Reachability in Timed Counter Systems

Florent Bouchy\textsuperscript{1}, Alain Finkel\textsuperscript{1}, Arnaud Sangnier\textsuperscript{1,2}

\textsuperscript{1}LSV, ENS Cachan, CNRS \hspace{1cm} \textsuperscript{2}EDF R&D

MeFoSyLoMa Seminar

October 10th, 2008
Créteil, France
Motivation

Initial observation

F.Bouchy, A.Finkel, A.Sangnier - Reachability in Timed Counter Systems - 10/10/2008
Motivation

Initial observation

- need to model time in formal verification ;
Motivation

Initial observation

- need to model time in formal verification;
  
  Timed Automata: widespread and efficient way to model time

Motivation

Initial observation

- need to model time in formal verification;
  **Timed Automata**: widespread and efficient way to model time

- need for a richer and more general model;
Motivation

**Initial observation**

- need to model time in formal verification;
  - **Timed Automata**: widespread and efficient way to model time

- need for a richer and more general model;
  - counters: most used datatype in verification case studies
Motivation

Initial observation

- need to model time in formal verification;
  Timed Automata: widespread and efficient way to model time
- need for a richer and more general model;
  counters: most used datatype in verification case studies
- models using counters have several different definitions;
Initial observation

- need to model time in formal verification;
  Timed Automata: widespread and efficient way to model time

- need for a richer and more general model;
  counters: most used datatype in verification case studies

- models using counters have several different definitions;
  Counter Systems: can be generalized to a unifying definition
Motivation

Initial observation

- need to model time in formal verification;
  
  **Timed Automata**: widespread and efficient way to model time

- need for a richer and more general model;
  
  counters: most used datatype in verification case studies

- models using counters have several different definitions;
  
  **Counter Systems**: can be generalized to a unifying definition

\\[
\text{\textcolor{red}{\textbf{\textit{We combine Timed Automata and Counter Systems}}}}
\]
Motivation

Initial observation

- need to model time in formal verification;
  **Timed Automata**: widespread and efficient way to model time

- need for a richer and more general model;
  counters: most used datatype in verification case studies

- models using counters have several different definitions;
  **Counter Systems**: can be generalized to a unifying definition

We combine **Timed Automata and Counter Systems**
and we study their reachability matters
Outline

1. Timed Counter Systems
   - Example
   - Definitions
   - Semantics

2. Reachability
   - Counter Reachability Problem

3. Analysis of TCS via clock abstraction
   - Region Graph construction
   - The Region Graph as a Counter System

4. Subclasses of TCS
   - Decidability results
   - Algorithm solving the CRP
Outline

1 Timed Counter Systems
   - Example
   - Definitions
   - Semantics

2 Reachability
   - Counter Reachability Problem

3 Analysis of TCS via clock abstraction
   - Region Graph construction
   - The Region Graph as a Counter System

4 Subclasses of TCS
   - Decidability results
   - Algorithm solving the CRP
Example

**a Timed Counter System**

\[ x_1 < 2 \land x_2 := 0 \]
\[ c := c + 1 \]

\[ x_2 > 1 \]
\[ c := c + 1 \]

![Diagram of a Timed Counter System](image)
Outline

1. Timed Counter Systems
   - Example
   - Definitions
   - Semantics

2. Reachability
   - Counter Reachability Problem

3. Analysis of TCS via clock abstraction
   - Region Graph construction
   - The Region Graph as a Counter System

4. Subclasses of TCS
   - Decidability results
   - Algorithm solving the CRP
Definitions

\( X = \) a set of \( m \) real-valued variables, called clocks.
\( x = \) a valuation of the clocks, in \( \mathbb{R}^m_+ \).
\( R_X = \) the set of relations on clocks
  - usual operations: resets and linear guards
Definitions

\( X = \) a set of \( m \) real-valued variables, called clocks.
\( x = \) a valuation of the clocks, in \( \mathbb{R}^m_+ \).
\( R_X = \) the set of relations on clocks
\( \equiv \) usual operations: resets and linear guards

\( C = \) a set of \( n \) integer-valued variables, called counters.
\( c = \) a valuation of the counters, in \( \mathbb{Z}^n \).
\( R_C = \) the set of relations on counters
\( \equiv \) Presburger-definable binary relations (\( \equiv \) semi-linear)
A **Timed Counter System** is a tuple $\langle Q, X, C, E \rangle$ where:

- $Q$ is a finite set of control states (also called *locations*)
- $E \subseteq Q \times R_X \times R_C \times Q$ is a finite set of transitions (edges)
Definitions (continued)

Definition

A **Timed Counter System** is a tuple \( \langle Q, X, C, E \rangle \) where:

- \( Q \) is a finite set of control states (also called *locations*).
- \( E \subseteq Q \times R_X \times R_C \times Q \) is a finite set of transitions (edges).

