Reachability in Timed Counter Systems

Florent Bouchy[1], Alain Finkel[1], Arnaud Sangnier[1,2]

[1]LSV, ENS Cachan, CNRS [2]EDF R&D

INFINITY'08
Workshop affiliated to CONCUR'08

August 2008
Toronto, ON, Canada

Motivation

Initial observation

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 ;

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

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*

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

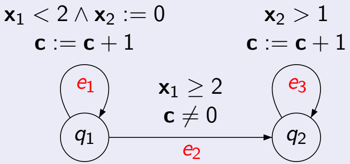
☞ *We combine Timed Automata and Counter Systems*
and we study their reachability matters

Outline

Outline

Example

a Timed Counter System



Outline

Definitions

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

C = a set of n integer-valued variables, called counters.
$\mathbf{c}$ = a valuation of the counters, in $\mathbb{Z}^n$.
R_C = the set of relations on counters
☞Presburger-definable binary relations ($\equiv$ semi-linear)

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)

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 $X = \emptyset$.

Outline

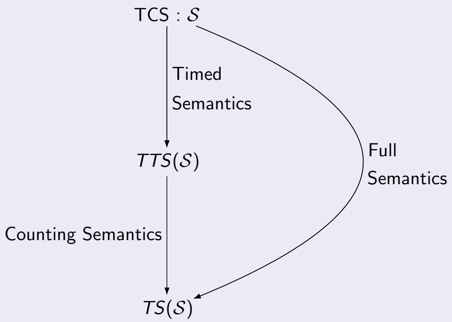
1. **Timed Counter Systems**
   - Example
   - Definitions
   - Semantics
2. **Reachability**
   - Counter Reachability Problem
3. **Analysis of TCS via clock abstraction**
   - Region Graph construction
   - The Region Graph as a Counter System
4. **Subclasses of TCS**
   - Decidability results
   - Algorithm solving the CRP

The different semantics of a TCS $\mathcal{S}$

- Counting Transition System $CTS(\mathcal{S})$
- Timed Transition System $TTS(\mathcal{S})$
- full Transition System $TS(\mathcal{S})$

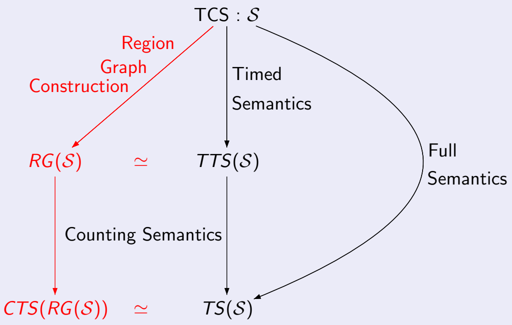
The different semantics of a TCS $\mathcal{S}$

- Counting Transition System $CTS(\mathcal{S})$
- Timed Transition System $TTS(\mathcal{S})$
- full Transition System $TS(\mathcal{S})$



The different semantics of a TCS $\mathcal{S}$

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



Outline

Reachability

Clocks are used for modelling temporal requirements ; their *exact* value does not really matter.

Reachability

Clocks are used for modelling temporal requirements ; their *exact* value does not really matter.

Counter Reachability Problem (CRP)

Inputs : A TCS $\mathcal{S}$, an initial configuration s_0 of $TS(\mathcal{S})$, and a configuration $(q, \mathbf{c})$ of $CTS(\mathcal{S})$.
Question : Is there a clock valuation $\mathbf{x}$ such that $(q, \mathbf{x}, \mathbf{c})$ is reachable from s_0 in $TS(\mathcal{S})$?

Reachability

Clocks are used for modelling temporal requirements ; their *exact* value does not really matter.

Counter Reachability Problem (CRP)

Inputs : A TCS $\mathcal{S}$, an initial configuration s_0 of $TS(\mathcal{S})$, and a configuration $(q, \mathbf{c})$ of $CTS(\mathcal{S})$.

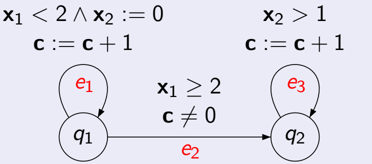
Question : Is there a clock valuation $\mathbf{x}$ such that $(q, \mathbf{x}, \mathbf{c})$ is reachable from s_0 in $TS(\mathcal{S})$?

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

Outline

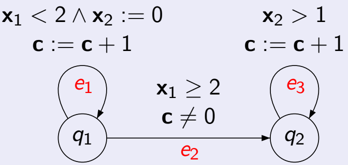
Example

a Timed Counter System...

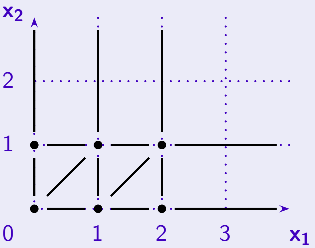


Example

a Timed Counter System...



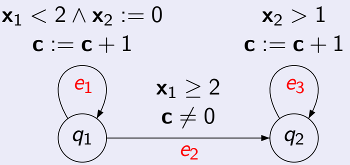
...and its clock Regions



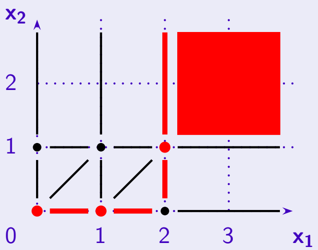
28 regions in total :
6 points, 9 line segments, 5 half-lines, 4 triangular closed areas, and 4 open areas

Example

a Timed Counter System...



