An Introduction to Hybrid Systems Modeling

Ashutosh Trivedi

Department of Computer Science and Engineering,
IIT Bombay

CS620: New Trends in IT: Modeling and Verification of Cyber-Physical Systems
(2 August 2013)

Dynamical Systems

Dynamical System: A system whose state evolves with time governed by a fixed set of rules or dynamics.

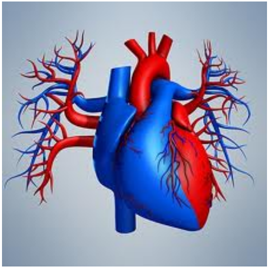
- state: valuation to variables (discrete or continuous) of the system
- time: discrete or continuous
- dynamics: discrete, continuous, or hybrid

Dynamical Systems

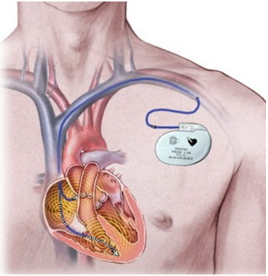
Dynamical System: A system whose state evolves with time governed by a fixed set of rules or dynamics.

- state: valuation to variables (discrete or continuous) of the system
- time: discrete or continuous
- dynamics: discrete, continuous, or hybrid

Discrete System



Continuous System



Hybrid Systems.

Discrete Dynamical Systems

Continuous Dynamical Systems

Hybrid Dynamical Systems

Abstract Model for Dynamical Systems

Definition (State Transition Systems)

A state transition system is a tuple $\mathcal{T} = (S, S_0, \Sigma, \Delta)$ where:

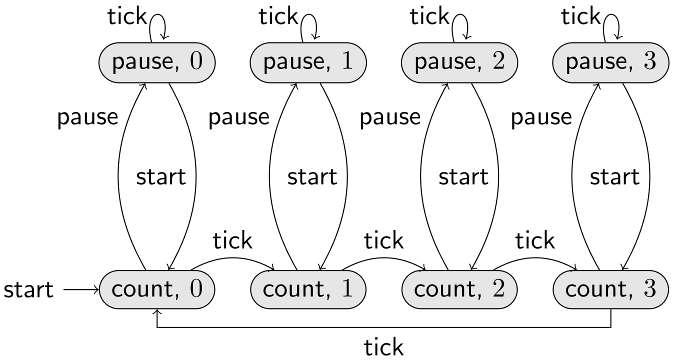
- S is a (potentially infinite) set of states;
- $S_0 \subseteq S$ is the set of initial states;
- Σ is a (potentially infinite) set of actions; and
- $\Delta \subseteq S \times \Sigma \times S$ is the transition relation;

Abstract Model for Dynamical Systems

Definition (State Transition Systems)

A state transition system is a tuple $\mathcal{T} = (S, S_0, \Sigma, \Delta)$ where:

- S is a (potentially infinite) set of states;
- $S_0 \subseteq S$ is the set of initial states;
- Σ is a (potentially infinite) set of actions; and
- $\Delta \subseteq S \times \Sigma \times S$ is the transition relation;



State Transition Systems

Definition (State Transition Systems)

A state transition system is a tuple $\mathcal{T} = (S, S_0, \Sigma, \Delta)$ where:

- S is a (potentially infinite) set of states;
- $S_0 \subseteq S$ is the set of initial states;
- Σ is a (potentially infinite) set of actions; and
- $\Delta \subseteq S \times \Sigma \times S$ is the transition relation;

- Finite and countable state transition systems
- A finite run is a sequence

$$\langle s_0, a_1, s_1, s_2, s_2, \ldots, s_n \rangle$$

  such that $s_0 \in S_0$ and for all $0 \leq i < n$ we have that $(s_i, a_{i+1}, s_{i+1}) \in \Delta$.
- Reachability and Safe-Schedulability problems

State Transition Systems

Definition (State Transition Systems)

A state transition system is a tuple $\mathcal{T} = (S, S_0, \Sigma, \Delta)$ where:

- S is a (potentially infinite) set of states;
- $S_0 \subseteq S$ is the set of initial states;
- Σ is a (potentially infinite) set of actions; and
- $\Delta \subseteq S \times \Sigma \times S$ is the transition relation;

- Finite and countable state transition systems
- A finite run is a sequence

$$\langle s_0, a_1, s_1, s_2, s_2, \ldots, s_n \rangle$$

  such that $s_0 \in S_0$ and for all $0 \leq i < n$ we have that $(s_i, a_{i+1}, s_{i+1}) \in \Delta$.
- Reachability and Safe-Schedulability problems

We need efficient computer-readable representations of infinite systems!

