Dealing with non-local choice in IEEE 1073.2's Standard for Remote Control

Arjan J. Mooij (and Nicolae Goga)

4th June 2004 – SAM 2004

Summary

Many protocol synthesis algorithms have been developed,

but they are not always directly applicable in practice.

Non-local branching choice nodes are usually excluded,

while such nodes cannot easily be eliminated or avoided.

We propose a way to deal with non-local choice

and apply it to the IEEE 1073.2 standard.

Overview of this talk

- The ISO/IEEE 1073 standard
- Synthesis algorithms
- The problem of non-local choice nodes
- Our solution
- Application on the remote control package
- Conclusions and further work

ISO/IEEE 1073

Draft Standard for Medical Device Communications

- communication protocols
- ...

Formal analysis is not common in their development

Current protocol description in the Remote Control package:

- collection of message sequence charts
- accompanying textual descriptions

Our targets: extract and analyze a formal description of the intended communication protocol

Protocol synthesis algorithms

Typical procedure:

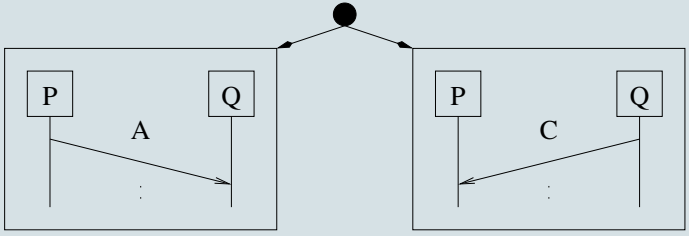
1. project the behavior of each MSC on the individual processes
2. compose the MSCs per process as described by the hMSC
3. minimize the process descriptions

Composing behaviors per processes:

- weak sequential composition
- delayed choice (i.e. "wait-and-see" approach)

No suitable implementation for non-local choice nodes.

Non-local choice nodes



High-level message sequence charts containing non-local choice nodes

- are erroneous high-level message sequence charts
- implicitly specify additional synchronization
- indicate implied behavior

Some opportunities to eliminate non-local choice nodes

- explicitly introduce additional synchronization
- introduce some parallelism and synchronization

Back to practice... (i)

Non-local choice nodes:

- no standard implementation
- elimination at the cost of simplicity
- elimination at the cost of introducing additional messages

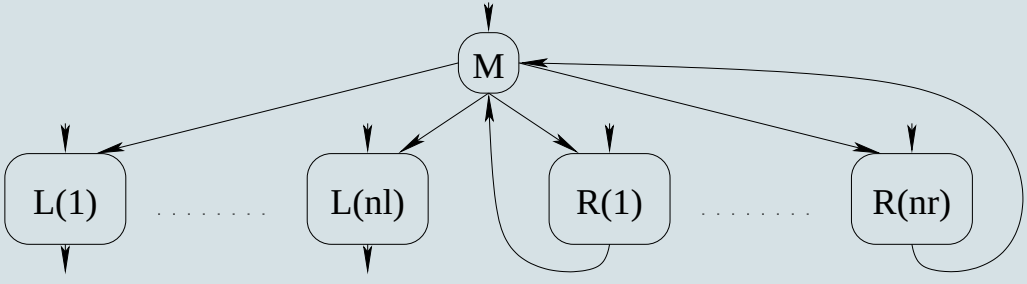
Back to practice... (i)

Non-local choice nodes:

- no standard implementation
- elimination at the cost of simplicity
- elimination at the cost of introducing additional messages

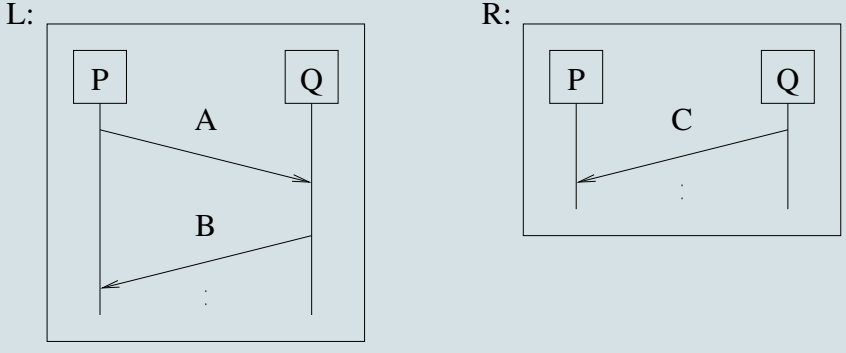
Remote control package does not require a generic solution

