Abstract Interpretation with Infinitesimals

Kengo Kido[1] Swarat Chaudhuri[2] Ichiro Hasuo[1]

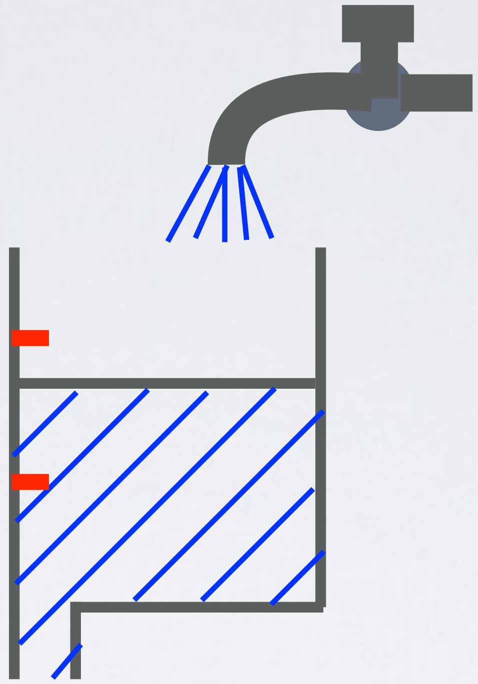
The University of Tokyo[1] Rice University[2]

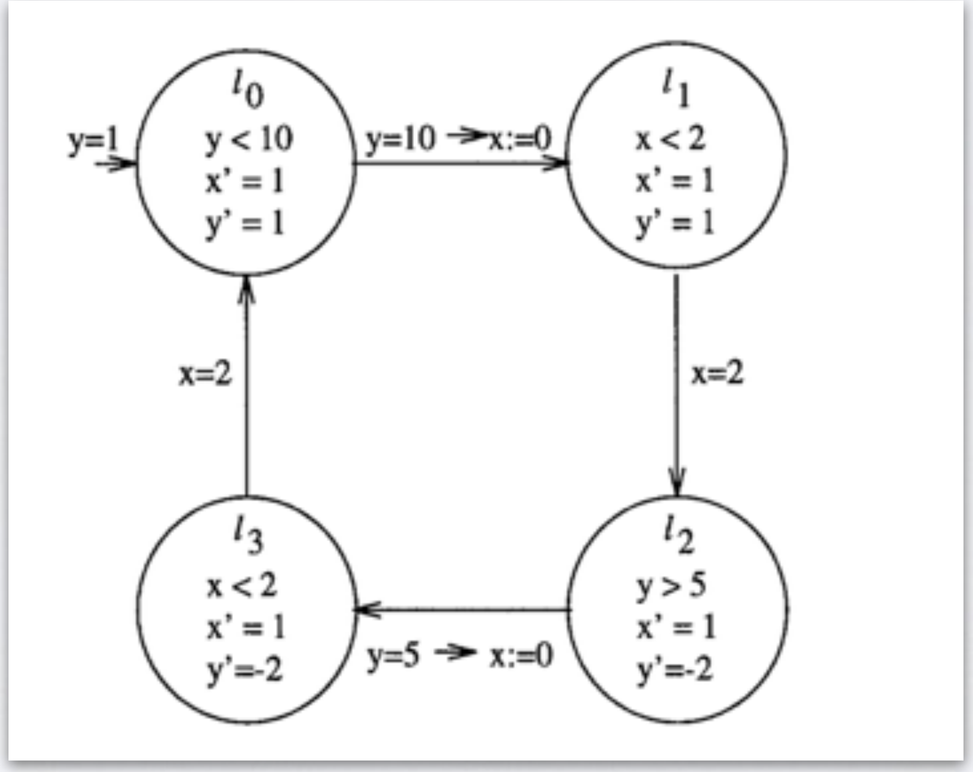
SNR2015 19 July 2015

- Example of analysis
- Semantics of WHILE^{dt}
- (Standard) abstract interpretation
- Abstract interpretation with infinitesimals

Example: Water-level Monitor

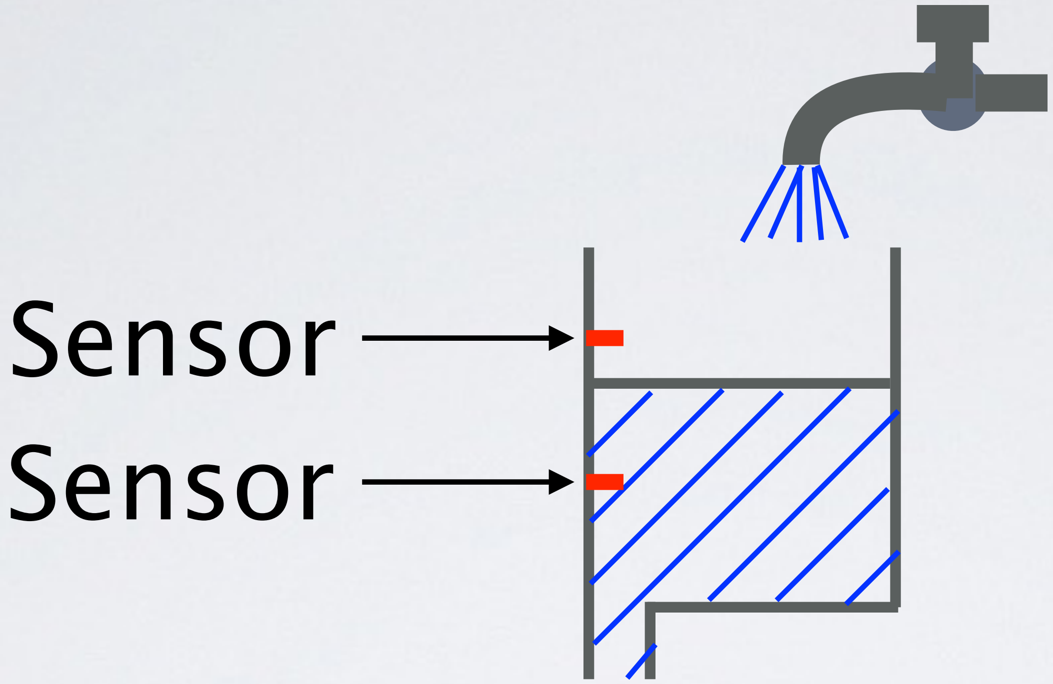
[Alur et al. TCS 95]





Example: Water-level Monitor

[Alur et al. TCS 95]



$t := 0; l := 0; x := 1; p := 1; s := 0;$
while $t < t_{max}$ **do**
 $t := t +$ <u>dt</u>;
 if $p = 1$ **then** $x := x +$ <u>dt</u>; **else** $x := x - 2$<u>dt</u>;
 if $(x \leq 5 \land p = 0) \lor (x \geq 10 \land p = 1)$ **then** $s := 1$ **else** $s := 0;$
 if $s = 1$ **then** $l := l +$ <u>dt</u>;
 if $s = 1 \land l \geq 2$ **then** $p := 1 - p; s := 0; l := 0$

WHILE^{dt} [Suenaga & Hasuo ICALP 11]

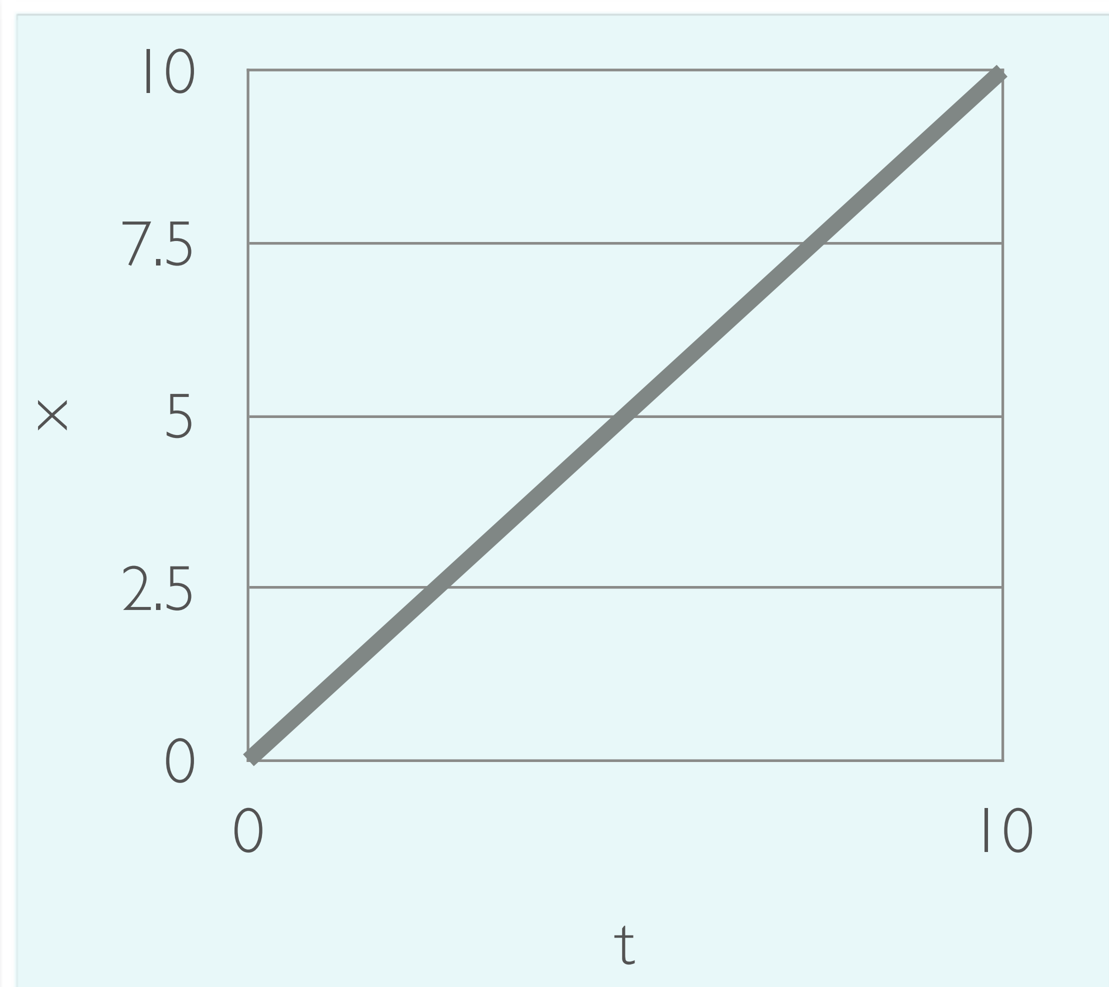
$$\mathbf{AExp} \ni a ::= x \mid r \mid a_1\ \mathtt{aop}\ a_2 \mid \mathtt{dt} \mid \infty$$

$$\text{where } x \in \mathbf{Var}, r \in \mathbb{R} \text{ and } \mathtt{aop} \in \{+, -, \cdot, \wedge\}$$

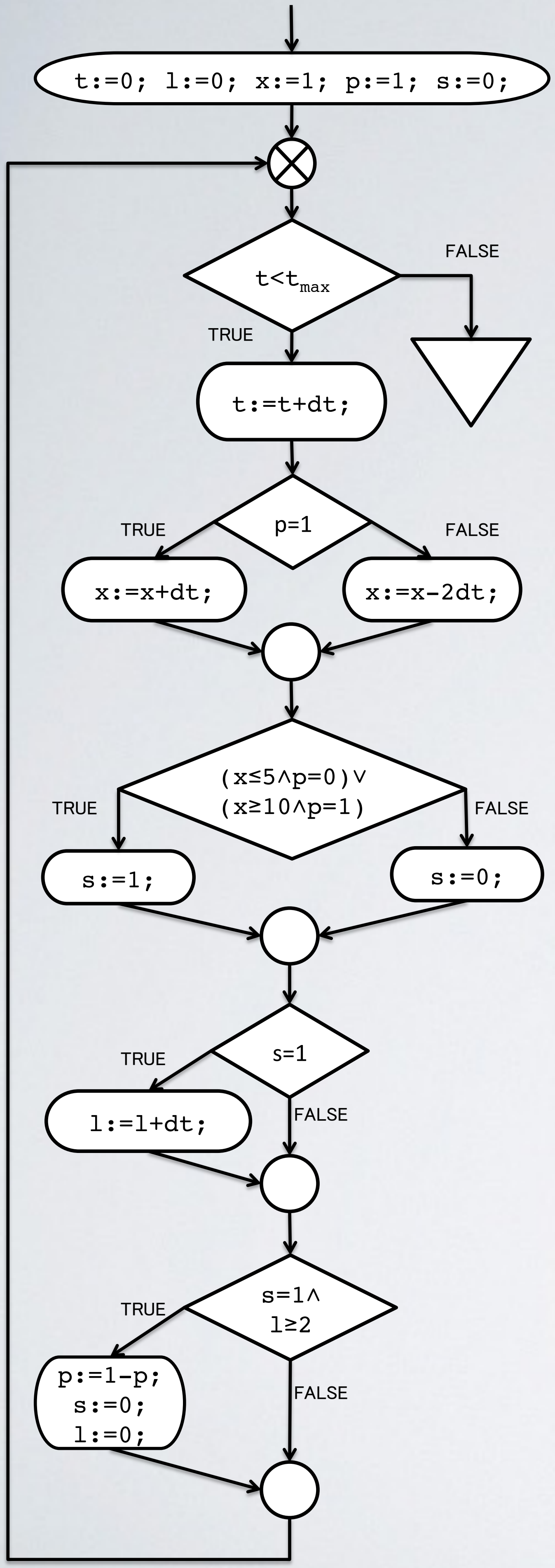
$$\mathbf{BExp} \ni b ::= \mathtt{true} \mid \mathtt{false} \mid b_1 \wedge b_2 \mid \neg b \mid a_1 < a_2$$

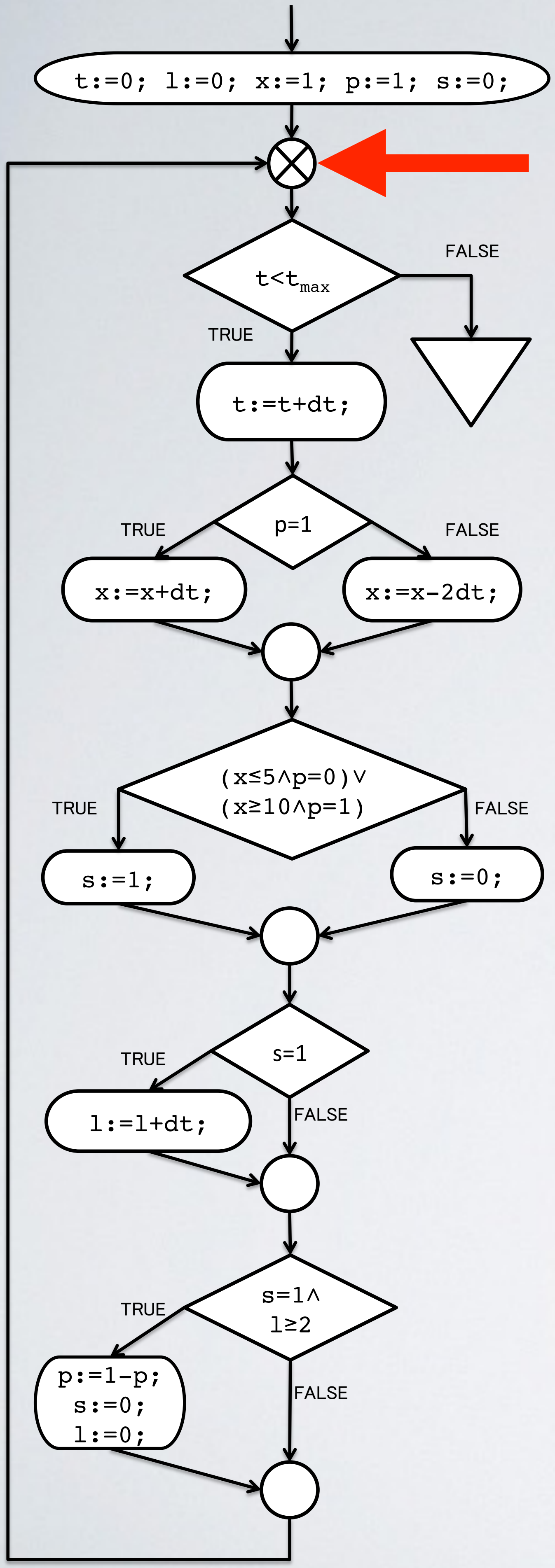
$$\mathbf{Cmd} \ni c ::= \mathtt{skip} \mid x := a \mid c_1; c_2 \mid \mathtt{if}\ b\ \mathtt{then}\ c_1\ \mathtt{else}\ c_2 \mid \mathtt{while}\ b\ \mathtt{do}\ c$$

