Model Checking Weighted Timed Automata

Lakshmi Manasa.G
Roll Number: 08405002

Under the guidance of
Prof. Krishna .S

Doctor of Philosophy
Indian Institute of Technology,Bombay

Motivation

- Formal verification of systems - model checking
- Model-checking problem is verifying whether a given formula is satisfied by a given structure.
- WTA model is particularly relevant for modelling resource consumption in real-time systems.

Overview of the talk

1. Introduction :
    - Timed automata
    - Region automata
    - Weighted timed automata
2. Weighted integer reset timed automata
3. Clock reduction in WIRTA
4. Undecidability result
5. Conclusion and future work

Introduction - Valuations

- Clock valuation of set X - $\nu : X \rightarrow R_+$
- Set of clock valuations : R_+^X
- Clock guards : $\mathcal{G}(X)$ :: $x \sim c$
  where $x \in X$, $c \in N$ and $\sim \in \{<, \leq, >, \geq, =\}$.
- clock resets : $\phi \in U_0(X)$ is $\phi \subseteq X$.
- $\nu + \tau$, $\nu \models \psi$ and $\nu[\phi := 0]$ defined as usual.

Timed Automata

Timed automaton [1] $\mathcal{A} = (L, L_0, \Sigma, X, E, F)$

- L is a set of locations;
- $L_0 \subseteq L$ is a set of initial locations;
- Σ is a set of symbols; X is a set of clocks;
- $\mathcal{G}(X)$ and $U_0(X)$ are the set of constraints and resets.
- $E \subseteq L \times L \times \Sigma \times \mathcal{G}(X) \times U_0(X)$. An edge $e = (l, l', a, \varphi, \phi)$ is a transition from l to l' on symbol a, with the valuation $\nu \in R_+^X$ satisfying the guard φ, and then ϕ gives the resets of certain clocks.

Path :

$(l_0, \nu_0') \xrightarrow{t_1} (l_0, \nu_1) \xrightarrow{(\sigma_1, \varphi_1, \phi_1)} (l_1, \nu_1') \xrightarrow{t_2} (l_1, \nu_2) \xrightarrow{(\sigma_2, \varphi_2, \phi_2)} (l_2, \nu_2') \cdots (l_n, \nu_n')$ such that $\nu_i = \nu_{i-1}' + (t_i - t_{i-1}), \nu_i \models \varphi_i$, and $\nu_i' = \nu_i[\phi_i := 0], i \geq 1$.

Regions of Timed Automata

- $\mathcal{R}$-finite set of partitions (α) of $\mathbf{T}^X$.
  $\alpha = \{\nu | \nu \ in \mathbf{T}^X\}$ (pos. infinite)
- $Succ(\alpha)$: $\alpha' \in \mathcal{R}$ if $\exists \nu \in \mathcal{R}, \exists t \in \mathbf{T}$ s.t $\nu + t \in \alpha'$
- *set of regions* [Time elapse consistency] iff
  $\alpha' \in Succ(\alpha) \iff \forall \nu \in \alpha, \exists t \in \mathbf{T}$ s.t $\nu + t \in \alpha'$.
- $\alpha \models \varphi$: $\forall \nu \in \alpha, \nu \models \varphi$.
- $\alpha[\phi := 0] = \{\alpha' | \exists \nu \in \alpha, \alpha' \cap \nu[\phi := 0] \neq \emptyset\}$.

Compatability of Regions

Set of regions $\mathcal{R}$ is compatabile [equivalence] with

1. $\mathcal{C}(X)$ iff for every constraint $\varphi \in \mathcal{C}(X)$ and for every region $\alpha \in \mathcal{R}$ exactly one of the following holds
   (1) $\alpha \models \varphi$ or (2) $\alpha \models \neg\varphi$.
2. $U_0(X)$ iff $\alpha' \in \alpha[\phi := 0] \implies \forall \nu \in \alpha, \exists \nu' \in \alpha'$ such that $\nu' \in \nu[\phi := 0]$.

Region Automaton

For $\mathcal{A} = (L, L_0, \Sigma, X, E, F)$
Region Automaton is $\mathcal{R}(\mathcal{A}) = (Q, Q_0, \Sigma, E', F')$ where

1. $\mathcal{R}$ set of regions compatible with $\mathcal{C}(X)$ and $U_0(X)$,
2. $Q = L \times \mathcal{R}$ - set of locations
3. $Q_0 \subseteq Q$ - set of initial locations
4. $F' \subseteq Q$ - set of final locations
   where $(l, \alpha) \in F'$ s.t $l \in F \wedge \alpha \in \mathcal{R}$.
5. $E' \subseteq (Q \times \Sigma \times Q)$ - set of edges s.t
   $(l, \alpha) \xrightarrow{a} (l', \alpha') \in E'$ if $\exists \alpha'' \in \mathcal{R}$ and $(l, l', a, \varphi, \phi) \in E$ s.t
   - $\alpha'' \in Succ(\alpha)$
   - $\alpha'' \models \varphi$
   - $\alpha' \in \alpha''[\phi := 0]$

$L(\mathcal{R}(\mathcal{A})) = \text{Untime}(L(\mathcal{A}))$.

Weighted Timed Automata

$\mathcal{A} = (L, L_0, X, Z, E, \theta, \eta, C)$ where

- L is a set of locations,
- $L_0 \subseteq L$ is a set of initial locations,
- X is a set of clocks,
- Z is a set of costs where $|Z| = m$,
- $E \subseteq L \times \mathcal{G}(X) \times U_0(X) \times L$ is the set of transitions. $e = (l, \varphi, \phi, l') \in E$ is a transition from l to l' with valuation $\nu \models \varphi$, and ϕ is the set of clock resets.
- $\theta : L \to 2^{\Sigma}$ is the labelling function.
- $\eta : L \to \mathcal{G}(X)$ invariant function.
- $C : L \cup E \to N^m$ is the cost function.

stopwatches if $C : L \cup E \to \{0, 1\}^m$.
Stopwatches are restricted costs.

Semantics of WTA

Given by labelled timed transition system $\mathcal{T}_{\mathcal{A}} = (S, \rightarrow)$ where $S = L \times R_+^X \times R_+^Z$ and $\rightarrow$ is composed of transitions

- Time elapse t in l: $(l, \nu, \mu) \xrightarrow{t} (l', \nu', \mu')$, $t \in R_+$.
  Then $l' = l$, $\nu' = \nu + t$, $\mu' = \mu + C(l) * t$ and for all $0 \leq t' \leq t$, $\nu + t' \models \eta(l)$.
- Location switch: $(l, \nu, \mu) \xrightarrow{(\varphi, \phi)} (l', \nu', \mu')$ if there exists $e = (l, \varphi, \phi, l') \in E$, such that $\nu \models \varphi$, $\nu' = \nu[\phi := 0]$ and $\mu' = \mu + C(e)$. Here, $\nu \models \eta(l)$, $\nu' \models \eta(l')$.

