nuXmv: model checking timed systems

Enrico Magnago

University of Trento,
Fondazione Bruno Kessler

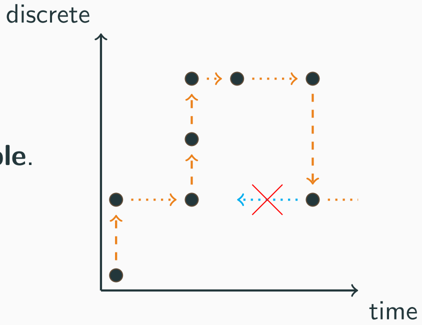
Timed systems

Real time systems

- Correctness depends not only on the logical result but also on the time required to compute it.
- Common in safety-critical domains like: defense, transportation, health-care, space and avionics.

Timed Transition System (TTS)

transitions are either discrete or time-elapses,
all clocks increase of the same amount in time-elapses.
Model checking for TTS is **undecidable**.

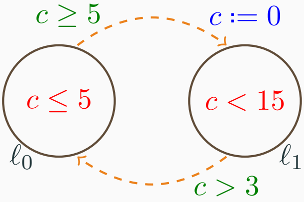


Timed Automata (TA)

decidable restriction of TTS,
finite time abstraction:
clocks compared only to constants.

Timed systems: representation

Timed Automata (TA)
Explicit graph representation of discrete states (nodes) and transitions (edges). Symbolic representation of temporal aspects via (convex) constraints (location invariants, transition guards and resets).

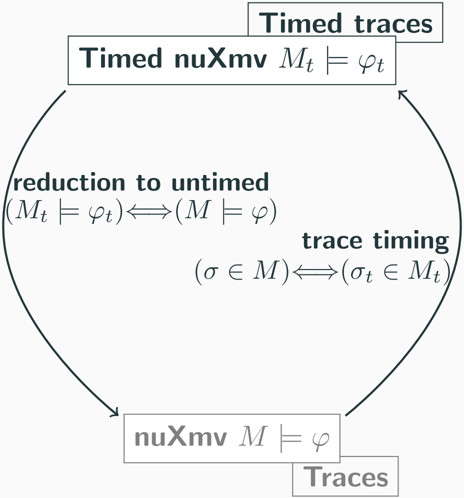


Symbolic TTS
Logical formulae represent sets of states: $p := \{s \mid s \models p)\}$.
Transition system symbolically represented by formula $\varphi(X, X')$.
There is a discrete transition from s_0 to s_1 iff $s_0(X), s_1(X') \models \varphi(X, X')$.

$$l = \ell_0 \rightarrow c \leq 5 \quad \wedge$$
$$l = \ell_1 \rightarrow c < 15 \quad \wedge$$
$$(l = \ell_1 \wedge l' = \ell_0) \rightarrow c > 3 \quad \wedge$$
$$(l = \ell_0 \wedge l' = \ell_1) \rightarrow (c \geq 5 \wedge c' = 0)$$

Timed nuXmv

nuXmv for timed system: architecture



Timed nuXmv: input language [1/4]

Overview

- Must start with `@TIME_DOMAIN continuous`;
- Symbolic description of infinite transition system using: `INIT`, `INVAR` and `TRANS` to specify initial, invariant and transition conditions.
- Model described as a synchronous composition of `MODULE` instances.
- Clock variables,
- `time`: built-in clock variable,
- convex invariants over clocks,
- `URGENT`: forbid time elapse.

Timed nuXmv: input language [2/4]

Timed nuXmv adds

- `clock` variable type, all `clocks` increase of the same amount during timed transitions;
- `time`: built-in `clock`, can be used only in comparisons with constants;
- `noncontinuous` type modifier: symbol can change its assignment during timed transitions;
- `URGENT`: freeze time: when one of the `URGENT` conditions is satisfied only discrete transitions are allowed;
- $\mathrm{MTL}_{0,\infty}$ specifications, by "extending" LTL;

Timed nuXmv: input language [3/4]

Timed nuXmv updates

- `TRANS` constrain the discrete behaviour only,
- `INVAR`: `clocks` allowed in invariants with shape: `no_clock_expr -> convex_clock_expr`;
- LTL operators: X, Y, U, S,
- Bounded LTL operators.