- shape of the high-level message sequence chart:



Back to practice... (ii)

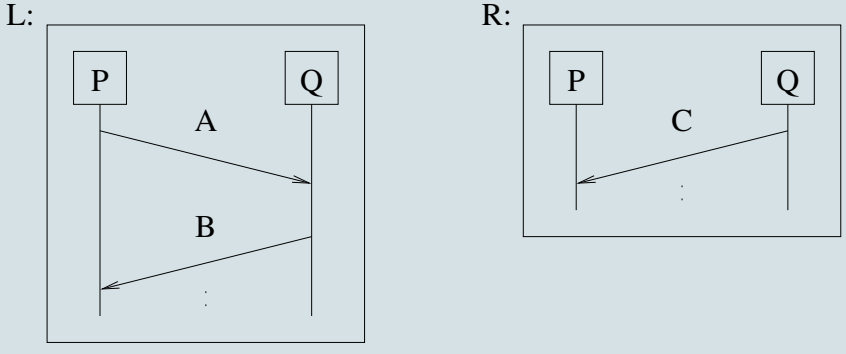
- typical prefixes of the message sequence charts:



Where could these messages be used for?

Back to practice... (ii)

- typical prefixes of the message sequence charts:



Where could these messages be used for?

In fact a synchronization protocol has been encoded !

A synchronization protocol

Initiative at two different processes

- complicated to encode in hMSC

For process P starting an L MSC:

- send a "Request" message to process Q
- wait for a "Confirmation" message from process Q
- execute the remainder of the L MSC

For process Q starting an R MSC:

- execute the R MSC

Formalization

Usual implementations:

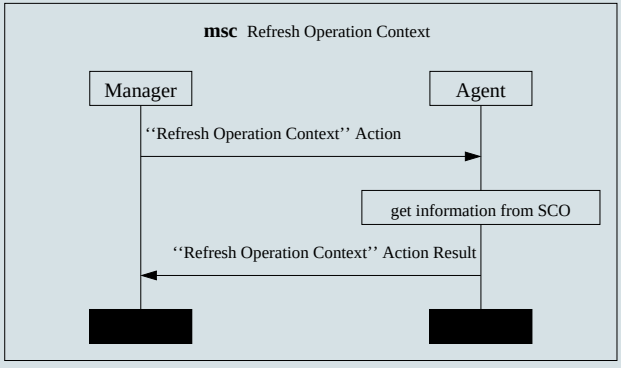
$$P = \Pi_P(M) = \left(\sum_{m \in L} \Pi_P(m)\right) + \left(\sum_{n \in R} \Pi_P(n) \cdot P\right)$$

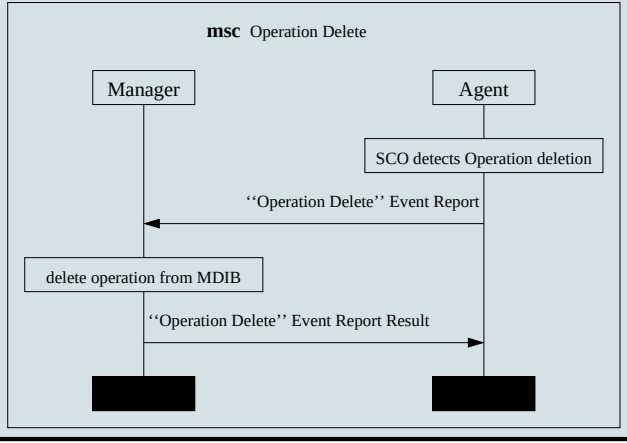
$$Q = \Pi_Q(M) = \left(\sum_{m \in L} \Pi_Q(m)\right) + \left(\sum_{n \in R} \Pi_Q(n) \cdot Q\right)$$