$\rho = (l_0, \nu_0', \mu_0') \xrightarrow{t_1} (l_0, \nu_1, \mu_1) \xrightarrow{(\varphi_1, \phi_1)} (l_1, \nu_1', \mu_1') \xrightarrow{t_2} (l_1, \nu_2, \mu_2) \xrightarrow{(\varphi_2, \phi_2)} (l_2, \nu_2', \mu_2') \cdots (l_n, \nu_n', \mu_n')$.
$\nu_i = \nu_{i-1}' + (t_i - t_{i-1}), \nu_i \models \varphi_i$, $\nu_i' = \nu_i[\phi := 0]$ and
$\mu_i = \mu_{i-1}' + C(l_{i-1}) * (t_i - t_{i-1})$, $\mu_i' = \mu_i + C(l_{i-1}, \varphi_i, \phi_i, l_i)$.
$\rho[i]$ and $\rho[\leq i]$ indicates the prefix of the path till position i.

WCTL

- $WCTL_2$ as defined in [16]
  $\psi ::= \mathit{true} \mid \sigma \mid \pi \mid z.\psi \mid \neg\psi \mid \psi \vee \psi \mid \mathbf{E}(\psi \mathbf{U} \psi) \mid \mathbf{A}(\psi \mathbf{U} \psi)$
- $WCTL_1$ as defined in [15]
  $\psi ::= \mathit{true} \mid \sigma \mid \neg\psi \mid \psi_1 \vee \psi_2 \mid \mathbf{E}\psi_1 \mathbf{U}_{z \sim c} \psi_2 \mid \mathbf{A}\psi_1 \mathbf{U}_{z \sim c} \psi_2$

where $z \in Z$, $\sigma \in \Sigma$, and π is a cost constraint of the form $z_i \sim c$ or $z_i - z_j \sim c$
The freeze quantifiers $z.$ allows us to reset costs, while the cost constraints $z \sim c$ allows us to test them.

If π is only of the form $z_i \sim c$, then logic is $WCTL_{2r}$

Interpretation of WCTL

The satisfication relation $\mathcal{A},(l,\nu,\mu) \models \psi$ is:

- $\mathcal{A},(l,\nu,\mu) \models \sigma$ iff $\sigma \in \theta(l)$
- $\mathcal{A},(l,\nu,\mu) \models \pi$ iff $\mu \models \pi$
- $\mathcal{A},(l,\nu,\mu) \models \neg\psi$ iff $\mathcal{A},(l,\nu,\mu) \not\models \psi$
- $\mathcal{A},(l,\nu,\mu) \models \psi_1 \vee \psi_2$ iff $\mathcal{A},(l,\nu,\mu) \models \psi_1$ or $\mathcal{A},(l,\nu,\mu) \models \psi_2$.
- $\mathcal{A},(l,\nu,\mu) \models z.\psi$ iff $\mathcal{A},(l,\nu,\mu[z := 0]) \models \psi$ where $\mu[z := 0]$ stands for μ with z reset to zero.
- $\mathcal{A},(l,\nu,\mu) \models \mathbf{E}\psi_1\mathbf{U}\psi_2$ iff there exists a run ρ starting at (l,ν,μ), such that $\exists i$, $\rho[i] = (l_i,\nu_i,\mu_i) \models \psi_2$ and forall $j < i, \rho[j] \models \psi_1$.
- $\mathcal{A},(l,\nu,\mu) \models \mathbf{E}\psi_1\mathbf{U}_{z\sim c}\psi_2$ iff there exists a run ρ starting at (l,ν,μ), such that $\exists i, \rho[i] = (l_i,\nu_i,\mu_i) \models \psi_2$ and forall $j < i, \rho[j] \models \psi_1$, with $\mu_i(z) - \mu(z) \sim c$.

Expresiveness

Lemma

$WCTL_{2r}$ is more expressive than $WCTL_1$.

Proof.

We only give a proof sketch. Consider the $WCTL_{2r}$ formula $\psi = z.\mathbf{EF}([a \wedge z \leq 1] \wedge \mathbf{EG}[z \leq 1 \Rightarrow \neg b])$, where $a, b \in \Sigma$. It can proved that there is no $WCTL_1$ formula equivalent to ψ using an argument similar to the one used for showing that TPTL is more expressive than MTL [14]. $\square$

Model Checking results

Logic	Clocks	Stopwatches	Result
$WCTL_1$	1	≥ 1 (costs)	Decidable [15]
$WCTL_1$	≥ 3	≥ 1	Undecidable [12]
$WCTL_1$	≥ 2	≥ 1	Undecidable [21]
$WCTL_2$	≥ 1	≥ 3	Undecidable [16]
$WCTL_2$	≥ 0	≥ 3	Undecidable [16] (costs on edges)
$WCTL_{2r}$	≥ 1	≥ 2	Infinite Bisimulation [16]
$WCTL_{2r}$	≥ 2	≥ 1	Infinite Bisimulation [16]
$WCTL_{2r}$	1	1	Decidable [16]

WIRTA

Definition

A Weighted Integer Reset Timed Automaton (WIRTA) is a WTA $\mathcal{A} = (L, L_0, X, Z, E, \theta, \eta, C)$ *with the restriction that for all* $e = (l, \varphi, \phi, l') \in E$ *if* $\phi \neq \emptyset$ *then* φ *consists of atleast one atomic clock constraint* $x = c$ *for some* $x \in X, c \in N$.

Lemma

Let $\mathcal{A} = (L, L_0, \Sigma, X, E, F)$ *be an IRTA and* ν *be a clock valuation in any given run in* $\mathcal{A}$*. Then* $\forall x, y \in X$, $frac(\nu(x)) = frac(\nu(y))$*. [27]*

WIRTA example

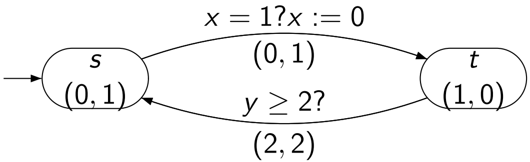


Figure: W-IRTA $\mathcal{A}$.

WIRTA regions

Let $c_m \in N$ be the maximum constant in $\mathcal{G}(X)$.
For every clock $x \in X$, define a set of intervals $\mathcal{I}_x$, as

$$\mathcal{I}_x = \{[c] | 0 \leq c \leq c_m\} \cup \{(c, c+1) | 0 \leq c < c_m\} \cup \{(c_m, \infty)\}$$

Let α be a tuple $((I_x)_{x \in X})$ where $I_x \in \mathcal{I}_x$
α is integral, non-integral or saturated.

$\mathcal{R}$ is $\{\alpha\}$ and it partitions R_+^X.

- $\mathcal{R}$ is a set of regions.
- $\mathcal{R}$ is compatible with $\mathcal{G}(X)$.
- $\mathcal{R}$ is compatible with $U_0(X)$.