Definition

A **Timed Automaton** is a TCS where \( C = \emptyset \).
A **Counter System** is a TCS where \( X = \emptyset \).
1. **Timed Counter Systems**
   - Example
   - Definitions
   - Semantics

2. **Reachability**
   - Counter Reachability Problem

3. **Analysis of TCS via clock abstraction**
   - Region Graph construction
   - The Region Graph as a Counter System

4. **Subclasses of TCS**
   - Decidability results
   - Algorithm solving the CRP
The different semantics of a TCS $S$

- Counting Transition System $CTS(S)$
- Timed Transition System $TTS(S)$
- full Transition System $TS(S)$
The different semantics of a TCS \( S \)

- Counting Transition System \( CTS(S) \)
- Timed Transition System \( TTS(S) \)
- Full Transition System \( TS(S) \)
The different semantics of a TCS $S$

- Counting Transition System $CTS(S)$
- Timed Transition System $TTS(S) \simeq \text{Region Graph } RG(S)$
- full Transition System $TS(S) \simeq CTS(RG(S))$

\[ \text{TCS} : S \]

\[ RG(S) \simeq TTS(S) \]

\[ CTS(RG(S)) \simeq TS(S) \]
Outline

1. Timed Counter Systems
   - Example
   - Definitions
   - Semantics

2. Reachability
   - Counter Reachability Problem

3. Analysis of TCS via clock abstraction
   - Region Graph construction
   - The Region Graph as a Counter System

4. Subclasses of TCS
   - Decidability results
   - Algorithm solving the CRP
Clocks are used for modelling temporal requirements; their exact value does not really matter.
Clocks are used for modelling temporal requirements; their *exact* value does not really matter.

**Counter Reachability Problem (CRP)**

**Inputs**: A TCS $S$, an initial configuration $s_0$ of $TS(S)$, and a configuration $(q, c)$ of $CTS(S)$.

**Question**: Is there a clock valuation $x$ such that $(q, x, c)$ is reachable from $s_0$ in $TS(S)$?
Clocks are used for modelling temporal requirements; their exact value does not really matter.

**Counter Reachability Problem (CRP)**

**Inputs:** A TCS $S$, an initial configuration $s_0$ of $TS(S)$, and a configuration $(q, c)$ of $CTS(S)$.

**Question:** Is there a clock valuation $x$ such that $(q, x, c)$ is reachable from $s_0$ in $TS(S)$?

The CRP extends the classical reachability problem of CS, known to be undecidable; therefore **CRP is undecidable for TCS.**
Outline

1. Timed Counter Systems
   - Example
   - Definitions
   - Semantics

2. Reachability
   - Counter Reachability Problem

3. Analysis of TCS via clock abstraction
   - Region Graph construction
   - The Region Graph as a Counter System

4. Subclasses of TCS
   - Decidability results
   - Algorithm solving the CRP
Example

A Timed Counter System...

\[ x_1 < 2 \land x_2 := 0 \]
\[ c := c + 1 \]
\[ x_2 > 1 \]
\[ c := c + 1 \]

Transition Diagram:

- \( e_1 \) from \( q_1 \) to \( q_2 \) with conditions:
  - \( x_1 \geq 2 \)
  - \( c \neq 0 \)

- \( e_2 \) from \( q_2 \) to \( q_1 \)

- \( e_3 \) from \( q_2 \) to \( q_2 \) with condition:
  - \( x_2 > 1 \)
  - \( c := c + 1 \)
Example

A Timed Counter System...

\[ x_1 < 2 \land x_2 := 0 \]
\[ c := c + 1 \]
\[ x_2 > 1 \]
\[ c := c + 1 \]