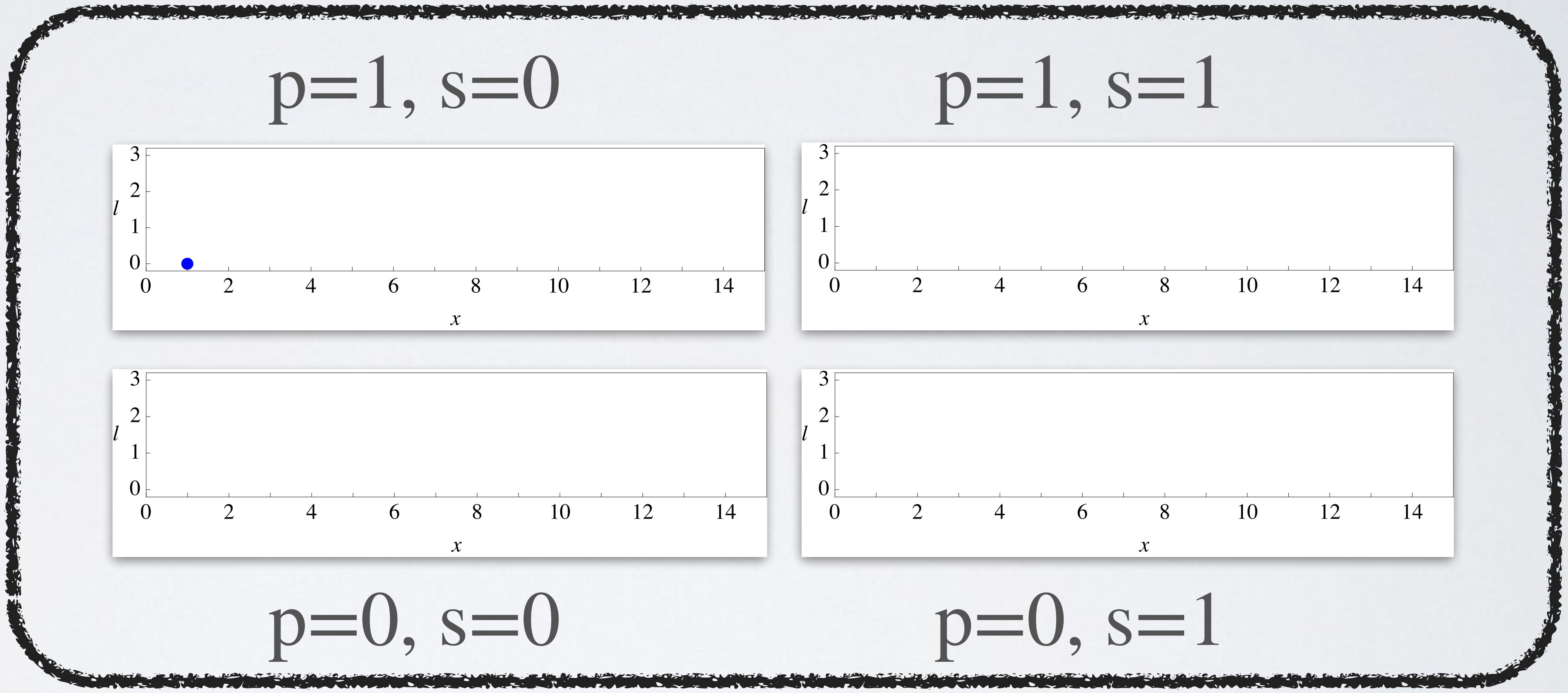
```
x := 0; t := 0;
while (x ≤ 10) {
  x := x + dt;
  t := t + dt
}
```

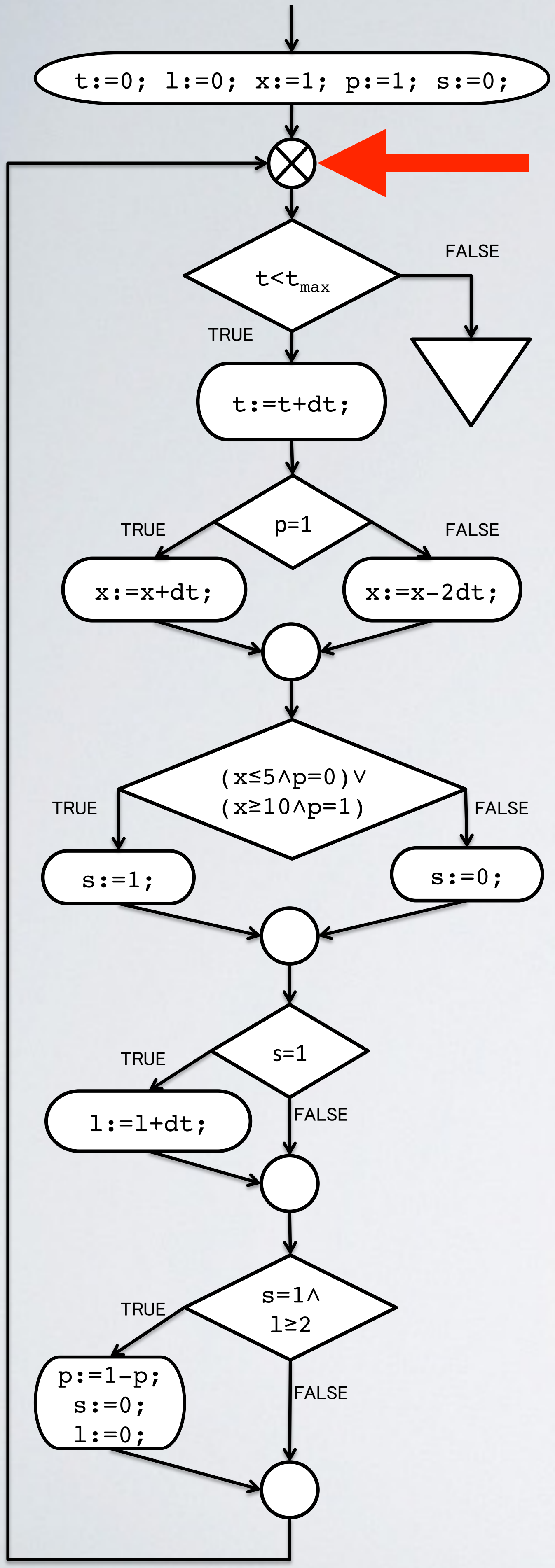


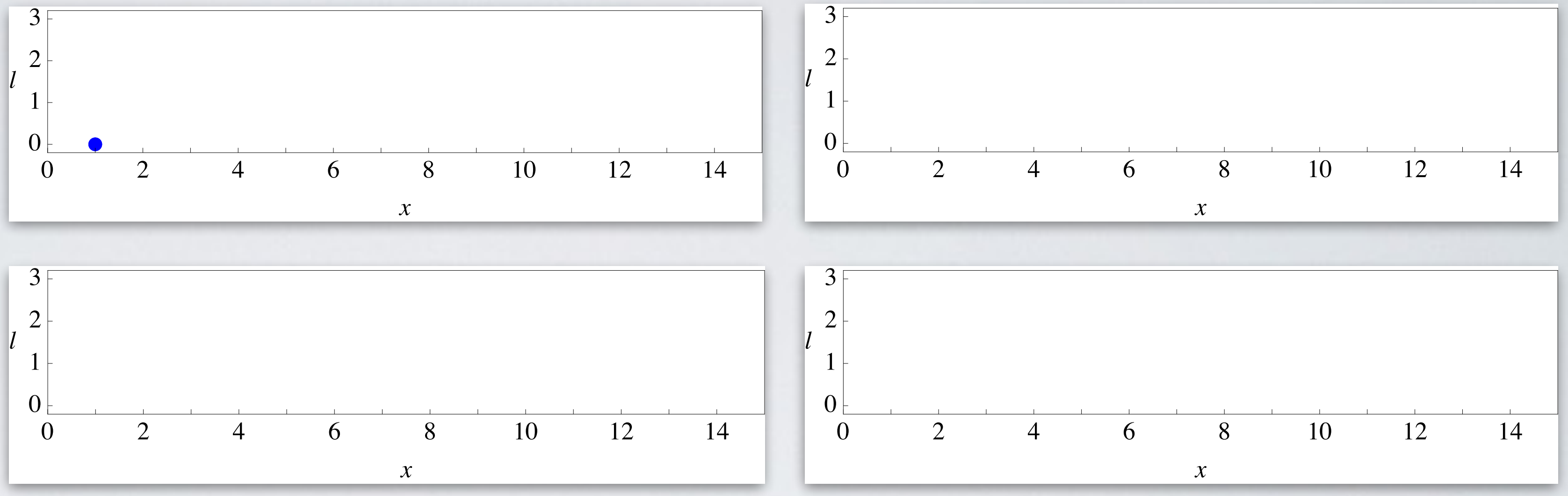
```
t := 0; l := 0; x := 1; p := 1; s := 0;
while t < t_max do
    t := t + dt;
    if p = 1 then x := x + dt; else x := x − 2dt;
    if (x ≤ 5 ∧ p = 0) ∨ (x ≥ 10 ∧ p = 1) then s := 1 else s := 0;
    if s = 1 then l := l + dt;
    if s = 1 ∧ l ≥ 2 then p := 1 − p; s := 0; l := 0
```


t:=0; l:=0; x:=1; p:=1; s:=0;
t<tmax
FALSE
TRUE
t:=t+dt;
p=1
TRUE
FALSE
x:=x+dt;
x:=x-2dt;
(x≤5∧p=0)∨
(x≥10∧p=1)
TRUE
FALSE
s:=1;
s:=0;
s=1
TRUE
FALSE
l:=l+dt;
s=1∧
l≥2
TRUE
FALSE
p:=1-p;
s:=0;
l:=0;

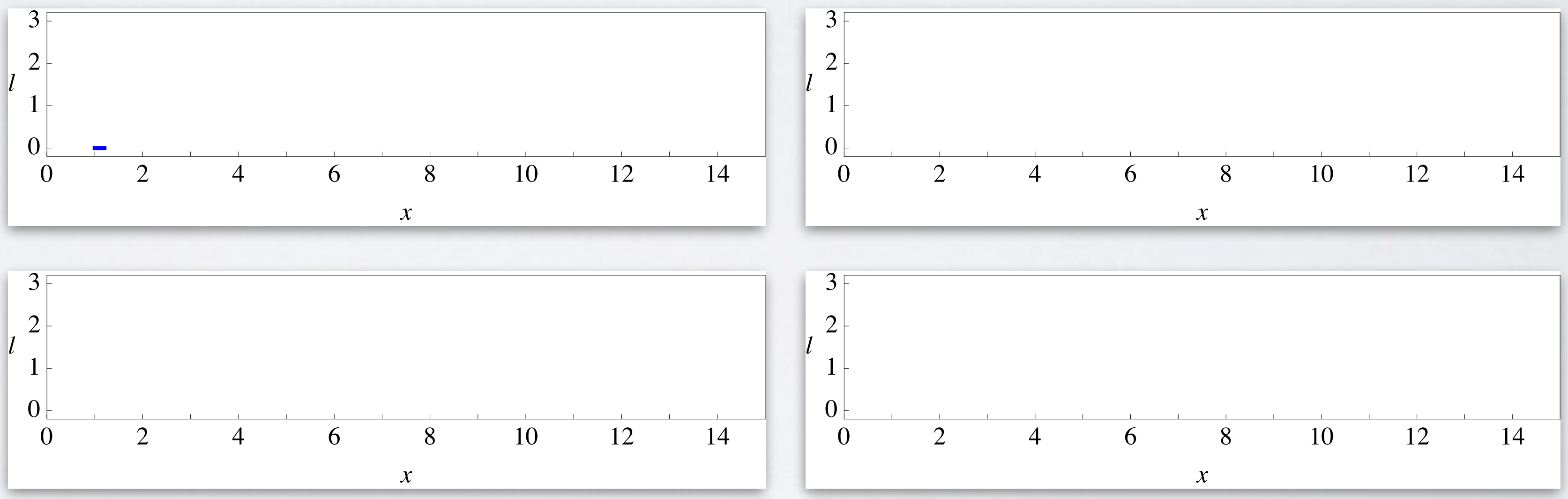

t:=0; l:=0; x:=1; p:=1; s:=0;
t<t_max
FALSE
TRUE
t:=t+dt;
p=1
TRUE
FALSE
x:=x+dt;
x:=x-2dt;
(x≤5∧p=0)∨
(x≥10∧p=1)
TRUE
FALSE
s:=1;
s:=0;
s=1
TRUE
FALSE
l:=l+dt;
s=1∧
l≥2
TRUE
FALSE
p:=1-p;
s:=0;
l:=0;