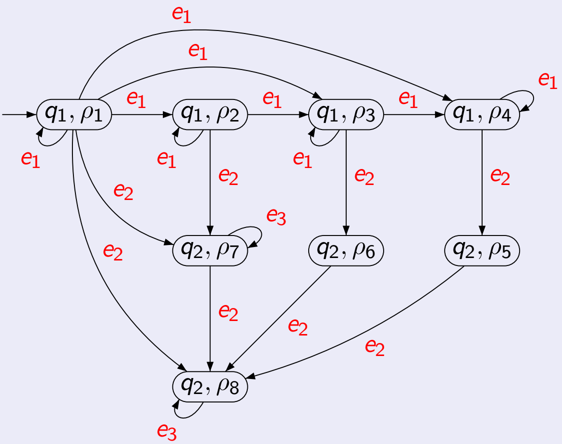
...and its reachable Regions



8 reachable regions (out of 28), considering the initial configuration $\left(q_1, \binom{0}{0}, 0\right)$

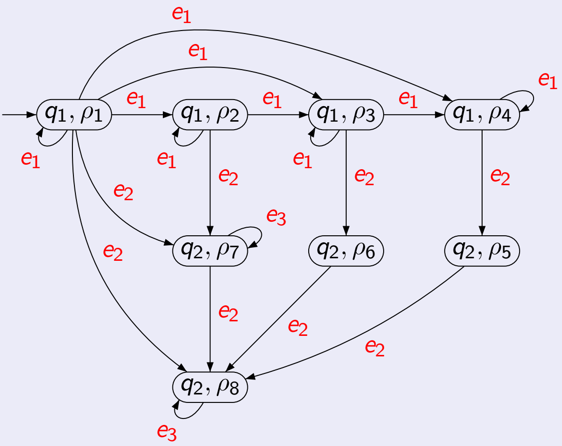
Example (continued)

...and its Region Graph



Example (continued)

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



Outline

The Region Graph as a Counter System

Key idea :

For a TCS $\mathcal{S}$, its region graph $RG(\mathcal{S})$ 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 $\mathcal{S}$, its region graph $RG(\mathcal{S})$ is also a Counter System (namely because it has a finite number of states).

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

Theorem

The Counter Reachability Problem is decidable for $\mathfrak{C}$.

The Region Graph as a Counter System

Key idea :

For a TCS $\mathcal{S}$, its region graph $RG(\mathcal{S})$ is also a Counter System (namely because it has a finite number of states).

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

Theorem

The Counter Reachability Problem is decidable for $\mathfrak{C}$.

Proof idea ▸ time-abstract bisimulation

By definition, $CTS(TTS(\mathcal{S})) = TTS(CTS(\mathcal{S})) = TS(\mathcal{S})$.
It is well-known that $RG(\mathcal{S}) \simeq TTS(\mathcal{S})$.
Therefore $CTS(RG(\mathcal{S})) \simeq TS(\mathcal{S})$. □

Outline

Subclasses of TCS

- Timed Counter Machine (TCM) $=$ TCS whose relations on counters are translations with guards of the form $b \leq \mathbf{c}$ or $b = \mathbf{c}$, where $b \in \mathbb{N}^n$
- Timed VASS (TVASS) $=$ TCM without $b = \mathbf{c}$ 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 $b \leq \mathbf{c}$ or $b = \mathbf{c}$, where $b \in \mathbb{N}^n$
- Timed VASS (TVASS) = TCM without $b = \mathbf{c}$ 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

Model	Region Graph	Counter Reachability
TCS	CS	Undecidable
TVASS	VASS	Decidable
Reversal-bounded TCM	Reversal-bounded CM	Decidable
Bounded TCS	Bounded CS	Decidable

Outline

Algorithm solving the CRP

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

Inputs : A TVASS $\mathcal{S}$, a configuration $(q, \mathbf{c})$, and an initial state s_0
Output : Answers "Is there a $\mathbf{x}$ such that $(q, \mathbf{x}, \mathbf{c})$ is reachable from s_0 in $TS(\mathcal{S})$?"

1. Build $RG(\mathcal{S})$
2. For all state $(q', [\mathbf{x}])$ of $RG(\mathcal{S})$ do
3. If $q' = q$ then
4. If $((q, [\mathbf{x}]), \mathbf{c})$ is reachable in $RG(\mathcal{S})$ 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...

Conclusion

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 :

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]

References I

Aurore Annichini, Eugene Asarin, and Ahmed Bouajjani.
Symbolic techniques for parametric reasoning about counter and clock systems.
In CAV, volume 1855 of LNCS, pages 419–434. Springer, 2000.

Rajeev Alur, Costas Courcoubetis, Thomas A. Henzinger, and Pei-Hsin Ho.
Hybrid automata: An algorithmic approach to the specification and verification of hybrid systems.
volume 736 of LNCS, pages 209–229, 1992.

Sébastien Bardin, Alain Finkel, Jérôme Leroux, and Laure Petrucci.
FAST: Fast Acceleration of Symbolic Transition systems.
In CAV, volume 2725 of LNCS, pages 118–121. Springer, 2003.

Tommaso Bolognesi, Ferdinando Lucidi, and Sebastiano Trigila.
From timed petri nets to timed lotos.
In PSTV, pages 395–408. North-Holland, 1990.

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.

References II

Zhe Dang, Oscar H. Ibarra, Pierluigi San Pietro, and Gaoyan Xie.
Real-counter automata and their decision problems.
In FSTTCS, volume 3328 of LNCS, pages 198–210, 2004.

P.M. Merlin.
A study of the recoverability of computing systems.
PhD thesis, University of California, Irvine, 1974.

Gaoyan Xie, Zhe Dang, Oscar H. Ibarra, and Pierluigi San Pietro.
Dense counter machines and verification problems.
In CAV, volume 2725 of LNCS, pages 93–105, 2003.