...and its clock Regions

28 regions in total:
6 points, 9 line segments, 5 half-lines, 4 triangular closed areas, and 4 open areas
Example

A Timed Counter System...

\[ x_1 < 2 \land x_2 := 0 \]
\[ c := c + 1 \]
\[ x_1 \geq 2 \]
\[ c \neq 0 \]
\[ c := c + 1 \]

\[ e_1 \rightarrow q_1 \quad e_2 \rightarrow q_2 \quad e_3 \rightarrow q_2 \]

...and its reachable Regions

8 reachable regions (out of 28), considering the initial configuration \( (q_1, (0,0), 0) \)
Example (continued)

...and its Region Graph

Diagram showing the states and transitions labeled with $q_i, \rho_j$ and edges labeled with $e_k$. The states are connected by directed edges indicating possible transitions. The diagram illustrates the reachability analysis in a timed counter system.
Example (continued)

...and its Region Graph which is a Counter System!
Outline

1. Timed Counter Systems
   - Example
   - Definitions
   - Semantics

2. Reachability
   - Counter Reachability Problem

3. Analysis of TCS via clock abstraction
   - Region Graph construction
   - The Region Graph as a Counter System

4. Subclasses of TCS
   - Decidability results
   - Algorithm solving the CRP
**Key idea:**

For a TCS $S$, its region graph $RG(S)$ is also a Counter System (namely because it has a finite number of states).
The Region Graph as a Counter System

Key idea:
For a TCS $S$, its region graph $RG(S)$ is also a Counter System (namely because it has a finite number of states).

Let $\mathcal{C}$ be a class of TCS such that there is an algorithm solving the classical reachability problem for $RG(S)$, for any $S \in \mathcal{C}$.

Theorem
The Counter Reachability Problem is decidable for $\mathcal{C}$. 
The Region Graph as a Counter System

**Key idea:**
For a TCS $S$, its region graph $RG(S)$ is also a Counter System (namely because it has a finite number of states).

Let $\mathcal{C}$ be a class of TCS such that there is an algorithm solving the classical reachability problem for $RG(S)$, for any $S \in \mathcal{C}$.

**Theorem**
The Counter Reachability Problem is decidable for $\mathcal{C}$.

**Proof idea**}[time-abstract bisimulation]
By definition, $CTS(TTS(S)) = TTS(CTS(S)) = TS(S)$.
It is well-known that $RG(S) \simeq TTS(S)$.
Therefore $CTS(RG(S)) \simeq TS(S)$. 

F.Bouchy, A.Finkel, A.Sangnier - Reachability in Timed Counter Systems - 10/10/2008
Outline

1. Timed Counter Systems
   - Example
   - Definitions
   - Semantics

2. Reachability
   - Counter Reachability Problem

3. Analysis of TCS via clock abstraction
   - Region Graph construction
   - The Region Graph as a Counter System

4. Subclasses of TCS
   - Decidability results
   - Algorithm solving the CRP
Subclasses of TCS

- **Timed Counter Machine** (TCM) = TCS whose relations on counters are translations with guards of the form $b \leq c$ or $b = c$, where $b \in \mathbb{N}^n$

- **Timed VASS** (TVASS) = TCM without $b = c$ guards

- **Bounded TCS** = TCS whose counter values are bounded

- **Reversal-Bounded TCM** = TCM whose counters do a bounded number of alternations between increasing and decreasing modes
Subclasses of TCS

- **Timed Counter Machine** (TCM) = TCS whose relations on counters are translations with guards of the form $b \leq c$ or $b = c$, where $b \in \mathbb{N}^n$

- **Timed VASS** (TVASS) = TCM without $b = c$ guards

- **Bounded TCS** = TCS whose counter values are bounded

- **Reversal-Bounded TCM** = TCM whose counters do a bounded number of alternations between increasing and decreasing modes

Decidability results

<table>
<thead>
<tr>
<th>Model</th>
<th>Region Graph</th>
<th>Counter Reachability</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCS</td>
<td>CS</td>
<td>Undecidable</td>
</tr>
<tr>
<td>TVASS</td>
<td>VASS</td>
<td>Decidable</td>
</tr>
<tr>
<td>Reversal-bounded TCM</td>
<td>Reversal-bounded CM</td>
<td>Decidable</td>
</tr>
<tr>
<td>Bounded TCS</td>
<td>Bounded CS</td>
<td>Decidable</td>
</tr>
</tbody>
</table>
1 Timed Counter Systems
   - Example
   - Definitions
   - Semantics