Extended Finite State Machines

- Let X be the set of variables (real-valued) of the system
- let $|X| = N$.
- A valuation ν of X is a function $\nu : X \to \mathbb{R}$.
- We consider a valuation as a point in $\mathbb{R}^N$ equipped with Euclidean Norm.
- A predicate is defined simply as a subset of $\mathbb{R}^N$ represented (non-linear) algebraic equations involving X.
  - Non-linear predicates, e.g. $x + 9.8\sin(z) = 0$
  - Polyhedral predicates:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \sim k$$

    where $a_i \in \mathbb{R}$, $x_i \in X$, and $\sim = \{<, \leq, =, \geq, >\}$.
  - Octagonal predicates

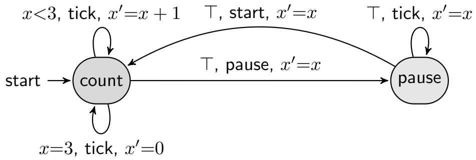
$$x_i - x_j \sim k \text{ or } x_i \sim k$$

    where $x_i, x_j \in X$, and $\sim = \{<, \leq, =, \geq, >\}$.
  - Rectangular predicates

$$x_i \sim k$$

    where $x_i \in X$, and $\sim = \{<, \leq, =, \geq, >\}$.
  - Singular Predicates $x_i = c$.

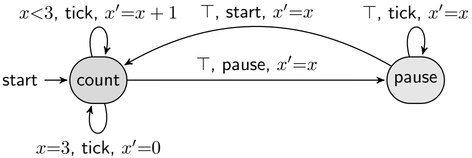
Extended Finite State Machines



Extended Finite State Machines (EFSMs):

- Finite state-transition systems coupled with a finite set of variables
- The valuation remains unchanged while system stays in a mode (state)
- The valuation changes during a transition when it jumps to the valuation governed by a predicate over $X \cup X'$ specified in the transition relation.
- Transitions are guarded by predicates over X
- Mode invariants
- Initial state and valuation

Extended Finite State Machines

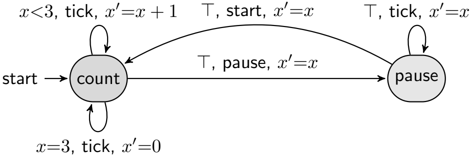


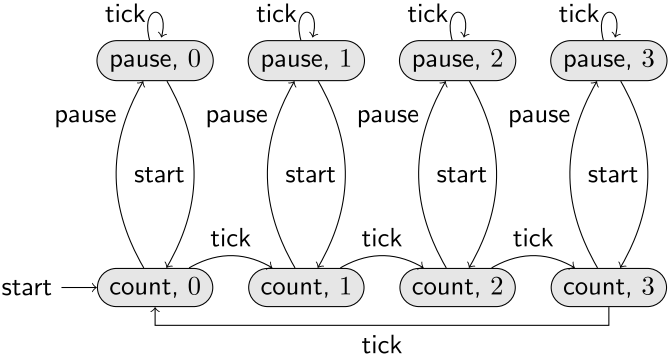
Definition (EFSM: Syntax)

An extended finite state machine is a tuple $\mathcal{M} = (M, M_0, \Sigma, X, \Delta, I, V_0)$ such that:

- M is a finite set of control modes including a distinguished initial set of control modes $M_0 \subseteq M$,
- Σ is a finite set of actions,
- X is a finite set of real-valued variable,
- $\Delta \subseteq M \times \mathrm{pred}(X) \times \Sigma \times \mathrm{pred}(X \cup X') \times M$ is the transition relation,
- $I : M \to \mathrm{pred}(X)$ is the mode-invariant function, and
- $V_0 \in \mathrm{pred}(X)$ is the set of initial valuations.

