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
• Clock valuation of set $X$ - $\nu : X \to R_+$

• Set of clock valuations : $R^X_+$

• Clock guards : $\mathcal{G}(X) :: x \sim c$
  where $x \in X$, $c \in \mathbb{N}$ 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;
- $\Sigma$ 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 $\nu \in \mathbb{R}_+^X$ satisfying the guard $\varphi$, and then $\phi$ 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 ($\alpha$) of $T^X$.
  $\alpha = \{ \nu | \nu \text{ in } T^X \}$ (pos. infinite)

- $\text{Succ}(\alpha)$: $\alpha' \in \mathcal{R}$ if $\exists \nu \in \mathcal{R}, \exists t \in T \text{ s.t } \nu + t \in \alpha'$

- set of regions [Time elapse consistency] iff
  $\alpha' \in \text{Succ}(\alpha) \iff \forall \nu \in \alpha, \exists t \in T \text{ s.t } \nu + t \in \alpha'$.

- $\alpha \models \varphi : \forall \nu \in \alpha, \nu \models \varphi$.

- $\alpha[\phi := 0] = \{ \alpha' | \exists \nu \in \alpha, \alpha' \cap \nu[\phi := 0] \neq \emptyset \}$. 
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 $C(X)$ 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 $l \in F \land \alpha \in \mathcal{R}$.
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
   - $\alpha'' \in Succ(\alpha)$
   - $\alpha'' \models \varphi$
   - $\alpha' \in \alpha''[\phi := 0]$

$L(\mathcal{R}(\mathcal{A})) = \text{Utime}(L(\mathcal{A}))$. 
Weighted Timed Automata

\[ A = (L, L_0, X, Z, E, \theta, \eta, C) \] 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 \( \phi \) is the set of clock resets.

- \( \theta : L \rightarrow 2^\Sigma \) is the labelling function.
- \( \eta : L \rightarrow \mathcal{G}(X) \) invariant function.
- \( C : L \cup E \rightarrow N^m \) is the cost function.

*stopwatches* if \( C : L \cup E \rightarrow \{0,1\}^m \).

Stopwatches are restricted costs.
Semantics of WTA

Given by labelled timed transition system $T_A = (S, \rightarrow)$ 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 $l' = l$, $\nu' = \nu + t$, $\mu' = \mu + C(l) \ast t$ 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 $\mu_i = \mu_{i-1}' + C(l_{i-1}) \ast (t_i - t_{i-1})$, $\mu_i' = \mu_i + C(l_{i-1}, \varphi_i, \phi_i, l_i)$.

$\rho[i]$ and $\rho[\leq i]$ indicates the prefix of the path till position $i$.
WCTL

- **WCTL**$_2$ as defined in [16]
  \[ \psi ::= \text{true} \mid \sigma \mid \pi \mid z.\psi \mid \neg\psi \mid \psi \lor \psi \mid E(\psi U \psi) \mid A(\psi U \psi) \]

- **WCTL**$_1$ as defined in [15]
  \[ \psi ::= \text{true} \mid \sigma \mid \neg\psi \mid \psi_1 \lor \psi_2 \mid E\psi_1 U z \sim c \psi_2 \mid A\psi_1 U z \sim c \psi_2 \]

where \( z \in Z, \sigma \in \Sigma, \) and \( \pi \) 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 \( \pi \) is only of the form \( z_i \sim c \), then logic is **WCTL**$_{2r}$
Interpretation of WCTL

The satisfaction relation $A,(l,\nu,\mu) \models \psi$ is:

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

\( \text{WCTL}_{2r} \) is more expressive than \( \text{WCTL}_1 \).

Proof.

