Arnaud Bailly

Presentation based on

Unreliable Channels are Easier To Verify Than Perfect Channels

by G. Cécé, A. Finkel, and S. Purushothaman Iyer

Communicating Finite-State Machines

- Are finite-state automata,
- Communicating through channels that are
  - unbounded,
  - fifo,
  - perfect (no losses, no duplications, no insertions).

Product Automaton

After combination, study on only one machine.
CFSMs, Formally

A machine is noted
\[
(S, C, \sum_{i \in C} s_i, \delta)
\]

with
\[
\delta \subseteq S \times \left( \bigcup_{c \in C} \{(c, a, c, a) \mid a \in \sum_c \} \right) \times S
\]

Configurations are in \( G(M) \) set of:
\[
\{ x, x_1, \ldots, x_n \} \text{ with } x_{n+1} \sum_{c_i}
\]

Problems of Interest

- With \( R(M) \) the set of reachable configurations of \( M \).
- **Reachability:** does \( \{ x, x_1, \ldots, x_n \} \) belong to \( R(M) \)?
- **Deadlock:** has \( \{ x, x_1, \ldots, x_n \} \) any successor?
- **Boundedness:** is \( R(M) \) finite?
- Others: finite termination, computation of \( R(M) \), model-checking against CTL*. Think about distributed software verification!

But... [BZ83]

- **CFSMs are Turing-Powerful!**
- Mark the first and last cell by a symbol.
- Add a symbol "&" to mark the head.
- Advance one cell is:
  - receive \( s \) from channel and repeat:
    - receive \( s \),
    - if \( s \) not "&" then emit \( s \) and \( s' := s \)
    - else emit & and emit \( s' \).
  - read the list until end symbol, emit symbol.
- Write and go-back are similar.
- Every problem of interest is undecidable!
Unreliable Channels

- Unreliable channels can:
  - lose messages, or
  - duplicate messages, or
  - insert new messages, or
  - a combination of all the above.

Lossy Channels [AJ94]

- Can lose any message.
- Subwords: $x \subseteq y$ if $x = a_n \ldots a_1$ and $y = y_m \ldots y_1$, with $y \subseteq \sum^*$
- Closure: $closure(s) = \{z \mid z \subseteq x, x \subseteq s\}$
- Higman’s theorem (1952):
  - There is no infinite set of words $W$ such that all members of $W$ are pairwise incomparable.
  - In particular, there is no infinite chain $W \subseteq W\ldots$ of upward-closed sets of words.
  - For $\Gamma \subseteq G(M)$ then the set of predecessors of $\Gamma$ forms an upward-closed chain. Hence it is finite.
  - A new proof is given.

Duplication Machines

- It is shown that they are Turing expressive.
- Modify the machine so that:
  - each symbol is followed by $\#$.
  - $\#$ is not in the alphabet of the machine.
- One can build an homomorphism from modified to plain machines.
- It is shown that one can build a “squeeze repeats” homomorphism from duplication machines to modified machines.
Insertion Machines

- It is shown that:
  Since one can insert symbols everywhere on the tape, channel languages are upward-closed.
- Hence:
  The reachability problem is solvable.

Combination of Errors

Insertion and Lossiness are "stronger" than duplication.

Questions?

Thank You!
References