Verification of Input-bounded FIFO Machines

Amrita Suresh
Supervised by Prof. Alain Finkel

Laboratoire Spécification et Vérification, ENS Paris-Saclay

March-July 2019

Special thanks to Dr. Benedikt Bollig
# Table of Contents

1. Introduction
2. Branch-WSTS
3. Reachability
FIFO Machines

Distributed processes such that

- each process is a finite state machine
- there are a fixed number of processes
- they communicate using queues
Example

Client-to-Server

Server-to-Client
Example

Client-to-Server

Server-to-Client
Example

Client

Server

Client-to-Server

Server-to-Client
Example
Example

Client-to-Server

Server-to-Client
A FIFO machine $S$ with one channel $c$ is defined as $S = (Q, \Sigma, T)$ where
- $Q$ is a finite set of control-states,
- $\Sigma$ is the alphabet,
- $T \subseteq Q \times \{!, ?\} \times \Sigma \times Q$ is the transition relation.

The system is said to be in a configuration $s = (q, w)$ when the control-state is $q$ and the contents of the channel are $w$. 
Formal definition

\[ Q = \{ q_0, q_1, q_2, q_3 \} \]

\[ \Sigma = \{ a, b \} \]

Figure: A FIFO system \( S \) with initial configuration \((q_0, \epsilon)\).
Verification problems

Give a FIFO machine $S$ with an initial configuration $s_0 = (q_0, w_0)$,
- $S$ terminates if it has no infinite run.
Verification problems

Give a FIFO machine $S$ with an initial configuration $s_0 = (q_0, w_0)$,

- $S$ terminates if it has no infinite run.
- $S$ is bounded if $Post^*(s_0)$ is finite.
Verification problems

Give a FIFO machine $S$ with an initial configuration $s_0 = (q_0, w_0)$,

- $S$ terminates if it has no infinite run.
- $S$ is bounded if $Post^*(s_0)$ is finite.

Note

Termination implies boundedness, but the converse is false.

\[(q_0, \epsilon) \rightarrow (q_1, a) \rightarrow (q_2, ab) \rightarrow (q_3, b) \rightarrow (q_0, \epsilon) \rightarrow \ldots \text{ is a non-terminating run.} \]

$Post^*(s_0)$ is bounded.
Verification problems

Give a FIFO machine $S$ with an initial configuration $s_0 = (q_0, w_0)$,
- $S$ terminates if it has no infinite run.
- $S$ is bounded if $Post^*(s_0)$ is finite.

Theorem

Testing the unboundedness of a channel in a general FIFO system is undecidable.¹

Verification problems

Give a FIFO machine $S$ with an initial configuration $s_0 = (q_0, w_0)$,

- $S$ terminates if it has no infinite run.
- $S$ is bounded if $Post^*(s_0)$ is finite.
- a configuration $(q, w)$ is reachable if $\exists \sigma$ such that $(q_0, w_0) \xrightarrow{\sigma} (q, w)$.
Verification problems

Give a FIFO machine \( S \) with an initial configuration \( s_0 = (q_0, w_0) \),

- **\( S \) terminates** if it has no infinite run.
- **\( S \) is bounded** if \( \text{Post}^*(s_0) \) is finite.
- A configuration \((q, w)\) is **reachable** if \( \exists \sigma \) such that \((q_0, w_0) \xrightarrow{\sigma} (q, w)\).
- A **control-state \( q \) is reachable** if \( \exists \sigma \) and \( \exists w \) a channel valuation such that \((q_0, w_0) \xrightarrow{\sigma} (q, w)\).
Approach to verification

- Idea: to use over and under-approximations for verification
Approach to verification

- Idea: to use over and under-approximations for verification

- "Input-bounded FIFO systems" - an underapproximation
Some subclasses of FIFO systems

The following subclasses have decidable properties.

- *Half-duplex systems* with two processes (but extension to three processes leads to undecidability). (Cécé and Finkel 2005)
- *Lossy FIFO systems*. (Abdulla et al. 2004)
- *Existentially-bounded deadlock-free FIFO automata*. (Genest, Kuske, and Muscholl 2007)
- *Synchronisable FIFO systems*. (Alain Finkel and Lozes 2017)
- *Flat FIFO systems* (most verification problems are in \(NP\)). (Alain Finkel and Praveen 2019)
Input-bounded FIFO Systems

- **Bounded** language - \( L \subseteq w_1^* \ldots w_k^* \).
- **Input**-bounded - \( L_{send} \) is bounded.
Input-bounded FIFO Systems

- **Bounded** language - $L \subseteq w_1^* ... w_k^*$.
- **Input**-bounded - $L_{send}$ is bounded.
- **Reachability**-bounded - Channel contents belong to a bounded language.

