On reduced forms of initialized Finite State Machines with timeouts

Speaker: Aleksandr Tvardovskii

E-mail: tvardal@mail.ru

Authors: [1]Aleksandr Tvardovskii, [2]Nina Yevtushenko

[1]National Research Tomsk State University
[2]Institute for System Programming of the Russian Academy of Sciences)

Minimization problem in FSM theory

Finite State Machines (FSM)

- There exist approaches for state minimization
- Minimal form is unique up to isomorphism

Motivation

- The complexity of solving many problems depends on the number of states of an FSM
- Existing the canonical form of a model usually simplifies solving a number of problem

Timed FSM motivation

Timed aspects can be important for nowadays systems

- Timeout disconnection in telecommunication protocols
- Temporary encryption key reset
- Sleep mode

Server can disconnection when a client does not respond within a given timeout

- How to derive a minimal form for TFSMs?
- Is such minimal form unique up to isomorphism?

Finite State Machine (FSM)

- FSM has finite non-empty sets of states, inputs and outputs
- FSM moves from state to state and produces an output when an input is applied
- FSM describes the behavior of a system w.r.t. infinite number of input sequences in a finite way

FSM with timeouts

TFSM S is 5-tuple $(S, s_0, I, O, \lambda_S, \Delta_S)$

- S, I and O are finite non-empty sets of states, inputs and outputs
- s_0 is the initial state
- $\lambda_S \subseteq S \times I \times O \times S \times D$ is a transition relation
- Δ_S is a timeout function

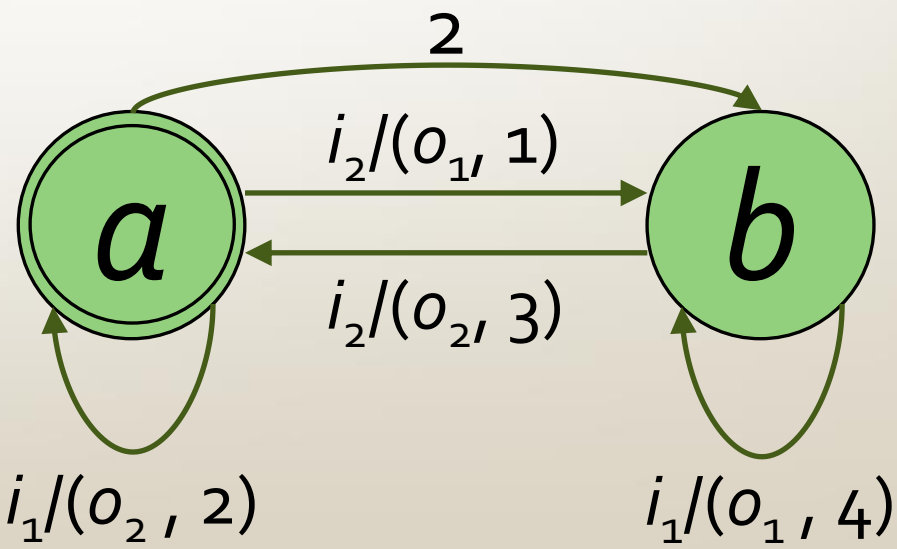
Example:

$S = \{a, b\}$, $I = \{i_1, i_2\}$ and $O = \{o_1, o_2\}$

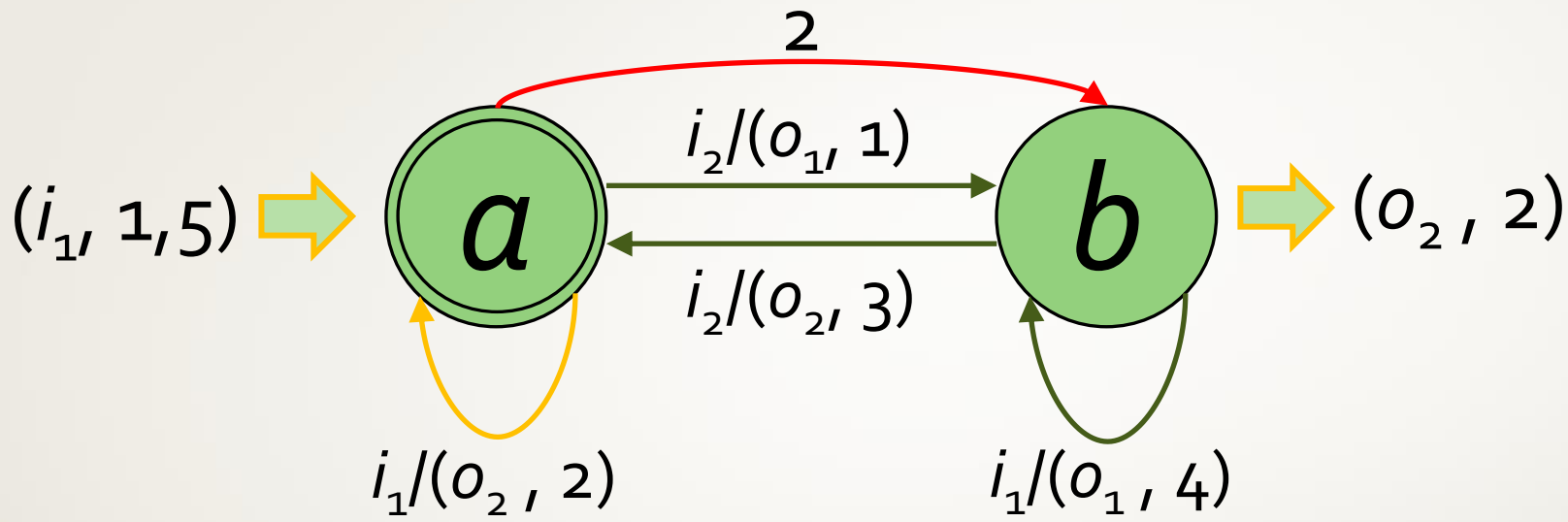
$\lambda_S = \{(a, i_1, o_2, a, 2), (a, i_2, o_1, b, 1),$

