

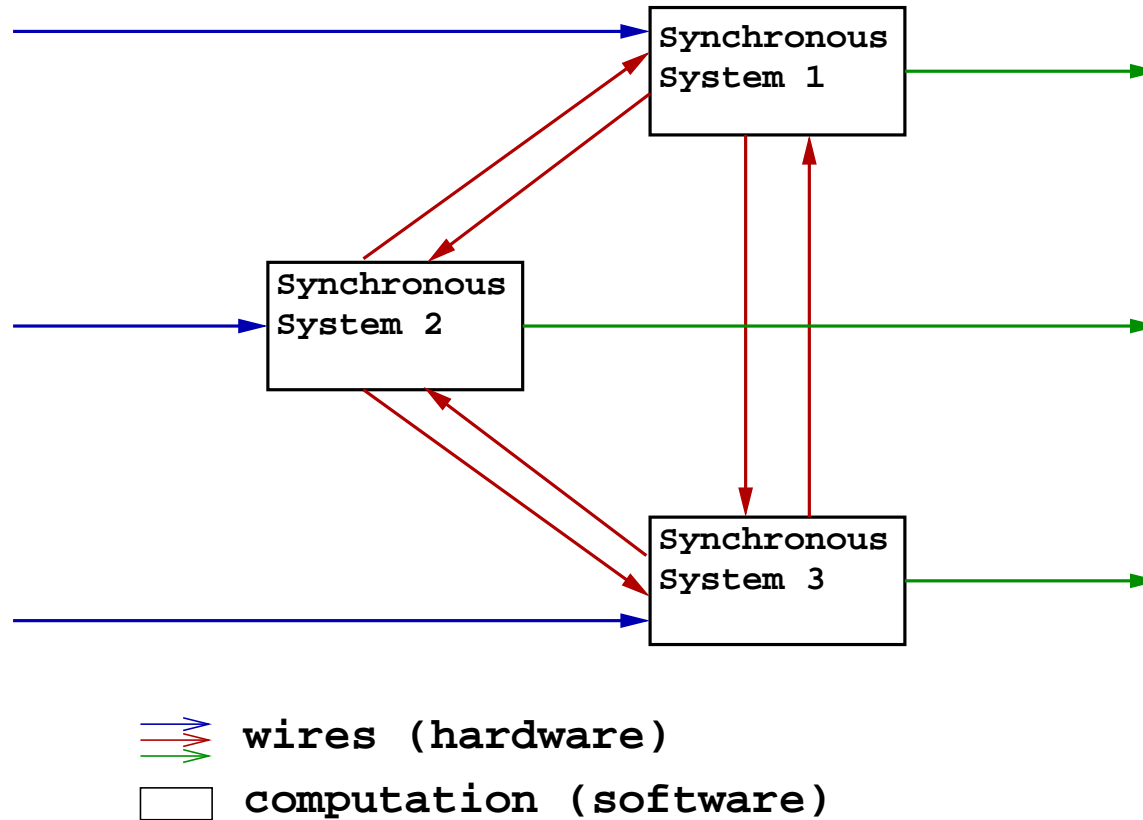
Static Analysis by Abstract Interpretation of the Quasi-Synchronous Composition of Synchronous Programs

Julien Bertrane, bertrane@di.ens.fr

École Normale Supérieure, Paris, France

VMCAI'05, 17 Janvier 2005

Certification of embedded systems



– goal : **Fault tolerance** properties

Modeling synchronous systems

- **Synchronous systems** :
 - Initialize(S)
 - while true do
 - (O, S) := Compute (S, I)
 - wait for clock
 - od

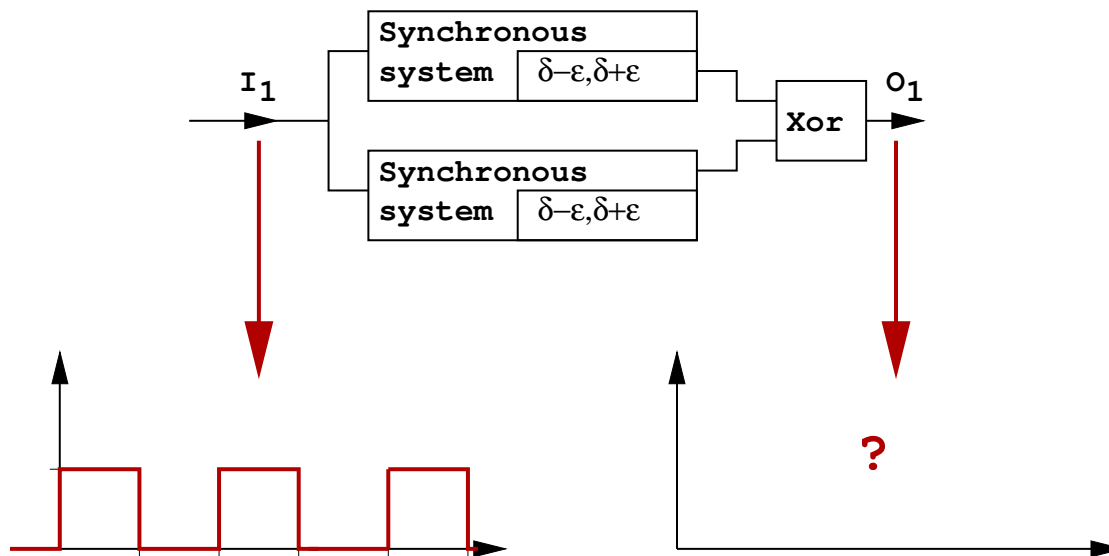
where I : inputs, S : state variables, O : outputs

Hypotheses for this model

- **Quasi-synchrony** :
 - Each “synchronous” system is executed according to a clock
 - Clock Skew : Duration between two clock ticks belongs to $[\alpha, \beta]$, $\alpha > 0$.
- **Serial** transmission between synchronous systems
- **A one-value buffer** store data waiting to be read
- **Initialisation** of data to 0 or *false* according to its type.

Difficulties

- Allowing clock imprecision (i.e. *quasi-synchronous* instead of *synchronous*) enables **non countable** different behaviors

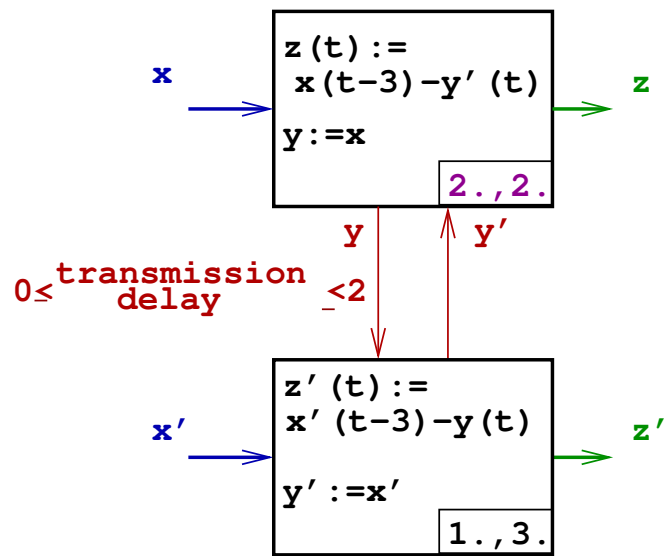


Plan

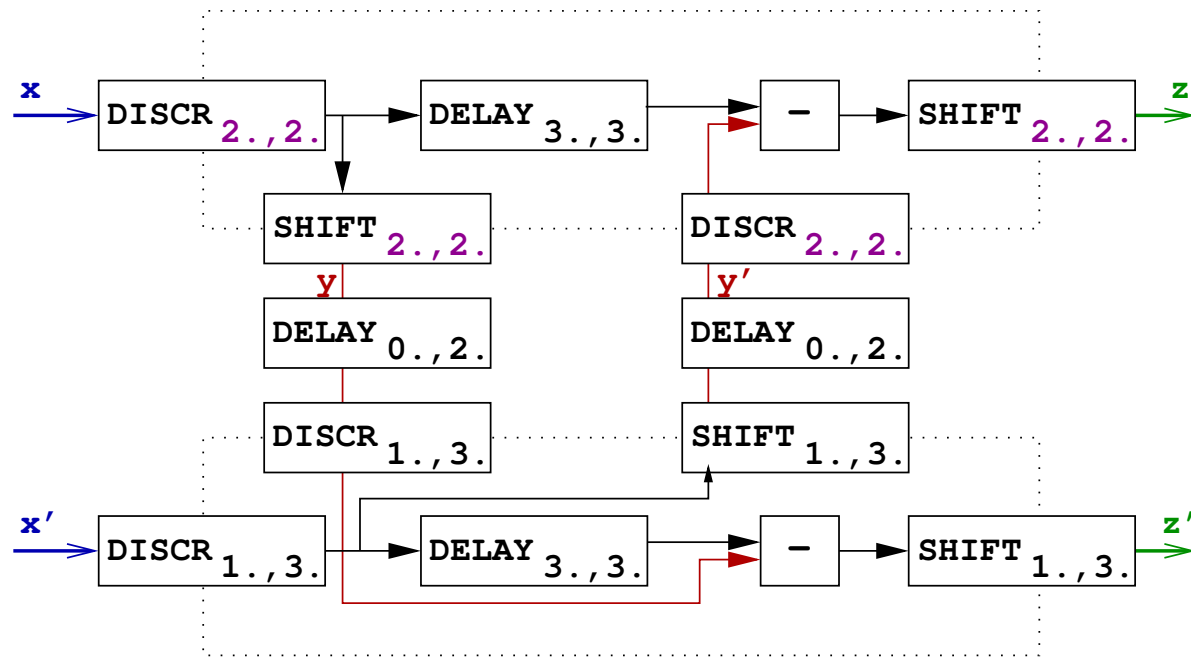
- **Model : syntax and semantics**
- Abstraction
- Analysis
- Simplification of concrete properties
- From concrete properties to abstract properties
- An example of analysis

Syntax

Intuitive description



Formal model

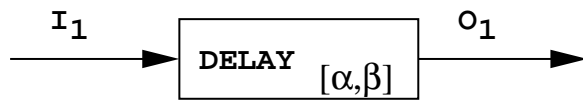
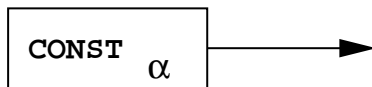
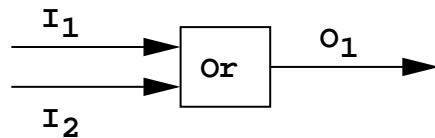
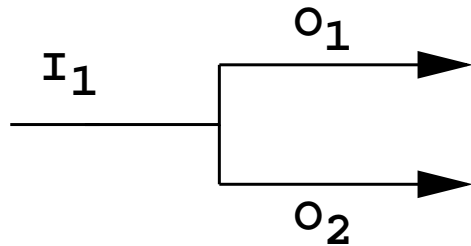


Modeling embedded systems

- **Continuous-time semantics**
which maps each point of control to a **set of signals**
($\mathbb{R} \mapsto \mathbb{B}$).
- **Easy** translation from synchronous frameworks, like
SCADE, to this syntax.