EFSM: Semantics





EFSM: Semantics

The semantics of an EFSM $\mathcal{M} = (M, M_0, \Sigma, X, \Delta, I, V_0)$ is given as a state transition graph $T^{\mathcal{M}} = (S^{\mathcal{M}}, S_0^{\mathcal{M}}, \Sigma^{\mathcal{M}}, \Delta^{\mathcal{M}})$ where

- $S^{\mathcal{M}} \subseteq (M \times \mathbb{R}^{|X|})$ is the set of configurations of $\mathcal{M}$ such that for all $(m, \nu) \in S^{\mathcal{M}}$ we have that $\nu \in [\![I(m)]\!]$;
- $S_0^{\mathcal{M}} \subseteq S^{\mathcal{M}}$ is the set of initial configurations such that $(m, \nu) \in S^{\mathcal{M}}$ if $m \in M_0$ and $\nu \in V_0$;
- $\Sigma^{\mathcal{M}} = \Sigma$ is the set of labels;
- $\Delta^{\mathcal{M}} \subseteq S^{\mathcal{M}} \times \Sigma^{\mathcal{M}} \times S^{\mathcal{M}}$ is the set of transitions such that $((m, \nu), a, (m', \nu')) \in \Delta^{\mathcal{M}}$ if there exists a transition $\delta = (m, g, a, j, m') \in \Delta$ such that
  - current valuation satisfies the guard $\nu \in [\![g]\!]$;
  - current and next valuations satisfy the jump constraint $(\nu, \nu') \in [\![j]\!]$; and
  - next valuation satisfies the invariant of the target mode $\nu' \in [\![I(m')]\!]$.

Discrete Dynamical Systems

Continuous Dynamical Systems

Hybrid Dynamical Systems

Continuous Dynamical Systems

- A finite set of continuous variables,
- a set of ordinary differential equations (ODE) characterizing the flow of these variables as a function of time
  - $F : \dot{X} \to \mathrm{pred}(X)$ where $\dot{x}$ is the first derivative of x.
  - Higher-order derivatives can be written using first derivatives by introducing auxiliary variables, e.g. write $\ddot{\theta} + (g/\ell)\sin(\theta) = 0$ can be written as

$$\dot{\theta} = y \text{ and } \dot{y} = -(g/\ell)\sin(\theta).$$

- an initial valuation to the variables.

Continuous Dynamical Systems

- A finite set of continuous variables,
- a set of ordinary differential equations (ODE) characterizing the flow of these variables as a function of time
  - $F : \dot{X} \to \mathrm{pred}(X)$ where $\dot{x}$ is the first derivative of x.
  - Higher-order derivatives can be written using first derivatives by introducing auxiliary variables, e.g. write $\ddot{\theta} + (g/\ell)\sin(\theta) = 0$ can be written as

$$\dot{\theta} = y \text{ and } \dot{y} = -(g/\ell)\sin(\theta).$$

- an initial valuation to the variables.

Definition (Continuous Dynamical System)

A continuous dynamical system is a tuple $\mathcal{M} = (X, F, \nu_0)$ such that

- X is a finite set of real-valued variable,
- $F : \dot{X} \to \mathrm{pred}(X)$ is the flow function, and
- $\nu_0 \in \mathbb{R}^{|X|}$ is the initial valuation.

Continuous Dynamical Systems

Definition (Continuous Dynamical System)

A continuous dynamical system is a tuple $\mathcal{M} = (X, F, \nu_0)$ such that

- X is a finite set of real-valued variable,
- $F : \dot{X} \to \mathrm{pred}(X)$ is the flow function, and
- $\nu_0 \in \mathbb{R}^{|X|}$ is the initial valuation.

- A run or a trajectory of $\mathcal{M} = (X, F, \nu_0)$ is given as a solution to the differential equations $\dot{X} = F(X)$ with initial valuation ν_0.
- Let a differentiable function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}^{|X|}$ be a solution to $\dot{X} = F(X)$ that provides the valuations of the variables as a function of time:

$$\begin{aligned} f(0) &= \nu_0 \\ \dot{f}(t) &= F(f(t)) \text{ for every } t \in \mathbb{R}_{\geq 0}, \end{aligned}$$

  where $\dot{f} : \mathbb{R}_{\geq 0} \to \mathbb{R}|X|$ is the time derivative of the function f.
- a run of a continuous dynamical system may not exist or may not be unique!