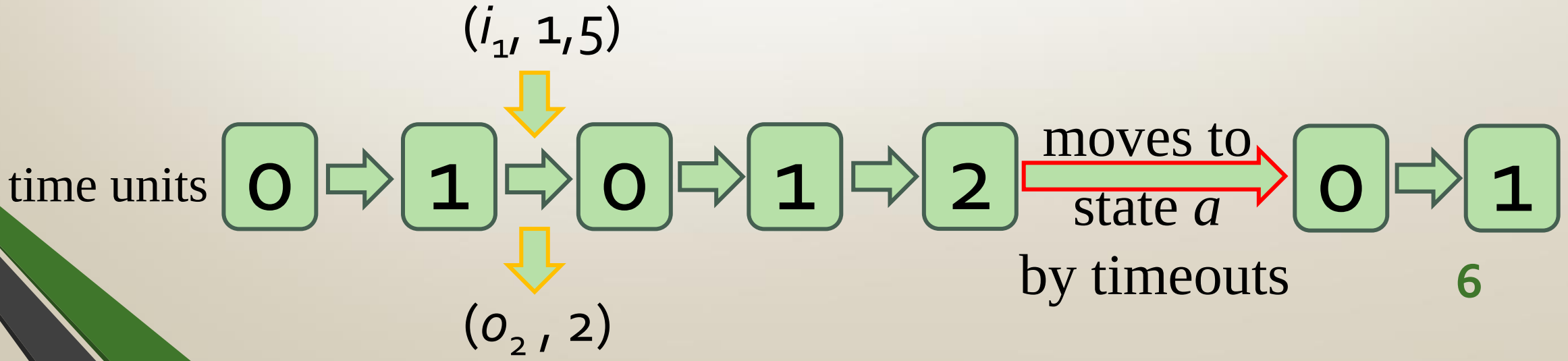
$(b, i_1, o_1, b, 4), (b, i_2, o_2, a, 3)\}$

$\Delta_S(a) = (2, b)$ $\Delta_S(a) = (\infty, b)$



Timed inputs





Timed sequences

Timed input sequence

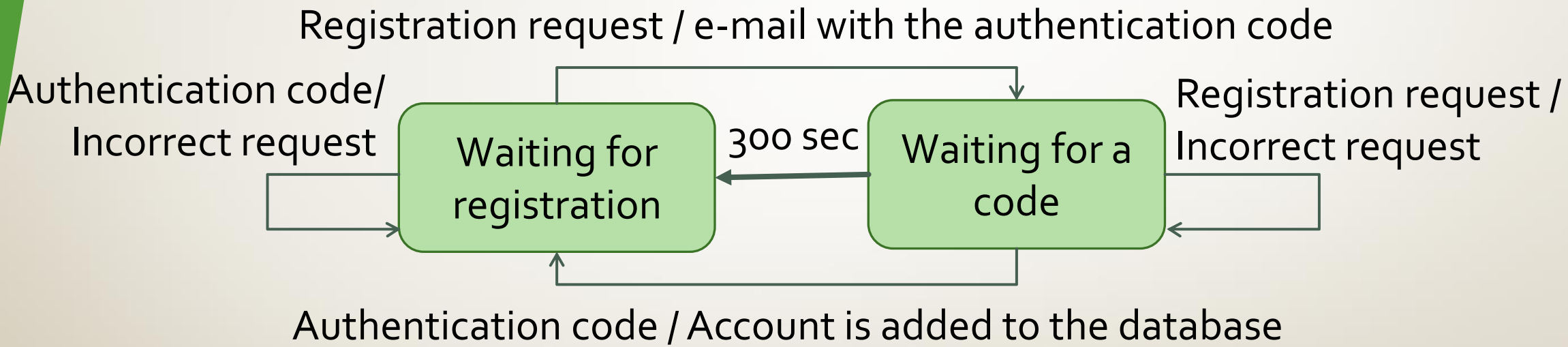
$(i_1, t_1), (i_2, t_2), \ldots (i_n, t_n)$