p=1, s=0
p=1, s=1
p=0, s=0
p=0, s=1
l
x

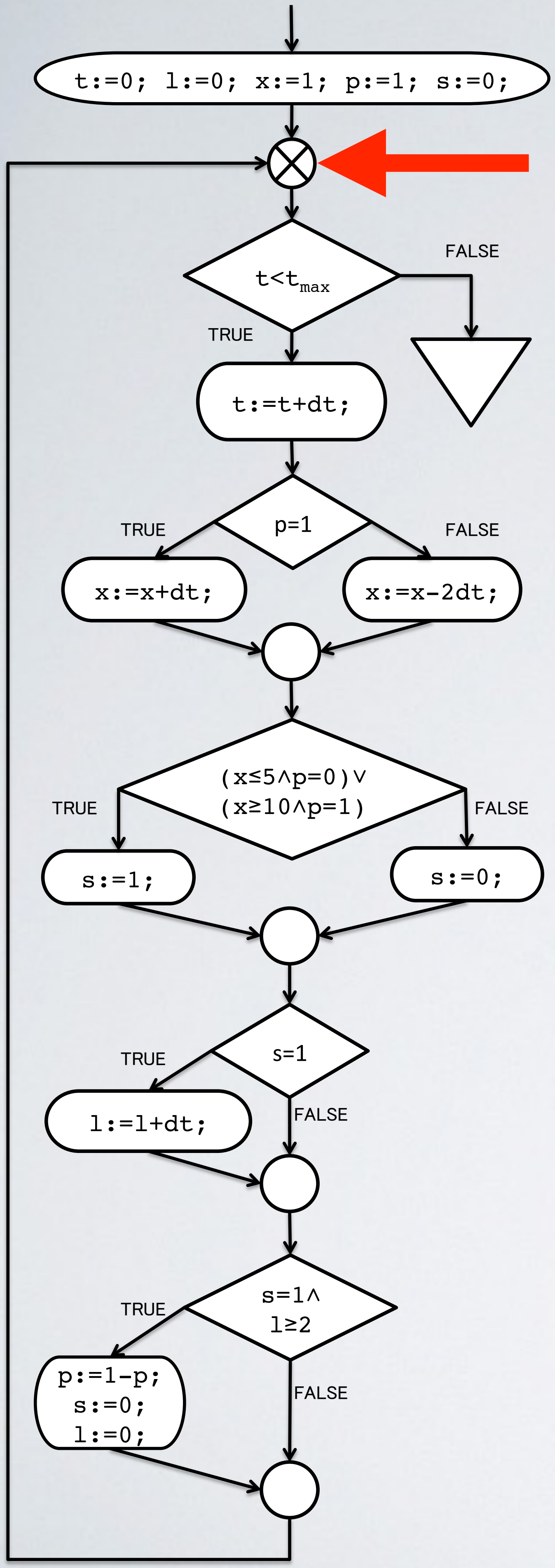


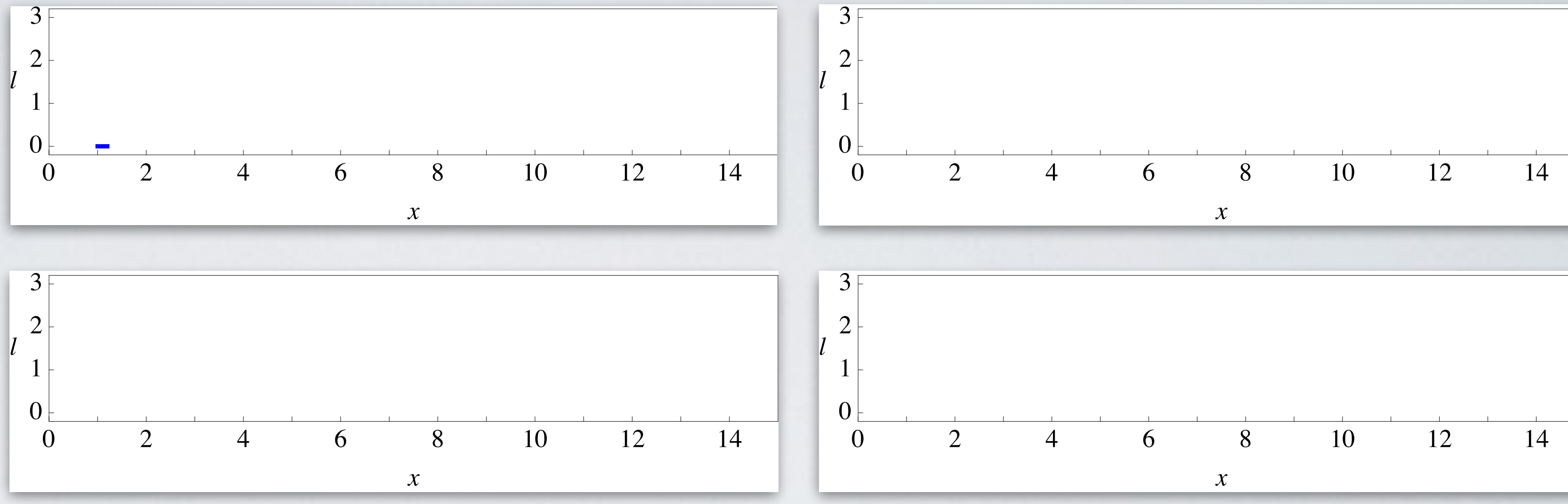


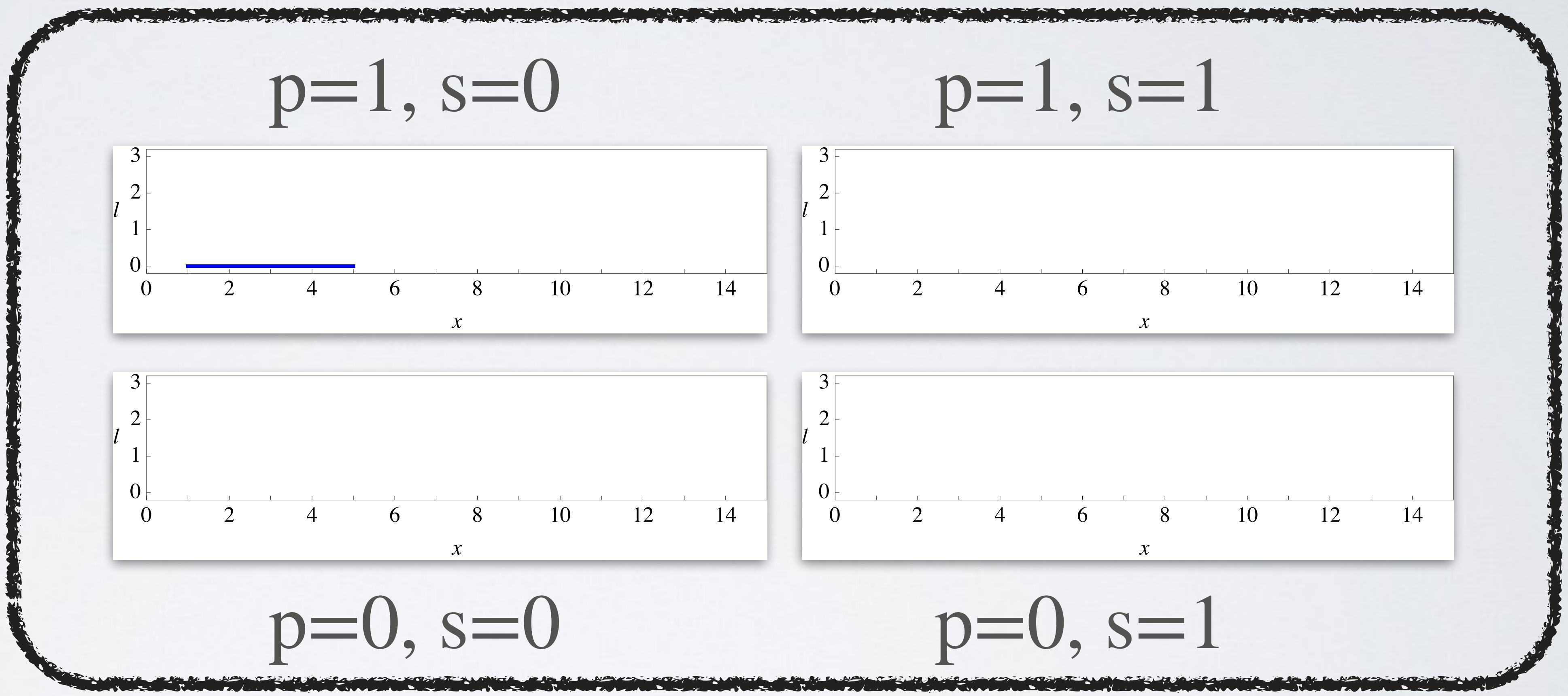
p=1, s=0 p=1, s=1

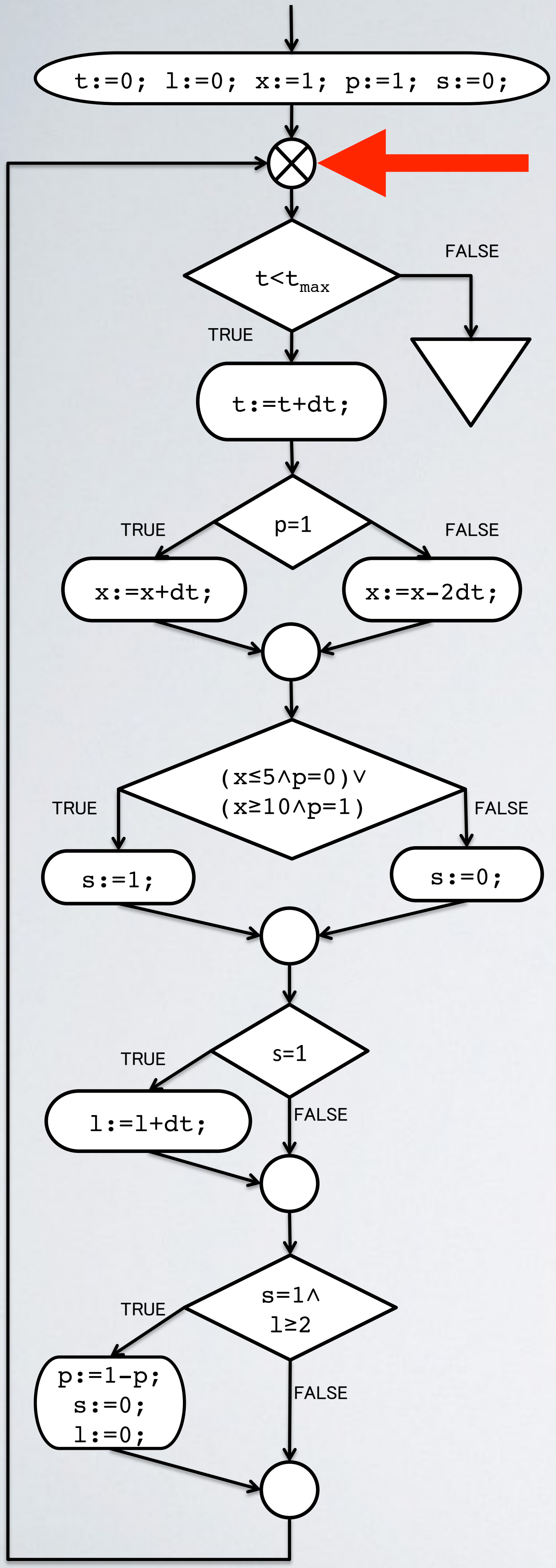


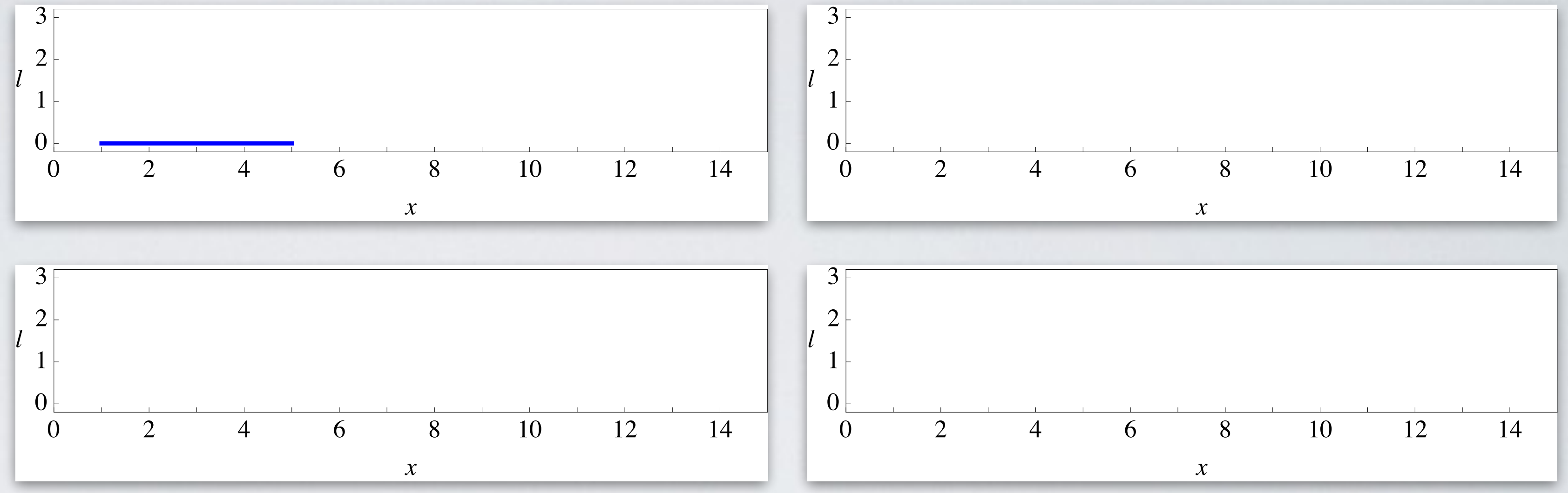
p=0, s=0 p=0, s=1


t:=0; l:=0; x:=1; p:=1; s:=0;
t<t_max
FALSE
TRUE
t:=t+dt;
p=1
TRUE
FALSE
x:=x+dt;
x:=x-2dt;
(x≤5∧p=0)∨
(x≥10∧p=1)
TRUE
FALSE
s:=1;
s:=0;
s=1
TRUE
FALSE
l:=l+dt;
s=1∧
l≥2
TRUE
FALSE
p:=1-p;
s:=0;
l:=0;