Syntax and equational semantics of diagrams

Syntax



equational semantics

$$\forall t \in \mathbb{R}^+, O_1(t) = I_1(t)$$

$$\forall t \in \mathbb{R}^+, O_2(t) = I_1(t)$$

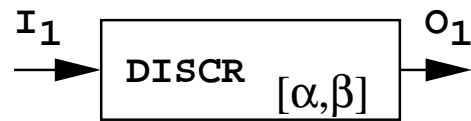
$$\forall t \in \mathbb{R}^+, O_1(t) = I_1(t) \text{ or } I_2(t)$$

$$\forall t \in \mathbb{R}^+, O_1(t) = \alpha$$

$$\forall t \in \mathbb{R}, O_1(t) = I_1(\delta(t))$$

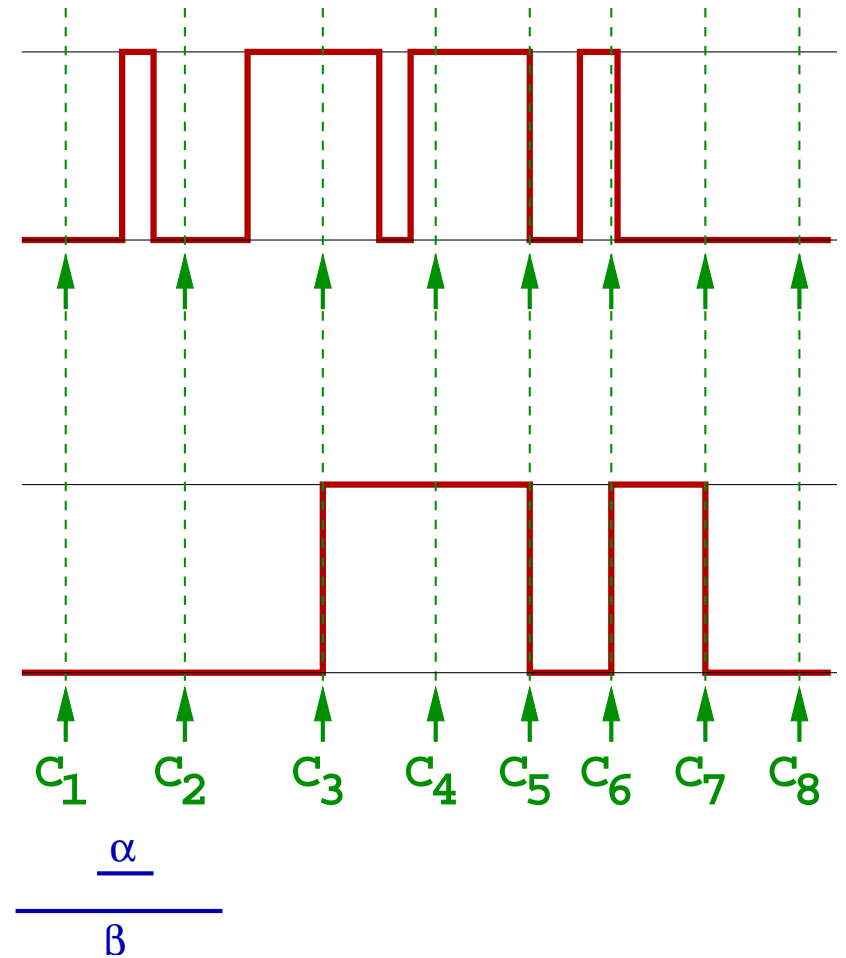
$$\delta : \begin{cases} \exists \delta : \mathbb{R} \rightarrow \mathbb{R}, \text{ monotonic,} \\ \forall t \in \mathbb{R}, \delta(t) - t \in [\alpha, \beta] \end{cases}$$

Syntax and equational semantics of diagrams

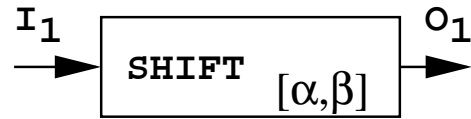


For any clock c satisfying $[\alpha, \beta]$,
 i.e. : $c_{n+1} - c_n \in [\alpha, \beta]$

$$O_1(t) = \begin{cases} \bullet 0 & \text{if } t < c(0) \\ \bullet I_1(c_n) & \text{if } t \in [c_n, c_{n+1}) \end{cases}$$



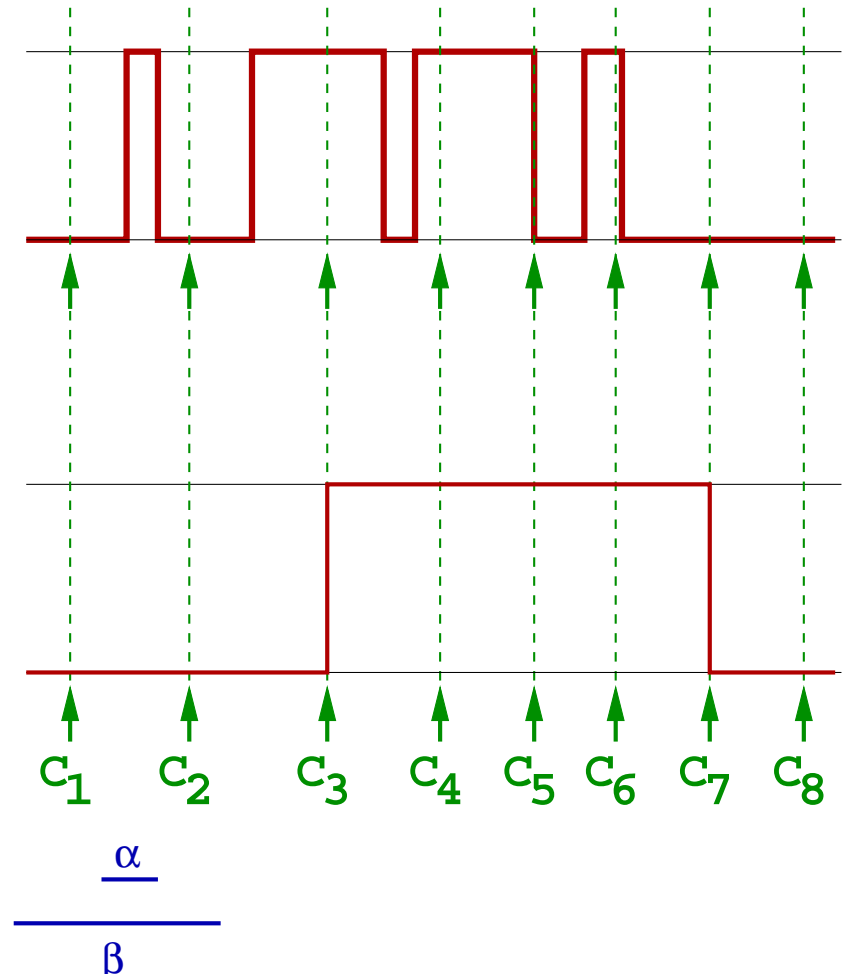
Syntax and equational semantics of diagrams



For any clock c satisfying $[\alpha, \beta]$

i.e. : $c_{n+1} - c_n \in [\alpha, \beta]$

$$O_1(t) = \begin{cases} \bullet 0 & \text{if } t < c(0) \\ \bullet \lim_{t \rightarrow c_n} I_1(t) & \text{if } t \in [c_n, c_{n+1}) \end{cases}$$



Concrete semantics

– **Concrete equational semantics** :

let D be a diagram.

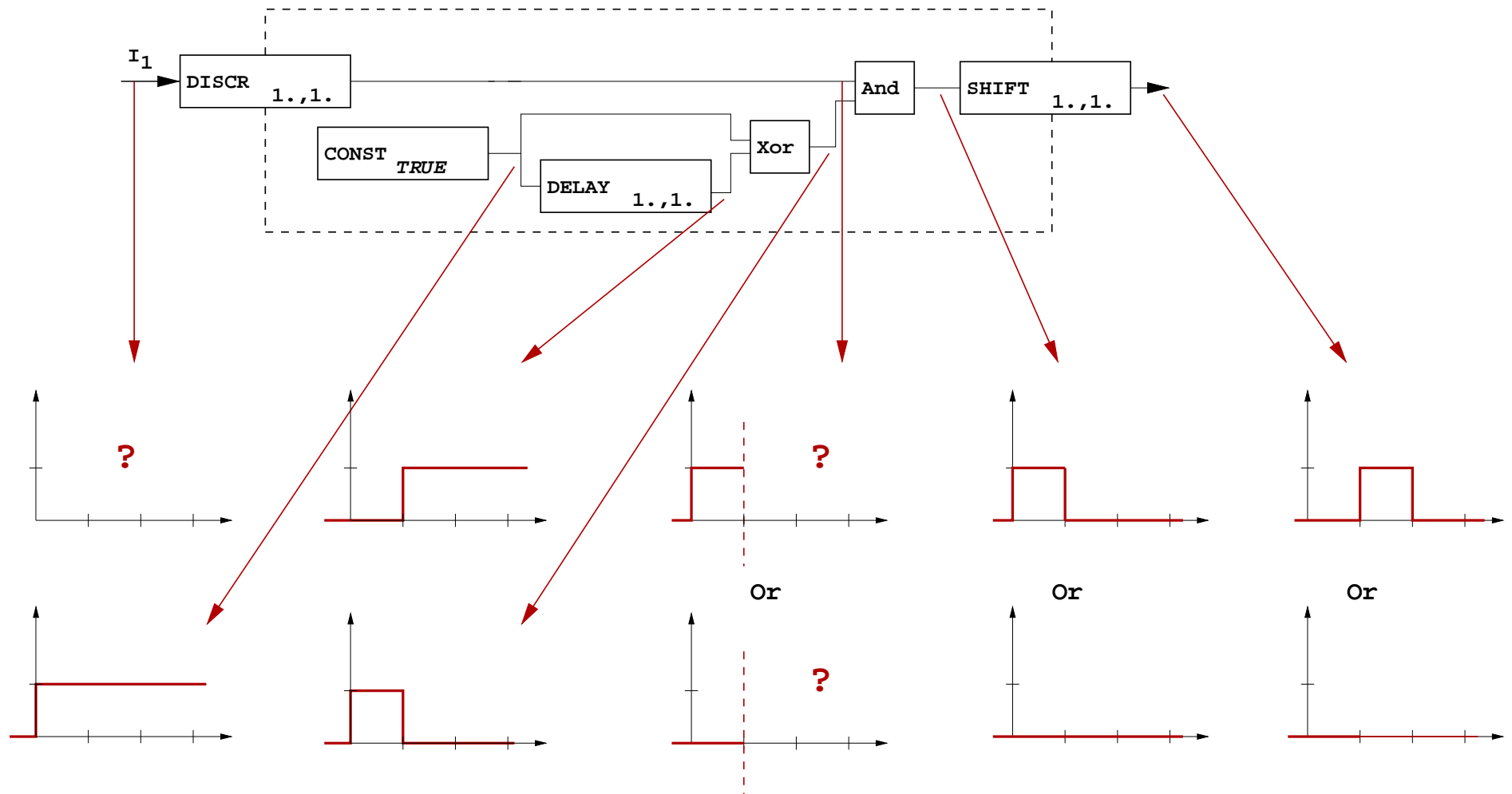
– $\llbracket D \rrbracket : V \rightarrow \mathcal{P}(\mathcal{S})$.