Timed output sequence

$(o_1, \theta), (o_2, \theta), \ldots (o_n, \theta)$

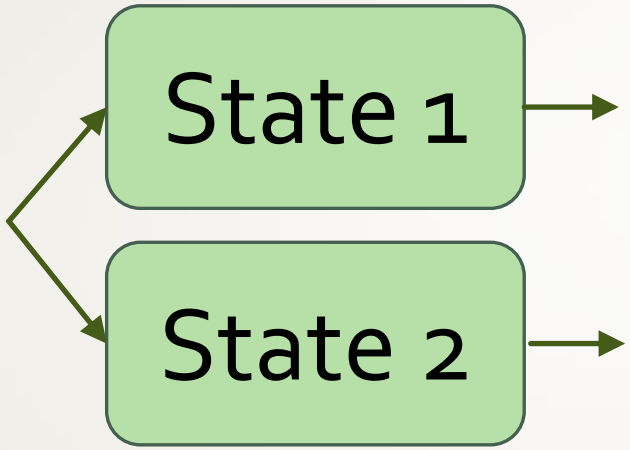
S is a deterministic complete (Timed) FSM if for each pair $(s, i) \in S \times I$, there is exactly one transition $(s, i, o, s') \in h_S$

Registration system with timeout



Equivalence relation for deterministic complete TFSMs

Input (*timed*) *sequence*



If the output responses coincide to each (timed) input sequence

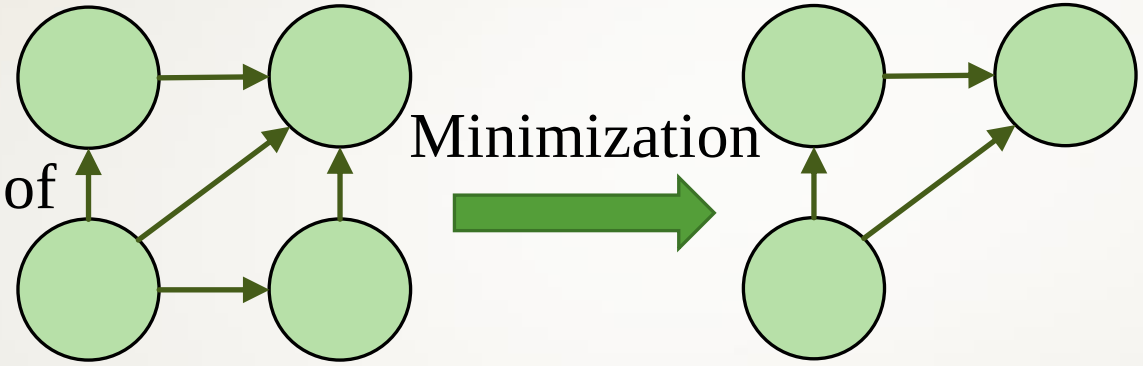
then states are *equivalent*

otherwise, states are *distinguishable*

- Initialized (Timed) FSMs S and P are equivalent (S ≅ P) if their initial states are equivalent ($s_0 \cong p_0$)