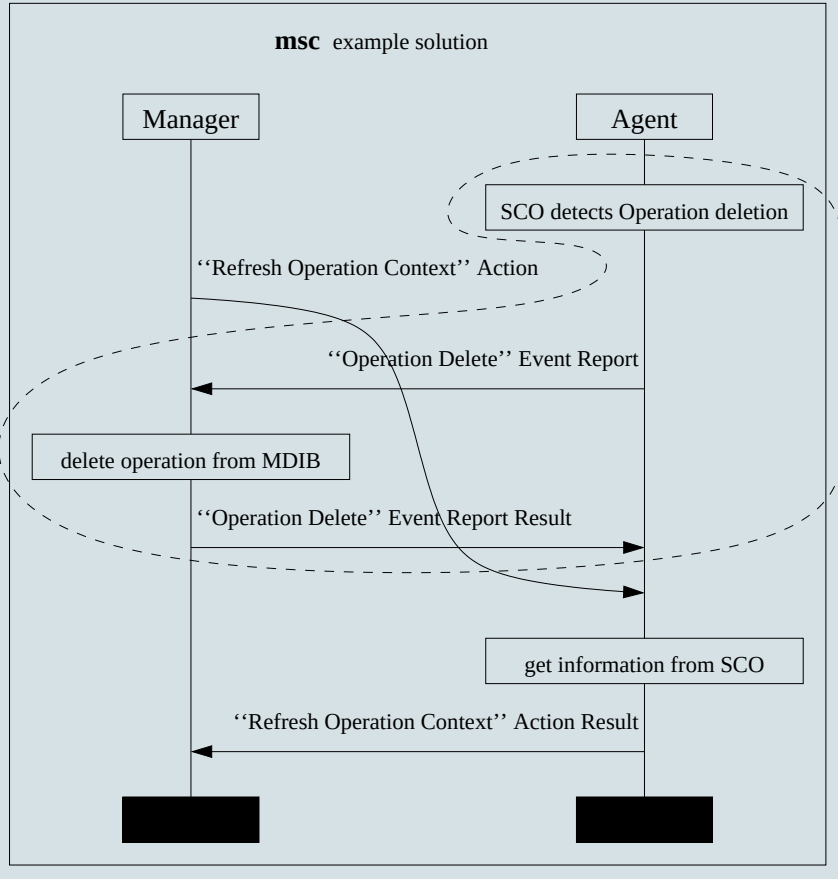
Our proposed implementation:

$$\begin{aligned} P &= \left(\sum_{m \in L} hd(\Pi_P(m)) \cdot P'(m)\right) + \left(\sum_{n \in R} \Pi_P(n) \cdot P\right) \\ P'(m) &= tl(\Pi_P(m)) + \left(\sum_{n \in R} \Pi_P(n) \cdot P'(m)\right) \\ Q &= \left(\sum_{m \in L} \Pi_Q(m)\right) + \left(\sum_{n \in R} \Pi_Q(n) \cdot Q\right) \end{aligned}$$

Back to the remote control package ...






msc example solution
Manager
Agent
SCO detects Operation deletion
‘‘Refresh Operation Context’’ Action
‘‘Operation Delete’’ Event Report
delete operation from MDIB
‘‘Operation Delete’’ Event Report Result
get information from SCO
‘‘Refresh Operation Context’’ Action Result

Analysis of the obtained protocol

Create state transition tables for inclusion in the standard

Derive Promela models of the protocol

Analyze these models using the Spin model checker

- deadlock scenario's
- unreachable code

Discuss with the developers of the protocol

The developers agree on this protocol implementation !

Conclusions

Non-local choice nodes

- are frequently excluded in the literature
- can easily be introduced in practice
- but they cannot easily be eliminated or avoided

Our proposed solution

- does not give an exact implementation of the message sequence chart
- but it matches the intentions of the protocol developers
- does not make the hMSC much more complicated

Further work

Theoretical aspects:

- generalize our solution
- extend the theory on non-local choice problems

IEEE 1073.2 Remote control:

- participate in extensions of the standard

Health Level Seven (HL7) standard:

- apply our solution to the non-local choice problems
- study other problems in obtaining protocol implementations

Questions ???

My homepage:
http://www.win.tue.nl/~amooij/

Improving the Quality of Protocol Standards:
http://www.win.tue.nl/oas/index.html?iqps/

We are very interested in communication protocols (possibly from protocol standards) where this kind of techniques might be effectively exploited.