– $\llbracket D \rrbracket(v)$ is the **set of signals** u such that

$\forall w \in V \setminus \{v\}, \exists s_w$, such that $(u, s_{w_1}, \dots, s_{w_{\#V-1}})$

satisfies all the equations generated by the elements
of D .

Concrete semantics : example



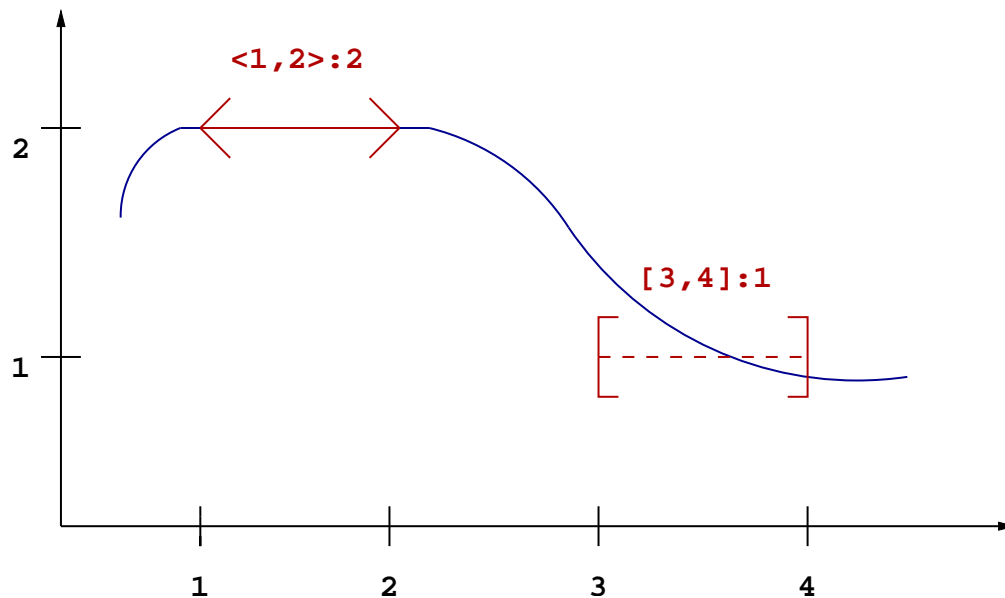
Plan

- Model : syntax and semantics
- **Abstraction**
- Analysis
- Simplification of concrete properties
- From concrete properties to abstract properties
- An example of analysis

Abstracting the signals

Constraints :

- A constraint $[a; b] : x$ forces signals to be equal to x **at least once** during $[a; b]$.
- A constraint $\langle a; b \rangle : x$ forces signals to be equal to x **during the whole** $[a; b]$.



Abstract set and concretization

- **The set of all constraints** is denoted by \mathcal{Z} .
- **Abstract set** : $V \rightarrow \mathcal{F}(\mathcal{Z})$. $\mathcal{F}(\mathcal{Z})$ is the set of expressions that use the constructors \wedge, \vee and \mathcal{Z} as atoms.

–

$$\dot{\gamma} = \left(\begin{array}{ll} \mathcal{Z} & \rightarrow \mathcal{P}(\mathcal{S}) \\ [a, b] : y & \mapsto \{x, \exists t \in [a, b], x(t) = y\} \\ \langle a, b \rangle : y & \mapsto \{x, \forall t \in [a, b], x(t) = y\} \end{array} \right)$$

Examples

- $\gamma(\{\emptyset\}) = \mathcal{S}$

- $$\gamma \left(\begin{array}{ccc} & & \langle 2, 3 \rangle : True \\ [0, 1] : True \quad \wedge \quad [0, 1] : False \quad \wedge & & \vee \\ & & \langle 2, 3 \rangle : False \end{array} \right)$$
$$= \left\{ \begin{array}{l} f : \mathbb{R} \mapsto \mathbb{B} \\ \text{changing its value between 0 and 1} \\ \text{but stable between 2 and 3} \end{array} \right\}$$

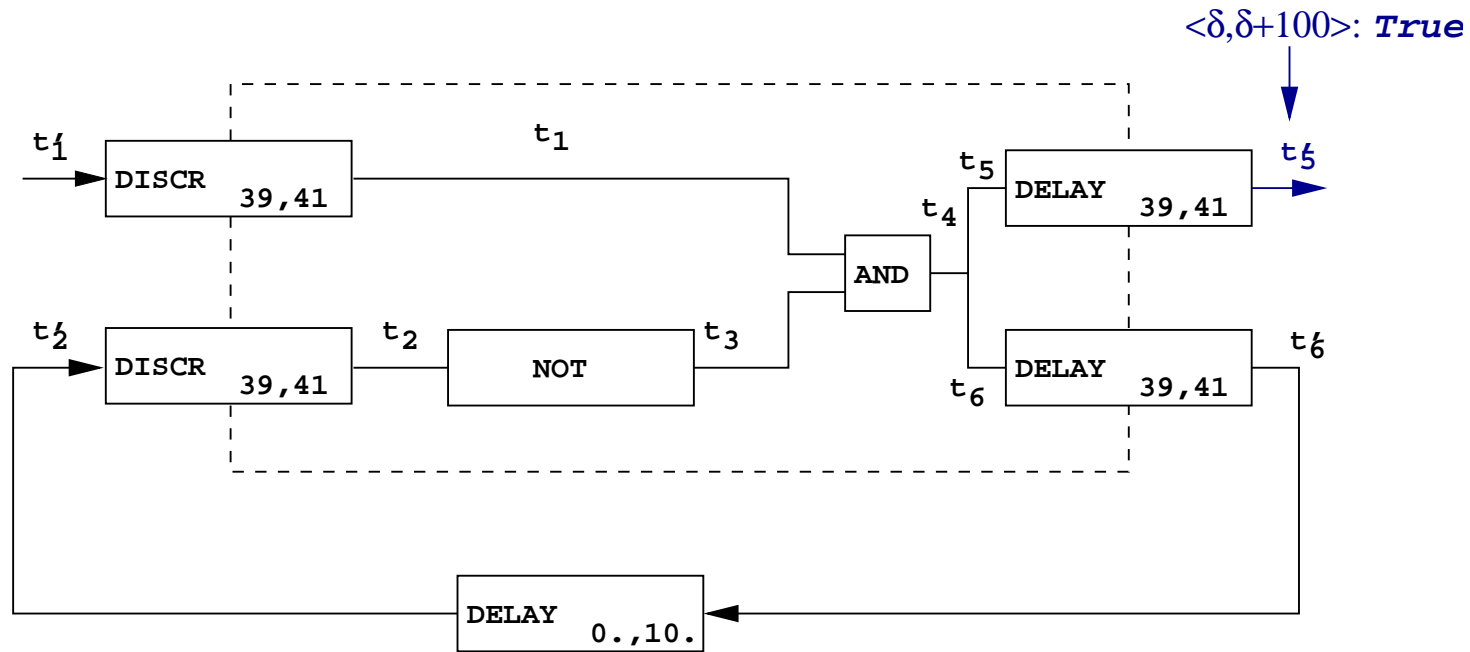
- signal s raises for more than 3 seconds without alarm a being raised in the next second :

$$s : \langle \delta, \delta + 3 \rangle : True \quad \wedge \quad a : \langle \delta + 3, \delta + 4 \rangle : False$$

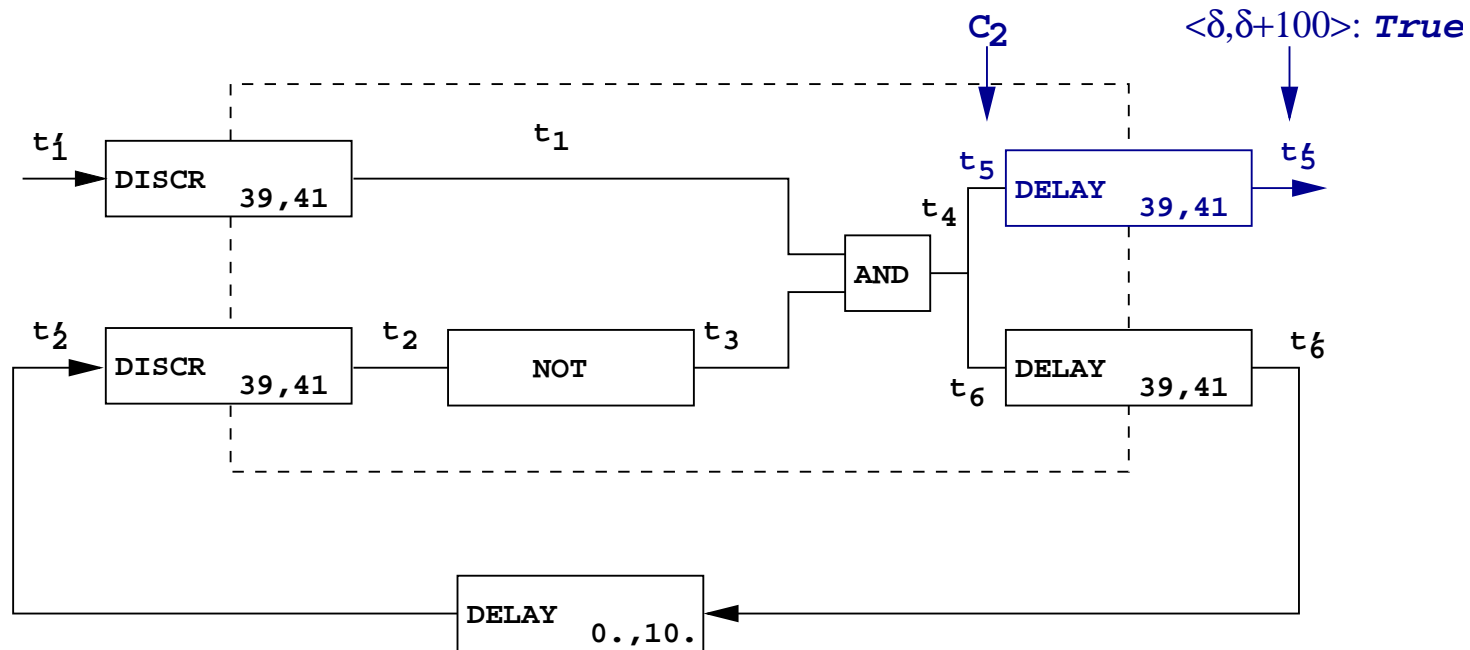
Plan

- Model : syntax and semantics
- Abstraction
- **Analysis**
- Simplification of concrete properties
- From concrete properties to abstract properties
- An example of analysis