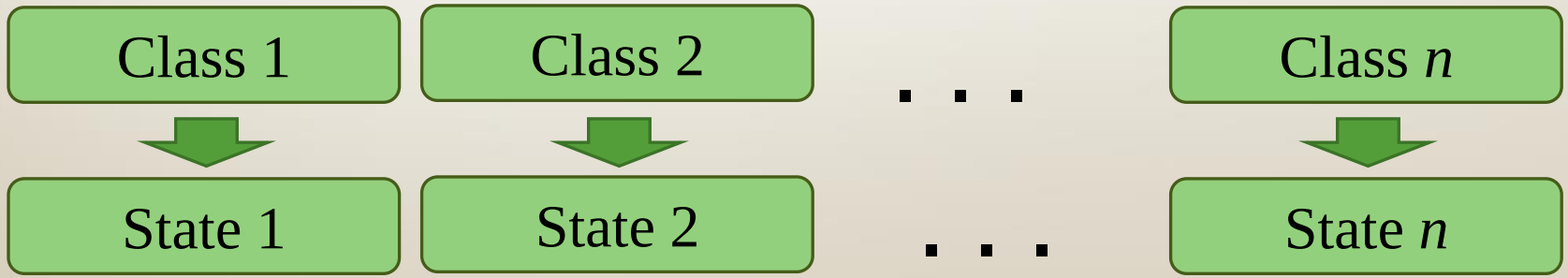
State minimization

Finite State Machine
There can exist pairs of equivalent states



Minimal form of FSM
Every two different states are distinguishable

Partition into equivalent states



States of reduced (minimal) form for FSM

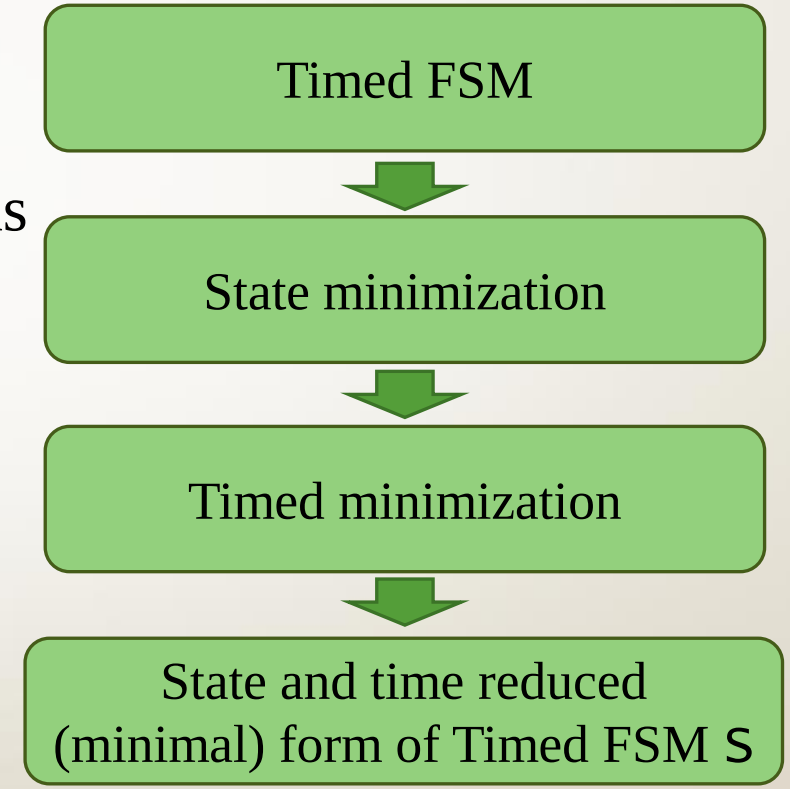
Minimization for non-initialized TFSMs

In order to derive a time reduced form

1. Each timeout should be set to minimum value
2. Transitions under the same input where timed guards can be merged should be replaced by a single transition

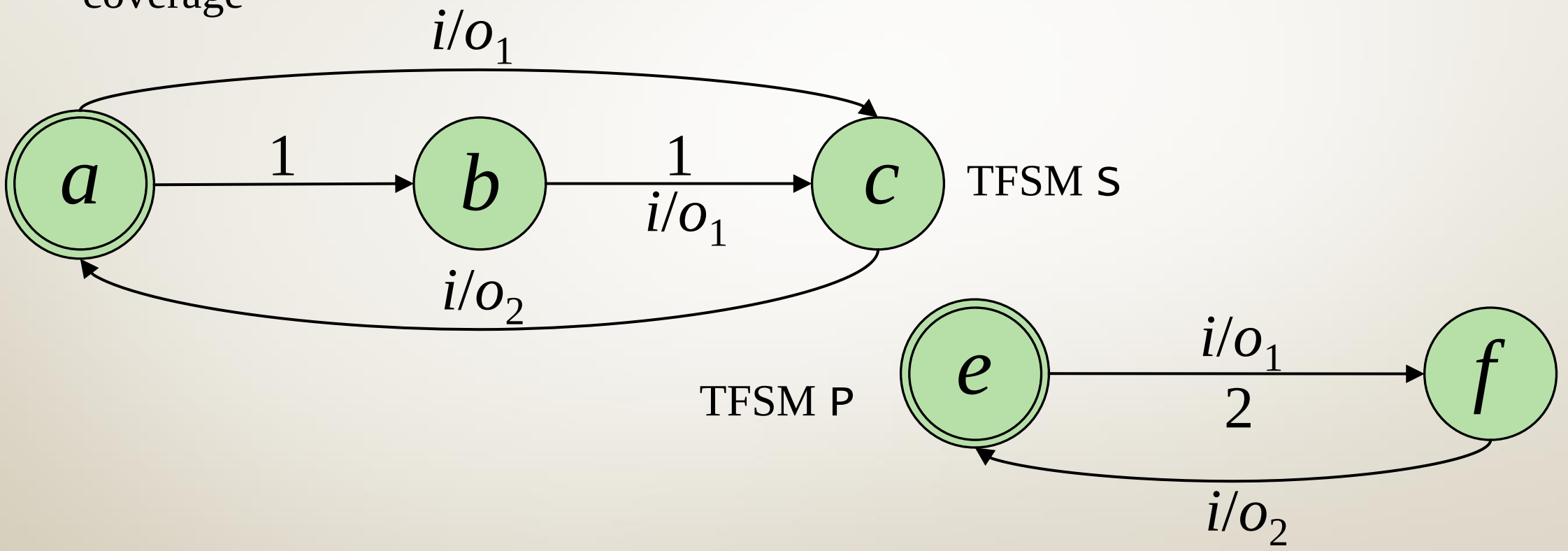
Two non-initialized deterministic complete state and time reduced TFSMs are equivalent if and only if they are isomorphic.