Theorem: A two-counter Minsky machine can be simulated by a reachability-bounded FIFO system.
Input-bounded FIFO Systems

- **Bounded** language - \( L \subseteq w_1^* \ldots w_k^* \).
- **Input**-bounded - \( L_{send} \) is bounded.
- **Reachability**-bounded - Channel contents belong to a bounded language.

**Theorem**

A two-counter Minsky machine can be simulated by a reachability-bounded FIFO system.
# Table of Contents

1. Introduction
2. Branch-WSTS
3. Reachability
Well Structured Transition Systems (A. Finkel and Schnoebelen 2001)

- A wqo over a set $X$ $\implies$ every infinite sequence $x_0, x_1, x_2, \ldots$ over $X$ contains an increasing pair:
  $\exists i < j$ s.t. $x_i \leq x_j$. 

Well Structured Transition Systems (A. Finkel and Schnoebelen 2001)

- A wqo over a set $X \implies$ every infinite sequence $x_0, x_1, x_2, \ldots$ over $X$ contains an increasing pair:
  $\exists i < j \text{ s.t. } x_i \leq x_j$.

- Example
  - $\mathbb{N}$ over the ordering $\leq$ is wqo.
  - $\mathbb{Z}$ over the ordering $\leq$ is not. e.g. $-1 \geq -2 \geq -3 \ldots$ has no increasing pair.
Well Structured Transition Systems (A. Finkel and Schnoebelen 2001)

- A wqo over a set $X$ $\implies$ every infinite sequence $x_0, x_1, x_2, ...$ over $X$ contains an increasing pair:
  $\exists i < j$ s.t. $x_i \leq x_j$.
- The transition system $(X, \rightarrow)$ has strong compatibility i.e.

\[
\begin{array}{ccc}
\delta & & \delta \\
\downarrow & & \downarrow \\
\delta & & \delta \\
\end{array}
\]

\[
\begin{array}{ccc}
s & \leq & t \\
\downarrow & & \downarrow \\
s' & \leq & t' \\
\end{array}
\]
Branch-WSTS

- $S = (X, \rightarrow, \leq)$ is branch-WSTS if it is
  - branch-wqo
    - if for every infinite run $n_0(x_0) \rightarrow n_1(x_1) \rightarrow n_2(x_2), \ldots$ of $S$, $x_0, x_1, \ldots$ is wqo.
\( S = (X, \rightarrow, \leq) \) is branch-WSTS if it is branch-wqo

- if for every infinite run \( n_0(x_0) \rightarrow n_1(x_1) \rightarrow n_2(x_2), \ldots \) of \( S \), \( x_0, x_1, \ldots \) is wqo.

This FIFO system is branch-wqo under the prefix ordering but it is not wqo.
Branch-WSTS

- \( S = (X, \rightarrow, \leq) \) is \textit{branch-WSTS} if it is
- \textit{branch-wqo}
- \textit{branch-compatible}
  - if for all configurations \( s, t, s' \) such that \( s \preceq t \) and \( s \xrightarrow{a} s' \xrightarrow{w} t \) implies that there exists a \( t' \) such that \( t \xrightarrow{a} t' \) and \( s' \preceq t' \).

\[\begin{array}{ccc}
  s & \ll & t \\
  \downarrow a & & \downarrow a \\
  s' & \ll & t' \\
  \downarrow w & & \downarrow w
\end{array}\]
Finite Reachability Tree

$q_0 \xrightarrow{!a} q_1 \xrightarrow{?a} q_2 \xrightarrow{!b} q_0$,

$q_0, \epsilon$

---

Finite Reachability Tree\(^1\)

\[q_0 \xrightarrow{!a} q_1 \xrightarrow{?a} q_2 \]

\[q_0, \epsilon \]

\[q_1, a \]

---

Finite Reachability Tree\(^1\)

Adapted from A. Finkel and Ph. Schnoebelen (2001). “Well-structured transition systems everywhere!”.

