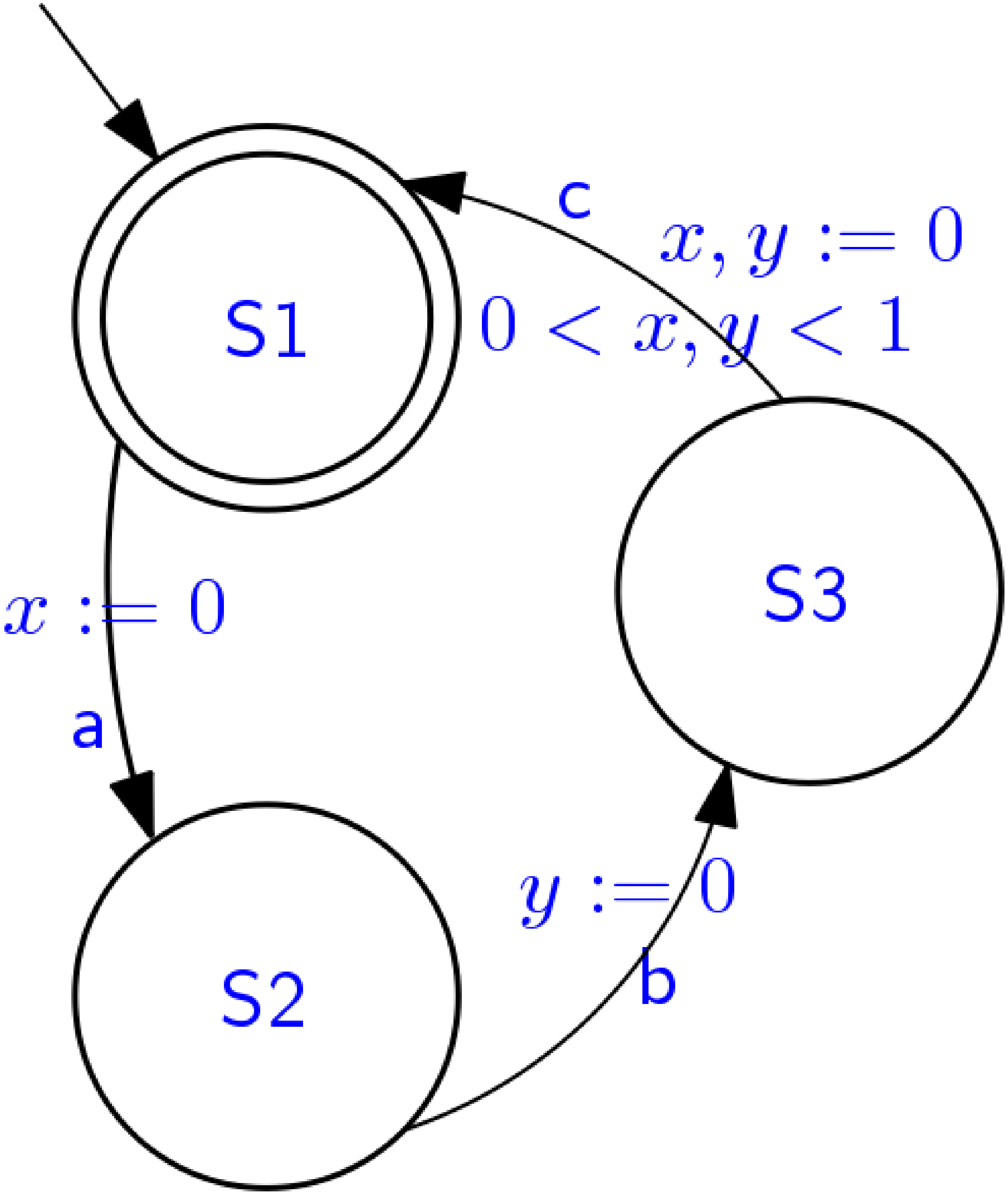


Build the region automaton for:

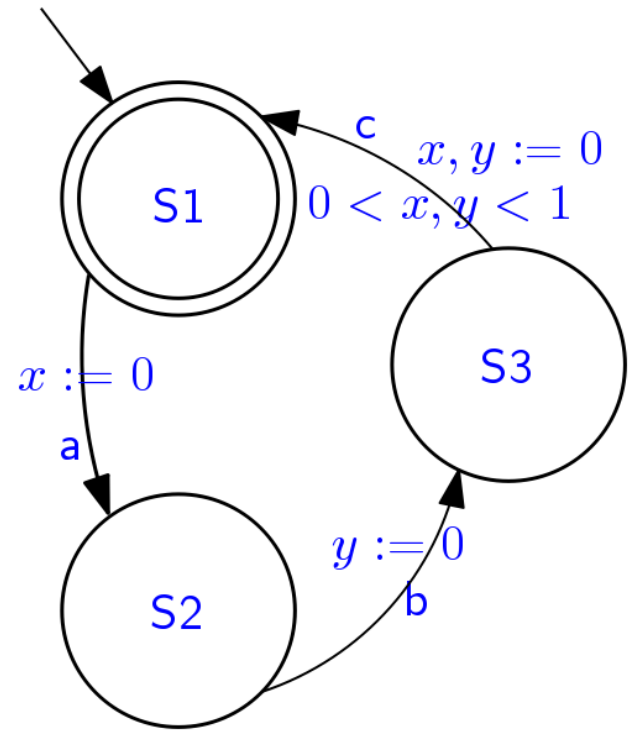


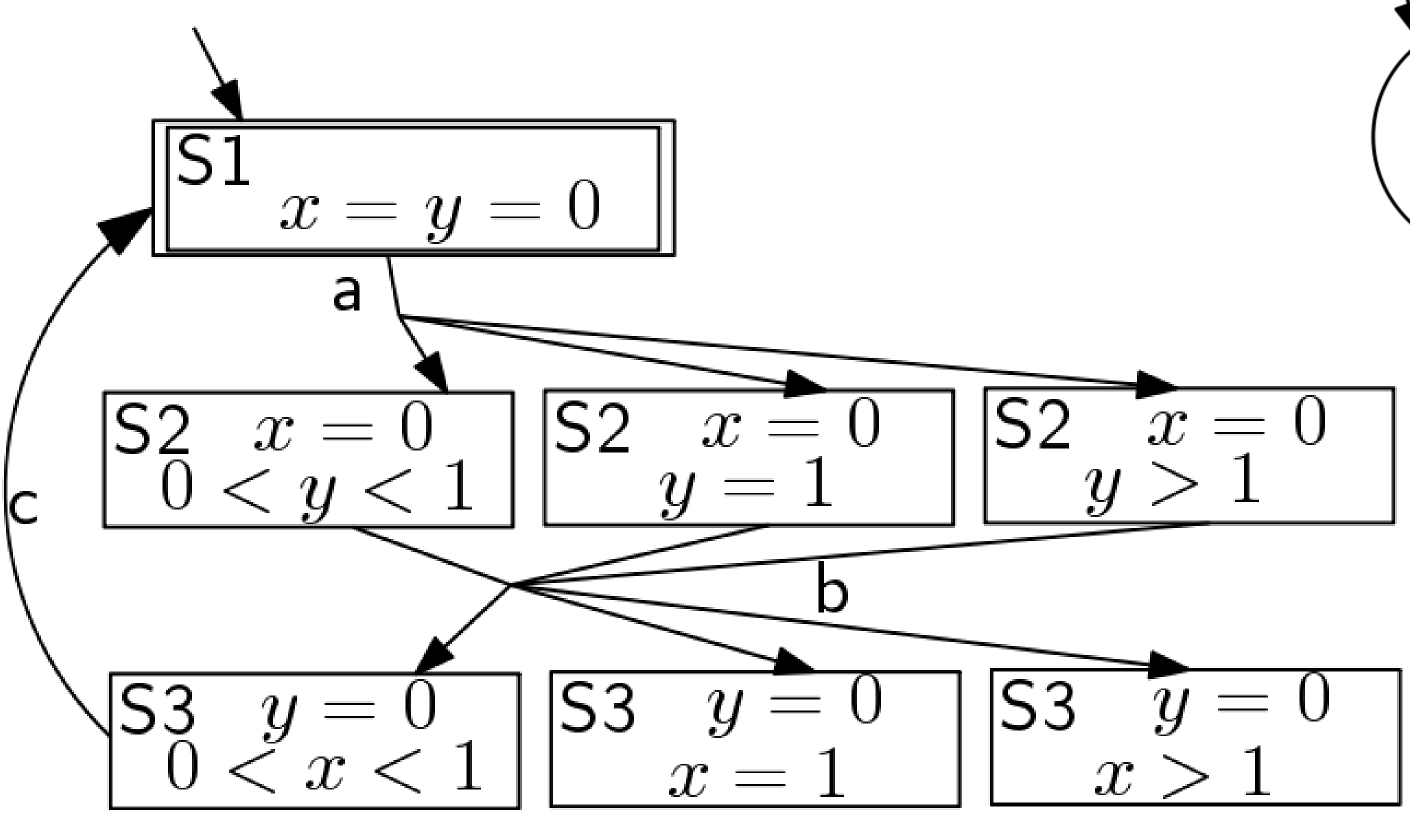


Build the region automaton for:

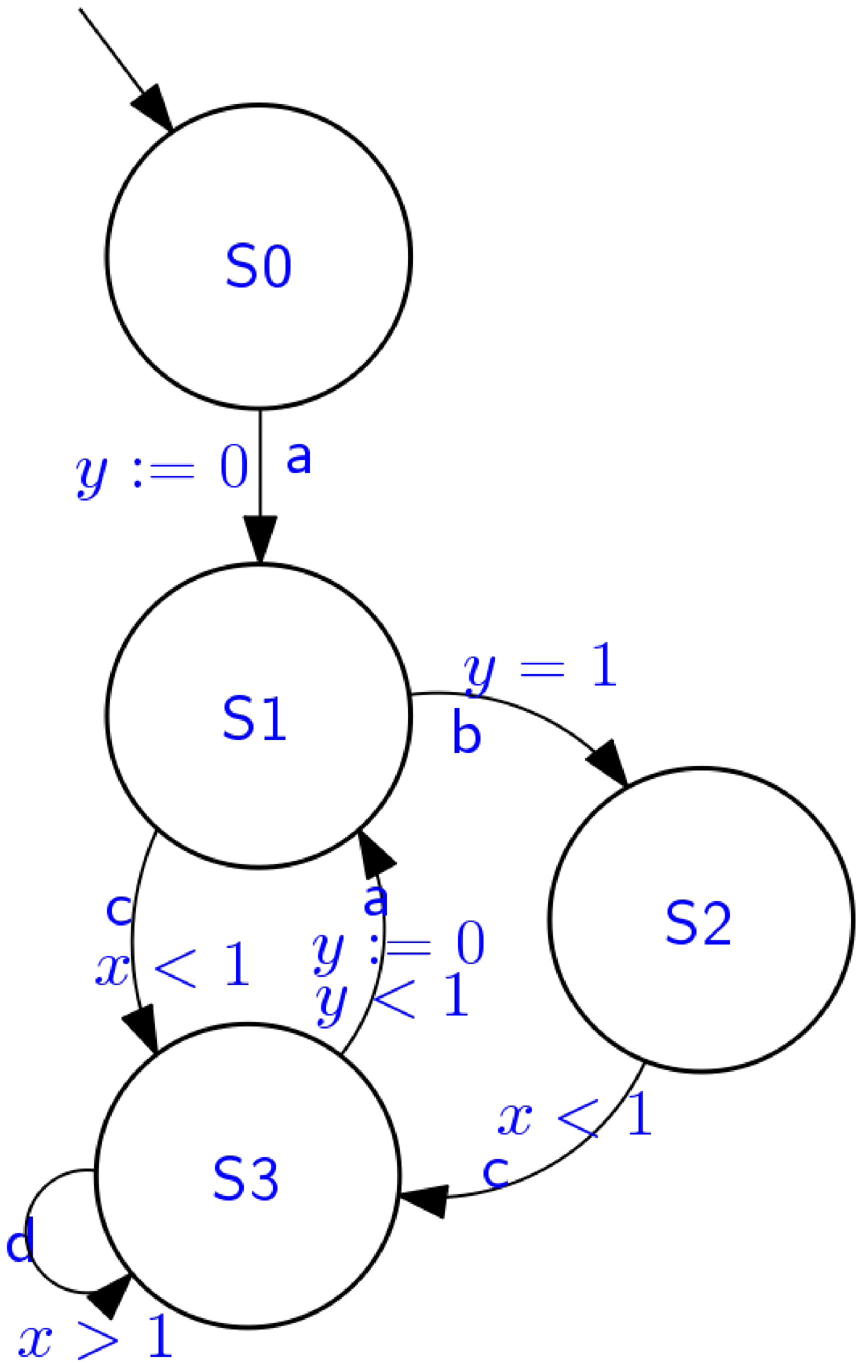


Build the region automaton for:



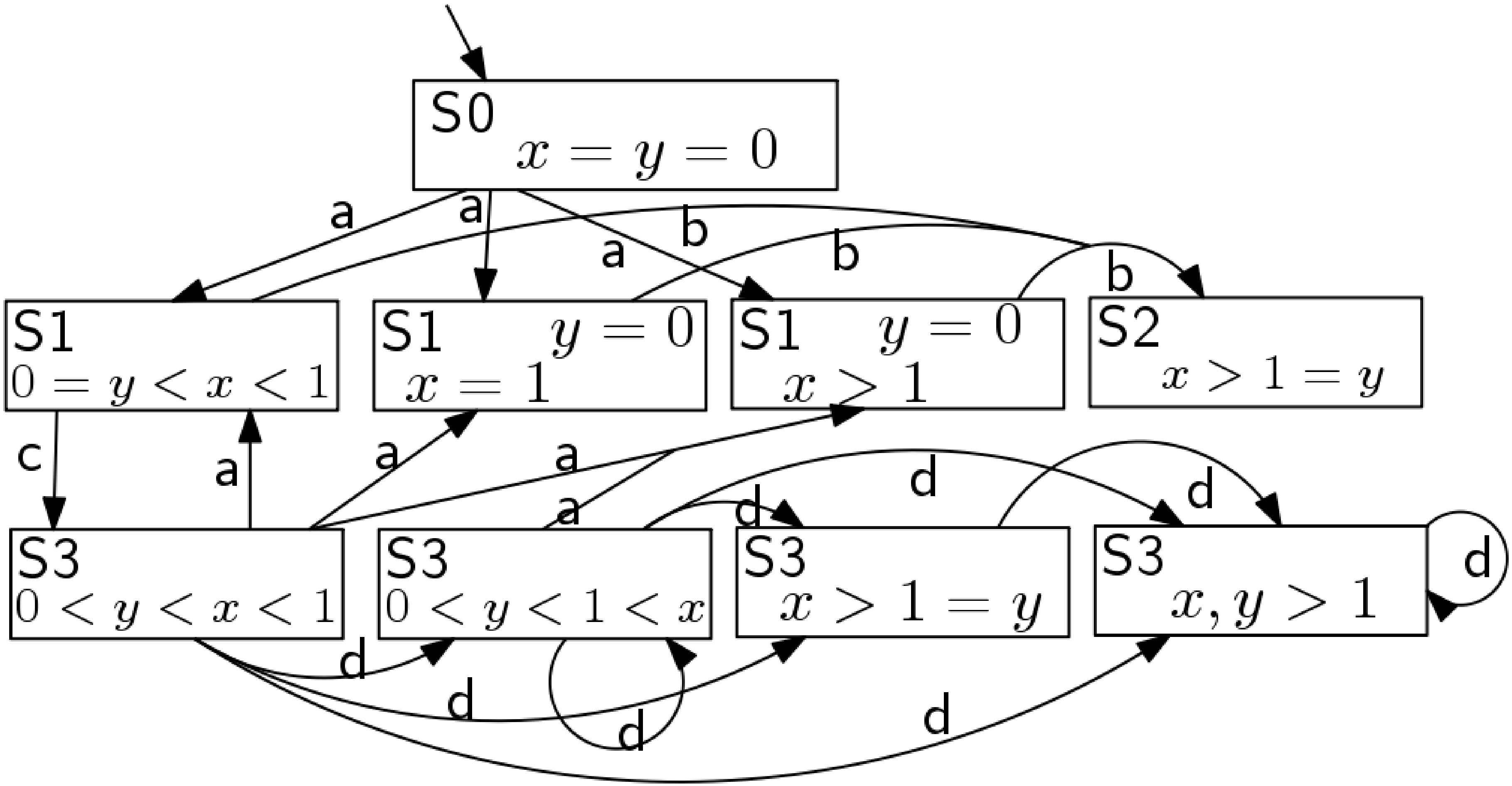


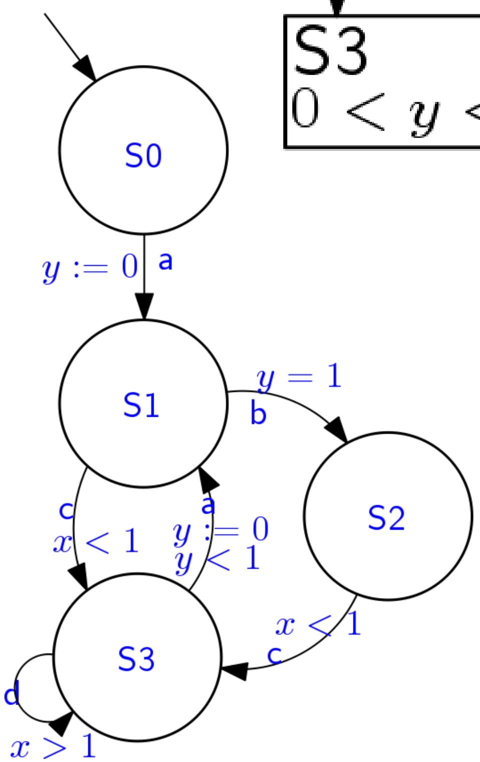
Build the region automaton for:



Example from: Alur & Dill, 1994

Build the region automaton for:





Example from: Alur & Dill, 1994

Exercises:
Semantics of derived operators

MTL derived operators: always

Prove that the satisfaction relation

$$w, i \models [\,]\langle a,b\rangle\ F$$

for bounded always, defined as:

$$[\,]\langle a,b\rangle\ F \ \triangleq \neg\,(\mathrm{True}\ U\langle a,b\rangle\ \neg F)$$

is equivalent to:

for all $i \leq j \leq n$ such that $t(j) - t(i) \in \langle a,b\rangle$ it is: $w, j \models F$