Corollary. The minimal form of a non-initialized Timed FSM is unique up to isomorphism



Initialized Timed FSMs

- Initialized Timed FSMs are widely used in testing with guaranteed fault coverage

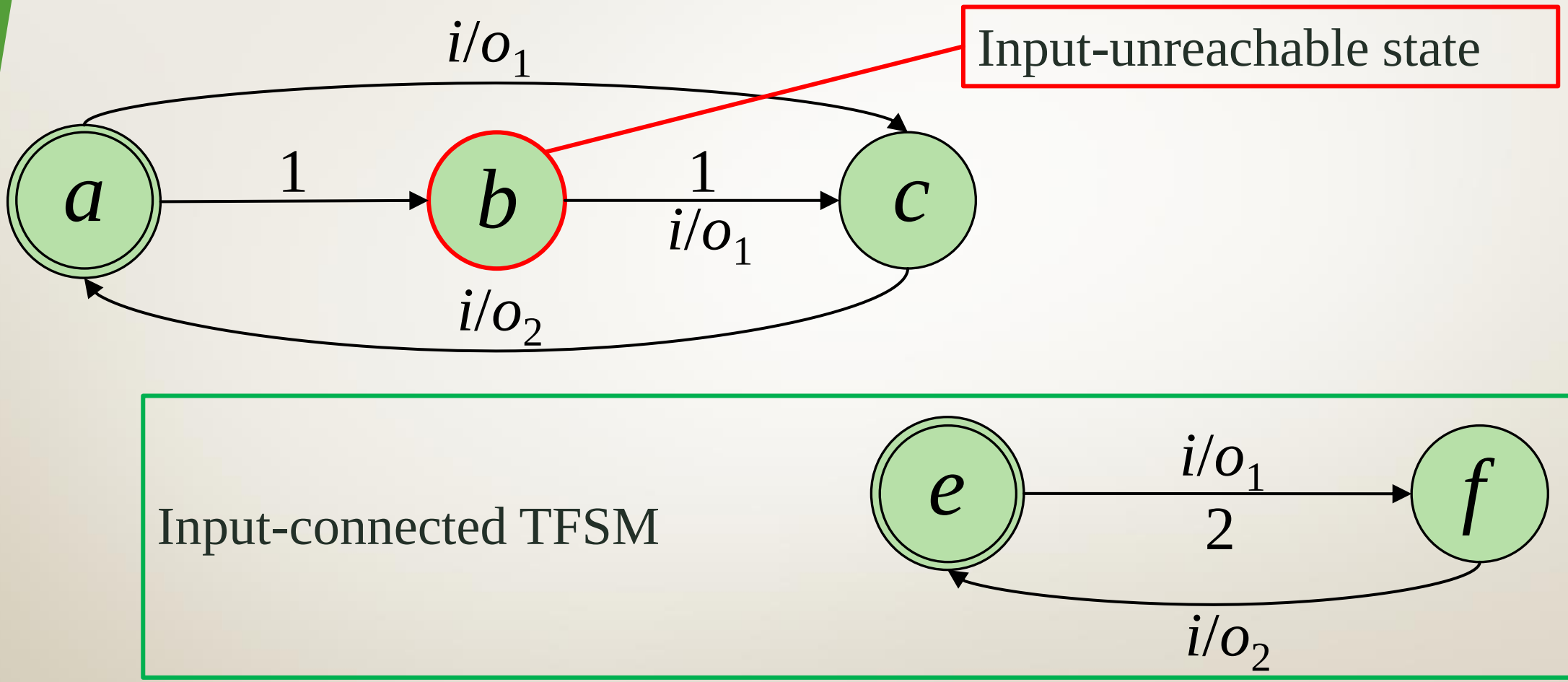


- Initial states *a* and *e* of TFSMs S and P are equivalent, but S and P are not isomorphic