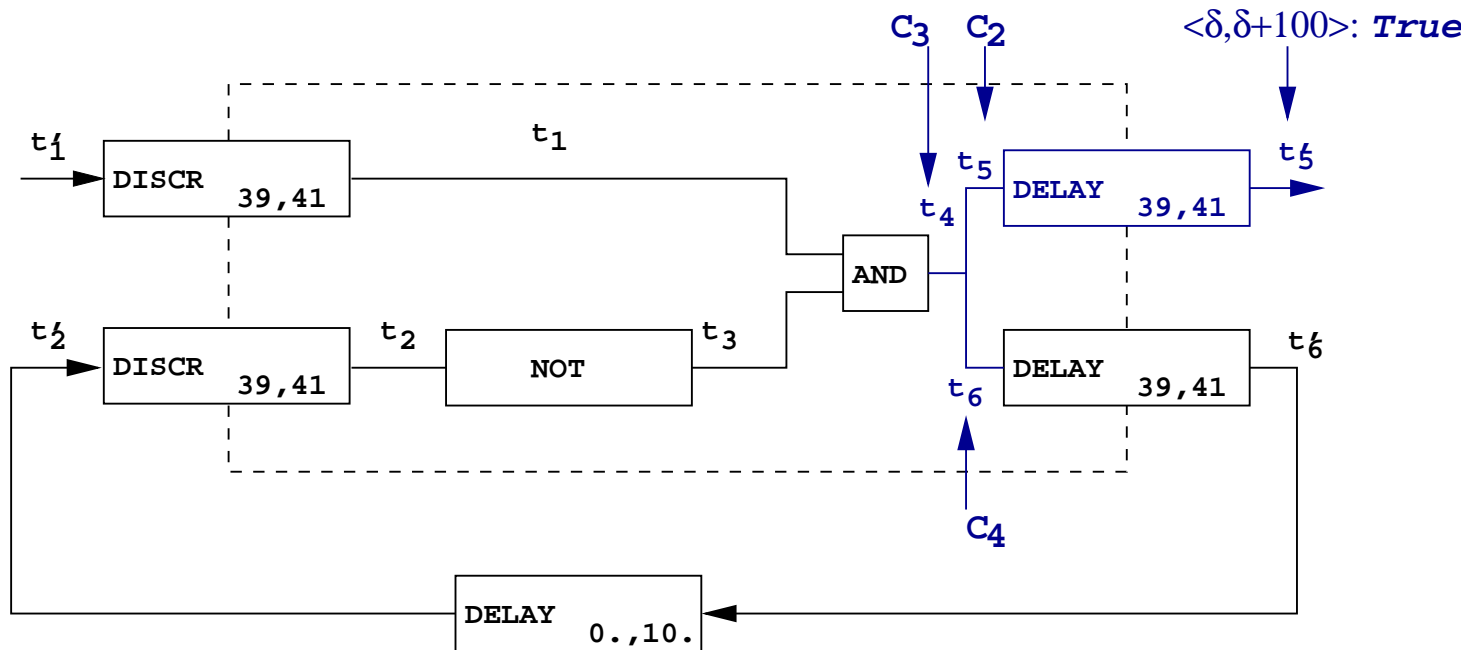
Omnidirectional analysis ?



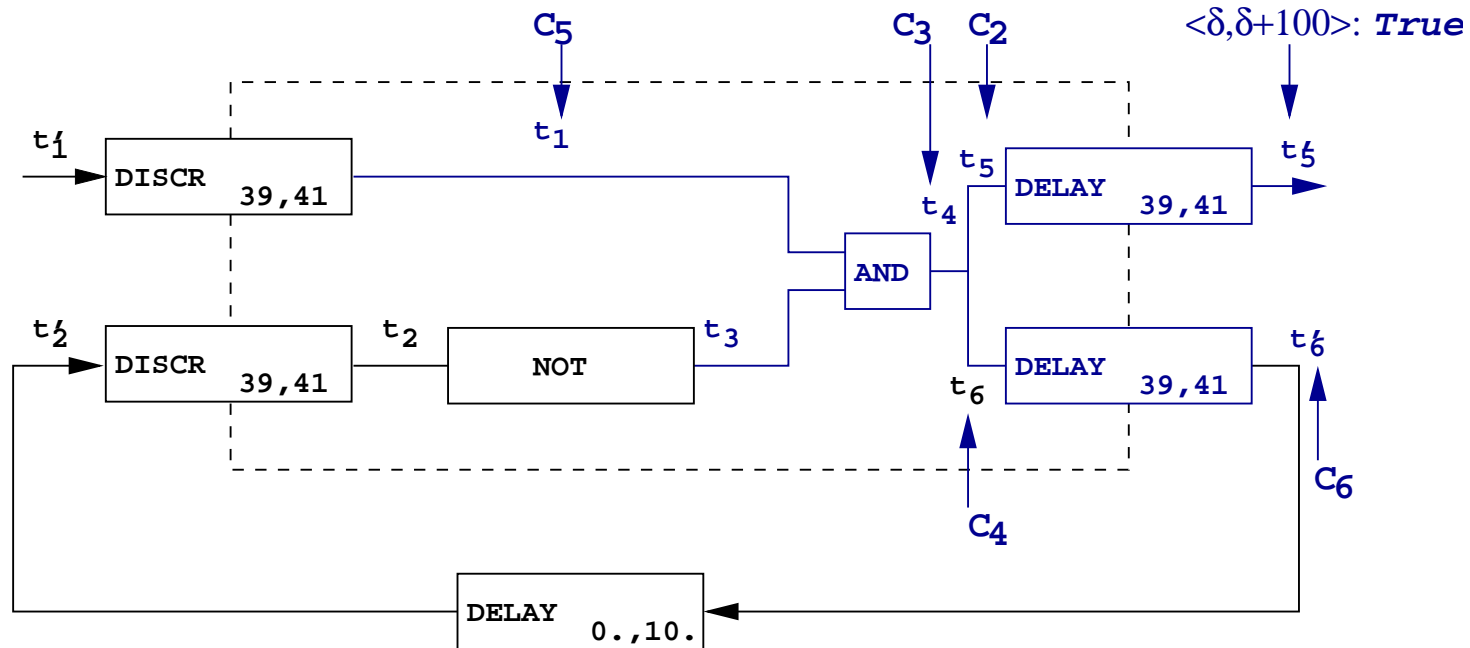
Omnidirectional analysis ?



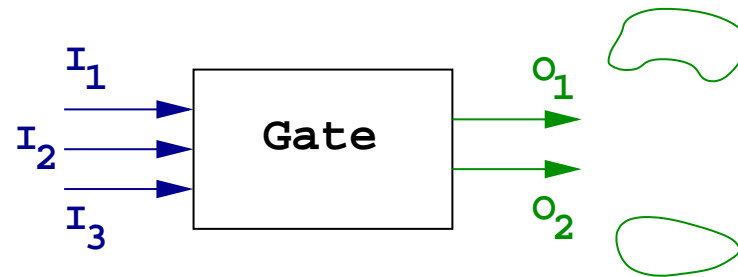
Omnidirectional analysis ?



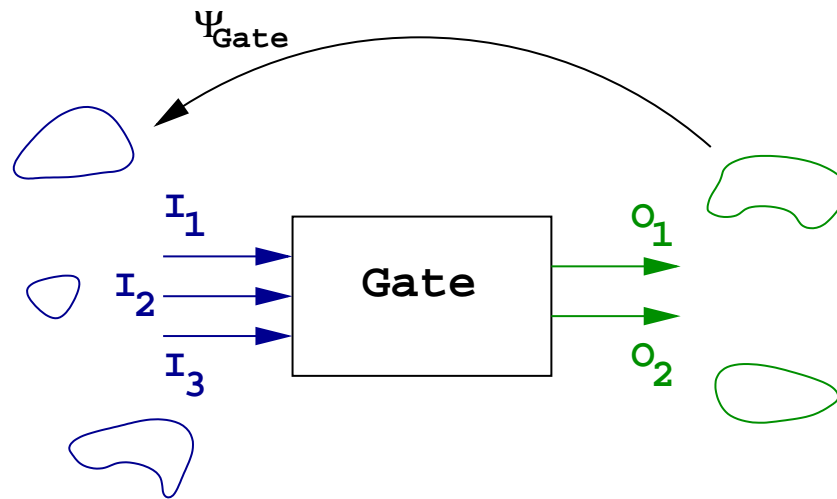
Omnidirectional analysis ?