2 Reachability
   - Counter Reachability Problem

3 Analysis of TCS via clock abstraction
   - Region Graph construction
   - The Region Graph as a Counter System

4 Subclasses of TCS
   - Decidability results
   - Algorithm solving the CRP
Algorithm solving the CRP

Since TVASS is a recursive class, we propose an algorithm solving the CRP for this class:

**Inputs:** A TVASS $S$, a configuration $(q, c)$, and an initial state $s_0$

**Output:** Answers "Is there a $x$ such that $(q, x, c)$ is reachable from $s_0$ in $TS(S)$?"

1. Build $RG(S)$
2. For all state $(q', [x])$ of $RG(S)$ do
3. If $q' = q$ then
4. If $((q, [x]), c)$ is reachable in $RG(S)$ from $s_0$ then
5. return $True$
6. return $False$
Conclusion

Contribution
Conclusion

Contribution

- Introduction of a new model mixing clocks and counters (TCS)
Conclusion

Contribution

- Introduction of a new model mixing clocks and counters (TCS)
- Variation of the classical reachability problem (CRP)
Conclusion

Contribution

- Introduction of a new model mixing clocks and counters (TCS)
- Variation of the classical reachability problem (CRP)
- Decidability results for CRP on 3 subclasses of TCS
Conclusion

Future work
Conclusion

Future work

- Broaden decidability results: flat TCS, etc...
Future work

- Broaden decidability results: flat TCS, etc...
- Extend the tool FAST [BFLP03] with time
Conclusion

Future work

- Broaden decidability results: flat TCS, etc...
- Extend the tool FAST [BFLP03] with time
- Generalize our main theorem to other datatypes than counters: pushdown stacks, lossy channels, etc...
Related work

Systems related to our Timed Counter Systems:

- F.Bouchy, A.Finkel, A.Sangnier - Reachability in Timed Counter Systems - 10/10/2008
Related work

Systems related to our Timed Counter Systems:

- Hybrid Automata [ACHH92]
Related work

Systems related to our Timed Counter Systems:

- Hybrid Automata [ACHH92]
- Parametric Timed Counter Systems [AAB00]
Related work

Systems related to our Timed Counter Systems:

- Hybrid Automata [ACHH92]
- Parametric Timed Counter Systems [AAB00]
- Petri Nets extensions [Mer74, BLT90]
Related work

Systems related to our Timed Counter Systems:

- Hybrid Automata [ACHH92]
- Parametric Timed Counter Systems [AAB00]
- Petri Nets extensions [Mer74, BLT90]
- Discrete Pushdown Timed Automata [DIB+00]
Related work

Systems related to our Timed Counter Systems:

- Hybrid Automata [ACHH92]
- Parametric Timed Counter Systems [AAB00]
- Petri Nets extensions [Mer74, BLT90]
- Discrete Pushdown Timed Automata [DIB+00]
- real-valued counters [DIPX04, XDIP03]
Aurore Annichini, Eugene Asarin, and Ahmed Bouajjani.
Symbolic techniques for parametric reasoning about counter and clock systems.

Rajeev Alur, Costas Courcoubetis, Thomas A. Henzinger, and Pei-Hsin Ho.
Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems.

Sébastien Bardin, Alain Finkel, Jérôme Leroux, and Laure Petrucci.
FAST: Fast Acceleration of Symbolic Transition systems.

Tommaso Bolognesi, Ferdinando Lucidi, and Sebastiano Trigila.
From timed petri nets to timed lotos.

Zhe Dang, Oscar H. Ibarra, Tevfik Bultan, Richard A. Kemmerer, and Jianwen Su.
Binary reachability analysis of discrete pushdown timed automata.
In CAV, volume 1855 of LNCS, pages 69–84, 2000.
Zhe Dang, Oscar H. Ibarra, Pierluigi San Pietro, and Gaoyan Xie.
Real-counter automata and their decision problems.

P.M. Merlin.
A study of the recoverability of computing systems.

Gaoyan Xie, Zhe Dang, Oscar H. Ibarra, and Pierluigi San Pietro.
Dense counter machines and verification problems.