We only give a proof sketch. Consider the \( \text{WCTL}_{2r} \) formula
\[
\psi = z.\text{EF}([a \land z \leq 1] \land \text{EG}[z \leq 1 \Rightarrow \neg b]),
\]
where \( a, b \in \Sigma \). It can proved that there is no \( \text{WCTL}_1 \) formula equivalent to \( \psi \) using an argument similar to the one used for showing that TPTL is more expressive than MTL [14].
### Model Checking results

<table>
<thead>
<tr>
<th>Logic</th>
<th>Clocks</th>
<th>Stopwatches</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>$WCTL_1$</td>
<td>1</td>
<td>$\geq 1$ (costs)</td>
<td>Decidable [15]</td>
</tr>
<tr>
<td>$WCTL_1$</td>
<td>$\geq 3$</td>
<td>$\geq 1$</td>
<td>Undecidable [12]</td>
</tr>
<tr>
<td>$WCTL_1$</td>
<td>$\geq 2$</td>
<td>$\geq 1$</td>
<td>Undecidable [21]</td>
</tr>
<tr>
<td>$WCTL_2$</td>
<td>$\geq 1$</td>
<td>$\geq 3$</td>
<td>Undecidable [16]</td>
</tr>
<tr>
<td>$WCTL_2$</td>
<td>$\geq 0$</td>
<td>$\geq 3$</td>
<td>Undecidable [16] (costs on edges)</td>
</tr>
<tr>
<td>$WCTL_{2r}$</td>
<td>$\geq 1$</td>
<td>$\geq 2$</td>
<td>Infinite Bisimulation [16]</td>
</tr>
<tr>
<td>$WCTL_{2r}$</td>
<td>$\geq 2$</td>
<td>$\geq 1$</td>
<td>Infinite Bisimulation [16]</td>
</tr>
<tr>
<td>$WCTL_{2r}$</td>
<td>1</td>
<td>1</td>
<td>Decidable [16]</td>
</tr>
</tbody>
</table>
**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 \( \varphi \) consists of at least one atomic clock constraint \( x = c \) for some \( x \in X, c \in \mathbb{N} \).

**Lemma**

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

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

**Diagram:**
- **Start State:** $s (0, 1)$
- **Transition:** $x = 1 ? x := 0$
- **Next State:** $(0, 1)$
- **Transition:** $y \geq 2 ?$
- **Next State:** $(2, 2)$
- **Transition:** $x = 1 ? x := 0$
- **Next State:** $(0, 1)$
- **Transition:** $y \geq 2 ?$
- **Next State:** $(1, 0)$
Let $c_m \in \mathbb{N}$ be the maximum constant in $G(X)$.
For every clock $x \in X$, define a set of intervals $I_x$, as
\[
I_x = \{ [c] | 0 \leq c \leq c_m \} \cup \{ (c, c + 1) | 0 \leq c < c_m \} \cup \{ (c_m, \infty) \}
\]
Let $\alpha$ be a tuple $((I_x)_{x \in X})$ where $I_x \in I_x$
$\alpha$ 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 $G(X)$.  
- $\mathcal{R}$ is compatible with $U_0(X)$.  

Some definitions

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

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

- $dte(\tau_1, \tau_2)$ - $\check{\sqrt{\cdot}}$-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 $\rho$ and $\rho'$ in $\mathcal{T}_A$, are said to be equivalent ($\rho \simeq \rho'$) iff $f(g(\rho)) = f(g(\rho'))$.

**Proposition**

Let $A$ be a WIRTA. Let $\rho \simeq \rho'$ be paths visiting the sequence of locations $l_0l_1 \ldots l_n$ in order, such that $l_i$ is visited at time $t_i$ and $t'_i$ resply, with $t_0 = t'_0 = 0$. Then $\rho$ is a path in $\mathcal{T}_A$ iff $\rho'$ is a path in $\mathcal{T}_A$.