Input-connected FSM with timeouts

- State *s* of TFSM S is ***input-reachable*** if there exists an input sequence which takes the TFSM from the initial state to state *s*, otherwise *s* is ***input-unreachable***
- If an input-unreachable state *s* is reachable from input-reachable state *s* only by timeout then *s* is ***time-reachable***
- An FSM with timeouts S is ***input-connected*** if each state $s \in S$ is input-reachable

Initialized Timed FSMs



- One to one correspondence can be established between states of two equivalent state reduced input connected TFSMs

Input-connected FSM with timeouts

Proposition. Two deterministic complete state and time reduced initialized input-connected FSMs with timeouts are equivalent if and only if they are isomorphic

Minimal form for input-connected FSM with timeouts is unique up to isomorphism

BUT: there exist TFSMs for which an equivalent input-connected FSM with timeout cannot be derived

FSM with timed guards

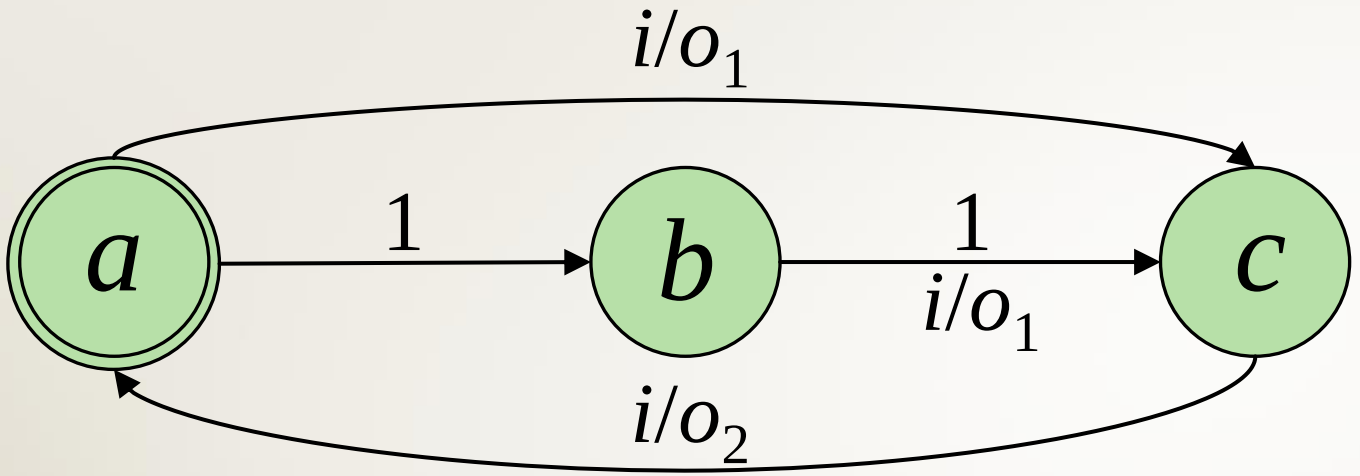
Timed Finite State Machine $\mathsf{S} = (S, s_0\, I, O, \lambda_S)$

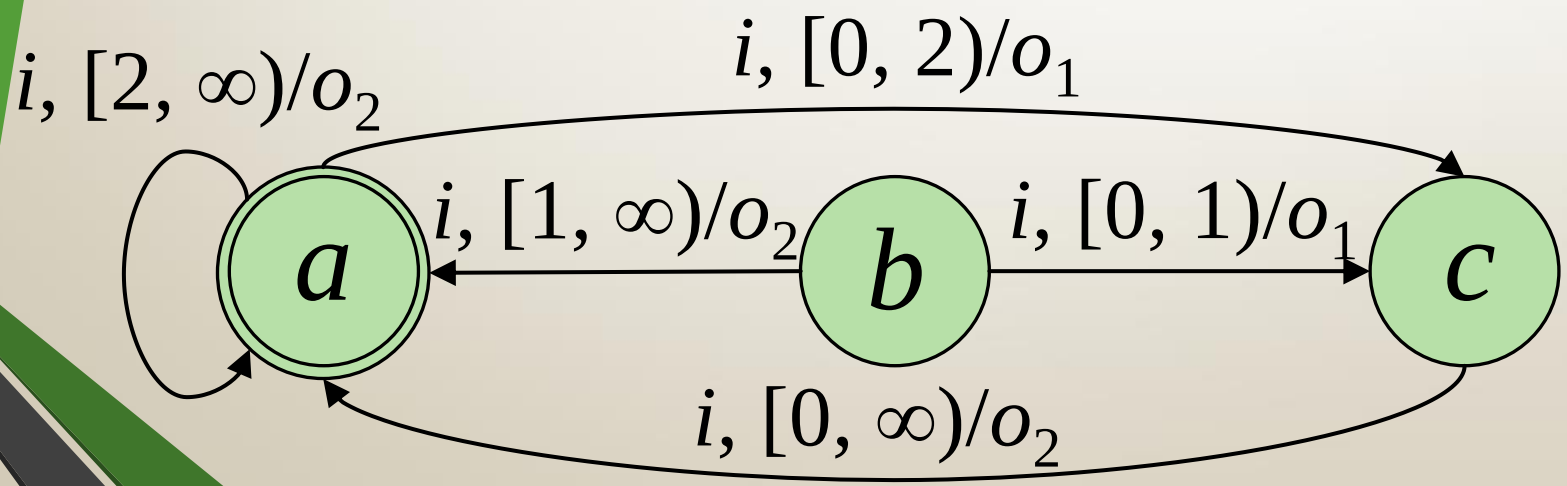
- S, I and O – finite non-empty sets of states, inputs and outputs, s_0 – initial state
- $\lambda_S \subseteq S \times I \times O \times S \times \Pi \times Z$ – transition relation
  - Z – set of output delays (output timeouts)
  - Π – set of timed guards (input timed intervals) from interval $[0; \infty)$