MTL derived operators: always

$w, i \models [\,]\langle a,b\rangle\, F$

iff

$w, i \models \neg\,(True\ U\langle a,b\rangle\ \neg F)$ (definition of bounded always)

iff

it is not the case that:

for some $i \leq j \leq n$ such that $t(j) - t(i) \in \langle a,b\rangle$ it is: $w, j \models \neg F$

and for all $i \leq k < j$ it is $w, k \models True$

(definition of bounded until)

iff

for all $i \leq j \leq n$ such that $t(j) - t(i) \in \langle a,b\rangle$ it is: not $w, j \models \neg F$

or for all $i \leq k < j$ it is $w, k \models False$

(push negation inward)

iff

for all $i \leq j \leq n$ such that $t(j) - t(i) \in \langle a,b\rangle$ it is: not $w, j \models \neg F$

(dropping false term in disjunction)

iff

for all $i \leq j \leq n$ such that $t(j) - t(i) \in \langle a,b\rangle$ it is: $w, j \models F$

(simplification of double negation)

MTL derived operators: X and X-

Compare the semantics of:

$$X+\ F \triangleq True\ U_{=1}\ F$$

with the semantics of:

$$X-\ F \triangleq F\ U_{>0}\ True$$

Semantic of X+

$w, i \models X+ F$

iff

$w, i \models True\ U{=}1\ F$ (definition of X+)

iff

for some $i \le j \le n$ such that $t(j) - t(i) = 1$ it is: $w, j \models F$

and for all $i \le k < j$ it is $w, k \models True$

(definition of bounded until)

iff

for some $i \le j \le n$ such that $t(j) = t(i) + 1$ it is: $w, j \models F$

(simplify term)

Semantic of X-

w, i ⊨ X- F

iff

w, i ⊨ F U>0 True (definition of X-)

iff

for some i ≤ j ≤ n such that t(j) – t(i) > 0 it is: w, j ⊨ True
and for all i ≤ k < j it is w, k ⊨ F

(definition of bounded until)

iff

for some i < j ≤ n it is: w, j ⊨ True and for all i ≤ k < j it is w, k ⊨ F
(timestamps are strictly increasing by assumption)

iff

i < n and w, i ⊨ F
(take j = i+1 so that [i, j) = [i,i])

Exercises:
Equivalence of MTL formulas

Comparison of formulas

Is formula:

[] <>>0 True

satisfied by any timed word?

Is formula satisfied?

Semantics of: $w \models [\,] <>>0$ True

for all positions $1 \leq i \leq n$: $w,i \models <>>0$ True

Semantics of: $w,i \models <>>0$ True

for some $j > i$ it is: $w,j \models$ True

i.e.: $i < n$

Hence: $w \models [\,] <>>0$ True

holds only for the empty word!

Comparison of formulas

Is formula:

$[\,]\, \langle\rangle_{\geq 0}$ True

satisfied by any (non-empty) timed word?

Is formula satisfied?

Semantics of: w ⊨ [] <>≥0 True

for all positions 1 ≤ i ≤ n: w,i ⊨ <>≥0 True

Semantics of: w,i ⊨ <>≥0 True

for some j ≥ i it is: w,j ⊨ True

i.e.: True

because one can always take j = i

Hence: w ⊨ [] <>≥0 True

holds for any word.

Comparison of formulas

Is formula:

<>[a,b] <>[c,d] q

equivalent or non-equivalent to:

<>[a+c,b+d] q

Inequivalent formulas

Informal meaning of: <>[a,b] <>[c,d] q

- let i be the current position
- there exist a future position j > i in the word with time in [a,b] relative to i such that:
- there exist another future position k > j in the word with time in [c,d] relative to j, where q holds
- in all, the time at which q holds is in [a+c, b+d] relative to i

Informal meaning of: <>[a+c,b+d] q

- let i be the current position
- there exist another future position k > i in the word with time in [a+c,b+d] relative to i, where q holds

Hence, for instance: timed word w = ({}, 3) ({q}, 3+b+c)

is such that: w satisfies <>[a+c,b+d] q but it does not satisfy <>[a,b] <>[c,d] q because there is no intermediate position between the first and the one where q holds