Existence and Uniqueness

Definition (Lipschitz-continuous Function)

We say that a function $F : \mathbb{R}^n \to \mathbb{R}^n$ is Lipschitz-continuous if there exists a constant $K{>}0$, called the Lipschitz constant, such that for all $x, y \in \mathbb{R}^n$ we have that $\|F(x) - F(y)\| < K\|x - y\|$.

Existence and Uniqueness

Definition (Lipschitz-continuous Function)

We say that a function $F : \mathbb{R}^n \to \mathbb{R}^n$ is Lipschitz-continuous if there exists a constant $K{>}0$, called the Lipschitz constant, such that for all $x, y \in \mathbb{R}^n$ we have that $\|F(x) - F(y)\| < K\|x - y\|$.

Theorem (Picard-Lindelöf Theorem)

If a function $F : \mathbb{R}^{|X|} \to \mathbb{R}^{|X|}$ is Lipschitz-continuous then the differential equation $\dot{X}{=}F(X)$ with initial valuation $\nu_0{\in}\mathbb{R}^{|X|}$ has a unique solution $f : \mathbb{R}_{\geq 0}{\to}\mathbb{R}^{|X|}$ for all $\nu_0{\in}\mathbb{R}^{|X|}$.

Existence and Uniqueness

Definition (Lipschitz-continuous Function)

We say that a function $F : \mathbb{R}^n \to \mathbb{R}^n$ is Lipschitz-continuous if there exists a constant $K{>}0$, called the Lipschitz constant, such that for all $x, y \in \mathbb{R}^n$ we have that $\|F(x) - F(y)\| < K\|x - y\|$.

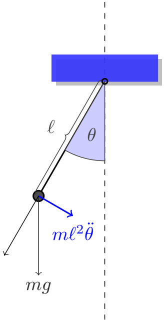
Theorem (Picard-Lindelöf Theorem)

If a function $F : \mathbb{R}^{|X|} \to \mathbb{R}^{|X|}$ is Lipschitz-continuous then the differential equation $\dot{X}{=}F(X)$ with initial valuation $\nu_0{\in}\mathbb{R}^{|X|}$ has a unique solution $f : \mathbb{R}_{\geq 0}{\to}\mathbb{R}^{|X|}$ for all $\nu_0{\in}\mathbb{R}^{|X|}$.

Theorem (Stability wrt initial valuation)

Let F be a Lipschitz-continuous function with constant $K{>}0$ and let $f{:}\mathbb{R}_{\geq 0}{\to}\mathbb{R}^{|X|}$ and $f'{:}\mathbb{R}_{\geq 0}{\to}\mathbb{R}^{|X|}$ be solutions to the differential equation $\dot{X}{=}F(X)$ with initial valuation $\nu_0{\in}\mathbb{R}^{|X|}$ and $\nu_0'{\in}\mathbb{R}^{|X|}$, respectively. Then, for all $t{\in}\mathbb{R}_{\geq 0}$ we have that $\|f(t){-}f'(t)\| \leq \|\nu{-}\nu_0\|e^{Kt}$.

Example: Simple Pendulum



- Variables y and θ
- flow equations: $m\ell^2\ddot{\theta} = -mg\ell\sin(\theta)$, or

$$\begin{aligned} \dot{\theta} &= y, \\ \dot{y} &= -(g/\ell)\sin(\theta), \end{aligned}$$

- initial valuations $(\theta, y) = (\theta_0, 0)$.

Simple Pendulum

- To analytically solve these equations, assume that initial angular displacement θ is small.
- hence $\sin(\theta) \approx \theta$.
- Now the equations simplify to

$$\dot{\theta} = y \text{ and } \dot{y} = -(g/\ell)\theta.$$

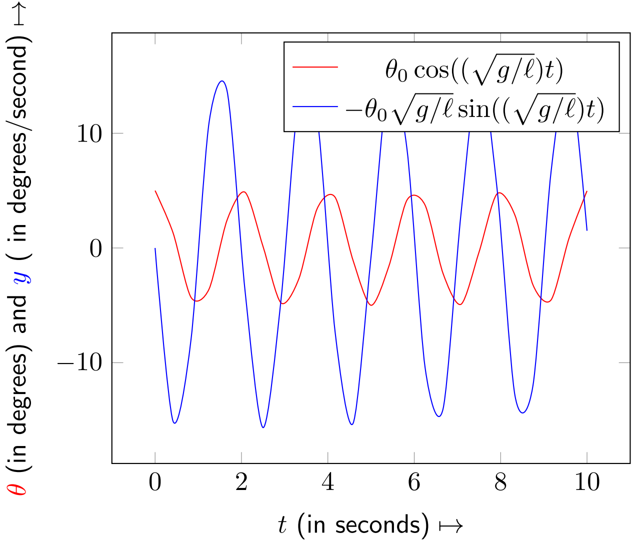
- The solution for these differential equations is