Known results

- FSMs with timeouts which can be represented by a corresponding FSM with timed guards
- Two deterministic complete time and state reduced initialized connected FSMs with timed guards are equivalent if and only if they are isomorphic

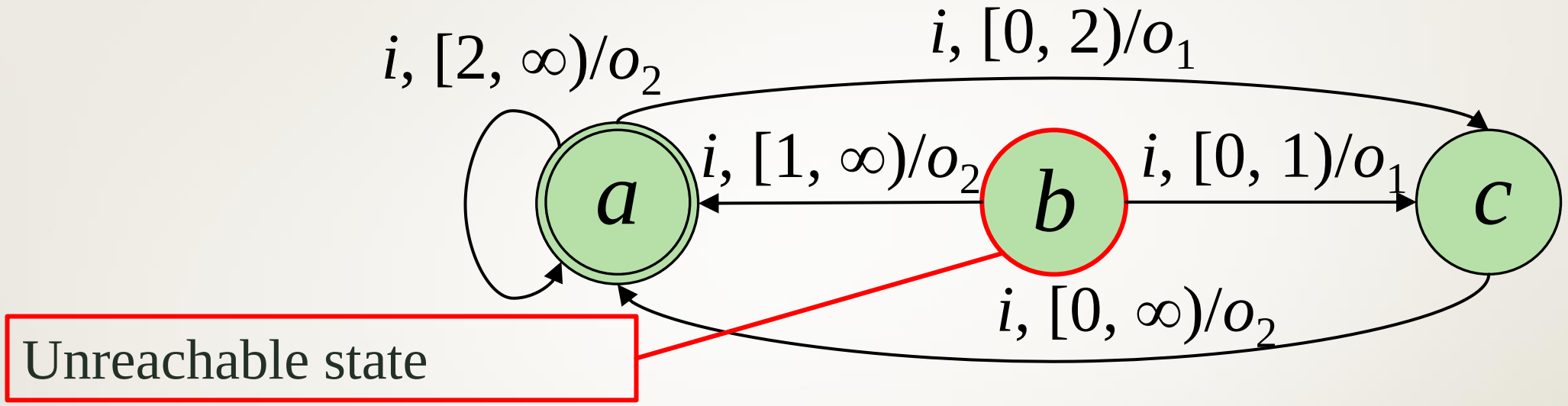
Transformation of timeouts to timed guards