**Corollary**

The above result is not true if $A$ is a WTA but not a WIRTA.
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

- $E_m \subseteq Q \times \{\delta, \checkmark, \epsilon\} \times G(\{f\}) \times U_0(\{f\}) \times Q$ 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 $q = q'$, $a \in \{\delta, \checkmark\}$, $\varphi_m :: \text{true}$ and $\phi_m = \phi$,
  2. if $l = l'$, $\alpha$ is integral and $\alpha' = \alpha^i$, then $a = \delta$, $\varphi_m :: 0 < f < 1$ and $\phi_m = \emptyset$,
  3. if $l = l'$, $\alpha'$ 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 $\alpha$ is integral, else $\varphi_m :: 0 < f < 1$,
Path in $\mathcal{T}_M$

$$r = ((l_0, \alpha_0), \gamma_0, \chi_0) \xrightarrow{t_{1,1}} ((l_0, \alpha_0), \gamma_1, \chi_1) \xrightarrow{\delta} ((l_0, \alpha_1), \gamma_1, \chi_1) \xrightarrow{t_{1,2}}$$

$$((l_0, \alpha_1), \gamma_2, \chi_2) \xrightarrow{\checkmark} ((l_0, \alpha_2), 0, \chi_2) \ldots \xrightarrow{t_{1,k+1}} ((l_0, \alpha_k), \gamma_{k+1}, \chi_{k+1}) \xrightarrow{a}$$

$$((l_0, \alpha_{k+1}), \gamma'_{k+1}, \chi_{k+1}) \xrightarrow{\epsilon} ((l_1, \alpha'_{k+1}), \gamma'_{k+1}, \chi'_{k+1}) \ldots \xrightarrow{\epsilon}$$

$$((l_n, \alpha'_m), \gamma'_m, \chi'_m)$$, where $a = \delta$ iff $0 < \gamma_{k+1} < 1$ and $a = \checkmark$ iff $\gamma'_{k+1} = 0$.

For $((l_i, \alpha_{j-1}), \gamma_{j-1}, \chi_{j-1}) \xrightarrow{t_{i+1,j}} ((l_i, \alpha_{j-1}), \gamma_j, \chi_j)$

$$\chi_j = \chi_{j-1} + C_m(l_i, \alpha_{j-1}) \cdot (t_{i+1,j} - t_{i+1,j-1})$$ 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, $\gamma_j$ changes (to zero) iff transition is $\checkmark$. 

---

Lakshmi Manasa.G (PhD,CSE,IITB )  Model Checking WTA  23 / 49
Paths chosen in $\mathcal{T}_M$

We consider only those paths in which

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

$$h(\rho) = l_0 \omega_1 l_1 \omega_1 \ldots l_{n-1} \omega_n l_n$$
where $\omega_{i+1}$ is $\{\delta, \checkmark\}$ word between $(l_i, \alpha)$ and $(l_i, \alpha_{k_i + 1})$. 
path between \((l, \alpha)\) and \((l, \alpha')\)

**Proposition**

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

**Lemma**

Let $\mathcal{A}=(L, L_0X, Z, E, \theta, C)$ be a WIRTA and let $\mathcal{M}_A=(Q, Q_0, \{f\}, Z, E_m, \theta_m, C_m)$ be its marked automaton.

1. For every path $\rho$ of $\mathcal{T}_A$, there exists a path $\rho_m$ of $\mathcal{T}_M$ such that $f(g(\rho)) = h(\rho_m)$.

2. For every path $\rho_m$ of $\mathcal{T}_M$ where the $\delta, \checkmark$ strictly alternate, there exists a path $\rho$ of $\mathcal{T}_A$ such that $f(g(\rho)) = h(\rho_m)$.

3. Let $\rho$ be a path in $\mathcal{T}_A$ such that $f(g(\rho)) = h(\rho')$ for a path $\rho'$ in $\mathcal{T}_M$. Then all paths $\rho''$ in $\mathcal{T}_A$ such that $\rho'' \cong \rho$, $f(g(\rho'')) = h(\rho')$. 
Let \((l, \alpha)\) be a location in \(M_A\).