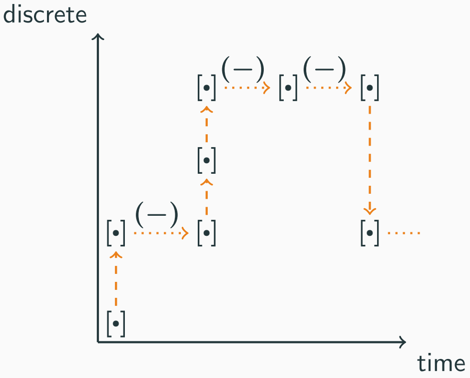
Timed nuXmv: input language [4/4]

Specification

- Different operators to refer to the *timed* next and *discrete* next: `X`, `X~`; symmetrically for the past: `Y`, `Y~`.
- Time interval semantic to handle open intervals: a predicate p might hold in an interval $(a, b]$ for $a, b \in \mathbb{R}$.
- Operators to retrieve value of expression the next/last time an expression will hold/held: `time_until`, `time_since`, `@F~` and `@O~`.

Timed to untimed model

- `clock` symbols and `time`: variables of type `real`.
- δ: continuous positive variable, prescribes the amount of time elapse for every transition.
- ι: prescribes the alternation of singular $[\bullet]$ and open $(-)$ time intervals.



Timed nuXmv: untiming

Properties rewriting

MTL $_{fragment}$ $F_{[0,5]}\ p$

↓ rewrite

LTL $_{timed}$

$$((\neg p U p) \wedge time\_until(p) \leq 5) \vee$$
$$((\neg p U \tilde{X} p) \wedge time\_until(p) < 5)$$

↓ untime

LTL $_{untimed}$

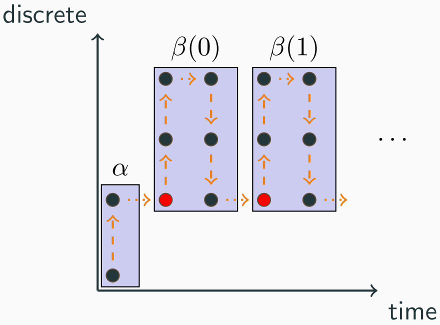
$$((\neg p U p) \wedge (time@\tilde{F}p) - time \leq 5) \vee$$
$$((\neg p U ((\neg \iota \wedge p) \vee X(\neg \iota \wedge p))) \wedge (time@\tilde{F}p) - time < 5)$$

Timed and infinite traces

Timed and infinite traces

From untimed model execution to timed trace.

Issue
NUXMV traces must have shape: $\alpha\beta^\omega$,
α and β sequences of states.
Complete for finite state systems.
TTS: time monotonically increasing, infinite state system, **undecidable**.
Identify traces expressible as: $\alpha\beta(i)^\omega$.
Same problem can be found in infinite state transition systems.



Solution
Value assigned to variables at state s is function of the previous configuration assignments.
e.g. $next(time) := time + \delta$

Timed and infinite traces: operations

Three main operations on traces: **simulation**, **execution** and **completion**.

Simulation
Build a possible execution of the model. The trace can be built automatically by the system or the user can choose each state from the list of possible ones.
Exploit SMT-solver to perform a discrete transition or time-elapse to obtain next configuration.

Timed and infinite traces: operations

Execution
Check if a trace belongs to the language of the model.
Exploit SMT-solver to prove that **for all** possible iterations all prescribed transition can be performed.

Completion
A partial trace is completed so that it belongs to the model language.
Sound and complete technique requires to check if there **exists** a possible completion so that the completed trace belongs to the model language: quantifier alternation ($\exists\forall$).
Adopt sound but incomplete approach.

How to run: model [1/3]

- `./nuXmv -time -int`: start nuXmv interactively and enable commands for timed models.
- `go_time`: process the model.
- `write_untimed_model`: dump SMV model corresponding to the input timed system.

How to run: verify [2/3]

- `timed_check_invar`: check invariants.
- `timed_check_ltlspec`: check LTL.

Mostly the same command line options of the corresponding commands for untimed models.

How to run: simulation and traces [3/3]

- `timed_pick_state`: pick initial state.
- `timed_simulate`: simulate the model starting from a given state.
- `execute_traces`: re-execute stored traces.
- `execute_partial_traces`: try to complete stored traces.

Semantics of temporal operators

Formally NUXMV uses a super-dense weakly-monotonic time model $T \subset \mathbb{N} \times \mathbb{R}_0^+$.
A time point is a pair $\langle i, r \rangle$ where $i \in \mathbb{N}$ "counts the discrete steps" and $r \in \mathbb{R}_0^+$ is the time.
We say that $\langle i, r \rangle < \langle i', r' \rangle$ iff $i < i'$ or $i = i'$ and $r < r'$.

$\sigma, t \models \phi$ is defined recursively on the structure of ϕ:
usual definition for predicates, conjunction and negation.