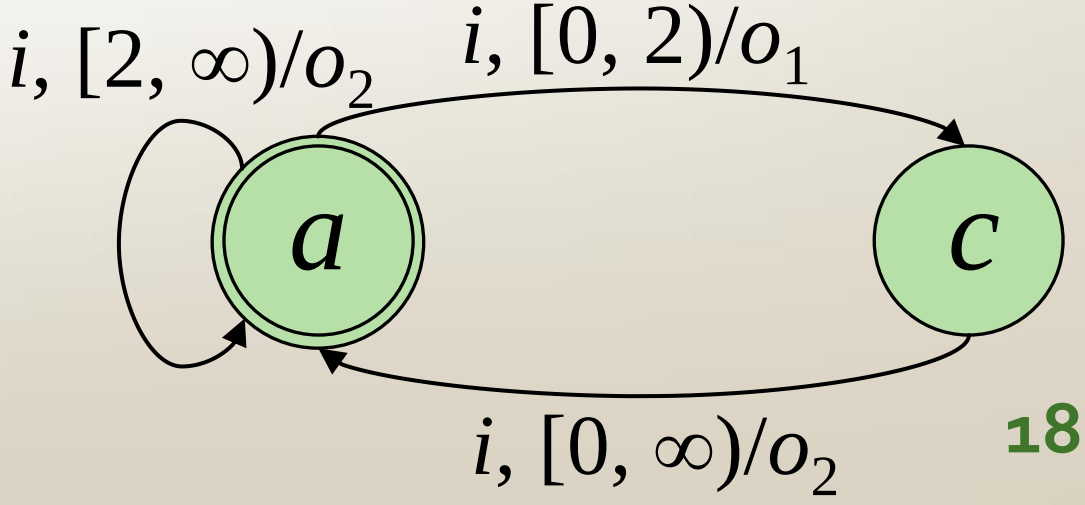


- An FSM with timeouts S is *timeout loop-free* if there is no cycle of transitions labeled with timeouts
- A timeout loop-free FSM can be represented as an FSM with timed guards

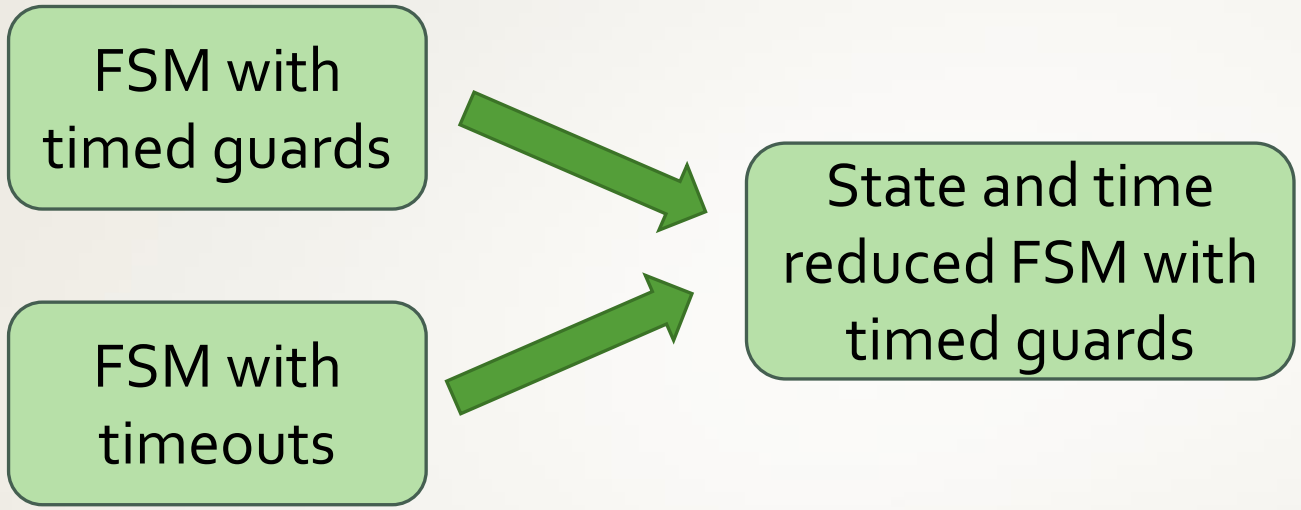
Transformation of timeouts to timed guards



A time-reachable state of an FSM with timeouts becomes unreachable from the initial state in the corresponding FSM with timed guards



Unique minimal form for Timed FSMs



Theorem. Given two deterministic complete FSMs with timed guards or timeouts S and P which are initialized connected timeout loop-free TFSMs, S and P are equivalent if and only if their time and state reduced forms of corresponding FSMs with timed guards are isomorphic

Minimal form for timeout loop-free FSM with timeouts is unique up to isomorphism

Conclusions

Two TFSM classes for which the minimal form is unique up to isomorphism have been determined:

1. Class of input-connected TFSMs which contains initialized TFSMs for which all states are reachable from initial state under a timed input sequence
2. Class of timeout loop-free TFSMs for which the transition diagram has no loops labeled with timeouts

How to use the minimal form of TFSM?

FSM-based test derivation methods (W-method and its derivatives) with guaranteed fault coverage

- Developed for initialized reduced FSMs
- Checking of equivalence (or another conformance relation) for INFINITE number of input sequences is reduced to checking the correspondence between FINITE sets of transitions

FSMs S and P are equivalent ⟺ Minimal forms of FSMs S and P are isomorphic

The uniqueness of the minimal form for Timed FSMs allows to directly adapt classical W-based test derivation methods for Timed FSMs

Thanks for your attention!
Questions?