A \(\delta - \checkmark\) sequence is \(l\alpha = (l, \alpha_0)(l, \alpha_1)\ldots(l, \alpha_n)\) such that \(\alpha_0 = \alpha\) and \(\forall j \geq 0, \alpha_{j+1} = \alpha_j^i\)

and any path in \(\mathcal{T}_M\) consisting of only these locations is of the form

\[
((l, \alpha_0), \gamma_0, \chi_0) \xrightarrow{t_{1,1}} ((l, \alpha_0), \gamma_1, \chi_1) \xrightarrow{a} ((l, \alpha_1), \gamma_1, \chi_1) \xrightarrow{t_{1,2}} ((l, \alpha_1), \gamma_2, \chi_2) \xrightarrow{a'} ((l, \alpha_2), \gamma_2, \chi_2) \ldots \xrightarrow{t_{1,k+1}} ((l, \alpha_k), \gamma_{k+1}, \chi_{k+1}) \xrightarrow{\delta} ((l, \alpha_{k+1}), \gamma_{k+1}, \chi_{k+1})
\]

where

1. \(a, a' \in \{\delta, \checkmark\}\),
2. \(\delta\) and \(\checkmark\) strictly alternate,
3. \((l, \alpha_{k+1})\) has a self loop on \(\delta, \checkmark\) in \(M_A\).
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 $\mathcal{M}_\mathcal{A}$,
- $E' \subseteq L' \times G(X') \times U_0(X') \times L'$ 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 $\varphi$ 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 $(l, \alpha) \in Q$,
- $C' : L' \cup E' \rightarrow N^{\left|Z\right|}$ 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

\( s_{(0,0,0)} (0,1) \)

\( n = 1? \)

\( n := 0 \)

\( t_{(0,1,0)} (1,0) \)

\( n \geq 1? \)

\( s_{(1,2,1)} (0,1) \)

\( n = 1? \)

\( t_{(0,2,0)} (1,0) \)

\( n := 0 \)

\( s_{(0,2,+0)} (0,1) \)

\( n := 0 \)

\( t_{(0,2,+0)} (1,0) \)

\( n = 1? \)

\( s_{(0,2,0)} (0,1) \)

\( n := 0 \)

\( n \geq 0? \)
Path in $\mathcal{T}_{A'}$

A path $\rho$ in $\mathcal{T}_{A'}$ 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 $\mathcal{T}_M$ and $\mathcal{T}_{A'}$

**Lemma**

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

1. For every path $\rho_m$ of $\mathcal{T}_M$ where the $\delta, \checkmark$ strictly alternate, there exists a path $\rho$ of $\mathcal{T}_{A'}$ such that $f(g(\rho)) = h(\rho_m)$.

2. For every path $\rho$ of $\mathcal{T}_{A'}$, there exists a path $\rho_m$ of $\mathcal{T}_M$ such that $f(g(\rho)) = h(\rho_m)$.

3. Let $\rho$ be a path in $\mathcal{T}_{A'}$ such that $f(g(\rho)) = h(\rho')$ for a path $\rho'$ in $\mathcal{T}_M$. Then all paths $\rho''$ in $\mathcal{T}_{A'}$ such that $\rho'' \equiv \rho$, $f(g(\rho'')) = h(\rho')$. 
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 $\rho'$ in $\mathcal{T}_{\mathcal{A}'}$ such that $\rho \cong \rho'$. Further, the accumulated costs in the corresponding locations of $\rho, \rho'$ are identical.

Complexity

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

\( M \) 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. \( l_i : \text{ goto } l_k \)
2. \( l_i : \quad C = C + 1 \)
3. \( l_i : \quad C = C - 1 \)
4. \( l_i : \quad \text{ if } C = 0 \text{ goto } l_i^1 \text{ else goto } l_i^2 \)
5. \( l_i : \text{ halt} \)

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 \( k \)th 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 $\Psi$ 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 $l_n :: \text{HALT}$, the sub-automata has a single state with the label $\text{HALT}$.
- $\Psi :: z_1.z_2.z_3.E \psi_{all} U (\text{HALT} \land z_3 = 0)$, $\psi_{all}$ 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 $\frac{1}{2^{n_1}+3^{n_2}}$ to $z_1 = 1 - \frac{1}{2^{n_1}3^{n_2}}$.