Finite Reachability Tree

\[ q_0 \xrightarrow{!a} q_1 \xrightarrow{?a} q_2 \]

\[ q_0, \epsilon \]

\[ q_1, a \]

\[ q_1, ab \]

\[ q_2, \epsilon \]

\[ q_2, b \]

\[ X \]

\[ X \]

---

Why branch-WSTS?

Theorem

Boundedness and termination are decidable for branch-WSTS, if $\leq$ is a decidable, partial ordering, and has computable successor.
Why branch-WSTS?

**Theorem**

Boundedness and termination are decidable for branch-WSTS, if $\leq$ is a decidable, partial ordering, and has computable successor.

**Proof sketch**

- A branch-WSTS $S = (S, \rightarrow, \leq)$ has a finite reachability tree.
- Unbounded iff there exist two configurations in the finite reachability tree such that $s_1 \xrightarrow{*} s_2$ and $s_1 < s_2$.
- Non-terminating iff there exists a subsumed node in the FRT.
Input-bounded FIFO systems over the prefix-ordering

**Theorem**

Input-bounded FIFO automata are branch-wqo for the prefix-ordering $\leq_{\text{pref}}$.

But they are not branch-compatible.

**Figure:** Consider $S$, and configurations $(q_1, \epsilon)$ and $(q_1, a)$.
Prefix compatible relation

For two configurations \( s = (q, w), s' = (q', w') \), \((q, w) \preceq_{\text{comp}} (q', w')\) if
- \((q, w) \preceq_{\text{pref}} (q', w')\) and
- \(\exists \sigma\) (with send and receive actions \(y_{\sigma}\) and \(x_{\sigma}\) resp.) such that \(s \xrightarrow{\sigma} s'\) and
  - \(x_{\sigma} = \epsilon\) or
  - \(|x_{\sigma}| \leq |y_{\sigma}|\) and \(x_{\sigma}^{\omega} = w.y_{\sigma}^{\omega}\).

Theorem

FIFO systems are branch-compatible for the relation \(\preceq_{\text{comp}}\).
The prefix compatible relation is not an ordering.

Theorem

Under this relation, we can construct a finite reachability tree for input-bounded FIFO systems.\textsuperscript{2}

Termination

Theorem

Termination is decidable for input-bounded FIFO systems
# Table of Contents

1. Introduction
2. Branch-WSTS
3. Reachability
Reachability results

Theorem
Reachability and control-state reachability are reducible to one another for input-bounded FIFO systems.
Reachability of input-letter bounded systems

Theorem

Control state reachability for input-letter bounded FIFO systems is decidable.
Proof idea

Input-letter bounded FIFO systems can be simulated by counter machines with hierarchical zero tests.

A FIFO machine $S$. 

\[ q_0 \xrightarrow{\epsilon} q_1 \]

\[ q_0 \overset{!a}{\xrightarrow{}} q_1 \]

\[ q_1 \overset{a}{\xrightarrow{\epsilon}} q_0 \]

\[ q_1 \overset{!b}{\xrightarrow{}} q_0 \]

\[ q_0 \overset{c_a++}{\xrightarrow{}} q_1 \]

\[ q_1 \overset{c^\prime_{a} --}{\xrightarrow{}} q_0 \]

\[ q_0 \overset{c_b++}{\xrightarrow{}} q_1 \]
Proof idea

Input-letter bounded FIFO systems can be simulated by counter machines with hierarchical zero tests.

Counter automata corresponding to the FIFO machine $S$. 
## Conclusion

<table>
<thead>
<tr>
<th>System</th>
<th>Boundedness</th>
<th>Termination</th>
<th>Reachability</th>
</tr>
</thead>
<tbody>
<tr>
<td>General FIFO systems</td>
<td>No [B83]</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Lossy Channel systems</td>
<td>Yes [A04]</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Flat Systems</td>
<td>Yes [F19]</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Reachability Bounded systems</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Input-bounded systems</td>
<td>Yes [J93]</td>
<td>Yes</td>
<td>?</td>
</tr>
<tr>
<td>Input-different-letter bounded systems</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes [F87]</td>
</tr>
<tr>
<td>Input-letter bounded systems</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Table:** Verification problems
Thank you!
Questions?
The half-duplex property for two machines and two channels (one in each direction) says that each reachable configuration has at most one channel non-empty.


Choquet, A and A Finkel (1987). “Simulation of linear FIFO nets having a structured set of terminal markings”. In:

Finkel, Alain and Etienne Lozes (2017). “Synchronizability of communicating finite state machines is not decidable”. In: ICALP.