Some definitions

- $dt(\tau)$ given $int(\tau) = k$.

$$dt(\tau) \triangleq \begin{cases} (\delta\checkmark)^k & \text{if } \tau \text{ is integral,} \\ (\delta\checkmark)^k\delta & \text{if } \tau \text{ is non-integral.} \end{cases}$$

- $dte(\tau_1, \tau_2)$ - $\delta\checkmark$-pattern to be right concatenated to $dt(\tau_1)$ to get $dt(\tau_2)$.
- For a path $\rho \in \mathcal{T}_A$ visiting location l_i at time t_i
  $g(\rho)$ to be
  $w = (l_0, t_0)(l_0, t_1)(l_1, t_1)(l_1, t_2) \ldots (l_{n-1}, t_{n-1})(l_{n-1}, t_n)(l_n, t_n)$.
- $f(w) = l_0 \; dte(t_1, t_0) \; l_1 \; dte(t_2, t_1) l_2 \ldots l_{n-1} \; dte(t_n, t_{n-1}) l_n$.
- Two words w, w' are said to be f-equivalent iff $f(w) = f(w')$.

Path equivalence in $\mathcal{T}_A$

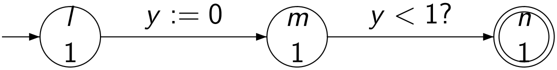
Two paths ρ and ρ' in $\mathcal{T}_A$, are said to be equivalent ($\rho \cong \rho'$) iff $f(g(\rho)) = f(g(\rho'))$.

Proposition

Let $\mathcal{A}$ be a WIRTA. Let $\rho \cong \rho'$ be paths visiting the sequence of locations $l_0 l_1 \ldots l_n$ in order, such that l_i is visited at time t_i and t'_i resply, with $t_0 = t'_0 = 0$. Then ρ is a path in $\mathcal{T}_\mathcal{A}$ iff ρ' is a path in $\mathcal{T}_\mathcal{A}$.

Corollary

The above result is not true if $\mathcal{A}$ is a WTA but not a WIRTA.



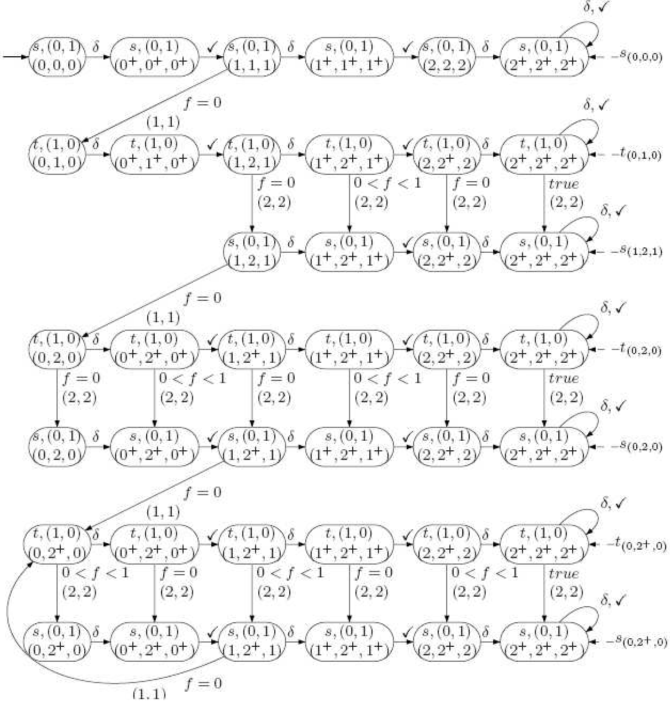
Clock Reduction - Marked WTA

Given a WIRTA $\mathcal{A}= (L, L_0, X, Z, E, \theta, C)$
its marked weighted timed automaton $\mathcal{M}_\mathcal{A}$ is
$\mathcal{M}_\mathcal{A} = (Q, Q_0, \{f\}, Z, E_m, \theta_m, C_m)$ where

- $Q = L \times \mathcal{R}$ where $\mathcal{R}$ are regions for $X \cup \{n\}$,
- $Q_0 = L_0 \times \{\alpha_0\}$ where $\alpha_0 = 0^{|X \cup \{n\}|}$,
- Z is the set of costs,
- $\theta_m : Q \rightarrow 2^\Sigma$ such that $\theta_m(q) = \theta(l)$ for $q = (l, \alpha)$,
- $C_m : Q \cup E_m \rightarrow N^{|Z|}$ such that
  1. $C_m(q) = C(l)$ if $q = (l, \alpha)$,
  2. $C_m(e_m) = C(e)$ if $e_m = (q, \epsilon, \varphi_m, \phi_m, q')$, $e = (l, \varphi, \phi, l')$, $q = (l, \alpha)$ and $q' = (l', \alpha')$,
  3. $C_m(e_m) = 0$ if $e_m = (q, \delta, \varphi_m, \phi_m, q')$ or $e_m = (q, \checkmark, \varphi_m, \phi_m, q')$ where $q = (l, \alpha)$ and $q' = (l, \alpha')$.

Marked weighted timed automaton II

- $E_m \subseteq Q \times \{\delta, \checkmark, \epsilon\} \times \mathcal{G}(\{f\}) \times U_0(\{f\}) \times Q$ is the set of edges. For $q = (l, \alpha)$ and $q' = (l', \alpha')$, an edge $e_m = (q, a, \varphi_m, \phi_m, q') \in E_m$ is such that
  1. if $\alpha(x) = (c_m, \infty)$ for all $x \in X \cup \{n\}$, then $q = q'$, $a \in \{\delta, \checkmark\}$, $\varphi_m ::$ *true* and $\phi_m = \phi$,
  2. if $l = l'$, α is integral and $\alpha' = \alpha^i$, then $a = \delta$, $\varphi_m :: 0 < f < 1$ and $\phi_m = \emptyset$,
  3. if $l = l'$, α' is integral and $\alpha' = \alpha^i$, then $a = \checkmark$, $\varphi_m :: f = 1$ and $\phi_m = \{f\}$,
  4. For a discrete transition $(l, \varphi, \phi, l') \in E$, $((l, \alpha), \epsilon, \varphi_m, \emptyset, (l', \alpha')) \in E_m$ such that
     (1) $\alpha \models \varphi$, (2) $\alpha' = \alpha[\phi \cup \{n\}]$ if $\phi \neq \emptyset$, else $\alpha' = \alpha$, and (3) $\varphi_m :: f = 0$ if α is integral, else $\varphi_m :: 0 < f < 1$,