$$\begin{aligned} \theta(t) &= A\cos(Kt) + B\sin(Kt) \\ y(t) &= -AK\sin(Kt) + BK\cos(Kt), \end{aligned}$$

  where $K = \sqrt{g/\ell}$.
- Substituting $\theta(0) = \theta_0$ and $y(0) = 0$ from the initial valuation, we get that $A = \theta_0$ and $B = 0$.
- The unique run of the pendulum system can be given as the function $f : \mathbb{R}_{\geq 0} \to \{\theta, y\}$ as

$$t \mapsto (\theta_0 \cos(Kt), -\theta_0 K \sin(Kt)).$$

Pendulum Motion



(b)

Discrete Dynamical Systems

Continuous Dynamical Systems

Hybrid Dynamical Systems

Another example: Bouncing Ball

Bouncing Ball

- Consider a bouncing ball system dropped from height ℓ and velocity 0.
- Is it a continuous system?

Another example: Bouncing Ball

Bouncing Ball

- Consider a bouncing ball system dropped from height ℓ and velocity 0.
- Is it a continuous system?
- variables of interest : height of the ball x_1 and velocity of the ball x_2
- flow function:

Another example: Bouncing Ball

Bouncing Ball

- Consider a bouncing ball system dropped from height ℓ and velocity 0.
- Is it a continuous system?
- variables of interest : height of the ball x_1 and velocity of the ball x_2
- flow function:

$$\dot{x_1} = x_2 \text{ and } \dot{x_2} = -g$$

- What happens at impact?

Another example: Bouncing Ball

Bouncing Ball

- Consider a bouncing ball system dropped from height ℓ and velocity 0.
- Is it a continuous system?
- variables of interest : height of the ball x_1 and velocity of the ball x_2
- flow function:

$$\dot{x_1} = x_2 \text{ and } \dot{x_2} = -g$$

- What happens at impact?
- $x_1' = x_1$ and $x_2' = -cx_2$ where c is Restituition coefficient.

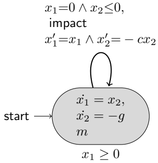
Another example: Bouncing Ball

Bouncing Ball

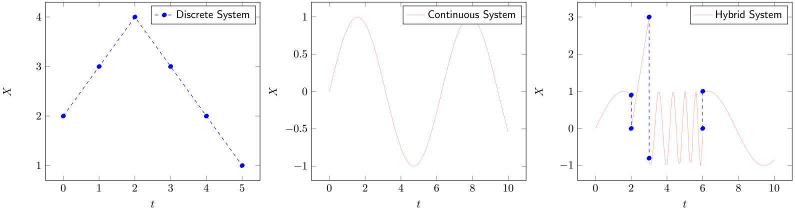
- Consider a bouncing ball system dropped from height ℓ and velocity 0.
- Is it a continuous system?
- variables of interest : height of the ball x_1 and velocity of the ball x_2
- flow function:

$$\dot{x_1} = x_2 \text{ and } \dot{x_2} = -g$$

- What happens at impact?
- $x_1' = x_1$ and $x_2' = -cx_2$ where c is Restituition coefficient.



Discrete, Continuous, and Hybrid Systems

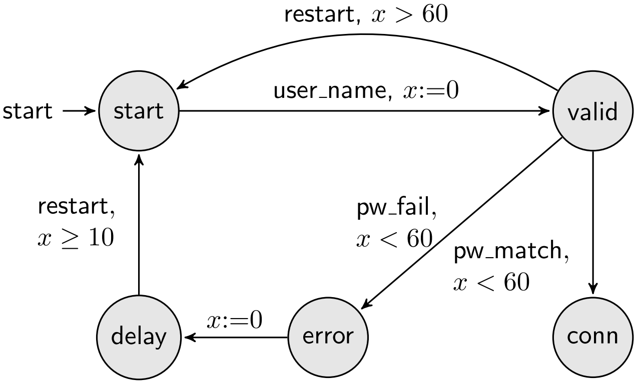


Hybrid Automata: Syntax

Some examples:

- Two leaking-water tanks systems
- Water-level monitor with delayed switch
- A leaking gas-burner
- Green scheduling with lower dwell-time requirements
- Light-bulb with three modes- dim, bright, and off.
- Job-shop scheduling problem

Login Protocol



Hybrid Automata: Syntax

Definition (HA: Syntax)

A hybrid automaton is a tuple $\mathcal{H} = (M, M_0, \Sigma, X, \Delta, I, F, V_0)$ where:

- M is a finite set of control modes including a distinguished initial set of control modes $M_0 \subseteq M$,
- Σ is a finite set of actions,
- X is a finite set of real-valued variable,
- $\Delta \subseteq M \times \mathrm{pred}(X) \times \Sigma \times \mathrm{pred}(X \cup X') \times M$ is the transition relation,
- $I : M \to \mathrm{pred}(X)$ is the mode-invariant function,
- $F : M \to (\dot{X} \to \mathrm{pred}(X))$ is the mode-dependent flow function, and
- $V_0 \in \mathrm{pred}(X)$ is the set of initial valuations.

Hybrid Automata: Syntax

Definition (HA: Syntax)

A hybrid automaton is a tuple $\mathcal{H} = (M, M_0, \Sigma, X, \Delta, I, F, V_0)$ where:

- M is a finite set of control modes including a distinguished initial set of control modes $M_0 \subseteq M$,
- Σ is a finite set of actions,
- X is a finite set of real-valued variable,
- $\Delta \subseteq M \times \text{pred}(X) \times \Sigma \times \text{pred}(X \cup X') \times M$ is the transition relation,
- $I : M \to \text{pred}(X)$ is the mode-invariant function,
- $F : M \to (\dot{X} \to \text{pred}(X))$ is the mode-dependent flow function, and
- $V_0 \in \text{pred}(X)$ is the set of initial valuations.

- A configuration (m, ν) and a timed action (t, a)
- A transition $((m, \nu), (t, a), (m', \nu')$
  - solve flow ODE of mode m with ν as the starting state $\nu \oplus_{F(m)} t$.
  - invariant, guard, and jump conditions.
- A run or execution is a sequence of transitions

$$(m_0, \nu_0), (t_1, a_1), (m_1, \nu_1), (t_2, a_2) \ldots$$

Hybrid Automata: Semantics

Definition (HA: Semantics)

The semantics of a HA $\mathcal{H} = (M, M_0, \Sigma, X, \Delta, I, F, V_0)$ is given as a state transition graph $T^{\mathcal{H}} = (S^{\mathcal{H}}, S_0^{\mathcal{H}}, \Sigma^{\mathcal{H}}, \Delta^{\mathcal{H}})$ where

- $S^{\mathcal{H}} \subseteq (M \times \mathbb{R}^{|X|})$ is the set of configurations of $\mathcal{H}$ such that for all $(m, \nu) \in S^{\mathcal{H}}$ we have that $\nu \in [\![I(m)]\!]$;
- $S_0^{\mathcal{H}} \subseteq S^{\mathcal{H}}$ s.t. $(m, \nu) \in S_0^{\mathcal{H}}$ if $m \in M_0$ and $\nu \in V_0$;
- $\Sigma^{\mathcal{H}} = \mathbb{R}_{\geq 0} \times \Sigma$ is the set of labels;
- $\Delta^{\mathcal{H}} \subseteq S^{\mathcal{H}} \times \Sigma^{\mathcal{H}} \times S^{\mathcal{H}}$ is the set of transitions such that $((m, \nu), (t, a), (m', \nu')) \in \Delta^{\mathcal{H}}$ if there exists a transition $\delta = (m, g, a, j, m') \in \Delta$ such that
  - $(\nu \oplus_{F(m)} t) \in [\![g]\!]$;
  - $(\nu \oplus_{F(m)} \tau) \in [\![I(m)]\!]$ for all $\tau \in [0, t]$;
  - $\nu' \in (\nu \oplus_{F(m)} t)[j]$; and
  - $\nu' \in [\![I(m')]\!]$.