Arnaud Bailly

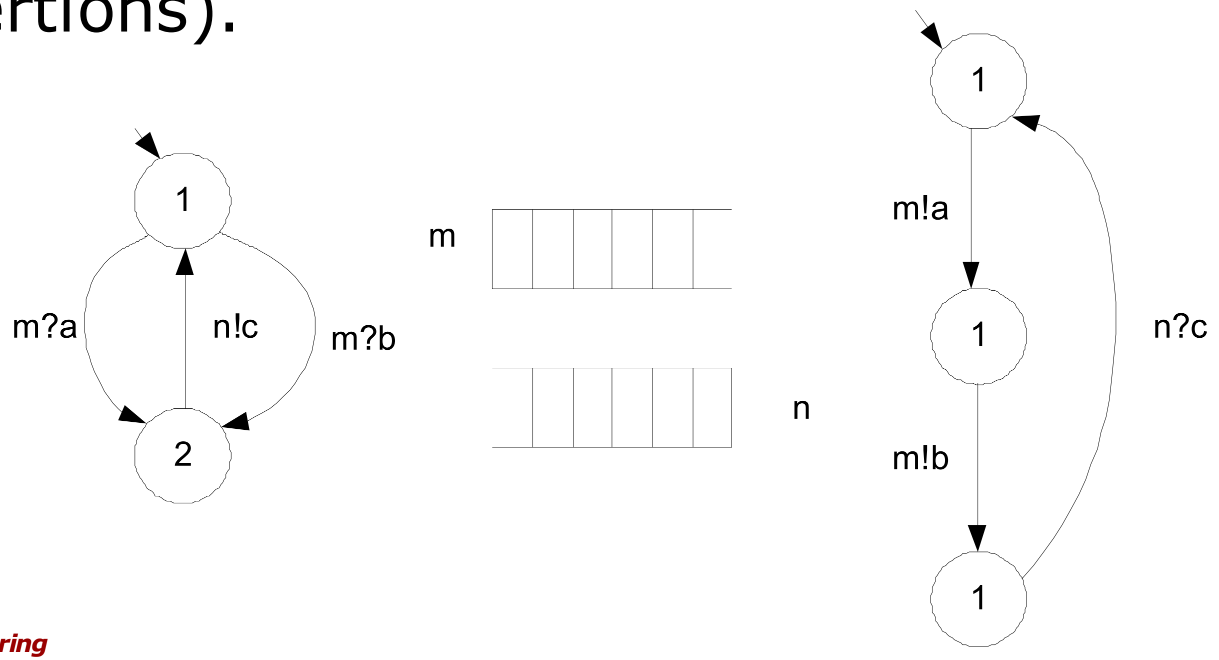
Presentation based on

Unreliable Channels are Easier To Verify Than Perfect Channels

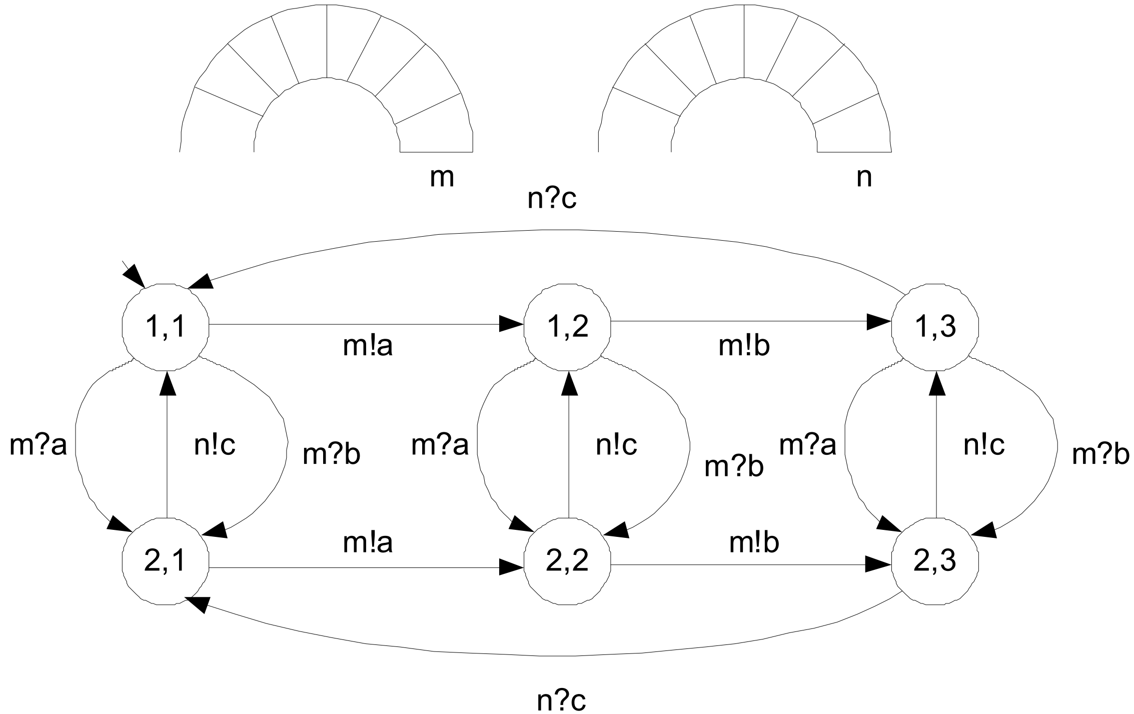
by G. Cécé, A. Finkel, and S. Purushotaman Iyer

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

$$(S, C, \bigcup_{c \in C} \Sigma_c, s_0, \delta)$$

with

$$\delta \subseteq S \times (\bigcup_{c \in C} \{c?a, c!a \mid a \in \sum_c \}) \times S$$

Configurations are in $G(M)$ set of:

$$\langle s, x_1, \ldots, x_n \rangle \text{ with } x_i \in \sum_{ci}^{*}$$

Problems of Interest

- With $R(M)$ the set of reachable configurations of M.
- **Reachability**:

  does $\langle s, x_1, \ldots, x_n \rangle$ belong to $R(M)$?
- **Deadlock**: has $\langle s, x_1, \ldots, x_n \rangle$ 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 &, 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: $x \leq y$ if $x = a_1 \ldots a_n$ and $y = y_0 a_1 y_1 \ldots a_n y_n$ with $y_i \in \sum^*$
- Closure: $closure(x) = \{z \in \sum^* \mid x \leq z\}$
- 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 $W_1, W_2, \ldots$ of upward-closed sets of words.
- For $\Gamma \subset G(M)$ then the set of predecessors of Γ 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

- [BZ83] D. Brand and P. Zafiropulo. On communicating finite-state machines, Journal of the ACM, 30(2): 323-342, 1983.
- [AJ94] Parosh Aziz Abdulla and Bengt Jonsson: Undecidable Verification Problems for Programs with Unreliable Channels. ICALP 1994: 316-327