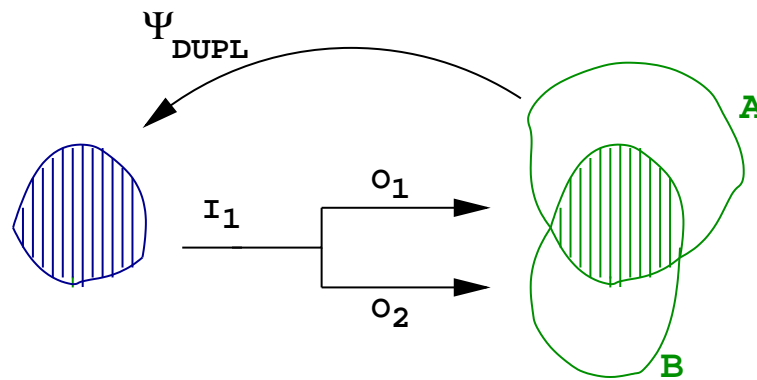
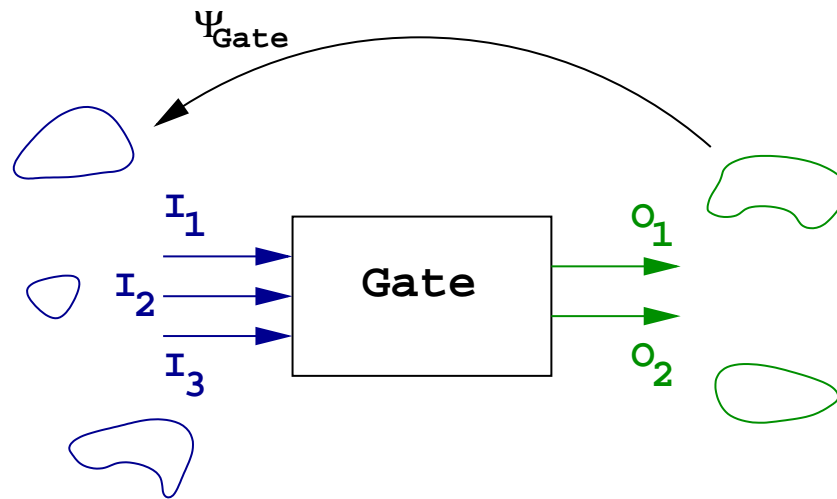
Concrete operators : backward analysis



Concrete operators : backward analysis



Concrete operators : backward analysis

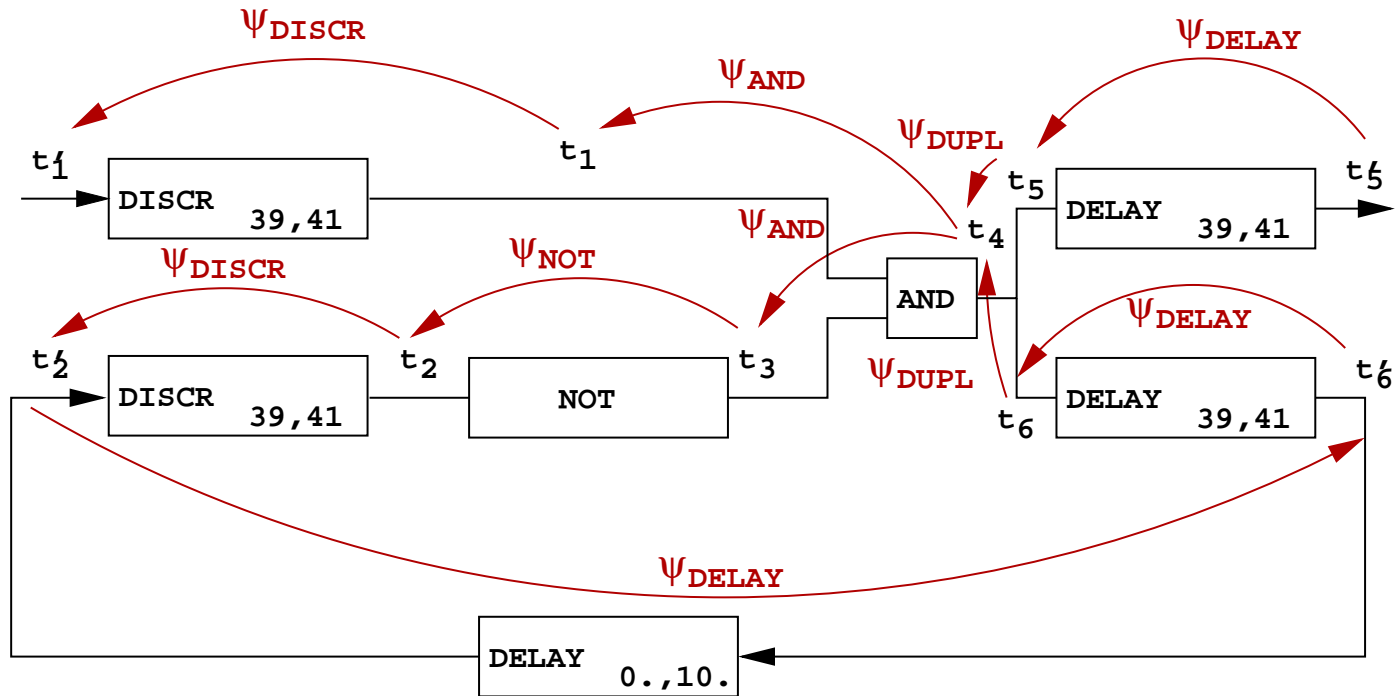


$$\Psi_{\text{DUPL}}(A, B) = A \cap B$$

Plan

- Model : syntax and semantics
- Abstraction
- Analysis
- **Simplification of concrete properties**
- From concrete properties to abstract properties
- An example of analysis

Coding a diagram with an operator



$$\llbracket D \rrbracket \subseteq \Psi(\llbracket D \rrbracket)$$

Expressing properties as fixpoints

– **Former goal** : Prove that $\forall t \in \llbracket D \rrbracket$, t satisfies P .

let $Z_{\neg P} : V \rightarrow \mathcal{P}(\mathcal{S})$ set of signals that doesn't satisfy P .

– **Now** : $A \triangleq \llbracket D \rrbracket \cap Z_{\neg P} \subseteq \text{gfp}_{Z_{\neg P}}(\Psi \cap Id)$

– **New stronger goal** : $\text{gfp}_{Z_{\neg P}}(\Psi \cap Id) = \emptyset$

Plan

- Model : syntax and semantics
- Abstraction
- Analysis
- Simplification of concrete properties
- **From concrete properties to abstract properties**
- An example of analysis

From concrete properties to abstract properties

If

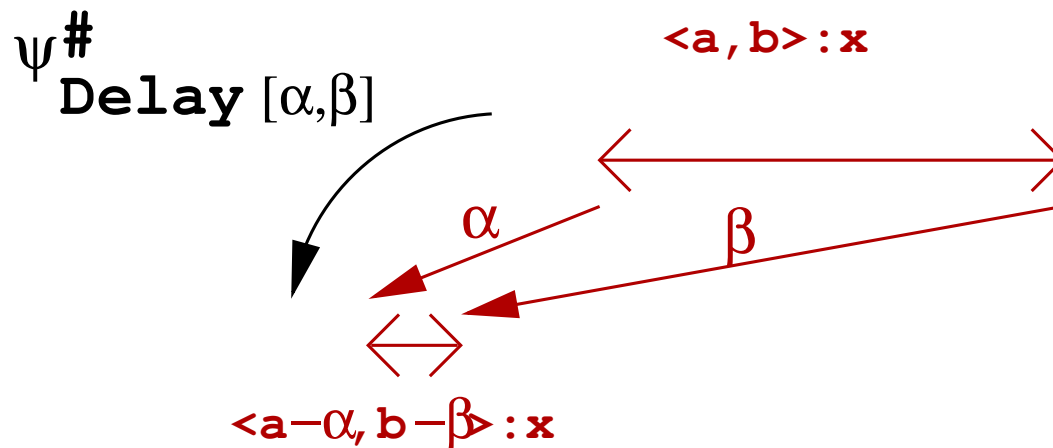
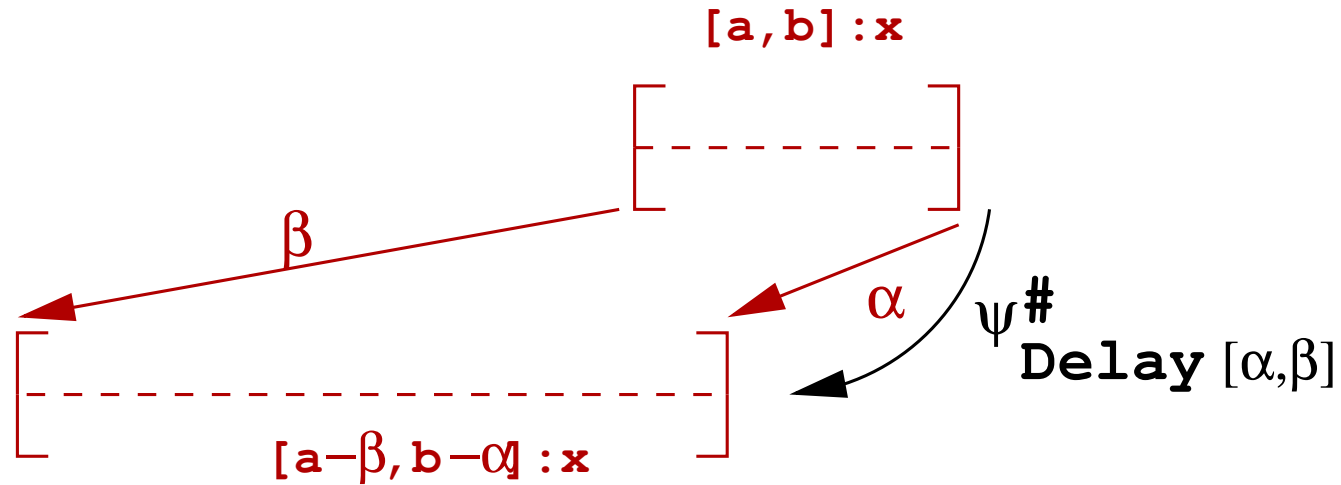
$$F \circ \gamma \subseteq \gamma \circ F^\#$$

then :

$$\text{gfp}F \subseteq \gamma(\text{gfp}F^\#)$$

- **New even stronger goal** : $\text{gfp}_{Z \rightarrow P}(\Psi^\# \cap^\# Id^\#) = \emptyset$

