Open Mixed Refinement

Marco Carbone
IT University of Copenhagen
Copenhagen, Denmark
carbonem@itu.dk

Thomas Hildebrandt
IT University of Copenhagen
Copenhagen, Denmark
hilde@itu.dk

Hugo A. López
IT University of Copenhagen
Copenhagen, Denmark
lopez@itu.dk

Abstract

We propose a generalization of covariant contravariant simulation that also takes account of termination and allows intermediate open parts of the specification.

1 Introduction

Consider a healthcare workflow process in which you have a patient Alice, a doctor Bob, and a Social Worker Charlie. The following set of activities are included in the first specification S:

1. Alice comes to Bob for a medical appointment.
2. Bob receives Alice and gathers her symptomatology.
3. After consulation, Bob formulates a medicine treatment for Alice.
4. Bob sends the medicine formulation to Charlie, so he can deliver it to Alice.
5. Alice gets the medicine from Charlie and starts taking her treatment regularly as specified by Bob.
6. After some days, Alice comes back to Bob for a control, and the symptoms have dissapeared.

Many details have been hindered from this example. First of all, it only details the interaction between three of the main actors involved. We may have a private health care institution that has to fulfill the auditing processes, where between activity 2 and 3. other actors will come into play. Our specification S could be extended accordingly to a new model S' including the two actions

- On insuficiency of information, Bob will take blood samples and supplementary tests from Alice.
- On cases with high variability, Bob will consult a pool of specialist on Alice's case.

between action 2. and 3.

It is to note, that even when S' has more behavior than S, it is still constrained to a set of activities that can be performed. The extra set of activities can be repeated many times and with different execution orders, but activities outside this set have to be ruled out. For instance, Bob cannot start operating Alice just after having gather her symptomatology.

How is S related to S'? It is clear that the notion that we are looking for has a lot to do with the notion of *refinement*. In many cases we will specify systems by adding up more and more roles (and their respective behaviors) over the time. This, will lead us to start with a specification like S, knowing that each of the actions can be further refined with more and more behavior. We propose a new controlled way, called *open refinement*, to specify where and which actions can be inserted. The idea is in addition to standard transitions $P \xrightarrow{a} P'$ where a process P exhibits an immediate action a before evolving into P' to also specify *open* states ${}_{A}\circlearrowleft P \xrightarrow{a} P'$, where the process P can exhibit a finite series of actions in A before evolving with a into P'. The open state allows us to describe explicit stages in a process in which a process can be refined with any of the actions in a constrained set A. Here, transitions become weaker, as they might need more than one step for moving from P to P', but they also become broader than the standard weak transitions, as the set A can involve several (and possibly visible) actions and not just a dedicated internal action.

These changes lead us to proposing a new notion of refinement we call *open mixed refinement*. Starting from the covariant-contravariant simulations (that allow mixed, externally and internally controlled, activities and captures the necessary difference between such) we add the new notion of open states and also the ability to specify explicitly if a system may terminate in a state from which additional internally controlled activities are possible.

We believe the proposed model has both good uses in practice and good properties, i.e. can be given a clean categorical representation. We start in this brief abstract by giving the definition and the first result that open mixed refinement specializes to covariant-contravariant simulation if one allows no open states and always allow termination.

2 Open Mixed Trees and Refinement

Definition 1 (Open Mixed Trees)**.** *An* open mixed tree *is defined as the tuple* $OT = \langle S, s_0, \mathsf{Act}^-, \mathsf{Act}^+, \sigma, T, \rightarrow \rangle$ *such that:*

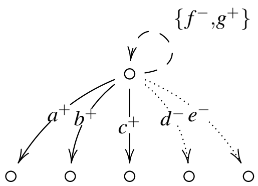
- S *is a set of* states*,*
- $s_0 \in S$ *is the* initial state*,*
- $\mathsf{Act} = \mathsf{Act}^- \cup \mathsf{Act}^+$ *is a set of actions characterized as externally controlled actions in* Act^- *(denoted by* $\rightarrow^-$*) and internally controlled actions in* Act^+ *(denoted by* $\rightarrow^+$*).*
- $\rightarrow \subseteq S \times \mathsf{Act} \times S$ *is a labelled transition relation between states, where d is a polarity* $\{+,-\}$*,*
- $\sigma : S \rightarrow \mathscr{P}(\mathsf{Act})$ *defines for each state a set of* open actions*,*
- $T \subseteq S$ *and* $s \notin T \implies \exists s \xrightarrow{b^+}$*, which defines the states in which the process may terminate without further internally controlled actions,*
- $\forall s \in S$*, there exists a unique path* $S_0 \rightarrow^* s$ *(i.e. the transition relation forms a tree)*

An open mixed tree where $\sigma(s) = \emptyset$ *for all* $s \in S$ *and* $T = S$*, i.e. an open mixed tree with no open actions and which allow termination in every state, is referred to as just a mixed tree. A mixed tree is equivalent to a normal tree labelled with positive and negative labels.*

Intuitively, an open mixed tree represents the specification of a reactive, non-deterministic system with both internally controlled actions (e.g. output) and externally controlled actions denoted by $\rightarrow^-$. Note that there may be actions in $\mathsf{Act}^- \cap \mathsf{Act}^+$ that are both externally and internally controlled.