$\sigma, t \models \phi_1 U \phi_2$ iff there exists $t' \geq t, \sigma, t' \models \phi_2$ and
for all $t'', t \leq t'' < t', \sigma, t'' \models \phi_1$

$\sigma, t \models \phi_1 S \phi_2$ iff there exists $t' \leq t, \sigma, t' \models \phi_2$ and
for all $t'', t' < t'' \leq t, \sigma, t'' \models \phi_1$

$\sigma, t \models X\phi$ iff there exists $t' > t, \sigma, t' \models \phi$ and
there exists no $t'', t < t'' < t'$

$\sigma, t \models \tilde{X}\phi$ iff for all $t' > t,$ there exists $t'', t < t'' < t', \sigma, t'' \models \phi$

$\sigma, t \models Y\phi$ iff $t > 0$ and there exists $t' < t, \sigma, t' \models \phi$ and
there exists no $t'', t' < t'' < t$

$\sigma, t \models \tilde{Y}\phi$ iff $t > 0$ and for all $t' < t,$
there exists $t'', t' < t'' < t', \sigma, t'' \models \phi$

LTL- MTL properties [1/2]

Let k, $k1$ and $k2$ be some constant real values such that $0 \leq k \leq k1 < k2$ and let b a boolean symbol.
The following properties true or false?

- $\tilde{Y}\top$

LTL- MTL properties [1/2]

Let k, $k1$ and $k2$ be some constant real values such that $0 \leq k \leq k1 < k2$ and let b a boolean symbol.
The following properties true or false?

- $\tilde{Y}\top$: false in the initial state.
- $(\neg X b) \rightarrow (X \neg b)$

LTL- MTL properties [1/2]

Let k, $k1$ and $k2$ be some constant real values such that $0 \leq k \leq k1 < k2$ and let b a boolean symbol.
The following properties true or false?

- $\tilde{Y}\top$: false in the initial state.
- $(\neg Xb) \rightarrow (X\neg b)$: false, the first one holds in every time elapse, the second one holds only in discrete steps where $\neg b$ holds in the next state.
- $(\neg\tilde{X}\ b) \rightarrow (\tilde{X}\neg b)$

LTL- MTL properties [1/2]

Let k, $k1$ and $k2$ be some constant real values such that $0 \leq k \leq k1 < k2$ and let b a boolean symbol.
The following properties true or false?

- $\tilde{Y}\top$: false in the initial state.
- $(\neg Xb) \rightarrow (X\neg b)$: false, the first one holds in every time elapse, the second one holds only in discrete steps where $\neg b$ holds in the next state.
- $(\neg \tilde{X}\ b) \rightarrow (\tilde{X}\neg b)$: false, as above but for time elapses.
- $(X\neg b) \rightarrow (\neg Xb)$

LTL- MTL properties [1/2]

Let k, $k1$ and $k2$ be some constant real values such that $0 \leq k \leq k1 < k2$ and let b a boolean symbol.
The following properties true or false?

- $\tilde{Y}\top$: false in the initial state.
- $(\neg Xb) \rightarrow (X\neg b)$: false, the first one holds in every time elapse, the second one holds only in discrete steps where $\neg b$ holds in the next state.
- $(\neg\tilde{X}\ b) \rightarrow (\tilde{X}\neg b)$: false, as above but for time elapses.
- $(X\neg b) \rightarrow (\neg Xb)$: true, the first one holds iff there is a discrete step and $\neg b$ holds in the next state, hence Xb is false.
- $(\tilde{X}\neg b) \rightarrow (\neg\tilde{X}b)$

LTL- MTL properties [1/2]

Let k, $k1$ and $k2$ be some constant real values such that $0 \leq k \leq k1 < k2$ and let b a boolean symbol.
The following properties true or false?

- $\tilde{Y}\top$: false in the initial state.
- $(\neg Xb) \rightarrow (X\neg b)$: false, the first one holds in every time elapse, the second one holds only in discrete steps where $\neg b$ holds in the next state.
- $(\neg\tilde{X}\ b) \rightarrow (\tilde{X}\neg b)$: false, as above but for time elapses.
- $(X\neg b) \rightarrow (\neg Xb)$: true, the first one holds iff there is a discrete step and $\neg b$ holds in the next state, hence Xb is false.
- $(\tilde{X}\neg b) \rightarrow (\neg\tilde{X}b)$: true, as above but for time elapses.
- $(G\tilde{X}\top) \rightarrow ((Gb) \vee (G\neg b))$

LTL- MTL properties [1/2]

Let k, $k1$ and $k2$ be some constant real values such that $0 \leq k \leq k1 < k2$ and let b a boolean symbol.
The following properties true or false?