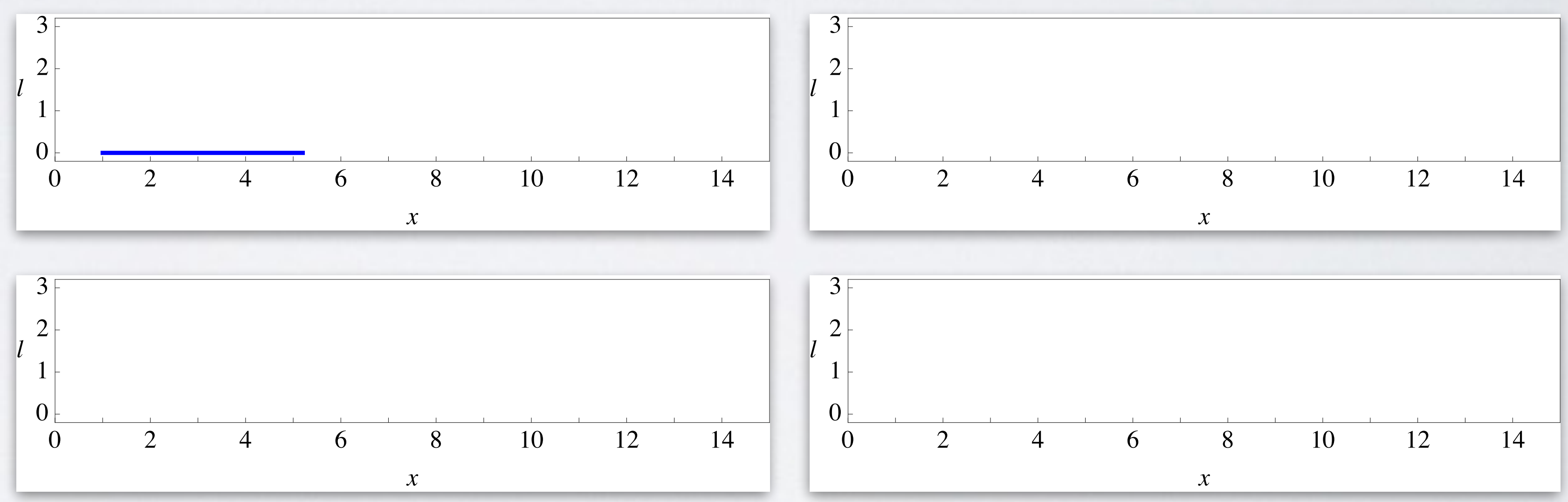

p=1, s=0
p=1, s=1
p=0, s=0
p=0, s=1





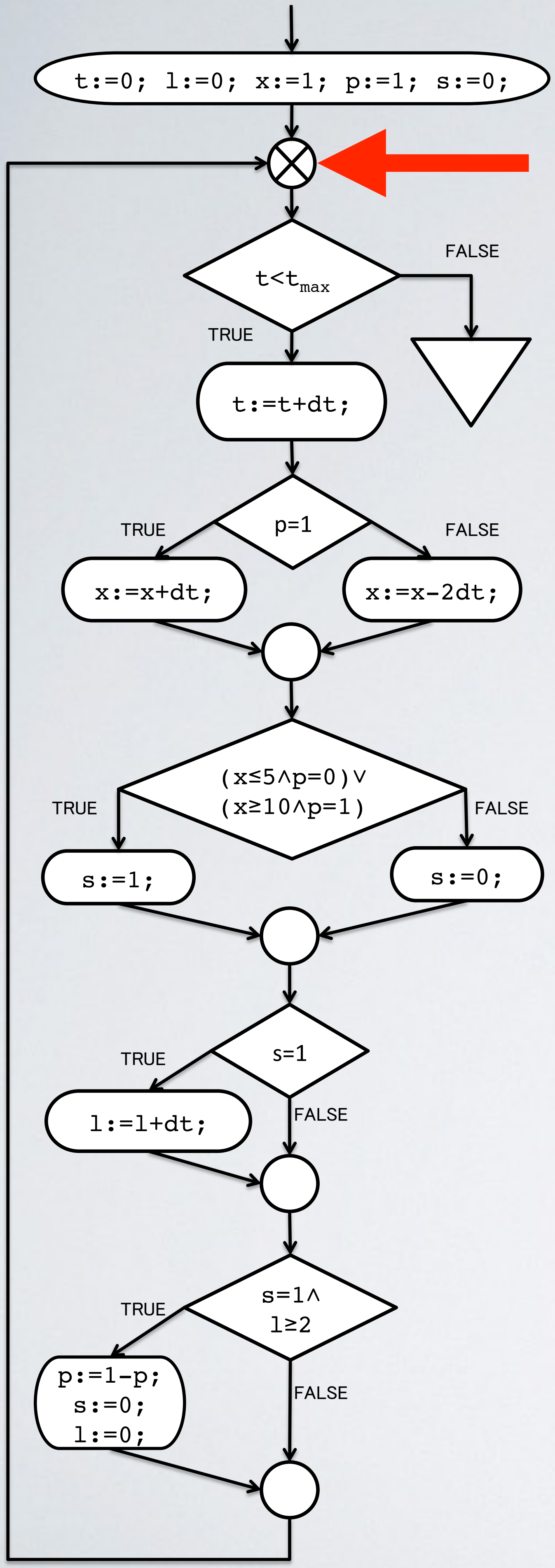
p=1, s=0

p=1, s=1

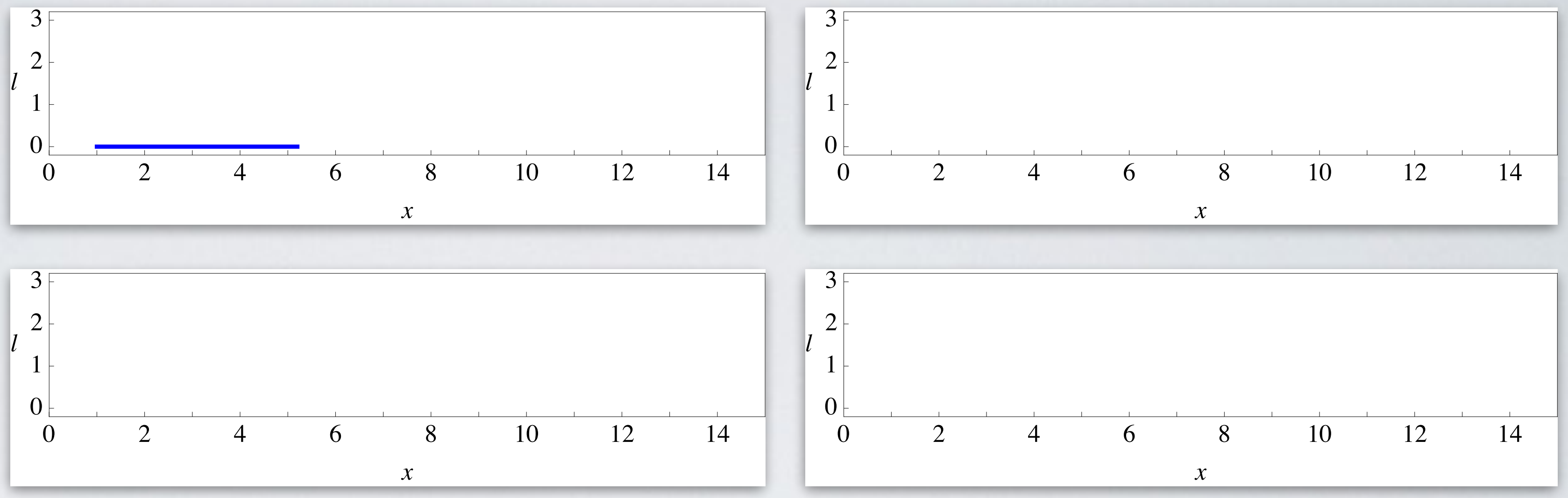


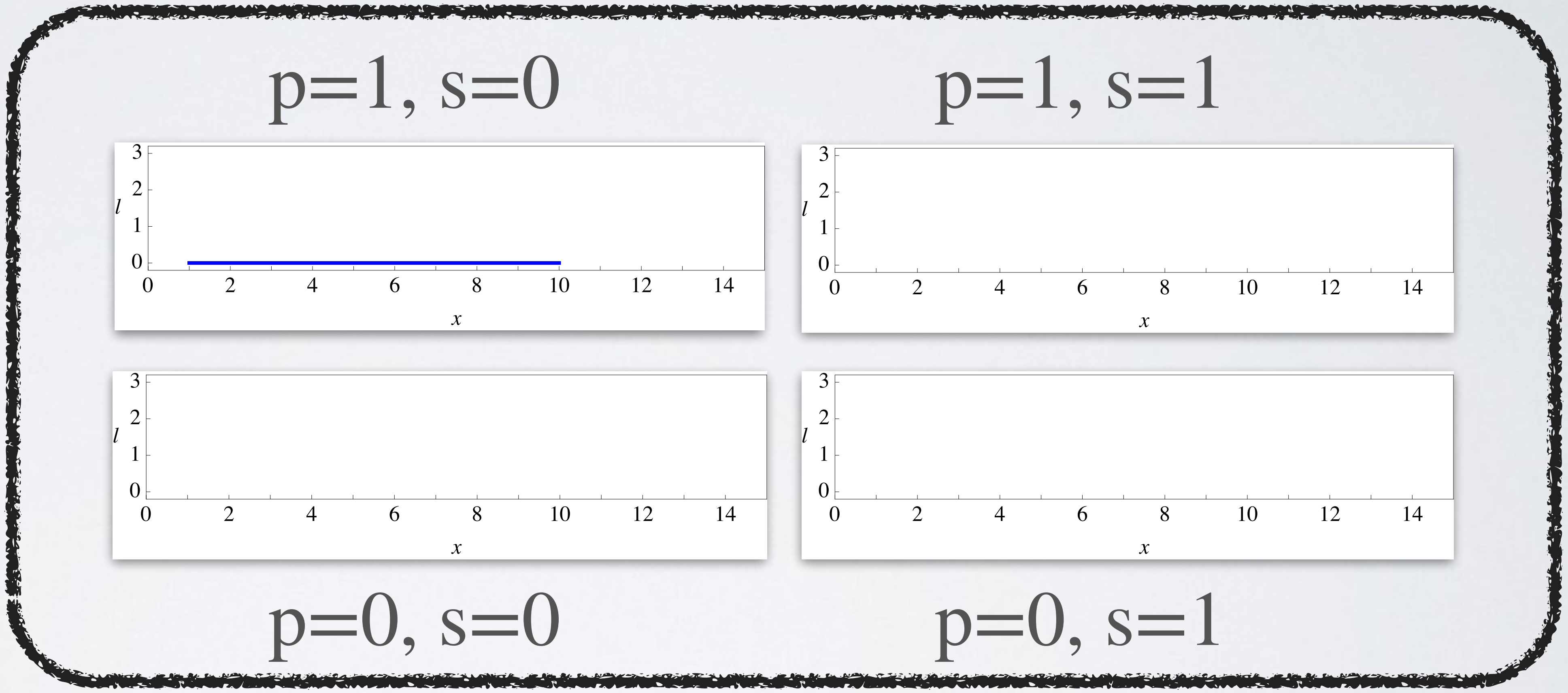
p=0, s=0

p=0, s=1

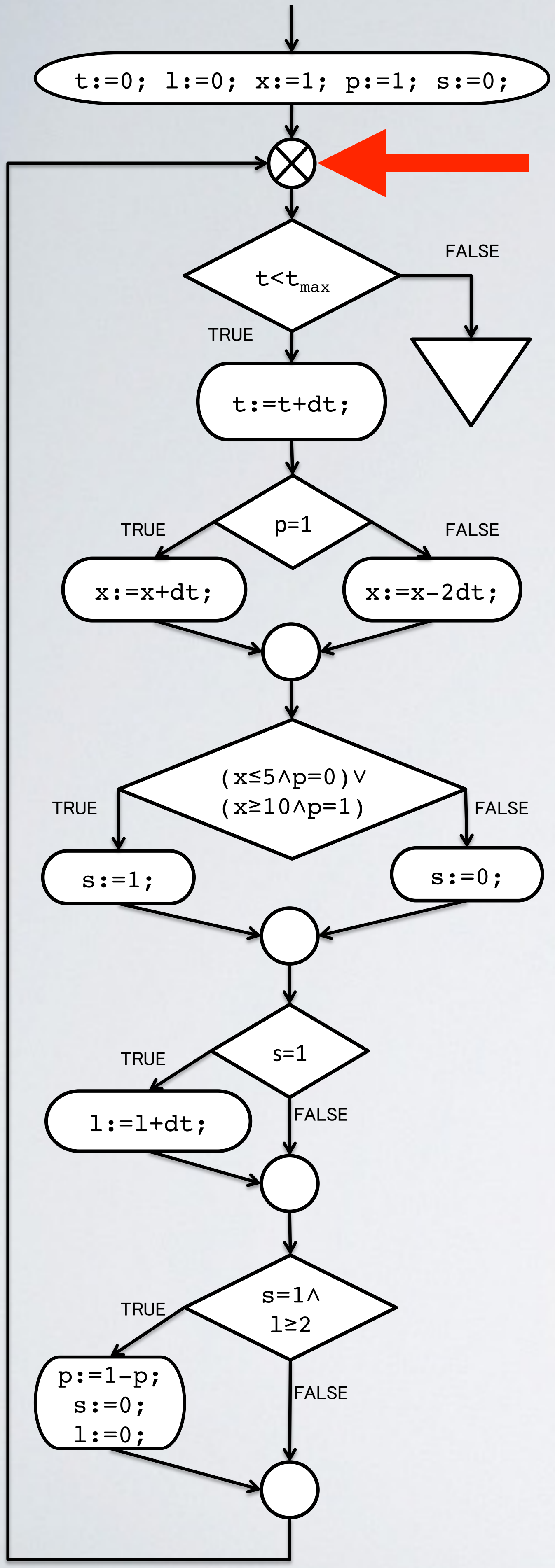


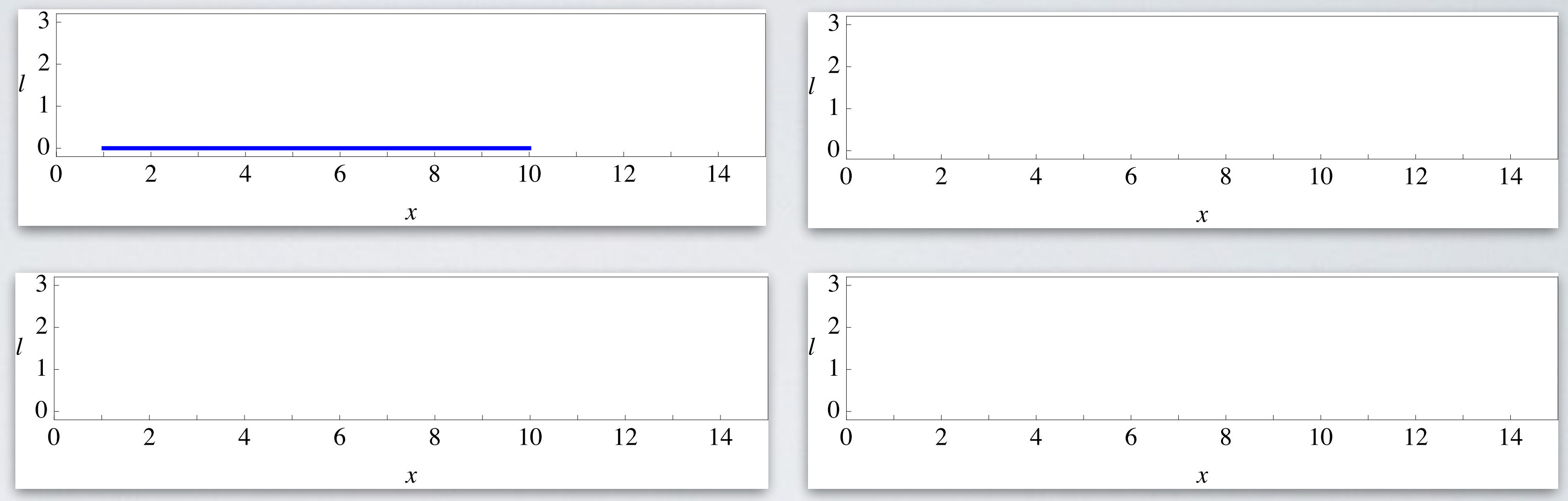
t:=0; l:=0; x:=1; p:=1; s:=0;
t<t_max
FALSE
TRUE
t:=t+dt;
p=1
TRUE
FALSE
x:=x+dt;
x:=x-2dt;
(x≤5∧p=0)∨
(x≥10∧p=1)
TRUE
FALSE
s:=1;
s:=0;
s=1
TRUE
FALSE
l:=l+dt;
s=1∧
l≥2
TRUE
FALSE
p:=1-p;
s:=0;
l:=0;