s, (0,1) (0,0,0)
s, (0,1) (0+,0+,0+)
s, (0,1) (1,1,1)
s, (0,1) (1+,1+,1+)
s, (0,1) (2,2,2)
s, (0,1) (2+,2+,2+)
δ, ✓
−s(0,0,0)
f = 0
(1,1)
t, (1,0) (0,1,0)
t, (1,0) (0+,1+,0+)
t, (1,0) (1,2,1)
t, (1,0) (1+,2+,1+)
t, (1,0) (2,2+,2)
t, (1,0) (2+,2+,2+)
−t(0,1,0)
f = 0 (2,2)
0 < f < 1 (2,2)
f = 0 (2,2)
true (2,2)
s, (0,1) (1,2,1)
s, (0,1) (1+,2+,1+)
s, (0,1) (2,2+,2)
s, (0,1) (2+,2+,2+)
−s(1,2,1)
t, (1,0) (0,2,0)
t, (1,0) (0+,2+,0+)
t, (1,0) (1,2+,1)
t, (1,0) (1+,2+,1+)
t, (1,0) (2,2+,2)
t, (1,0) (2+,2+,2+)
−t(0,2,0)
s, (0,1) (0,2,0)
s, (0,1) (0+,2+,0+)
s, (0,1) (1,2+,1)
s, (0,1) (1+,2+,1+)
s, (0,1) (2,2+,2)
s, (0,1) (2+,2+,2+)
−s(0,2,0)
t, (1,0) (0,2+,0)
t, (1,0) (0+,2+,0+)
t, (1,0) (1,2+,1)
t, (1,0) (1+,2+,1+)
t, (1,0) (2,2+,2)
t, (1,0) (2+,2+,2+)
−t(0,2+,0)
s, (0,1) (0,2+,0)
s, (0,1) (0+,2+,0+)
s, (0,1) (1,2+,1)
s, (0,1) (1+,2+,1+)
s, (0,1) (2,2+,2)
s, (0,1) (2+,2+,2+)
−s(0,2+,0)
δ
✓

Path in $\mathcal{T}_{\mathcal{M}}$

$r = ((l_0, \alpha_0), \gamma_0, \chi_0) \xrightarrow{t_{1,1}} ((l_0, \alpha_0), \gamma_1, \chi_1) \xrightarrow{\delta} ((l_0, \alpha_1), \gamma_1, \chi_1) \xrightarrow{t_{1,2}}$
$((l_0, \alpha_1), \gamma_2, \chi_2) \xrightarrow{\checkmark} ((l_0, \alpha_2), 0, \chi_2) \ldots \xrightarrow{t_{1,k+1}} ((l_0, \alpha_k), \gamma_{k+1}, \chi_{k+1}) \xrightarrow{a}$
$((l_0, \alpha_{k+1}), \gamma'_{k+1}, \chi_{k+1}) \xrightarrow{\epsilon} ((l_1, \alpha'_{k+1}), \gamma'_{k+1}, \chi'_{k+1}) \ldots \xrightarrow{\epsilon}$
$((l_n, \alpha'_m), \gamma'_m, \chi'_m)$, where $a = \delta$ iff $0 < \gamma_{k+1} < 1$ and $a = \checkmark$ iff $\gamma'_{k+1} = 0$.

For $((l_i, \alpha_{j-1}), \gamma_{j-1}, \chi_{j-1}) \xrightarrow{t_{i+1,j}} ((l_i, \alpha_{j-1}), \gamma_j, \chi_j)$
$\chi_j = \chi_{j-1} + C_m(l_i, \alpha_{j-1}) * (t_{i+1,j} - t_{i+1,j-1})$ and
$\gamma_j = \gamma_{j-1} + t_{i+1,j} - t_{i+1,j-1}$.
For $((l_i, \alpha_j), \gamma_j, \chi_j) \xrightarrow{\epsilon} ((l_{i+1}, \alpha'_j), \gamma'_j, \chi'_j)$,
$\chi'_j = \chi_j + C_m((l_i, \alpha_j), \epsilon, (l_{i+1}, \alpha'_j))$ and $\gamma'_j = \gamma_j$.
During transitions, γ_j changes (to zero) iff transition is $\checkmark$.

Paths chosen in $\mathcal{T}_{\mathcal{M}}$

We consider only those paths in which

- All the ϵ transitions immediately follow the δ or $\checkmark$ transitions.
  ϵ after $\checkmark$ will follow it immediately
  Time elapse (< 1) between δ and ϵ can be pushed before δ.
- δ and $\checkmark$ alternate.

$h(\rho) = l_0 w_1 l_1 w_1 \ldots l_{n-1} w_n l_n$ where w_{i+1} is $\{\delta, \checkmark\}$ word between (l_i, α) and (l_i, α_{k_i+1}).

path between (l, α) and (l, α')

Proposition

Let (l, α) and (l, α') be two locations in $\mathcal{M}_{\mathcal{A}}$. Let (l, α') be reachable in $\mathcal{M}_{\mathcal{A}}$ from (l, α) by a sequence of time elapse and $\delta, \checkmark$ transitions. Then for a word $w \in \{\delta, \checkmark\}^*$ leading (l, α) to (l, α'), we have

1. *$\delta, \checkmark$ strictly alternate in w,*
2. *$w = dte(t', t)$ such that $t \in \alpha(n), t' \in \alpha'(n)$.*

Paths in $\mathcal{A}$ and $\mathcal{M}_{\mathcal{A}}$

Lemma

Let $\mathcal{A}$=$(L, L_0 X, Z, E, \theta, C)$ *be a WIRTA and let* $\mathcal{M}_{\mathcal{A}}$=$(Q, Q_0, \{f\}, Z, E_m, \theta_m, C_m)$ *be its marked automaton.*

1. *For every path* ρ *of* $\mathcal{T}_{\mathcal{A}}$*, there exists a path* ρ_m *of* $\mathcal{T}_{\mathcal{M}}$ *such that* $f(g(\rho)) = h(\rho_m)$.
2. *For every path* ρ_m *of* $\mathcal{T}_{\mathcal{M}}$ *where the* $\delta, \checkmark$ *strictly alternate, there exists a path* ρ *of* $\mathcal{T}_{\mathcal{A}}$ *such that* $f(g(\rho)) = h(\rho_m)$.
3. *Let* ρ *be a path in* $\mathcal{T}_{\mathcal{A}}$ *such that* $f(g(\rho)) = h(\rho')$ *for a path* ρ' *in* $\mathcal{T}_{\mathcal{M}}$. *Then all paths* ρ'' *in* $\mathcal{T}_{\mathcal{A}}$ *such that* $\rho'' \cong \rho$, $f(g(\rho'')) = h(\rho')$.