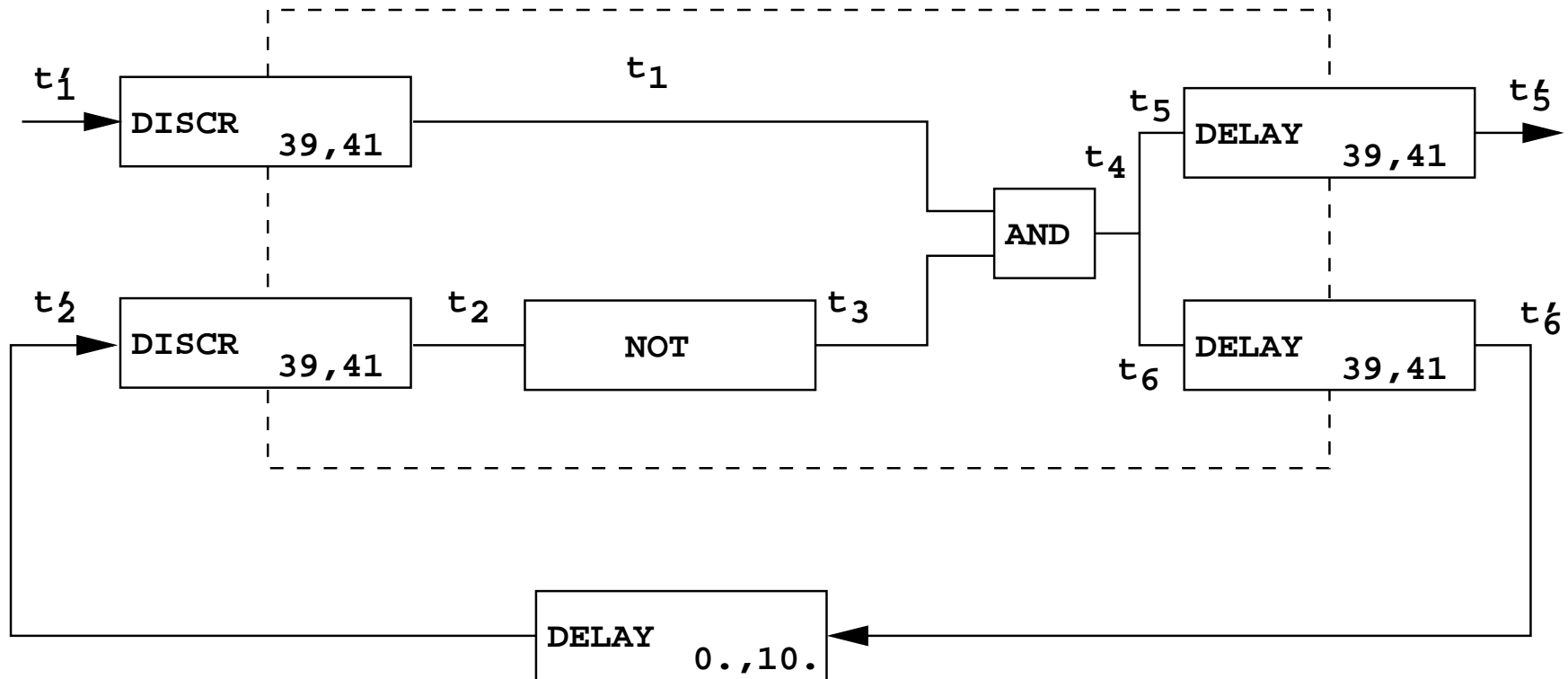
Abstract operators



Plan

- Model : syntax and semantics
- Abstraction
- Analysis
- Simplification of concrete properties
- From concrete properties to abstract properties
- **An example of analysis**

Example

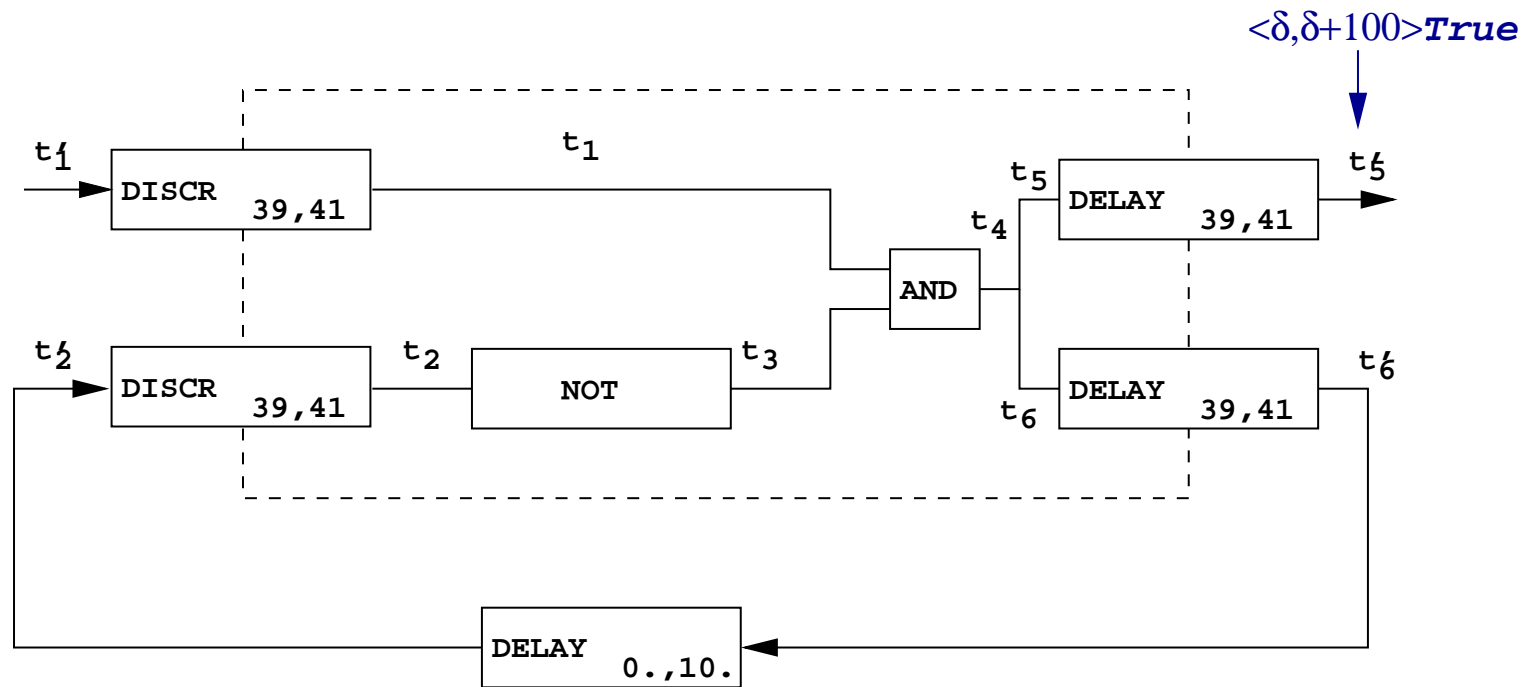


Example : property to prove

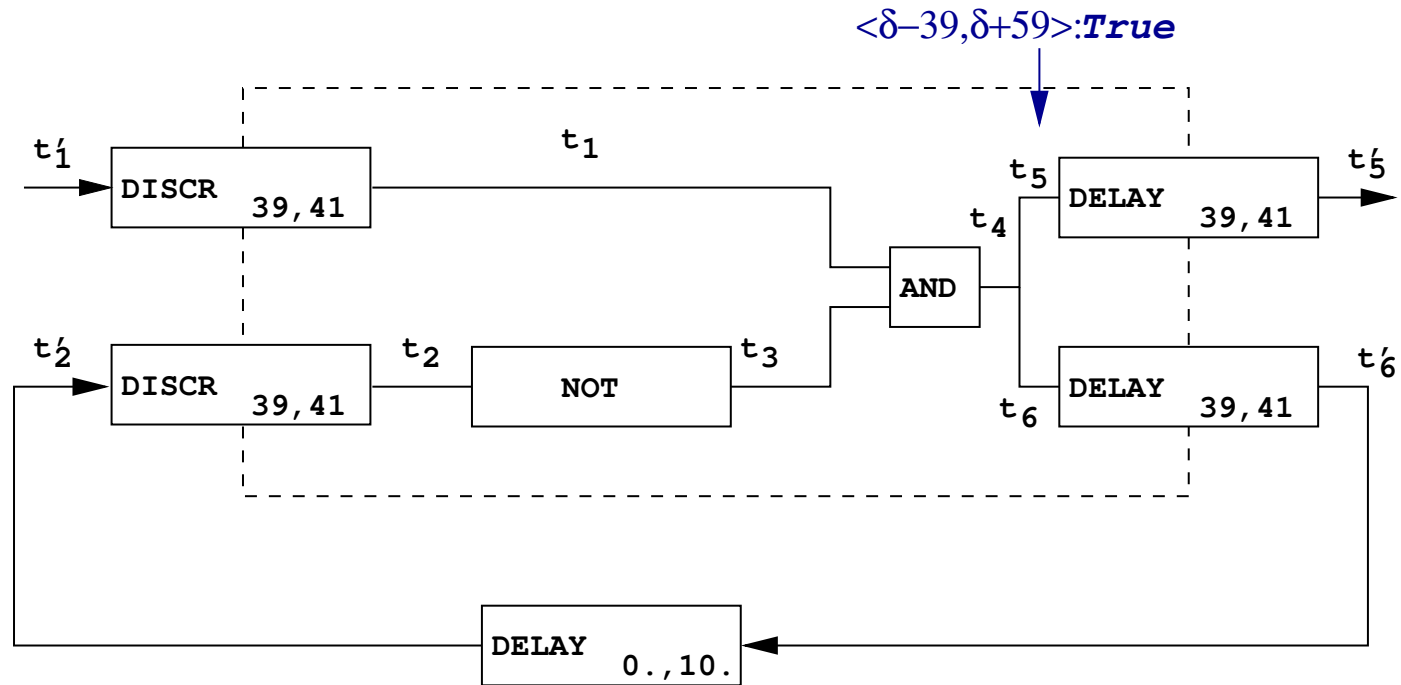
$\mathbf{P} : \exists t \in [\delta, \delta + 100], ((\llbracket \mathbf{D} \rrbracket) t'_5)(t) \neq \mathbf{True}$

$\mathbf{Z}_{\neg \mathbf{P}}^\# = \langle \delta, \delta + 100 \rangle : \mathbf{true}$