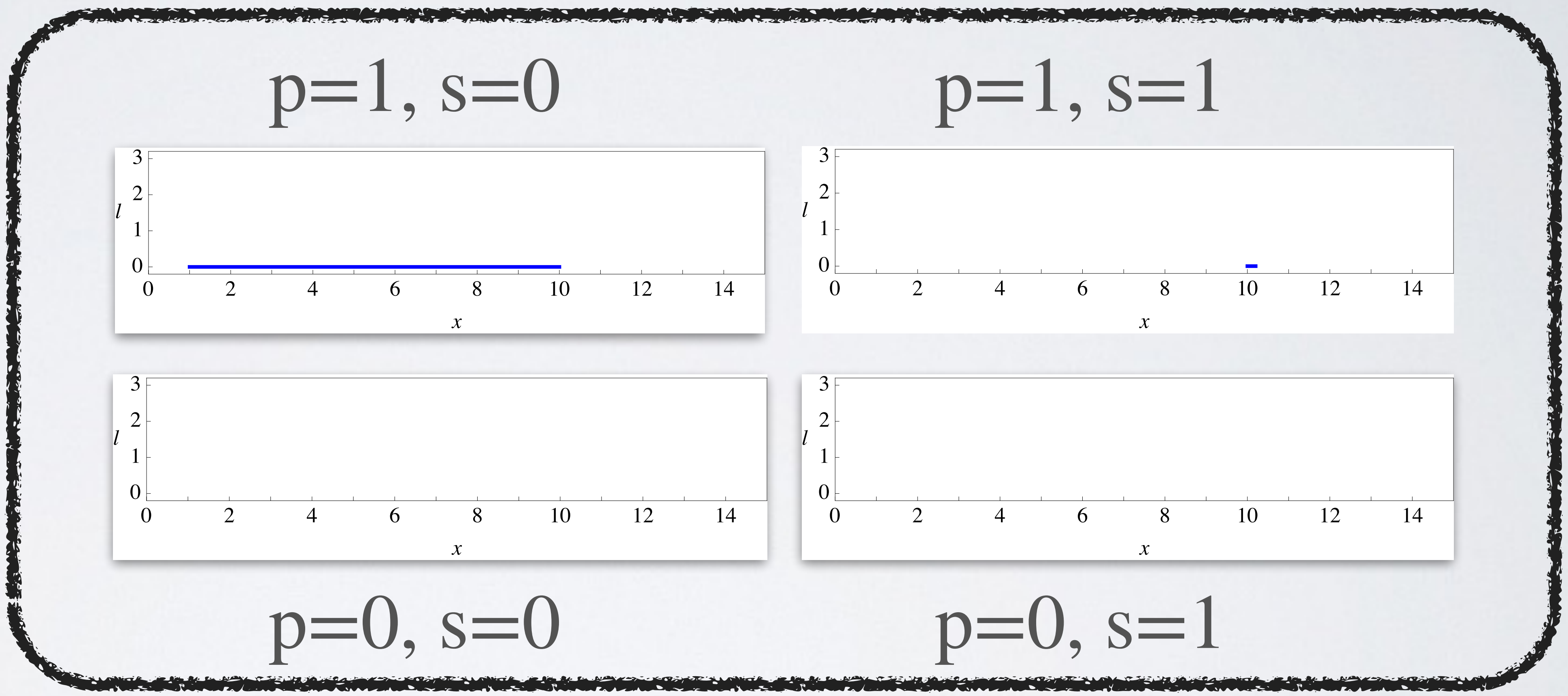


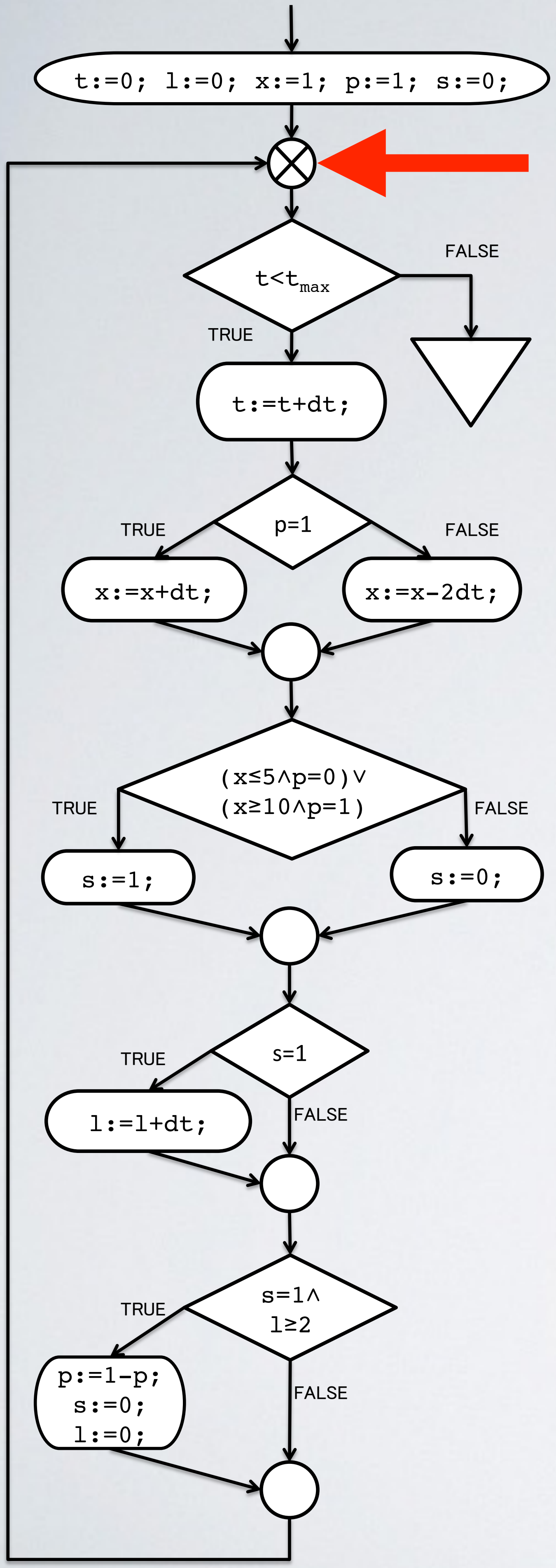


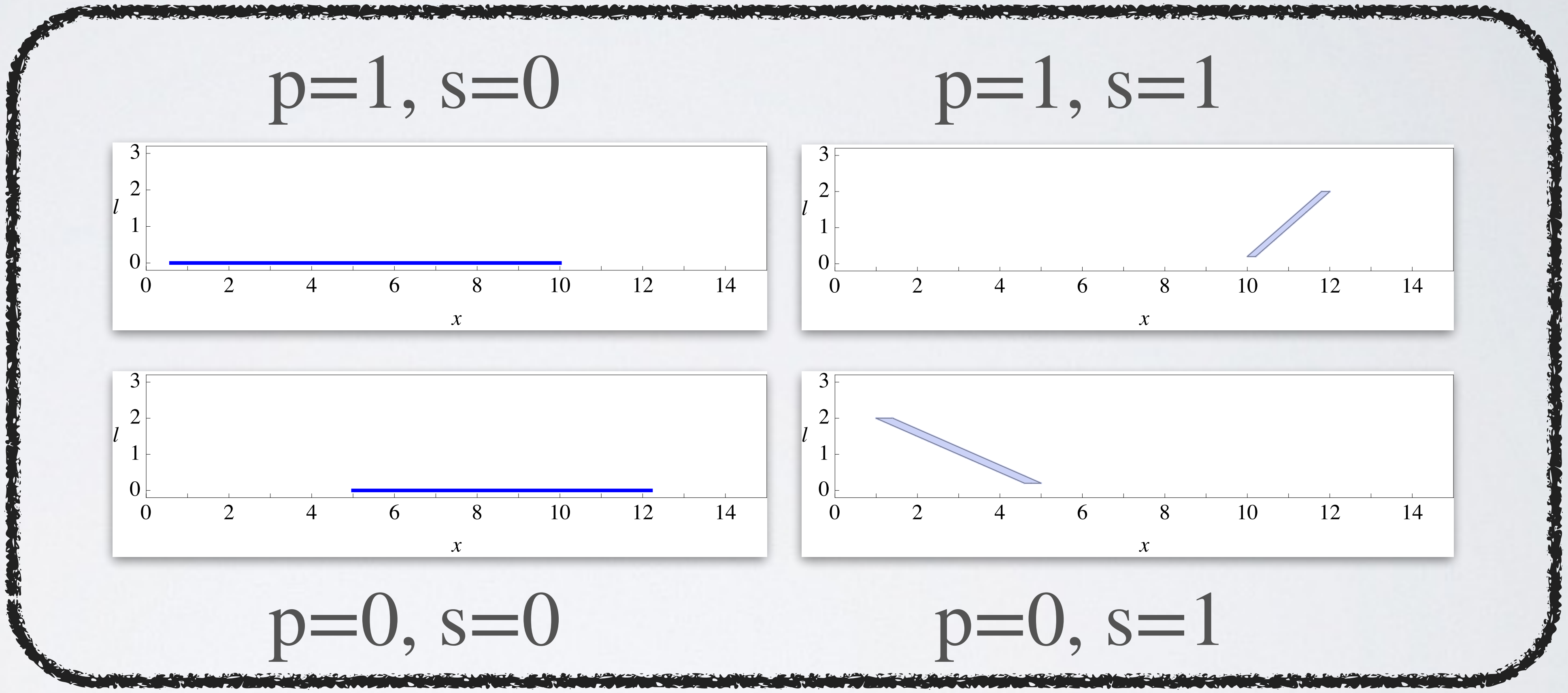
p=1, s=0
p=1, s=1
p=0, s=0
p=0, s=1

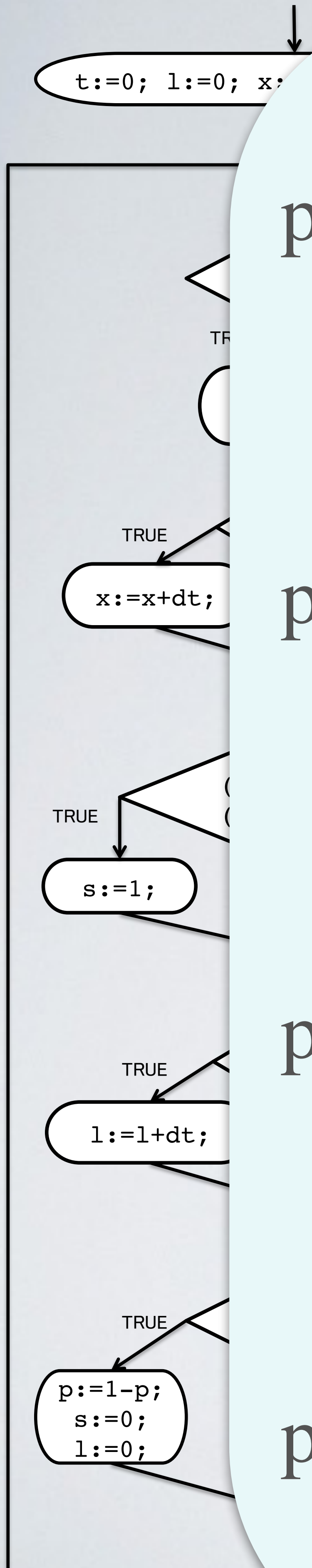

t:=0; l:=0; x:=1; p:=1; s:=0;
t<t_max
FALSE
TRUE
t:=t+dt;
p=1
TRUE
FALSE
x:=x+dt;
x:=x-2dt;
(x≤5∧p=0)∨
(x≥10∧p=1)
TRUE
FALSE
s:=1;
s:=0;
s=1
TRUE
FALSE
l:=l+dt;
s=1∧
l≥2
TRUE
FALSE
p:=1-p;
s:=0;
l:=0;


l
x

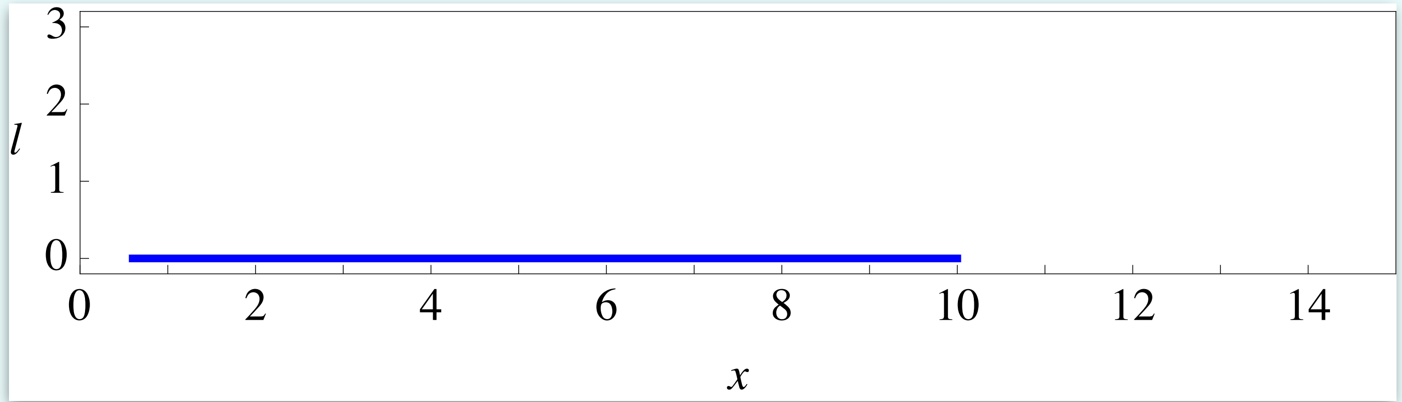

p=1, s=0
p=1, s=1
p=0, s=0
p=0, s=1
l
x


t:=0; l:=0; x:=1; p:=1; s:=0;
t<t_max
FALSE
TRUE
t:=t+dt;
p=1
TRUE
FALSE
x:=x+dt;
x:=x-2dt;
(x≤5∧p=0)∨
(x≥10∧p=1)
TRUE
FALSE
s:=1;
s:=0;
s=1
TRUE
FALSE
l:=l+dt;
s=1∧
l≥2
TRUE
FALSE
p:=1-p;
s:=0;
l:=0;