In any state with at least one internally controlled action any implementation must be able to do at least one of the internally controlled actions, or terminate if termination is also allowed by the specification. The states in which it is allowed to terminate is defined by the set T. Note that in order to not have any contradictions a state which is not in T (i.e. termination without further internally controlled actions is not allowed) must have at least one internally controlled action out of it.

Finally, the function σ pairs each state with a set of *open* (or underspecified) behavior, which allows an implementation to perform any action within the set a finite number of times before progressing (or terminating if the state is in T. We can depict open trees easily:



Below we write $s_1 \xrightarrow{\ell^d} s_2$ when $\{s_1, \ell, s_2\} \in \rightarrow$ and $\ell \in \mathsf{Act}^d$. Similarly, we write $\sigma^+(s_1)$ for the set of transitions such that $s_1 \xrightarrow{a^+} s_1' \in \sigma$

Definition 2 (Open Mixed Refinement)**.** *A binary relation $\mathscr{R}$ over open mixed trees is considered a refinement whenever, given $a, b \in \mathsf{Act}$, $P = \langle S_1, s_1, \mathsf{Act}^-, \mathsf{Act}^+, \sigma_1, T_1, \rightarrow_1\rangle$ and $Q = \langle S_2, s_2, \mathsf{Act}^-, \mathsf{Act}^+, \sigma_2, T_2, \rightarrow_2 \rangle$ such that $s_1 \mathscr{R} s_2$, the following conditions are met:*

1. *$\forall s_1 \xrightarrow{a^-} s_1'$, implies $\exists s_2 \xrightarrow{a^-} s_2'$ and $s_1' \mathscr{R} s_2'$,*

2. *$\forall s_2 \xrightarrow{a^+} s_2'$ implies (i) $\exists s_1 \xrightarrow{a^+} s_1'$, and $s_1' \mathscr{R} s_2'$ or (ii) $a \in \sigma_1^+(s_1)$ and $s_1 \mathscr{R} s_2'$*

3. *$\sigma_2(s_2) \subseteq \sigma_1(s_1)$,*

4. *$s_2 \in T_2 \implies s_1 \in T_1$*

5. *$s_1 \in T_1 \implies s_2 \xrightarrow{a_1} s_{2,1} \xrightarrow{a_2} \cdots \xrightarrow{a_n} s_{2,n}$ and $a_i \in \sigma_1(s_1)$, $s_1 \mathscr{R} s_{2,i}$ and $s_{2,n} \in T_2$.*

6. *if $s_1 = s_{1,0}$ and $s_2 = s_{2,0}$, ($s_{1,i} \xrightarrow{a_i} s_{1,i+1}$ or ($s_{1,i} = s_{1,1+1}$ and $a_i \in \sigma_1(s_{1,i})$)), $s_{2,i} \xrightarrow{a_i} s_{2,i+1}$, and $s_{1,i} \mathscr{R} s_{2,i}$ for $i \in \omega$ then $|s_{1,i}| = \omega$.*

We say that Q is an open mixed refinement *of P, written $P \sqsubseteq Q$, whenever there exists a relation $\mathscr{R}$ such that $P \mathscr{R} Q$.*

Proposition 1. *The open mixed refinement relation $\sqsubseteq$ between open mixed trees as defined above*

1. *is reflexive and transitive, and*

2. *contains the identity relation*

As stated in the proposition below, open refinement specializes for mixed trees (i.e. open mixed trees with no open actions and which allow termination in every state) to the notion of covariant-contravariant simulation defined in [2, 1].

Proposition 2. *Open refinement for mixed trees coincides with* $(\mathsf{Act}^+ \backslash \mathsf{Act}^-, \mathsf{Act}^- \backslash \mathsf{Act}^+)$*-simulation as defined in [2], taking* $\mathsf{Act}^- \cap \mathsf{Act}^-$ *as the set of actions with "bi"-polarity, i.e. both internally and externally controlled.*

References

[1] L. Aceto, I. Fábregas, D. de Frutos Escrig, A. Ingólfsdóttir, and M. Palomino. Relating modal refinements, covariant-contravariant simulations and partial bisimulations. *Fundamentals of Software Engineering, FSEN*, 2011.

[2] I. Fabregas, D. de Frutos Escrig, and M. Palomino. Logics for contravariant simulations. In *Formal Techniques for Distributed Systems: Joint 12th IFIP WG 6.1 International Conference, FMOODS 2010 and 30th IFIP WG 6.1 International Conference, FORTE 2010, Amsterdam, The Netherlands, June 7-9, 2010, Proceedings*, volume 6117, page 224. Springer-Verlag New York Inc, 2010.