$\delta - \checkmark$ sequence

Let (l, α) be a location in $\mathcal{M}_{\mathcal{A}}$.
A $\delta - \checkmark$ sequence is $l_\alpha = (l, \alpha_0)(l, \alpha_1)\dots(l, \alpha_n)$
such that $\alpha_0 = \alpha$ and $\forall j \geq 0,\ \alpha_{j+1} = \alpha_j^i$
and any path in $\mathcal{T}_{\mathcal{M}}$ consisting of only these locations is of the form
$((l, \alpha_0), \gamma_0, \chi_0) \xrightarrow{t_{1,1}} ((l, \alpha_0), \gamma_1, \chi_1) \xrightarrow{a} ((l, \alpha_1), \gamma_1, \chi_1) \xrightarrow{t_{1,2}}$
$((l, \alpha_1), \gamma_2, \chi_2) \xrightarrow{a'} ((l, \alpha_2), \gamma_2, \chi_2) \dots \xrightarrow{t_{1,k+1}} ((l, \alpha_k), \gamma_{k+1}, \chi_{k+1}) \xrightarrow{\delta}$
$((l, \alpha_{k+1}), \gamma_{k+1}, \chi_{k+1})$ where

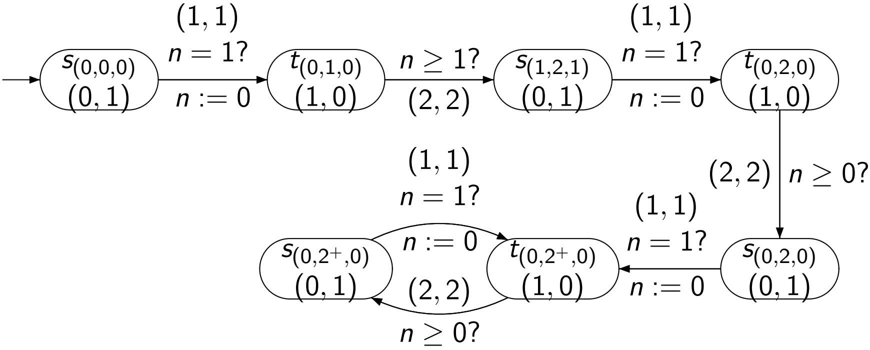
1. $a, a' \in \{\delta, \checkmark\}$,
2. δ and $\checkmark$ strictly alternate,
3. (l, α_{k+1}) has a self loop on $\delta, \checkmark$ in $\mathcal{M}_{\mathcal{A}}$.

One clock WIRTA

Let $\mathcal{M}_{\mathcal{A}} = (Q, Q_0, \{f\}, Z, E_m, \theta_m, C_m)$ correspond to a WIRTA $\mathcal{A}$.
The one clock WIRTA is $\mathcal{A}'$=$(L', L'_0, X' = \{n\}, Z, E', \theta', C')$ where

- $L' = \{l_\alpha \mid (l, \alpha) \in Q\}$,
- $L'_0 = \{s_\alpha \mid (s, \alpha) \in Q_0\}$,
- Z= the set of costs as in $\mathcal{M}_{\mathcal{A}}$,
- $E' \subseteq L' \times \mathcal{G}(X') \times U_0(X') \times L'$ is set of transitions $e = (l_\alpha, \varphi, \phi, l'_{\alpha'}) \in E'$ iff there exists $e_m = ((l, \alpha_i), \epsilon, (l', \alpha'_j)) \in E_m$ with φ is $n \in \alpha_i(n)$ and $\phi = \{n\}$ iff $\alpha'_j(n) = 0$, $l_\alpha[i] = (l, \alpha_i)$ and $l'_{\alpha'}[j] = (l', \alpha'_j)$
- $\theta' : L' \rightarrow 2^\Sigma$ is given as $\theta(l_\alpha) = \theta_m(l, \alpha)$, where $(l, \alpha) \in Q$,
- $C' : L' \cup E' \rightarrow N^{|Z|}$ is defined as $C'(l_\alpha) = C_m(l, \alpha)$ where $(l, \alpha) \in Q$, $C'(e) = C_m(e_m)$ where $e \in E'$ corresponds to e_m of E_m.

One clock WIRTA example



Path in $\mathcal{T}_{\mathcal{A}'}$

A path ρ in $\mathcal{T}_{\mathcal{A}'}$ is

$$(l_\alpha, \nu_0, \mu_0) \xrightarrow{t_1} (l_\alpha, \nu_1, \mu_1) \xrightarrow{(\varphi,\phi)} (l'_{\alpha'}, \nu_2, \mu_2) \ldots \xrightarrow{(\varphi',\phi')} (l^n_\beta, \nu_m, \mu_m)$$

$$g(\rho) = (l_\alpha, t_0)(l_\alpha, t_1)(l'_{\alpha'}, t_1) \ldots (l^n_\beta, t_n).$$

Simplifying notation, we say $g(\rho) = (l, t_0)(l, t_1)(l', t_1) \ldots (l^n, t_n)$.

Paths in $\mathcal{T}_{\mathcal{M}}$ and $\mathcal{T}_{\mathcal{A}'}$

Lemma

Let $\mathcal{M}_{\mathcal{A}}=(Q, Q_0, \{f\}, Z, E_m, \theta_m, C_m)$ *be the marked automaton for WIRTA* $\mathcal{A}$ *and let* $\mathcal{A}'=(L', L'_0, \{n\}, Z, E', \theta', C')$ *be its one clock WIRTA.*

1. *For every path* ρ_m *of* $\mathcal{T}_{\mathcal{M}}$ *where the* $\delta, \checkmark$ *strictly alternate, there exists a path* ρ *of* $\mathcal{T}_{\mathcal{A}'}$ *such that* $f(g(\rho)) = h(\rho_m)$.
2. *For every path* ρ *of* $\mathcal{T}_{\mathcal{A}'}$*, there exists a path* ρ_m *of* $\mathcal{T}_{\mathcal{M}}$ *such that* $f(g(\rho)) = h(\rho_m)$.
3. *Let* ρ *be a path in* $\mathcal{T}_{\mathcal{A}'}$ *such that* $f(g(\rho)) = h(\rho')$ *for a path* ρ' *in* $\mathcal{T}_{\mathcal{M}}$*. Then all paths* ρ'' *in* $\mathcal{T}_{\mathcal{A}'}$ *such that* $\rho'' \cong \rho$, $f(g(\rho'')) = h(\rho')$.

Complexity

Theorem

Let $\mathcal{A}$ be a WIRTA and let $\mathcal{A}'$ be the one clock WIRTA obtained from $\mathcal{M}_{\mathcal{A}}$. Then for every path $\rho \in \mathcal{T}_{\mathcal{A}}$, there is a path ρ' in $\mathcal{T}_{\mathcal{A}'}$ such that $\rho \cong \rho'$. Further, the accumulated costs in the corresponding locations of ρ, ρ' are identical.

Complexity

- Given WIRTA $\mathcal{A} = (L, L_0, X, Z, E, \theta, C)$.
- The number of regions of $\mathcal{A}$ is $(2 * (c_m + 1))^{|X|}$.
- The number of locations in the marked automaton $\mathcal{M}_{\mathcal{A}}$ is $|L| \times (2 * c_m + 2)^{|X|+1}$.
- The number of $\delta - \checkmark$ sequences is $|L'| = |L| \times (2 * c_m + 2)^{|X|+1}$.
- Single clock WIRTA $\mathcal{A}'$ has $|L| \times (2 * c_m + 2)^{|X|+1}$ locations. (Each $\delta - \checkmark$ sequence l_α is a location in $\mathcal{A}'$.)