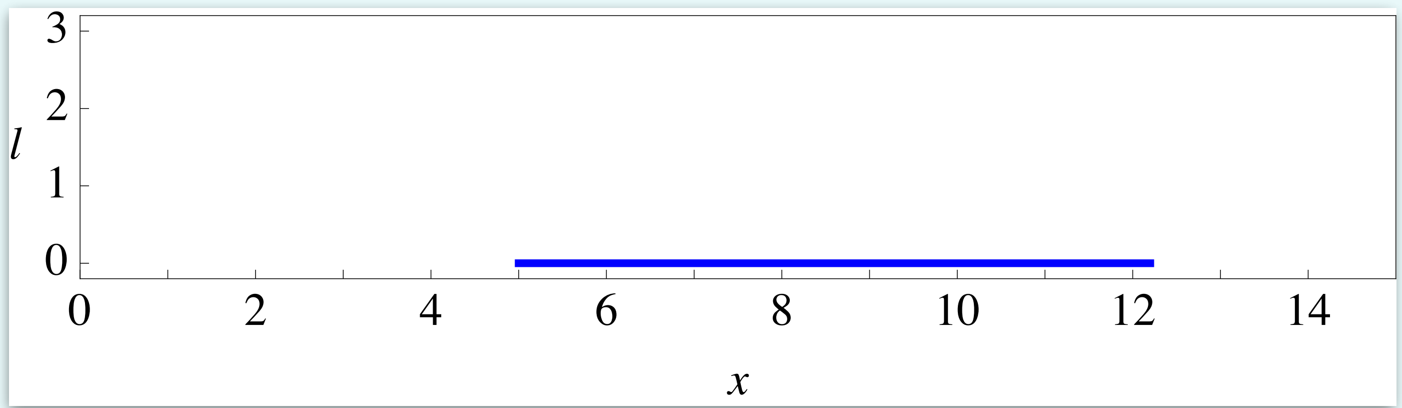

p=1, s=0
p=1, s=1
p=0, s=0
p=0, s=1
l
x



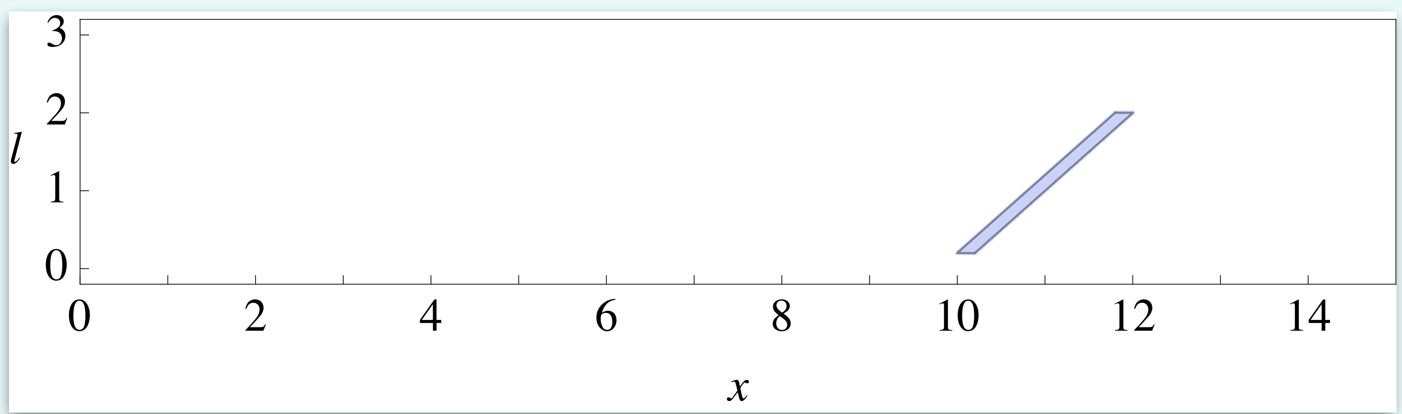
p=1, s=0



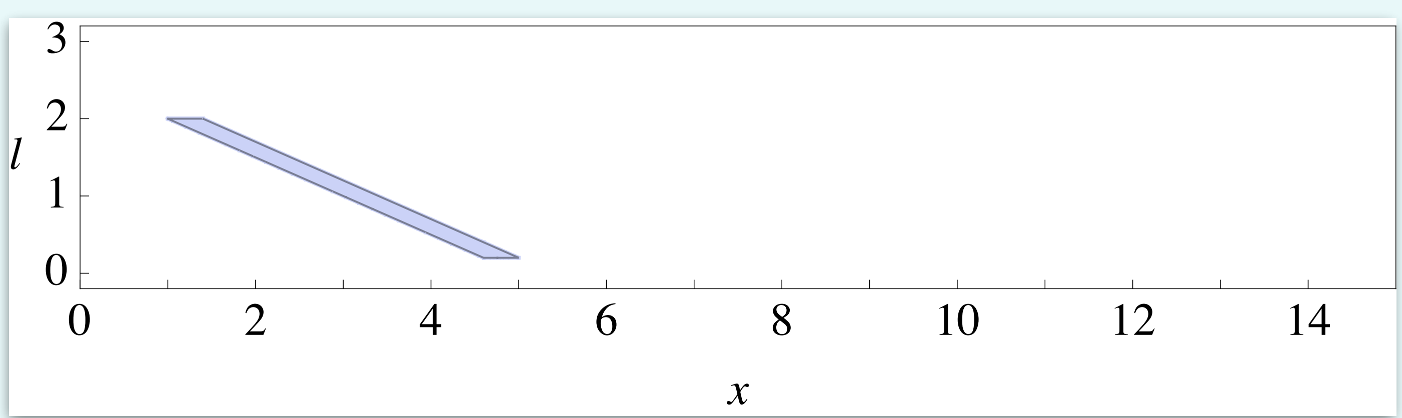
p=0, s=0

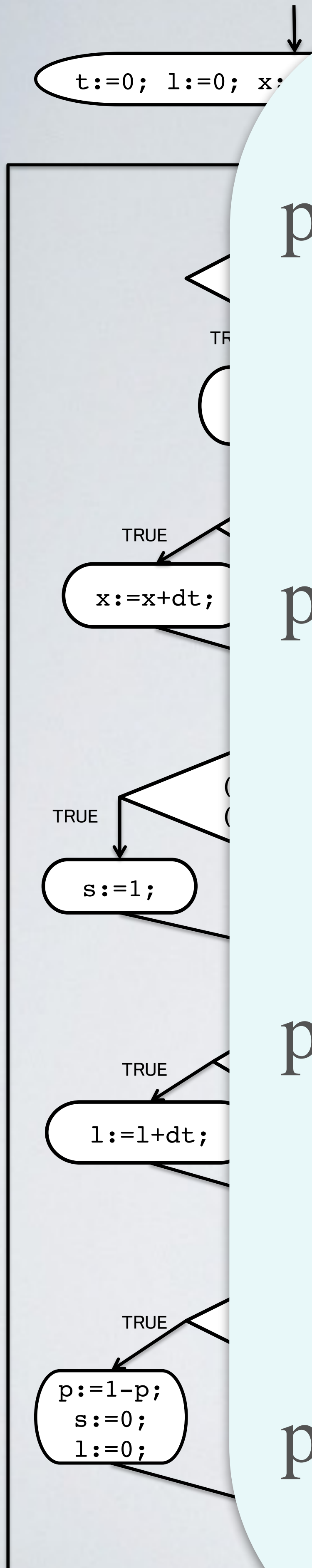


p=1, s=1

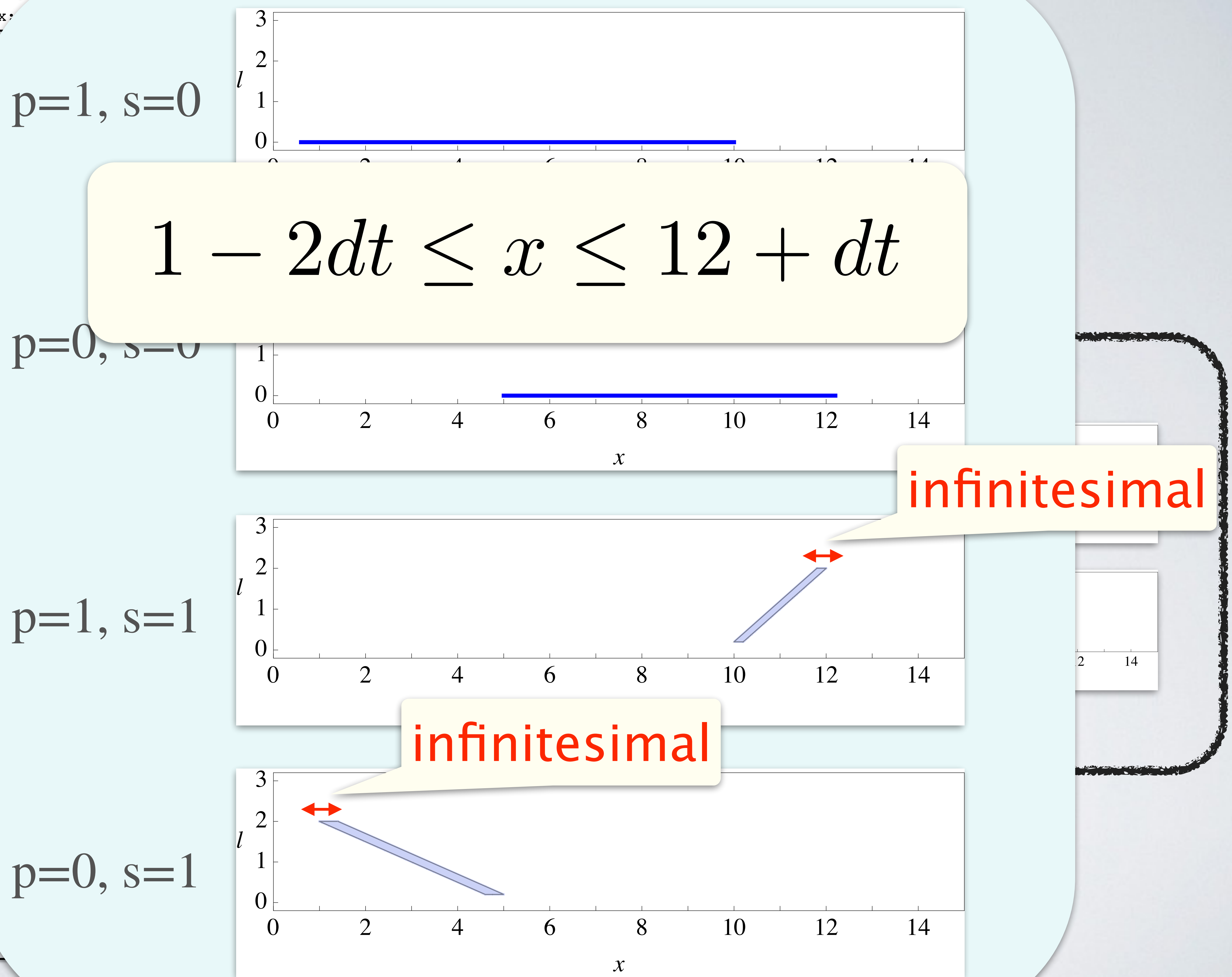


p=0, s=1





$$1 - 2dt \leq x \leq 12 + dt$$



- Example of analysis
- Semantics of WHILE^{dt}
- (Standard) abstract interpretation
- Abstract interpretation with infinitesimals

WHILE$^{\mathrm{dt}}$ [Suenaga & Hasuo ICALP 11]

$$\mathbf{AExp} \ni a ::= x \mid r \mid a_1 \;\mathtt{aop}\; a_2 \mid \mathtt{dt} \mid \infty$$

$$\text{where } x \in \mathbf{Var}, r \in \mathbb{R} \text{ and } \mathtt{aop} \in \{+, -, \cdot, \wedge\}$$

$$\mathbf{BExp} \ni b ::= \mathtt{true} \mid \mathtt{false} \mid b_1 \wedge b_2 \mid \neg b \mid a_1 < a_2$$

$$\mathbf{Cmd} \ni c ::= \mathtt{skip} \mid x := a \mid c_1 ; c_2 \mid \mathtt{if}\; b \;\mathtt{then}\; c_1 \;\mathtt{else}\; c_2 \mid \mathtt{while}\; b \;\mathtt{do}\; c$$

Nonstandard Analysis

[Robinson 60's]

$$\mathbb{R} \mapsto {}^*\mathbb{R} := \mathbb{R}^{\mathbb{N}} / \sim_{\mathcal{F}}$$

$$\mathbb{N} \mapsto {}^*\mathbb{N} := \mathbb{N}^{\mathbb{N}} / \sim_{\mathcal{F}}$$

$${}^*r := [(r, r, r, \cdots)]$$

$$\omega := [(1, 2, 3, \cdots)]$$

$$\omega^{-1} := [(1, \frac{1}{2}, \frac{1}{3}, \cdots)]$$

Nonstandard Analysis

[Robinson 60's]

$$\mathbb{R} \mapsto {}^*\mathbb{R} := \mathbb{R}^{\mathbb{N}} / \sim_{\mathcal{F}}$$

∋ infinitesimals, infinites

$$\mathbb{N} \mapsto {}^*\mathbb{N} := \mathbb{N}^{\mathbb{N}} / \sim_{\mathcal{F}}$$

∋ infinites

$$ {}^*r := [(r, r, r, \cdots)] $$

$$ \omega := [(1, 2, 3, \cdots)] $$

$$ \omega^{-1} := [(1, \frac{1}{2}, \frac{1}{3}, \cdots)] $$

Collecting Semantics for WHILE^{dt}

$$[\![x]\!]\boldsymbol{\sigma} := \boldsymbol{\sigma}(x) \text{ for each } x \in \mathbf{Var}$$

$$[\![r]\!]\boldsymbol{\sigma} := r \text{ for each } r \in \mathbb{R}$$

$$[\![a_1 \ \texttt{aop} \ a_2]\!]\boldsymbol{\sigma} := [\![a_1]\!] \ \texttt{aop} \ [\![a_2]\!]$$

$$[\![\mathrm{dt}]\!]\boldsymbol{\sigma} := [(1, \tfrac{1}{2}, \tfrac{1}{3}, \cdots)]$$

$$[\![\texttt{true}]\!]\boldsymbol{\sigma} := \mathrm{tt}$$

$$[\![\texttt{false}]\!]\boldsymbol{\sigma} := \mathrm{ff}$$

$$[\![b_1 \wedge b_2]\!]\boldsymbol{\sigma} := [\![b_1]\!] \wedge [\![b_2]\!]$$

$$[\![\neg b]\!]\boldsymbol{\sigma} := \neg([\![b]\!]\boldsymbol{\sigma})$$

$$[\![\texttt{skip}]\!]\mathbf{S} := \mathbf{S}$$

$$[\![x := a]\!]\mathbf{S} := \{\boldsymbol{\sigma}[[\![a]\!]\boldsymbol{\sigma}/x] \mid \boldsymbol{\sigma} \in \mathbf{S}\}$$

$$[\![c_1; c_2]\!]\mathbf{S} := [\![c_2]\!]([\![c_1]\!]\mathbf{S})$$

$$[\![\texttt{if } b \texttt{ then } c_1 \texttt{ else } c_2]\!]\mathbf{S} := \begin{array}{l}\{[\![c_1]\!]\boldsymbol{\sigma} \mid \boldsymbol{\sigma} \in \mathbf{S},\ [\![b]\!]\boldsymbol{\sigma} = \mathrm{tt}\} \\ \cup \{[\![c_2]\!]\boldsymbol{\sigma} \mid \boldsymbol{\sigma} \in \mathbf{S},\ [\![b]\!]\boldsymbol{\sigma} = \mathrm{ff}\}\end{array}$$

$$[\![\texttt{while } b \texttt{ do } c]\!]\mathbf{S} := \mathrm{lfp}({}^*\Phi([\![b]\!])([\![c]\!]))$$

where $\Phi : (\mathbf{St} \to \mathbb{B} \cup \{\bot\}) \to (\mathcal{P}(\mathbf{Var} \to \mathbb{R}) \to \mathcal{P}(\mathbf{Var} \to \mathbb{R})) \to ((\mathcal{P}(\mathbf{Var} \to \mathbb{R}) \to \mathcal{P}(\mathbf{Var} \to \mathbb{R})) \to (\mathcal{P}(\mathbf{Var} \to \mathbb{R}) \to \mathcal{P}(\mathbf{Var} \to \mathbb{R})))$

is defined by $\Phi(f)(g) = \lambda\psi.\ \lambda S.\ \{\psi(g(\sigma)) \mid \sigma \in S,\ f(\sigma) = \mathrm{tt}\} \cup \{\sigma \mid \sigma \in S,\ f(\sigma) = \mathrm{ff}\}.$

- Example of analysis
- Semantics of WHILE^{dt}
- (Standard) abstract interpretation
  [Cousot & Cousot 1977]
- Abstract interpretation with infinitesimals

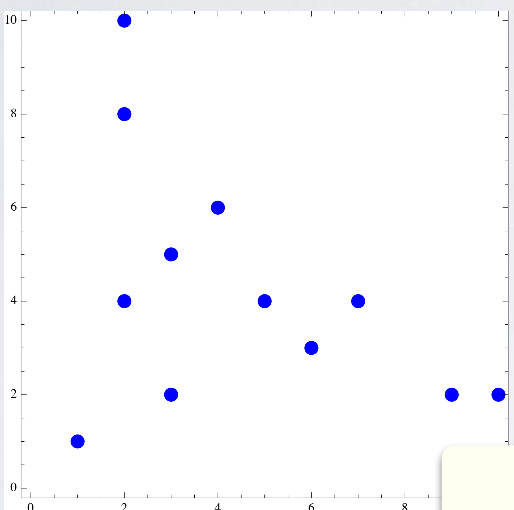
Abstract Interpretation

[Cousot & Cousot 1977]

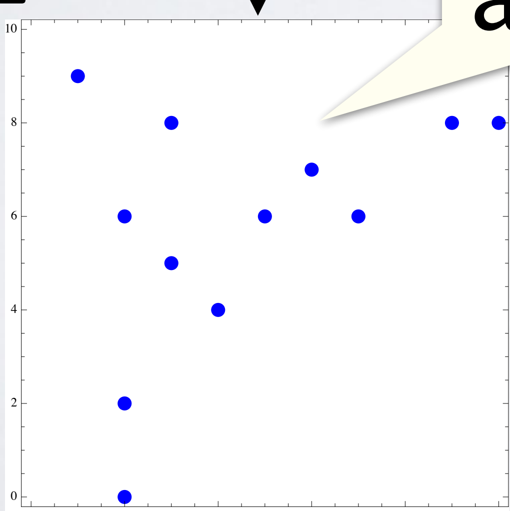
concrete domain $\mathcal{P}(\mathbb{R}^2)$

$$L \underset{\gamma}{\overset{\alpha}{\rightleftharpoons}} \overline{L}$$

abstract domain $\mathbb{CP}_2$



`y:=-y+10`



over-approximate!