2. **Decrement $C_2$** : Increment $n_2$ by adding $\frac{2}{3} \times \frac{1}{2^{n_1}3^{n_2}}$ 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 multiplying 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 $n_1$

\begin{align*}
x &= 0? \\
&\xrightarrow{l_i} (0,0,0) \\
&\xrightarrow{x = 0?} l_i + 1 \\
&\xrightarrow{x = 1?} p_1 = 0 \\
&\xrightarrow{x := 0} I_1 = (0,0,1) \\
&\xrightarrow{x = 1?} p_2 = 0 \\
&\xrightarrow{x := 0} l_i + 1 = (0,0,0) \\
\end{align*}

\begin{align*}
x &\leq 1 \\
\text{check_z_2c} &\xrightarrow{} \\
\end{align*}

<table>
<thead>
<tr>
<th></th>
<th>entering $l_i$</th>
<th>leaving $l_i+1$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$z_1$</td>
<td>$1 - \frac{1}{2^n_1*3^n_2}$</td>
<td>$1 - \frac{1}{2^n_1*3^n_2} + t$</td>
</tr>
<tr>
<td>$z_2$</td>
<td>$1 - \frac{1}{2^n_3*3^n_4}$</td>
<td>$1 - \frac{1}{2^n_3*3^n_4}$</td>
</tr>
<tr>
<td>$z_3$</td>
<td>0</td>
<td>0 (due to $\Psi$)</td>
</tr>
</tbody>
</table>
\( \psi_A :: (A \land z_3 = 0) \implies E \neg A_F U (A_F \land z_1 = 1 \land z_3 = 0) \)

ensures that time spent in location \( a_2 \) is the same as the value in \( z_1 \).
If initial values were $z_1 = 1 - \alpha + t$, $z_2 = t_3$ and $z_3 = t$ then $\psi_{C_2}$ holds iff $t_3 = \alpha$. 

\begin{align*}
\psi_{C_2} &:: C_2 \implies \text{E}\neg C_2 F\text{ U } (C_2 F \land z_2 = 1 \land z_1 = 2 \land z_3 = 2) 
\end{align*}
Module \( \text{check}_z\_2c : (t = \frac{1}{2^{n_1+1} \times 3^{n_2}}) \)

\[ z_2 \cdot z_3 \cdot E \neg C_1 \ U [C_1 \land z_2 = 1 \land z_2 \cdot E \neg C_2 \ U \{C_2 \land \psi C_2 \land z_3. E (\neg C_F \land \psi A) \ U (C_F \land z_2 = 2 \land z_3 = 0)\}] \]

<table>
<thead>
<tr>
<th>entering</th>
<th>( z_1 )</th>
<th>( z_2 )</th>
<th>( z_3 )</th>
<th>( x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( q_1 )</td>
<td>( 1 - \alpha + t )</td>
<td>( 0 )</td>
<td>( 0 )</td>
<td>( t )</td>
</tr>
<tr>
<td>( C_1 )</td>
<td>( 1 - \alpha + t )</td>
<td>( 1 )</td>
<td>( t )</td>
<td>-</td>
</tr>
<tr>
<td>( C_2 )</td>
<td>( 1 - \alpha + t )</td>
<td>( 1 - \alpha )</td>
<td>( t \rightarrow 0 )</td>
<td>-</td>
</tr>
<tr>
<td>( C_F )</td>
<td>( 1 - \alpha + t )</td>
<td>( \alpha + 1 - \alpha + t + 1 - \alpha + t )</td>
<td>( 0 )</td>
<td>-</td>
</tr>
</tbody>
</table>
Check if $C_1 = 0$

\[ \psi Z_1 : (l_1^1 \implies \psi_{check\_n_1=n_2}) \land (l_1^2 \implies \neg\psi_{check\_n_1=n_2}) \]
\[ \psi_{M_1} :: M_1 \Rightarrow E \neg M_{1F} U (M_{1F} \land z_2 = 1 \land z_3 = 1 \land z_1 = 1) \]