Undecidability - Deterministic Two Counter Machine

$\mathcal{M}$ consists of a two counters C_1 and C_2 and a finite sequence of labelled instructions.
For a counter $C \in \{C_1, C_2\}$, the permitted instructions are as follows :

1. l_i : *goto* l_k
2. l_i : $C = C + 1$
3. l_i : $C = C - 1$
4. l_i : *if* $C = 0$ *goto* l_i^1 *else goto* l_i^2
5. l_i : *halt*

Behavior of M is a possibly infinite sequence of configurations
$\langle l_1, 0, 0\rangle, \langle l_1, C_1^1, C_2^1\rangle, \ldots \langle l_k, C_1^k, C_2^k\rangle \ldots$
C_1^k and C_2^k are counter values and l_k is label of kth instruction.
The halting problem of such a machine is undecidable. [24].

Model checking $WCTL_2$ over WIRTA

Lemma

Model checking $WCTL_2$ on WIRTA with 1 clock and 3 stopwatch costs is undecidable.

The proof given in [17] holds for a WRITA with minimal modifications. The constraint $x = 1?$ is replaced by $x = 1?x := 0$ while $x = 0?$ is the constraint over all the other edges.

$WCTL_{2r}$ over WIRTA 3 stopwatches and 1 clock

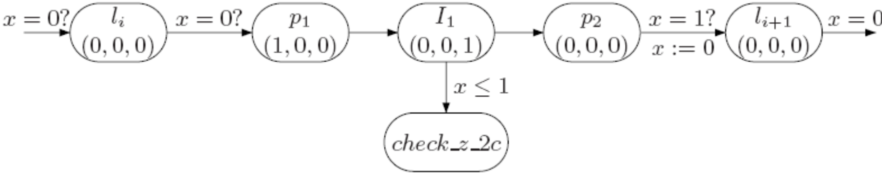
- A WIRTA $\mathcal{A}=(L, \{l_1\}, X, Z, E, \theta, C)$ and a $WCTL_{2r}$ formula Ψ simulate M.
- Each instruction l_i of M is simulated by a sub-automaton $\mathcal{A}_i$ and a $WCTL_{2r}$ formula.
- $X = \{x\}$, $Z = \{z_1, z_2, z_3\}$ where $z_i, 1 \leq i \leq 3$ is a stopwatch and $\theta(l_i) = l_i$.
- The normal form in l_i is $x = 0$, $z_3 = 0$, $z_1 = 1 - \frac{1}{2^{n_1} * 3^{n_2}}$ and $z_2 = 1 - \frac{1}{2^{n_3} * 3^{n_4}}$ where $1 \leq i \leq 4, n_i \geq 0$ encode the counters of M as $C_1 = n_1 - n_2$ and $C_2 = n_3 - n_4$.
- For l_n :: $HALT$, the sub-automata has a single state with the label $HALT$.
- Ψ :: $z_1.z_2.z_3.\mathbf{E}\ \psi_{all}\ \mathbf{U}\ (HALT\ \wedge\ z_3 = 0)$, ψ_{all} will be given later.
- The final WIRTA $\mathcal{A}$ is obtained connecting all $\mathcal{A}_i$ such that l_i in $\mathcal{A}_{i-1}$ and $\mathcal{A}_i$ coincide.

Overview of simulation

The instructions of M are simulated as follows.

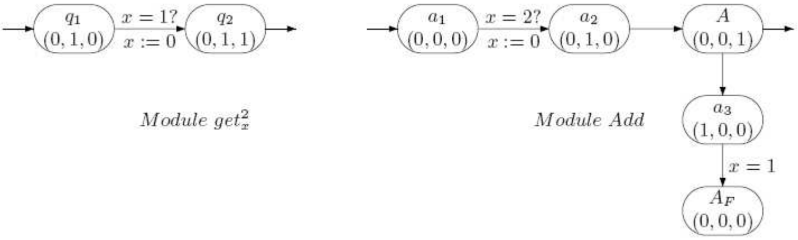
1. Increment C_1 : Increment n_1 by adding $\frac{1}{2^{n_1+1} * 3^{n_2}}$ to $z_1 = 1 - \frac{1}{2^{n_1} * 3^{n_2}}$.
2. Decrement C_2 : Increment n_2 by adding $\frac{2}{3} * \frac{1}{2^{n_1} * 3^{n_2}}$ to $z_1 = 1 - \frac{1}{2^{n_1} * 3^{n_2}}$.
3. Checking if C_1 is zero : $C_1 = 0$ iff $n_1 = n_2$. This is achieved by multipying the value $\frac{1}{2^{n_1} * 3^{n_2}}$ by 6 an integral number of times till it becomes 1.
4. For counter C_2 - reverse the roles of z_1 and z_2 in all the modules.

Increment n_1



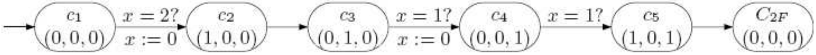
	entering l_i	leaving l_{i+1}
x	0	0
z_1	$1 - \frac{1}{2^{n_1} * 3^{n_2}}$	$1 - \frac{1}{2^{n_1} * 3^{n_2}} + t$
z_2	$1 - \frac{1}{2^{n_3} * 3^{n_4}}$	$1 - \frac{1}{2^{n_3} * 3^{n_4}}$
z_3	0	0 (due to Ψ)

Helper modules I



$\psi_A :: (A \ \wedge \ z_3 = 0) \Longrightarrow \mathbf{E} \ \neg A_F \ \mathbf{U} \ (A_F \ \wedge \ z_1 = 1 \ \wedge \ z_3 = 0)$
ensures that time spent in location a_2 is the same as the value in z_1.

Helper modules II

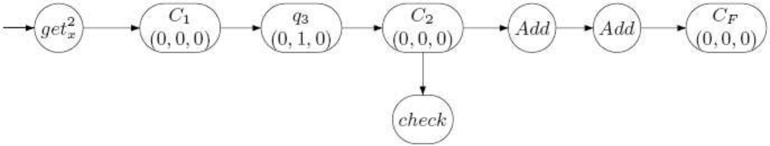


Module check

$$\psi_{C_2} :: C_2 \Longrightarrow \mathbf{E}\ \neg C_{2F}\ \mathbf{U}\ (C_{2F}\ \wedge\ z_2 = 1\ \wedge\ z_1 = 2\ \wedge\ z_3 = 2)$$

If initial values were $z_1 = 1 - \alpha + t$, $z_2 = t_3$ and $z_3 = t$ then ψ_{C_2} holds iff $t_3 = \alpha$.