- $\tilde{Y}\top$: false in the initial state.
- $(\neg Xb) \rightarrow (X\neg b)$: false, the first one holds in every time elapse, the second one holds only in discrete steps where $\neg b$ holds in the next state.
- $(\neg\tilde{X}\ b) \rightarrow (\tilde{X}\neg b)$: false, as above but for time elapses.
- $(X\neg b) \rightarrow (\neg Xb)$: true, the first one holds iff there is a discrete step and $\neg b$ holds in the next state, hence Xb is false.
- $(\tilde{X}\neg b) \rightarrow (\neg\tilde{X}b)$: true, as above but for time elapses.
- $(G\tilde{X}\top) \rightarrow ((Gb) \vee (G\neg b))$: true, the first part implies that we never perform a discrete transition and the truth value of b can only change in discrete transitions.

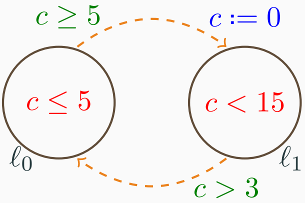
LTL- MTL properties [2/2]

See files in examples.

Exercises

Simple timed automaton

Write the SMV model corresponding to the timed automaton in the figure.



Properties

- from location ℓ_0 we always reach ℓ_1 within 5 time units;
- if we are in ℓ_1 then for the next 3 time units we remain in ℓ_1;
- if just arrived in ℓ_1 then for the next 3 time units we remain in ℓ_1.

Fischer mutual exclusion protocol

```
procedure FISCHER(pid, c, id)
    loop
        while id ≠ 0 do
            skip
        x ← random(0, c)
        wait_at_most(c)
        id ← pid
        wait_at_least(c)
        if id = pid then
            Critical Section
            id ← 0
```

Verify the mutual exclusion property.
NUXMV does not support asynchronous composition: model scheduler explicitly.

CSMA-CD [1/4]

In a broadcast network with a multi-access bus, the problem of assigning the bus to only one of many competing stations arises. The CSMA/CD protocol (Carrier Sense, Multiple-Access with Collision Detection) describes one solution. Roughly, whenever a station has data to send, if first listens to the bus. If the bus is idle (i.e., no other station is transmitting), the station begins to send a message. If it detects a busy bus in this process, it waits a random amount of time and then repeats the operation.

There are four events on which the `Bus` must synchronise with at least one `Station`: `begin`, `end`, `cd`, `busy`.

The `Bus` takes as inputs σ and the number of stations - 1 (`N`). Each `Station` takes as inputs σ and λ.

Only one among the bus and the stations can move at a time.

CSMA-CD: Bus [2/4]

The `Bus` has 4 locations (`idle`, `active`, `collision`, `transmit`), a clock variable `x` and a station index `j : 0..N` and a `IVAR` `cd_id : 0..N`.

- Upon event `begin` from `idle` it goes to `active` resetting the clock and j remains unchanged.
- From `active` j always remains unchanged and it goes to:
  - `idle` upon `end` by resetting the clock.
  - `collision` upon `begin`, provided $x < \sigma$ and by resetting the clock.
  - `active` upon `busy`, provided $x \geq \sigma$.
- It can remain in `collision` at most σ (excluded) and from `collision` it goes to `transmit` upon `cd`, provided `cd_id = j` and $x < \sigma$ by resetting the clock and increasing j by 1.
- In `transmit` time cannot elapse and while $j < N$ it remains there increasing j by 1 every time that `cd` happens and $cd\_id = j$. As soon as $j = N$, upon `cd` and $cd\_id = j$ it moves to `idle` resetting j to zero.

CSMA-CD: Station [3/4]

Each `Station` has 3 locations (`wait`, `transm`, `retry`) and a clock `x`.

- From `wait` it goes to:
  - `wait` upon `cd` by resetting the clock.
  - `transm` upon `begin` by resetting the clock.
  - `retry` upon `cd` or `busy` by resetting the clock.
- The station can never remain in `transm` more than λ and from there it either goes to `wait` upon `end` if $x \geq \lambda$ by resetting the clock, or it moves to `retry` upon `cd` if $x \leq 2\sigma$ by resetting the clock.
- It can remain in `retry` for at most 2σ, and it remains there upon `cd` by resetting the clock and it moves to `transm` upon `begin` by resetting the clock.

CSMA-CD: Properties [4/4]

Create a system with two stations on a single bus and verify the following hold:

- It is never the case that both stations are transmitting and the clock of the first one is greater than 2σ.
- it is possible for a station to go from transmitting to waiting in a single *discrete* step.

Timed thermostat

- a thermostat has 2 states: *on* and *off*;
  - if the temperature is below 18 degrees the thermostat switches *on*.
  - if the temperature is above 18 degrees the thermostat switches *off*.
- at every time unit the temperature increases (if *on*) or decreases (if *off*) by 1;
- the thermostat measures the temperature at most ($<$) every max_dt time units.
- the temperature initially is in $[18 - max\_dt; 18 + max\_dt]$.

Verify that the temperature is always in $[18 - 2max\_dt; 18 + 2max\_dt]$