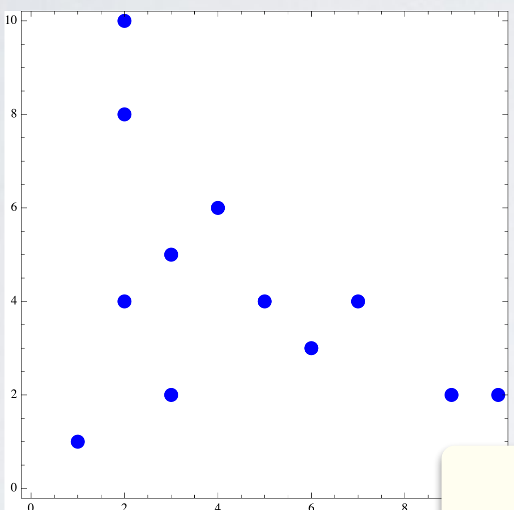
Abstract Interpretation

[Cousot & Cousot 1977]

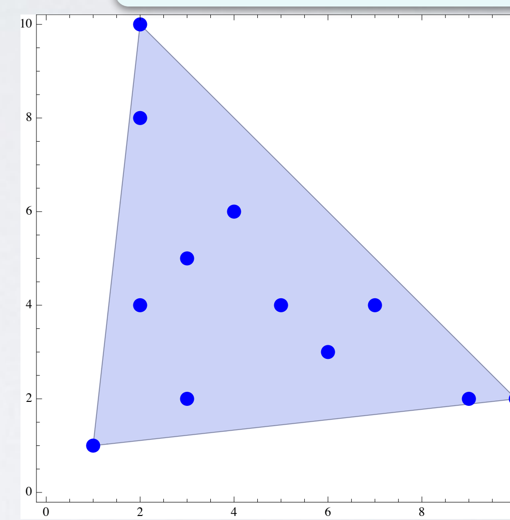
concrete domain $\mathcal{P}(\mathbb{R}^2)$

$$L \underset{\gamma}{\overset{\alpha}{\rightleftharpoons}} \overline{L}$$

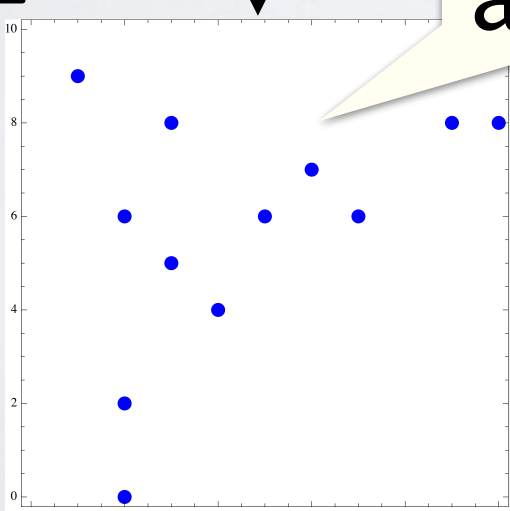
abstract domain $\mathbb{CP}_2$



α (abstraction) →



`y:=-y+10` ↓



over-approximate!

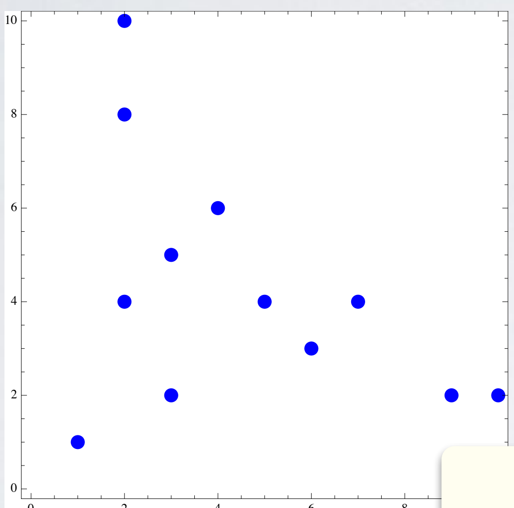
Abstract Interpretation

[Cousot & Cousot 1977]

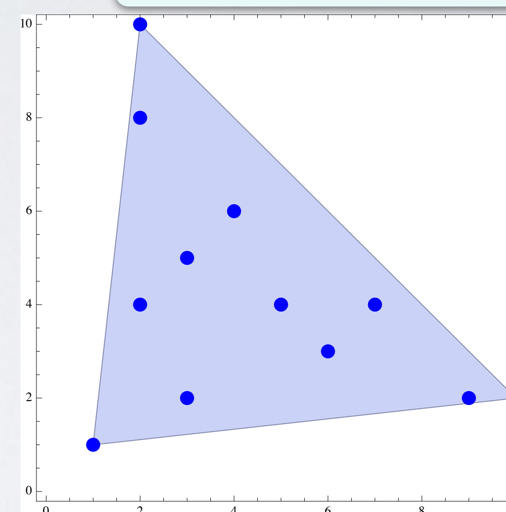
concrete domain $\mathcal{P}(\mathbb{R}^2)$

$$L \underset{\gamma}{\overset{\alpha}{\rightleftharpoons}} \overline{L}$$

abstract domain $\mathbb{CP}_2$

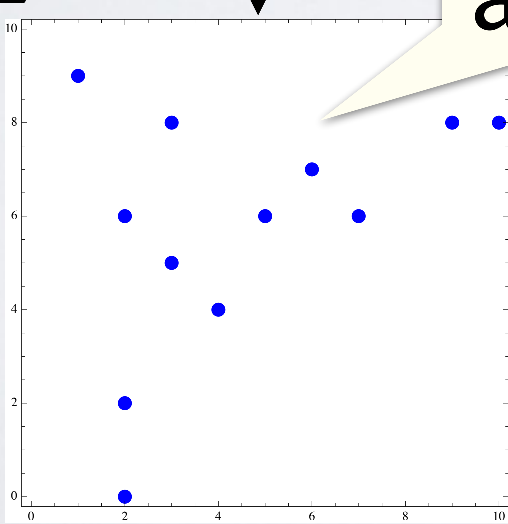


α (abstraction)

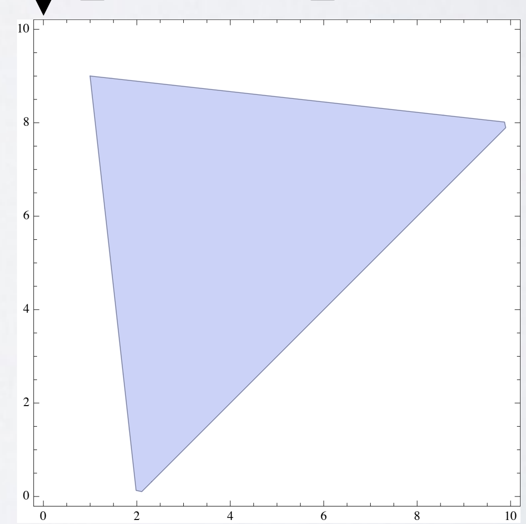


y:=-y+10

over-approximate!



y:=-y+10



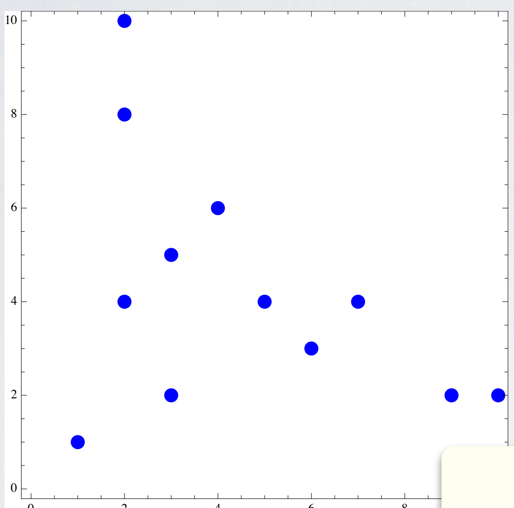
Abstract Interpretation

[Cousot & Cousot 1977]

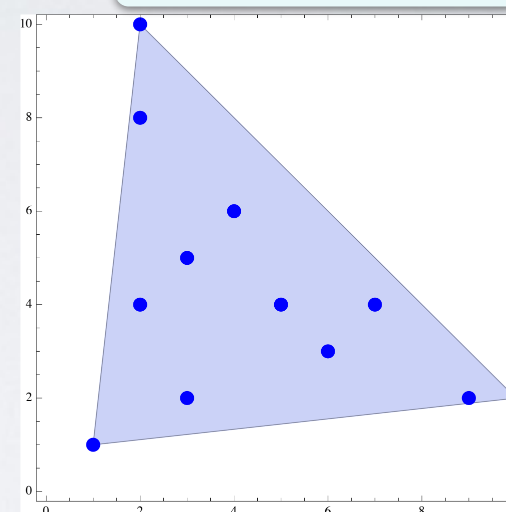
concrete domain $\mathcal{P}(\mathbb{R}^2)$

$$L \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} \overline{L}$$

abstract domain $\mathbb{CP}_2$



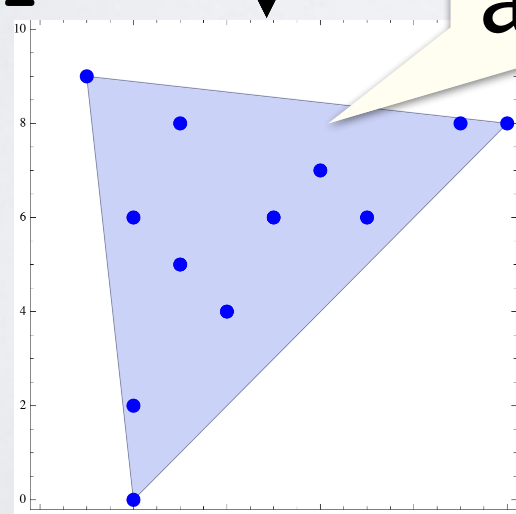
α (abstraction)



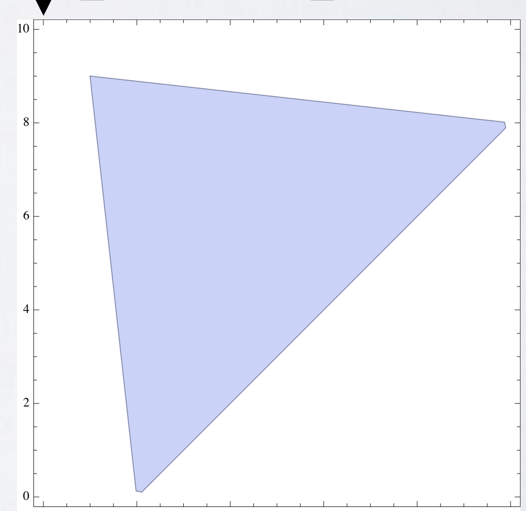
`y:=-y+10`

`y:=-y+10`

over-approximate!



γ (concretization)



Galois Connection

$$L \underset{\gamma}{\overset{\alpha}{\rightleftharpoons}} \overline{L}$$

e.g.

$$\mathcal{P}(\mathbb{R}^n) \rightleftharpoons \mathbb{CP}_n$$

Thm.
The least fixed point in L is overapproximated by a prefixed point in $\overline{L}$

Galois Connection

$$L \underset{\gamma}{\overset{\alpha}{\rightleftharpoons}} \overline{L}$$

e.g.

$$\mathcal{P}(\mathbb{R}^n) \rightleftharpoons \mathbb{CP}_n$$

Thm.
The least fixed point in L is overapproximated by a prefixed point in $\overline{L}$

Widening Operators

$$L \underset{\gamma}{\overset{\alpha}{\rightleftharpoons}} \overline{L}$$

Definition **(Widening operator)** Let $(L, \sqsubseteq)$ be a poset. An operator $\nabla : L \times L \to L$ is said to be a *widening operator* if the following two conditions hold:

- (Covering) for any $x, y \in L$, $x \sqsubseteq x \nabla y$ and $y \sqsubseteq x \nabla y$;
- (Termination) for any ascending chain $\langle x_i \rangle \in L^\omega$, the chain $\langle y_i \rangle \in L^\omega$ defined by $\begin{cases} y_0 = x_0 \\ y_{i+1} = y_i \nabla x_{i+1} & \text{(for all } i \in \mathbb{N}) \end{cases}$ is ultimately stationary.

Thm.
Prefixed point is computed within $n \in \mathbb{N}$ steps using ∇.

Widening Operators on ℂℙn

- Standard widening
  [Halbwachs Ph.D. Thesis 79]

- Widening up to
  [Halbwachs CAV 93]

- Precise widening
  [Bagnara, Hill, Ricci and Zaffanella SCP 05]

- Example of analysis
- Semantics of WHILE^{dt}
- (Standard) abstract interpretation
- Abstract interpretation with infinitesimals
    - Soundness
    - Termination

transfer principle

(ϕ: 1st-order $\mathcal{L}_{\mathbb{U}}$-sentence)

$$\mathbb{R} \models \phi \Leftrightarrow {}^*\mathbb{R} \models {}^*\phi$$

transfer principle

(ϕ: 1st-order $\mathcal{L}_{\mathbb{U}}$-sentence)

$$\mathbb{R} \models \phi \Leftrightarrow {}^*\mathbb{R} \models {}^*\phi$$

$$\forall x \in \mathbb{R}.\ \forall y \in \mathbb{R}.\ (x \leq y \lor y \leq x)$$

transfer principle

(ϕ: 1st-order $\mathcal{L}_{\mathbb{U}}$-sentence)

$$\mathbb{R} \models \phi \Leftrightarrow {}^*\mathbb{R} \models {}^*\phi$$

$$\forall x \in \mathbb{R}.\ \forall y \in \mathbb{R}.\ (x \leq y \vee y \leq x)$$

$$\forall x \in {}^*\mathbb{R}.\ \forall y \in {}^*\mathbb{R}.\ (x \leq y \vee y \leq x)$$

transfer principle

(ϕ: 1st-order $\mathcal{L}_{\mathbb{U}}$-sentence)

$$\mathbb{R} \models \phi \Leftrightarrow {}^*\mathbb{R} \models {}^*\phi$$

$$\forall x \in \mathbb{R}.\ (x \in A \cup B \Leftrightarrow x \in A \vee x \in B)$$

transfer principle

(ϕ: 1st-order $\mathcal{L}_{\mathbb{U}}$-sentence)

$$\mathbb{R} \models \phi \Leftrightarrow {}^*\mathbb{R} \models {}^*\phi$$

$$\forall x \in \mathbb{R}.\ (x \in A \cup B \Leftrightarrow x \in A \vee x \in B)$$

$$\forall x \in {}^*\mathbb{R}.\ (x \in {}^*(A \cup B) \Leftrightarrow x \in {}^*A \vee x \in {}^*B)$$

Transferring Abstract Interpretation

Standard

$$\mathcal{P}(\mathbb{R}^n) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} \mathbb{CP}_n \quad (\perp)$$

Thm.
The least fixed point in $\mathcal{P}(\mathbb{R}^n)$ is overapproximated by a prefixed point in $\mathbb{CP}_n$.