Module $check\_z\_2c$: $(t = \frac{1}{2^{n_1+1} * 3^{n_2}})$

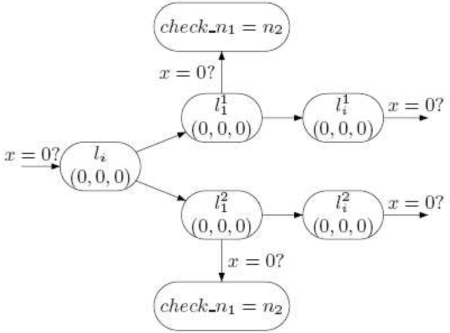


$z_2.z_3.$ **E** $\neg C_1$ **U** $[C_1 \ \wedge \ z_2 = 1$

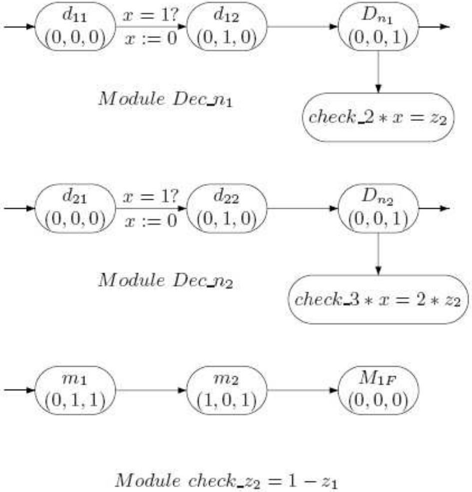
$\wedge \ z_2.$ **E** $\neg C_2$ **U** $\{C_2 \ \wedge \ \psi_{C_2}$
$\wedge \ z_3.$ **E** $(\neg C_F \ \wedge \ \psi_A)$ **U** $(C_F \ \wedge \ z_2 = 2 \ \wedge \ z_3 = 0)\}]$

entering	z_1	z_2	z_3	x
q_1	$1 - \alpha + t$	0	0	t
C_1	$1 - \alpha + t$	1	t	-
C_2	$1 - \alpha + t$	$1 - \alpha$	$t \rightarrow 0$	-
C_F	$1 - \alpha + t$	$\alpha + 1 - \alpha + t + 1 - \alpha + t$	0	-

Check if $C_1 = 0$

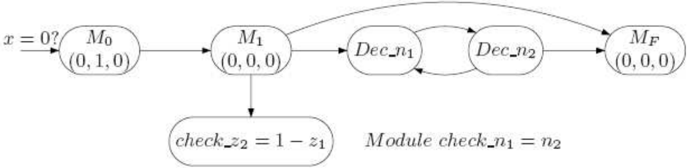


$$\psi_{Z_1} :: (l_1^1 \Longrightarrow \psi_{check\_n_1 = n_2}) \ \wedge \ (l_1^2 \Longrightarrow \neg\psi_{check\_n_1 = n_2})$$



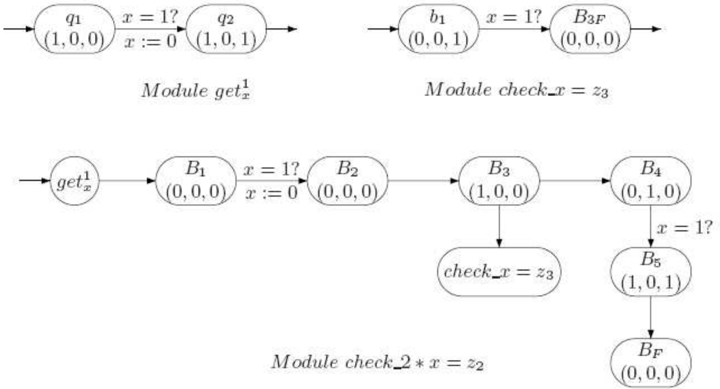
$$\psi_{M_1} :: M_1 \implies \mathbf{E}\ \neg M_{1F}\mathbf{U}(M_{1F}\ \wedge\ z_2 = 1\ \wedge\ z_3 = 1\ \wedge\ z_1 = 1)$$
$$\psi_{D_{n_1}} :: D_{n_1} \implies \mathbf{E}\ D_{n_2}\mathbf{U}(\neg D_{n_2}\ \wedge\ z_3 = 0\ \wedge\ \psi_{check\_2*x=z_2})$$
$$\psi_{D_{n_2}} :: D_{n_2} \implies \mathbf{E}\ D_{n_1}\mathbf{U}(\neg D_{n_1}\ \wedge\ z_3 = 0\ \wedge\ \psi_{check\_3*x=2*z_2})$$

Check if $n_1 = n_2$

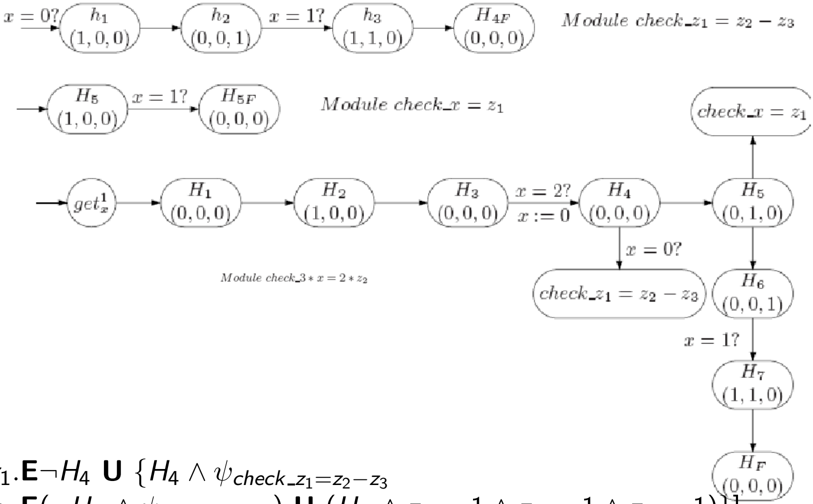


$\psi_{check\_n_1=n_2} :: z_2.z_3.\ \mathbf{E}\ (\neg M_F \ \wedge\ \psi_{M_1} \ \wedge\ \psi_{D_{n_1}} \ \wedge\ \psi_{D_{n_2}})\mathbf{U}$
$(M_F \ \wedge\ z_3 = 0 \ \wedge\ z_2 = 1)$.

Check if $2 * x = z_2$



$$\psi_{check\_2*x=z_2} :: z_1.z_3.\ \mathbf{E}\ \neg B_1\ \mathbf{U}\ [B\ \wedge\ z_1 = 1$$
$$\wedge\ z_1.\ \mathbf{E}(\neg B_F\ \wedge\ \psi_{check\_x=z_3})\ \mathbf{U}\ (B_F\ \wedge\ z_1 = 1\ \wedge\ z_2 = 1\ \wedge\ z_3 = 1)]$$
$$\psi_{check\_x=z_3} :: (B_3\ \wedge\ z_1 = 0) \Longrightarrow \mathbf{E}\ \neg B_{3F}\ \mathbf{U}\ (B_{3F}\ \wedge\ z_3 = 1\ \wedge\ z_1 = 0).$$



$\wedge z_1.\mathbf{E}\neg H_4 \ \mathbf{U} \ \{H_4 \wedge \psi_{check\_z_1=z_2-z_3}$
$\wedge z_2.\mathbf{E}(\neg H_F \wedge \psi_{check\_x=z_1}) \ \mathbf{U} \ (H_F \wedge z_1 = 1 \wedge z_2 = 1 \wedge z_3 = 1)\}].$