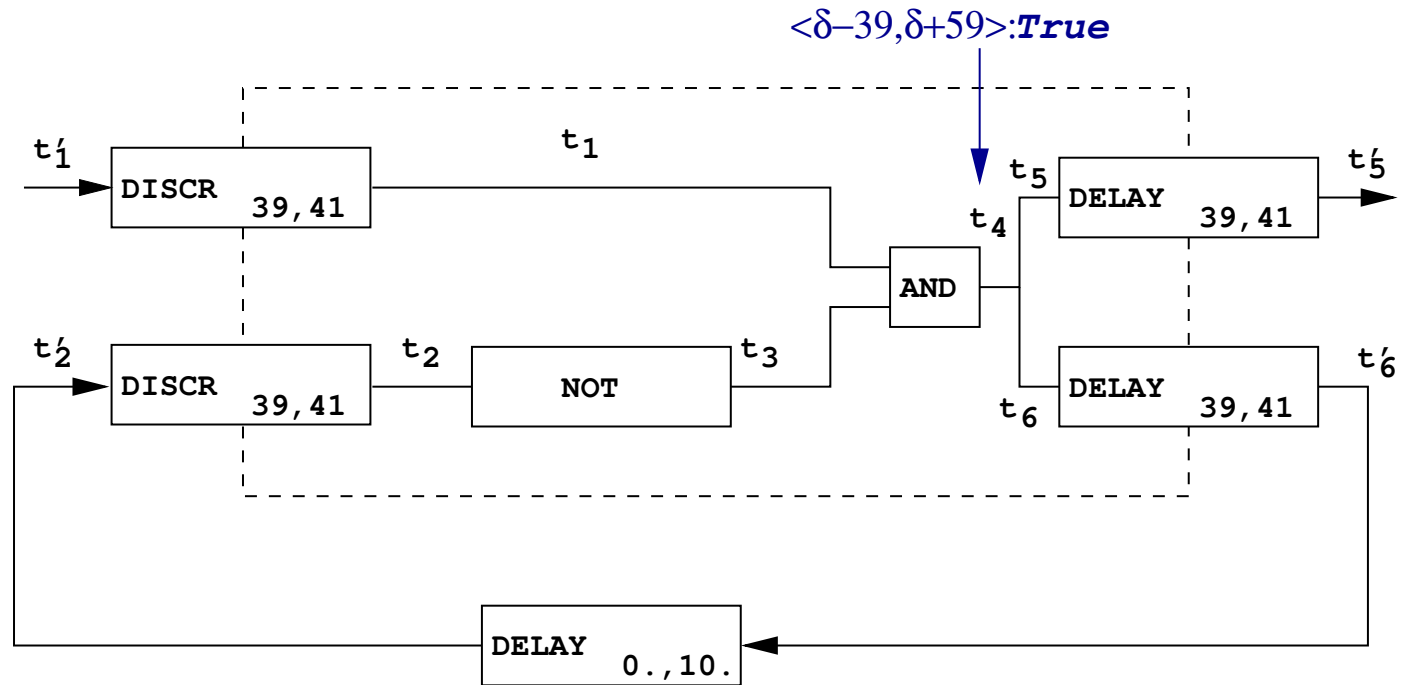
Example : Iterating to the fixpoint



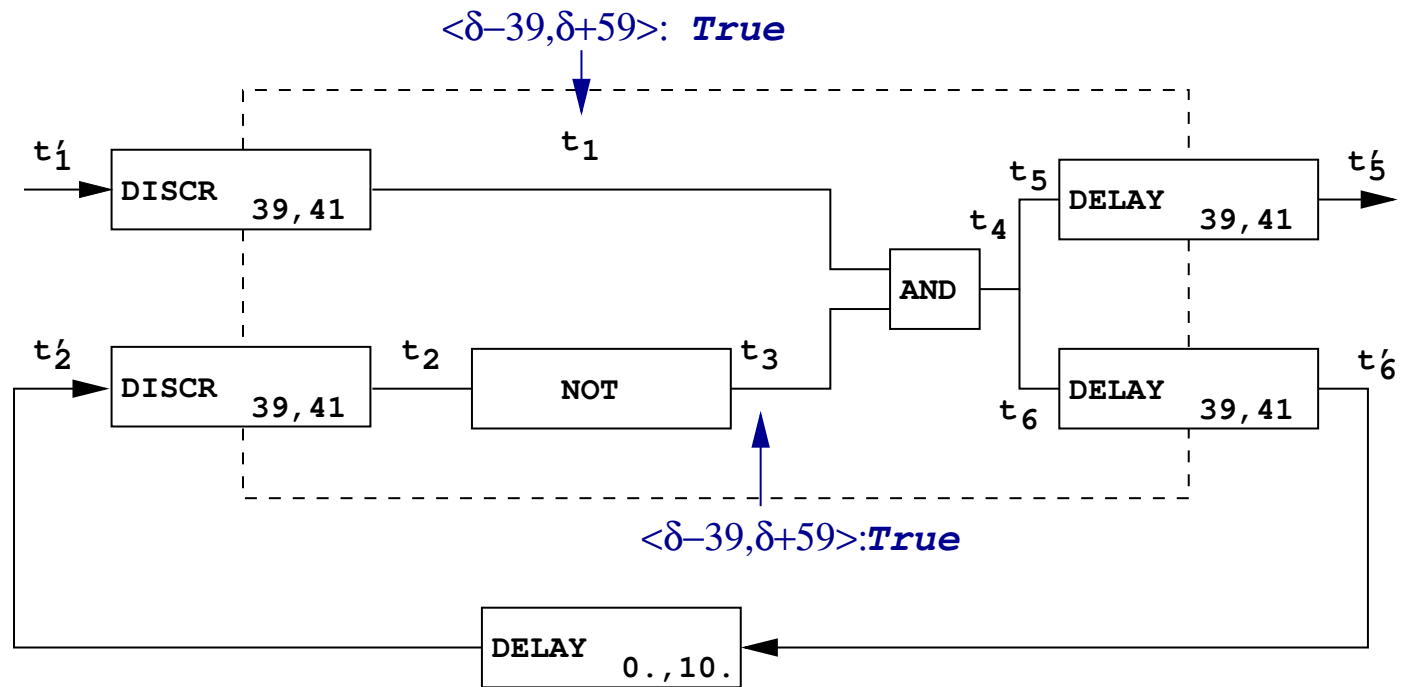
Example : Iterating to the fixpoint



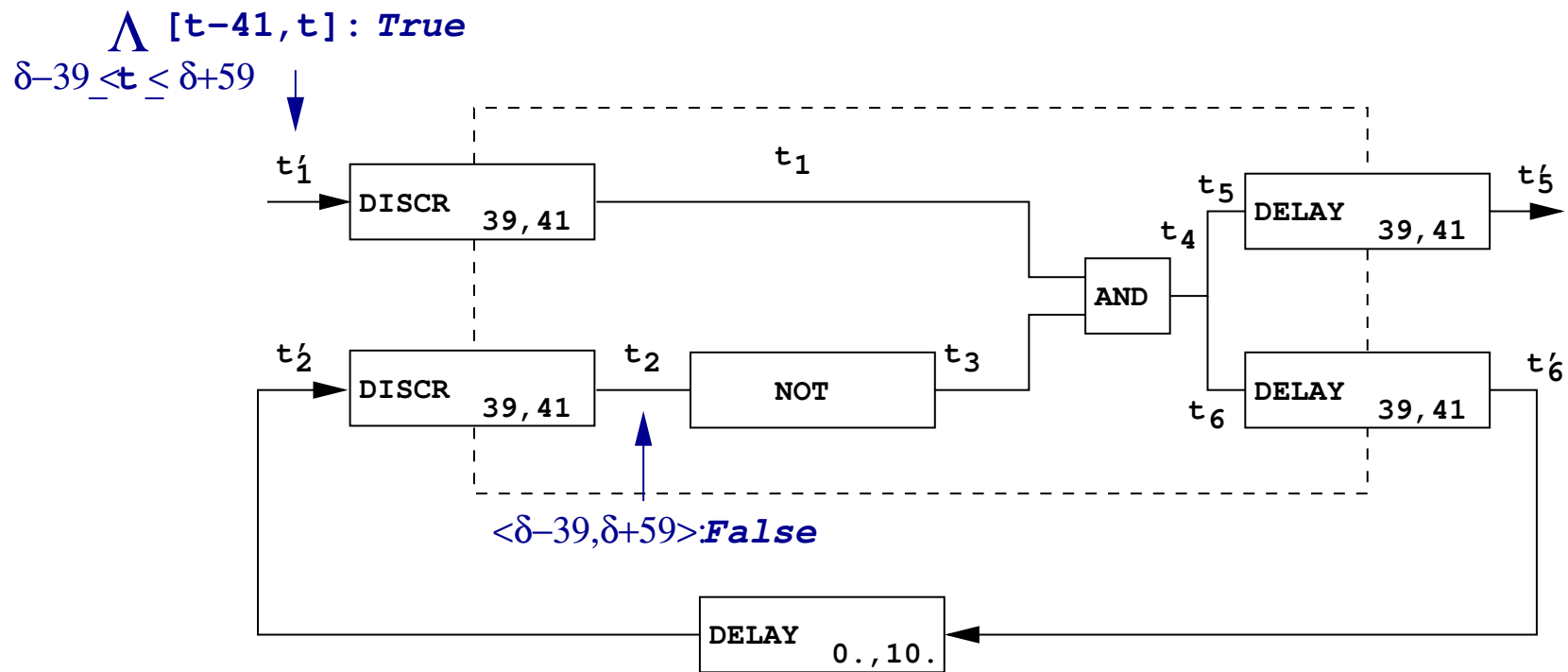
Example : Iterating to the fixpoint



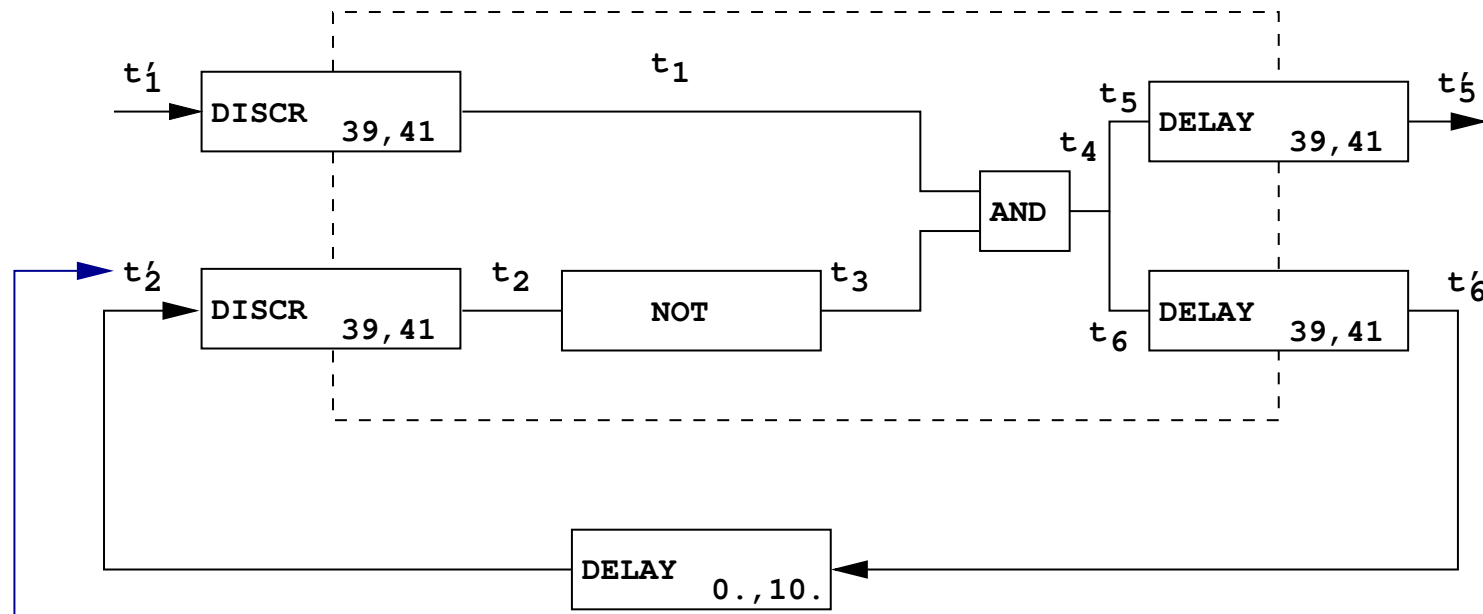
Example : Iterating to the fixpoint



Example : Iterating to the fixpoint

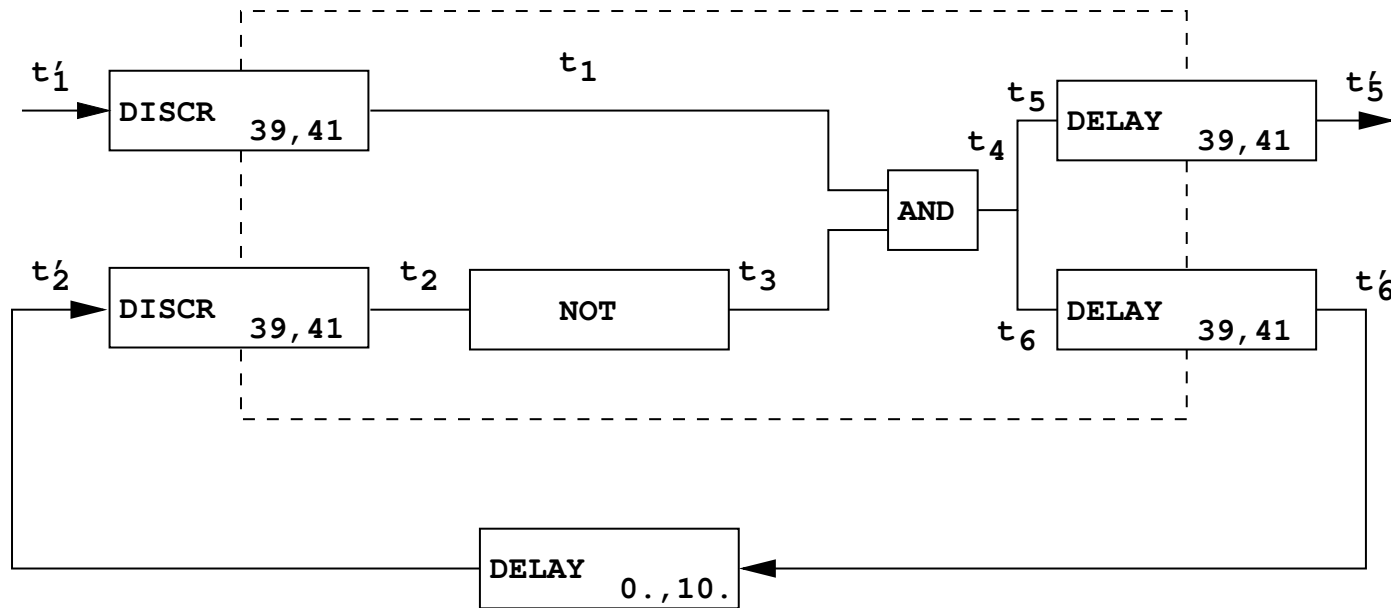


Example : Iterating to the fixpoint



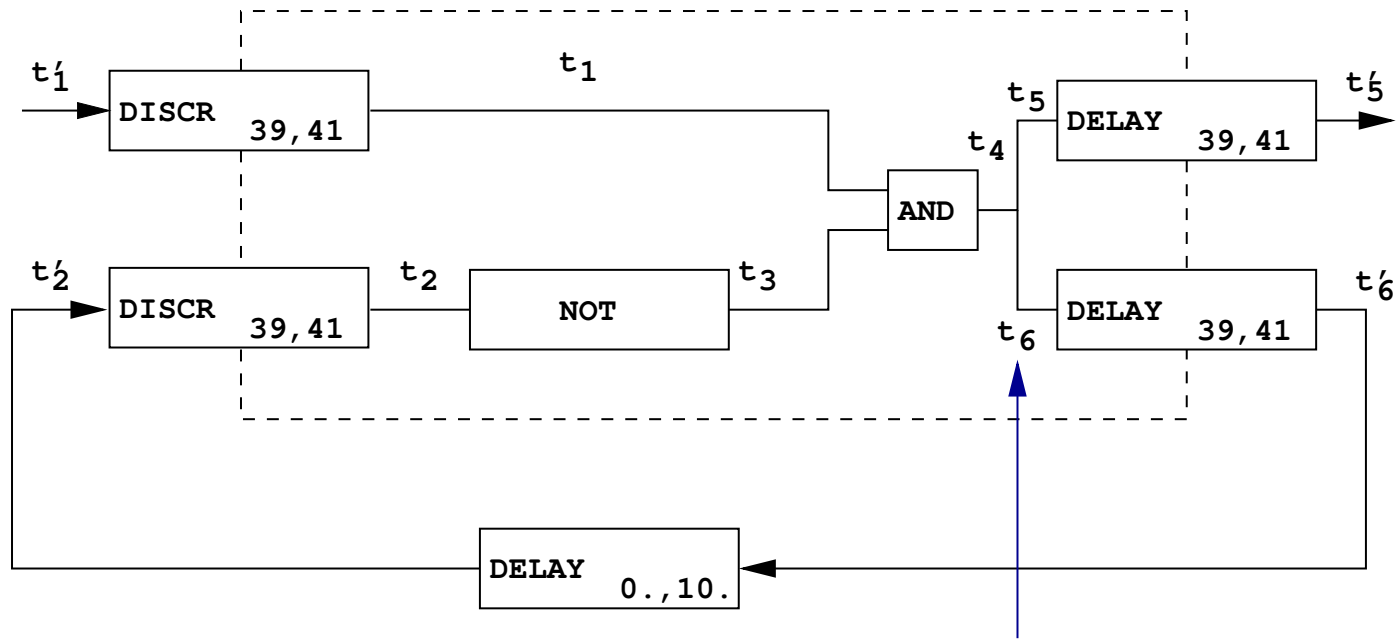
$\bigwedge [t-41, t]: \text{False}$
 $\delta-39 \leq t \leq \delta+59$

Example : Iterating to the fixpoint



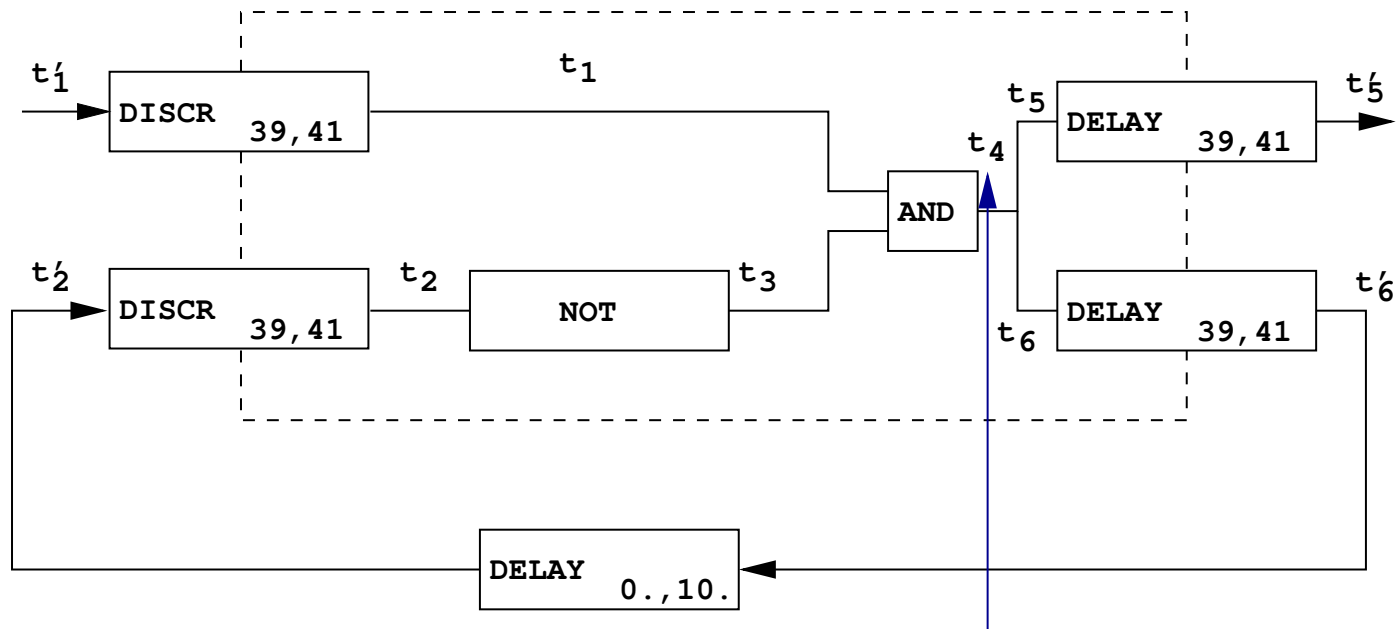
$\wedge [t-51, t] : \text{False}$
 $\delta-39 \leq t \leq \delta+59$

Example : Iterating to the fixpoint



$\wedge [t-92, t-39]: \text{False}$
 $\delta-39 \leq t \leq \delta+59$

Example : Iterating to the fixpoint



$\wedge [t-92, t-39]: \text{False}$
 $\delta-39 \leq t \leq \delta+59$

Example : Result

Signal must satisfy at point of control t_4 :

$$\langle \delta - 39, \delta + 59 \rangle : \textit{True} \textbf{ and} \bigwedge_{\delta - 39 \leq t \leq \delta + 59} ([t - 92, t - 39] : \textit{False})$$

which entails $[\delta - 33_{=\delta+59-92}, \delta + 20_{=\delta+59-39}] : \textit{False}$

Conclusion

- **Continuous-time semantics** instead of classical discrete one (PC, Message passing,...)
- **Not complete** : undecidable
- **Relational domain** used in order to improve abstract operators
- **Future work** : ASTRÉE presently certifies one synchronous unit of fly-by-wire system. Our goal : certify that the redundancy (several units) brings more security.