\[ \psi_{D_{n_1}} :: D_{n_1} \Rightarrow E D_{n_2} U (\neg D_{n_2} \land z_3 = 0 \land \psi_{\text{check}_2 \ast x = z_2}) \]

\[ \psi_{D_{n_2}} :: D_{n_2} \Rightarrow E D_{n_1} U (\neg D_{n_1} \land z_3 = 0 \land \psi_{\text{check}_3 \ast x = 2 \ast z_2}) \]
Check if \( n_1 = n_2 \)

\[
\psi_{\text{check}_{n_1=n_2}} \::\: Z_2 . Z_3 . \mathbf{E} \ (\neg M_F \land \psi_{M_1} \land \psi_{D_{n_1}} \land \psi_{D_{n_2}}) \mathbf{U} \ (M_F \land Z_3 = 0 \land Z_2 = 1).
\]
Check if $2 \times x = z_2$

\[ \psi_{\text{check}_2 \times x = z_2} :: z_1 \cdot z_3. \ E \neg B_1 \ U [B \land z_1 = 1 \land z_1. E (\neg B_F \land \psi_{\text{check}_x = z_3}) \ U (B_F \land z_1 = 1 \land z_2 = 1 \land z_3 = 1)] \]

\[ \psi_{\text{check}_x = z_3} :: (B_3 \land z_1 = 0) \implies E \neg B_{3F} \ U (B_{3F} \land z_3 = 1 \land z_1 = 0). \]
\[ x = 0? h_1 (1, 0, 0) \rightarrow h_2 (0, 0, 1) \rightarrow x = 1? h_3 (1, 1, 0) \rightarrow H_{4F} (0, 0, 0) \quad \text{Module check}_z z_1 = z_2 - z_3 \]

\[ H_5 (1, 0, 0) \rightarrow x = 1? H_{5F} (0, 0, 0) \quad \text{Module check}_x x = z_1 \]

\[ \text{get}_z (0, 0, 0) \rightarrow H_1 (0, 0, 0) \rightarrow H_2 (0, 0, 0) \rightarrow H_3 (0, 0, 0) \rightarrow x = 2? H_4 (0, 0, 0) \rightarrow H_5 (0, 1, 0) \]

\[ x = 0? \rightarrow H_6 (0, 0, 1) \quad x = 1? \rightarrow H_7 (1, 1, 0) \]

\[ \land z_1. E \neg H_4 U \{ H_4 \land \psi_{\text{check}_z z_1 = z_2 - z_3} \land z_2. E (\neg H_F \land \psi_{\text{check}_x x = z_1}) U (H_F \land z_1 = 1 \land z_2 = 1 \land z_3 = 1) \} \]

\[ \psi_{\text{check}_z 3 \times x = 2 \times z_2} :: z_1. z_3. E \neg H_1 U [H_1 \land z_1 = 1 \land z_2 = 0] \]

\[ \psi_{\text{check}_z z_1 = z_2 - z_3} :: H_4 \Rightarrow E \neg H_{4F} U (H_{4F} \land z_1 = 1 \land z_2 = 1 \land z_3 = 1) \]

\[ \psi_{\text{check}_x x = z_1} :: (H_5 \land z_2 = 0) \Rightarrow E H_5 U (H_{5F} \land z_1 = 1 \land z_2 = 0). \]
Correctness

\[ \Psi :: z_1.z_2.z_3.E \ \psi_{all} \ \mathbf{U} \ (HALT \ \land \ z_3 = 0) \ \text{where} \]
\[ \psi_{all} :: \land_{i=1,2} \ \psi_i \ \land \ \psi_{D_i} \ \land \ \psi_{Z_i}. \]

**Theorem**

*If* \( M \) *is the two counter machine represented by* \( \mathcal{A} \) *and* \( \Psi \) *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