Nonstandard

Transferring Abstract Interpretation

Standard

$$\mathcal{P}(\mathbb{R}^n) \underset{\gamma}{\overset{\alpha}{\rightleftarrows}} \mathbb{CP}_n \quad (\bot)$$

Nonstandard

$$\mathcal{P}({}^*\mathbb{R}^n) \underset{{}^*\gamma}{\overset{{}^*\alpha}{\rightleftarrows}} {}^*\mathbb{CP}_n \quad (\bot)$$

transfer

Thm.
The least fixed point in $\mathcal{P}(\mathbb{R}^n)$ is overapproximated by a prefixed point in $\mathbb{CP}_n$.

Thm.
The least fixed point in $\mathcal{P}({}^*\mathbb{R}^n)$ is overapproximated by a prefixed point in ${}^*\mathbb{CP}_n$.

Transferring Abstract Interpretation

Standard

Widening operator: ∇

Thm.
Prefixed point is computed within $n \in \mathbb{N}$ steps using ∇.

Nonstandard

Transferring Abstract Interpretation

Standard

Nonstandard

Widening operator: ∇

Hyperwidening operator: ${}^*\nabla$

transfer

Thm.
Prefixed point is computed within $n \in \mathbb{N}$ steps using ∇.

Transferring Abstract Interpretation

Lemma (Convergence of iteration sequences in $\mathcal{L}_{\mathbb{U}}$) *Let $L \in \mathbb{U}$ be a set, $\sqsubseteq \in \mathcal{P}(L \times L)$ be a binary relation on L and $\nabla : L \times L \to L$ be a function. Then, the following $\mathcal{L}_{\mathbb{U}}$-sentence holds:*

$$\begin{aligned}
&\forall F \in L \to L.\ \forall \bot \in L.\ \forall X \in \mathbb{N} \to L. \\
&\mathsf{Poset}_{L,\sqsubseteq} \land \mathsf{Monotone}_{L,\sqsubseteq,L,\sqsubseteq}(F) \land \mathsf{Basis}_{L,\sqsubseteq}(\bot, F) \land \mathsf{Widen}_{L,\sqsubseteq,\nabla} \\
&\land \mathsf{WidenSeq}_{L,\sqsubseteq,\nabla}(X, \bot, F) \\
&\Rightarrow \underline{\exists i \in \mathbb{N}.}\ \forall j \in \mathbb{N}.\ i \leq j \Rightarrow X(i) = X(j) \\
&\land \forall k \in \mathbb{N}.\ \Big((\forall l \in \mathbb{N}.\ k \leq l \Rightarrow X(k) = X(l)) \Rightarrow F(X(k)) \sqsubseteq X(k) \Big).
\end{aligned}$$

Thm.
Prefixed point is computed within $n \in \mathbb{N}$ steps using ∇.

Transferring Abstract Interpretation

Lemma **(Convergence of iteration sequences in $\mathcal{L}_{\mathbb{U}}$)** *Let $L \in \mathbb{U}$ be a set, $\sqsubseteq \in \mathcal{P}(L \times L)$ be a binary relation on L and $\nabla : L \times L \to L$ be a function. Then, the following $\mathcal{L}_{\mathbb{U}}$-sentence holds:*

$\forall F \in L \to L.$

$\mathsf{Poset}_{L,\sqsubseteq} \wedge \mathsf{M}$ … $\wedge\, \mathsf{Widen}_{L,\sqsubseteq,\nabla}$

$\wedge \mathsf{WidenSeq}_{L,\sqsubseteq,\nabla}(X, \bot, F)$

$\Rightarrow \exists i \in \mathbb{N}.\ \forall j \in \mathbb{N}.\ i \leq j \Rightarrow X(i) = X(j)$

$\wedge \forall k \in \mathbb{N}.\ \Big(\big(\forall l \in \mathbb{N}.\ k \leq l \Rightarrow X(k) = X(l) \big) \Rightarrow F\big(X(k)\big) \sqsubseteq X(k) \Big).$

transfer!

Thm.
Prefixed point is computed within n∈$\mathbb{N}$ steps using ∇.

Transferring Abstract Interpretation

Theorem
Let $L \in \mathbb{U}$ be a set, $\sqsubseteq \in \mathcal{P}(L \times L)$ be a binary relation on L and $\nabla : L \times L \to L$ be a function. Then, the following $\mathcal{L}_{\mathbb{U}}$-sentence holds:

$$\forall F \in {}^*(L \to L).\ \forall \bot \in {}^*L.\ \forall X \in {}^*(\mathbb{N} \to L).$$
$${}^*\mathsf{Poset}_{L,\sqsubseteq} \wedge {}^*\mathsf{Monotone}_{L,\sqsubseteq,L,\sqsubseteq}(F) \wedge {}^*\mathsf{Basis}_{L,\sqsubseteq}(\bot, F) \wedge {}^*\mathsf{Widen}_{L,\sqsubseteq,\nabla}$$
$$\wedge {}^*\mathsf{WidenSeq}_{L,\sqsubseteq,\nabla}(X, \bot, F)$$
$$\Rightarrow \underline{\exists i \in {}^*\mathbb{N}.}\ \forall j \in {}^*\mathbb{N}.\ i \leq j \Rightarrow X(i) = X(j)$$
$$\wedge \forall k \in {}^*\mathbb{N}.\ \Big(\big(\forall l \in {}^*\mathbb{N}.\ k \leq l \Rightarrow X(k) = X(l)\big) \Rightarrow F\big(X(k)\big)\ {}^*\sqsubseteq\ X(k) \Big)$$

Thm.
Prefixed point is computed within $n \in \mathbb{N}$ steps using ∇.

Transferring Abstract Interpretation

Theorem
Let $L \in \mathbb{U}$ be a set, $\sqsubseteq \in \mathcal{P}(L \times L)$ be a binary relation on L and $\nabla : L \times L \to L$ be a function. Then, the following $\mathcal{L}_{\mathbb{U}}$-sentence holds:

$$\forall F \in {}^*(L \to L).\ \forall \bot \in {}^*L.\ \forall X \in {}^*(\mathbb{N} \to L).$$
$${}^*\mathsf{Poset}_{L,\sqsubseteq} \wedge {}^*\mathsf{Monotone}_{L,\sqsubseteq,L,\sqsubseteq}(F) \wedge {}^*\mathsf{Basis}_{L,\sqsubseteq}(\bot, F) \wedge {}^*\mathsf{Widen}_{L,\sqsubseteq,\nabla}$$
$$\wedge {}^*\mathsf{WidenSeq}_{L,\sqsubseteq,\nabla}(X, \bot, F)$$
$$\Rightarrow \exists i \in {}^*\mathbb{N}.\ \forall j \in {}^*\mathbb{N}.\ i \leq j \Rightarrow X(i) = X(j)$$
$$\wedge \forall k \in {}^*\mathbb{N}.\ \Big((\forall l \in {}^*\mathbb{N}.\ k \leq l \Rightarrow X(k) = X(l)) \Rightarrow F\big(X(k)\big)\ {}^*\!\sqsubseteq X(k) \Big)$$

Thm.
Prefixed point is computed within $n \in \mathbb{N}$ steps using ∇.

Thm.
Prefixed point is computed within $n \in {}^*\mathbb{N}$ steps using ∇.

Transferring Abstract Interpretation

Theorem
Let $L \in \mathbb{U}$ be a set, $\sqsubseteq \in \mathcal{P}(L \times L)$ be a binary relation on L and $\nabla : L \times L \to L$ be a function. Then, the following $\mathcal{L}_{\mathbb{U}}$-sentence holds:

$$\forall F \in {}^*(L \to L).\ \forall \bot \in {}^*L.\ \forall X \in {}^*(\mathbb{N} \to L).$$
$$^*\mathsf{Poset}_{L,\sqsubseteq} \wedge {}^*\mathsf{Monotone}_{L,\sqsubseteq,L,\sqsubseteq}(F) \wedge {}^*\mathsf{Basis}_{L,\sqsubseteq}(\bot, F) \wedge {}^*\mathsf{Widen}_{L,\sqsubseteq,\nabla}$$
$$\wedge {}^*\mathsf{WidenSeq}_{L,\sqsubseteq,\nabla}(X, \bot, F)$$
$$\Rightarrow \exists i \in {}^*\mathbb{N}.\ \forall j \in {}^*\mathbb{N}.\ i \le j \Rightarrow X(i) = X(j)$$
$$\wedge \forall k \in {}^*\mathbb{N}.\ \Big(\big(\forall l \in {}^*\mathbb{N}.\ k \le l \Rightarrow X(k) = X(l)\big) \Rightarrow F\big(X(k)\big) \ {}^*\!\sqsubseteq X(k) \Big)$$

Thm.
Prefixed point is computed within $n \in \mathbb{N}$ steps using ∇.

Thm.
Prefixed point is com[puted] within $n \in {}^*\mathbb{N}$ steps us[ing ∇].

include infinites

Uniformity of Widening Operators

– (Termination) for any ascending chain $\langle x_i \rangle \in L^\omega$, the chain $\langle y_i \rangle \in L^\omega$ defined by $\begin{cases} y_0 = x_0 \\ y_{i+1} = y_i \nabla x_{i+1} \quad \text{(for all } i \in \mathbb{N}) \end{cases}$ is ultimately stationary.

– (Uniform termination) for any $x_0 \in L$, there exists a constant $i \in \mathbb{N}$ such that for any ascending chain $\langle x_i \rangle \in L^\omega$ starting from x_0, there exists $j \in \mathbb{N}$ such that $j \leq i$ and the chain $\langle y_i \rangle \in L^\omega$ defined by

$$\begin{cases} y_0 = x_0 \\ y_{i+1} = y_i \nabla x_{i+1} \quad \text{(for all } i \in \mathbb{N}) \end{cases}$$

satisfies $y_j = y_{j+1}$.

$$\mathsf{Term}_{L,\sqsubseteq,\nabla} :\equiv \ \forall x \in \mathbb{N} \to L.\ \mathsf{AscCn}(x) \Rightarrow \Big(\forall y \in \mathbb{N} \to L.\ \big((y(0) = x(0) \wedge \forall n \in \mathbb{N}.\ y(n+1) = y(n) \nabla x(n+1)) \Rightarrow \exists k \in \mathbb{N}.\ y(k) = y(k+1)\big)\Big)$$

$$\mathsf{UnifTerm}_{L,\sqsubseteq,\nabla} :\equiv \ \forall x_0 \in L.\ \exists i \in \mathbb{N}.\ \forall x \in \mathbb{N} \to L.\ (\mathsf{AscCn}(x) \wedge x(0) = x_0) \Rightarrow \Big(\forall y \in \mathbb{N} \to L.\ \big((y(0) = x(0) \wedge \forall n \in \mathbb{N}.\ y(n+1) = y(n) \nabla x(n+1)) \Rightarrow \exists j \in \mathbb{N}.\ (j \le i \wedge y(j) = y(j+1))\big)\Big)$$

Theorem 3.12 *Let* $(L, \sqsubseteq)$ *be a poset and* $\nabla \in L \times L \to L$ *be a uniform widening operator on* L*. Let* $F : {}^*L \to {}^*L$ *be a monotone and internal function; and* $\bot \in L$ *be such that* ${}^*\bot \; {}^*\!\sqsubseteq F({}^*\bot)$*. The iteration sequence* $\langle X_i \rangle_{i \in \mathbb{N}}$ *defined by*

$$X_0 = {}^*\bot, \quad X_{i+1} = \begin{cases} X_i & (if\ F(X_i)\ {}^*\!\sqsubseteq X_i) \\ X_i\ {}^*\nabla\ F(X_i) & (otherwise) \end{cases} \quad \text{for all } i \in \mathbb{N}$$

reaches its limit within some finite number of steps; and the limit $\bigsqcup_{i \in \mathbb{N}} X_i$ *is a prefixed point of* F *such that* ${}^*\bot \; {}^*\!\sqsubseteq \bigsqcup_{i \in \mathbb{N}} X_i$*.* □

Uniformity of Widening Operators on ℂℙn

- Standard widening
  [Halbwachs Ph.D. Thesis 79]

- Widening up to
  [Halbwachs CAV 93]

- Precise widening
  [Bagnara, Hill, Ricci and Zaffanella SCP 05]

Uniformity of Widening Operators on ℂℙn

- Standard widening ✔
  [Halbwachs Ph.D. Thesis 79]

- Widening up to ✔
  [Halbwachs CAV 93]

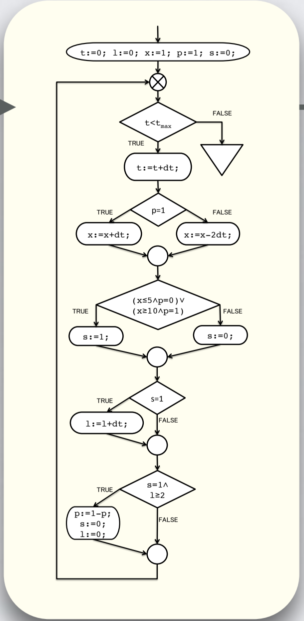
- Precise widening ✘
  [Bagnara, Hill, Ricci and Zaffanella SCP 05]

Tool Overview

WHILEdt program

$t := 0; l := 0; x := 1; p := 1; s := 0;$
while $t < t_{max}$ **do**
  $t := t + dt;$
  if $p = 1$ **then** $x := x + dt;$ **else** $x := x - 2dt;$
  if $(x \leq 5 \wedge p = 0) \vee (x \geq 10 \wedge p = 1)$ **then** $s := 1$ **else** $s := 0;$
  if $s = 1$ **then** $l := l + dt;$
  if $s = 1 \wedge l \geq 2$ **then** $p := 1 - p; s := 0; l := 0$

CFG



- iteration on $\mathbb{CP}_n$
- uniform widenings for While loops

Use CAS regarding dt as a variable

Overapproximation of reachable set (with dt)

$$1 - 2dt \leq x \leq 12 + dt$$

Conclusion

- Abstract interpretation with infinitesimals
    - Soundness
    - Uniform termination of widening
    - Prototype implementation
- Automated reachability analysis of hybrid systems

Future Work

- Transferring other abstract domains
- Hyperwidening operators
  other than transferred uniform widening operators
- Extending model checking with infinitesimals