$\psi_{check\_3*x=2*z_2} :: z_1.z_3.\mathbf{E}\neg H_1 \ \mathbf{U} \ [H_1 \wedge z_1 = 1$
$\psi_{check\_z_1=z_2-z_3} :: H_4 \Rightarrow \mathbf{E}\neg H_{4F} \ \mathbf{U} \ (H_{4F} \wedge z_1 = 1 \ \wedge \ z_2 = 1 \ \wedge \ z_3 = 1)$
$\psi_{check\_x=z_1} :: (H_5 \wedge z_2 = 0) \Rightarrow \mathbf{E}H_5\mathbf{U}(H_{5F} \wedge z_1 = 1 \wedge z_2 = 0).$

Correctness

$\Psi :: z_1.z_2.z_3.\mathbf{E}\ \psi_{all}\ \mathbf{U}\ (HALT\ \wedge\ z_3 = 0)$ where
$\psi_{all} :: \bigwedge_{i=1,2}\ \psi_{I_i}\ \wedge\ \psi_{D_i}\ \wedge\ \psi_{Z_i}$.

Theorem

If M is the two counter machine represented by $\mathcal{A}$ and Ψ then $\mathcal{A}, (l_1, 0, \langle 0, 0, 0\rangle) \models \Psi$ iff M halts.

Conclusion

- Number of clocks reduced to 1 for WIRTA.
- Hence, model checking $WCTL_1$ is decidable for WIRTA.
- Model checking $WCTL_2$ over WIRTA with 3 stopwatches is undecidable.
- Model checking $WCTL_{2r}$ over WIRTA with 3 stopwatches is undecidable.

Future work

- $WCTL_2$ over WIRTA.
- $WCTL_{2r}$ over WIRTA with costs.
- $WCTL_1$ with multi constrained modalities.
- Reducing the number of stopwatches in the undecidability result.
- Relation between costs and stopwatches.
- Investigate other interesting subclasses of WTA and variations of WCTL.
- Extend model checking study to other logics.

THANK YOU

- R. Alur and D. L. Dill, A Theory of Timed Automata, *Theoretical Computer Science*, 126(2), 1994.
- R. Alur, L. Fix and T. Henzinger, Event-clock automata, a determinizable class of timed automata, *Theoretical Computer Science*, 211, 253-273, 1999.
- R. Alur, Salvatore La Torre, and George Pappas, Optimal paths in weighted timed automata. In *Proceedings of HSCC'01*, LNCS 2034, 49-62, 2001.
- R. Alur, Salvatore La Torre and P.Madhusudan, Perturbed Timed Automata, *Proceedings of HSCC'05*, 70-85, 2005.
- R. Alur, T.A. Henzinger, and P.-H. Ho, Automatic Symbolic Verification of Embedded Systems, *IEEE Transactions on Software Engineering*, 22:181-201, 1996.
- R. Alur, C. Courcoubetis and D. L. Dill, Model-checking in dense real time, *Information and Computation*, 104(1), 2-34, 1993.

Eugene Asarin, Oded Maler and Amir Pnueli, Reachability analysis of dynamical sytems having piecewise-constant derivatives, *Theoretical Computer Science 138*, 35-65, 1995.

Béatrice Bérard and Catherine Duford, Timed automata and additive clock constraints, *Information Processing Letters*, 75(1-2): 1-7 2000.

Béatrice Bérard, Paul Gastin and Antoine Petit, On the power of non observable actions in timed automata, *Proceedings of STACS'96*, LNCS 1046, 257-268, 1996.

Gerd Behrmann, Alexandre David, Kim G. Larsen, Oliver MIler, Paul Pettersson, and Wang Yi, Uppaal - Present and Future, *Proceedings of the 40th IEEE Conference on Decision and Control*, Orlando, Florida, USA, December 4 to 7, 2001.

Gerd Behrmann, Ansgar Fehnkar, Thomas Hune, Kim Larsen, Paul Petterson, Judi Romijn and Frits Vaandrager. Minimum-cost reachability for priced timed automata. In *Proceedings of HSCC'01*, LNCS 2034, 147-161, 2001.

- Patricia Bouyer, Thomas Brihaye and Nicolas Markey, Improved undecidability results on weighted timed automata, *Information Processing Letters*, 98(5), 188-194, 2006.
- Patricia Bouyer, Catherine Duford, Emmanuel Fleury, and Antoine Petit, Updatable Timed Automata, *Theoretical Computer Science*, 321(2-3): 291-345, 2004.
- Patricia Bouyer, Fabrice Chevalier and Nicolas Markey, On the Expressiveness of TPTL and MTL, *Proceedings of FST&TCS'05*, LNCS 3821, 432-443, 2005.
- Patricia Bouyer, Kim G. Larsen and Nicolas Markey, Model Checking One-clock Priced Timed Automata, *Logical Methods in Computer Science*, 4(2:9),2008.
- Thomas Brihaye, Véronique Bruyère, Jean-François Raskin, Model-Checking for Weighted Timed Automata, *Proceedings of FORMATS/FTRTFT 2004*, 277-292, 2004.

Thomas Brihaye, Véronique Bruyère, Jean-François Raskin, On model-checking timed automata with stopwatch observers, *Information and Computation*, 204(3), 408-433, 2006.

Christian Choffrut, Massimiliano Goldwur,: Timed Automata with Periodic Clock Constraints, *Journal of Automata, Languages and Combinatorics*, 5(4): 371-404, 2000.

Conrado Daws, Alfredo Olivero, Stavros Tripakis, Sergio Yovine, The Tool KRONOS, Hybrid Systems 1995, 208-219.

François Demichelis and Wieslaw Zielonka, Controlled Timed Automata, *Proceedings of CONCUR'98*, LNCS 1466, 455-469, 1998.

Chinmay Jain, Decidability results on weighted timed automata, *Bachelor's thesis*, Indian Institute of Technology, Bombay, July 2008.

T. Henzinger, Z. Manna and A. Pnueli, What good are digital clocks?, *Proceedings of ICALP'92*, LNCS 623, 545-558, 1992.

- L. Manasa, S. N. Krishna and Kumar Nagaraj, Updatable Timed Automata with Additive and Diagonal Constraints, *Proceedings of CiE'08*, LNCS 5028, 407-416, 2008.
- M. L.Minsky, Computation: finite and infinite machines, Prentice-Hall Inc, USA, 1967.
- Kumar Nagaraj, Topics in Timed Automata, *Master's Thesis*, Department of Computer Science & Engineering, Indian Institute of Technology, Bombay, July 2006.
- Joel Ouaknine and James Worrell, On the language inclusion problem for timed automata : Closing a decidability gap, *Proceedings of LICS'04*, 54-63, 2004.
- P. V. Suman, P. K. Pandya, S. N. Krishna and L. Manasa, Timed Automata with Integer Resets: Language Inclusion and Expressiveness, *Proceedings of FORMATS'08*, LNCS 5215, 78-92, 2008.