Reihe Informatik. TR-2007-004

Robustness in Interaction Systems

Mila Majster-Cederbaum, Moritz Martens*

Universität Mannheim

Abstract. We deal with the effect of absence/failure of ports or components on properties of component-based systems. We do so in the framework of *interaction systems*, a formalism for component-based systems that strictly separates the issues of local behavior and interaction, for which ideas to establish properties of systems were developed. We propose how to adapt these ideas to analyze how the properties behave under absence or failure of certain components or merely some ports of components. We present results concering deadlock-freedom and liveness.

1 Introduction

Component-based design techniques are an important paradigm for mastering design complexity and enhancing reusability. In the object-oriented approach subsystems interact by invoking in their code operations or methods of other subsystems and hence rely on the availability of these subsystems. In contrast to this, components are designed independently from their context of use. They are put together by some kind of gluing mechanism. Various theoretical frameworks to model and investigate component-based systems have been proposed, see for example [Arb02,BB06,AG97,Bro99].

We build here on *interaction systems*, a model for component-based systems that was proposed and discussed by Sifakis et al. in [GS05,Sif05,GS03,GS02] and has been implemented in the PROMETHEUS [Gös01] as well as the BIP tool [BBS06].

We present the model and describe some of the properties that can be formulated. Then we explain in what sense we want to investigate whether a certain property is not affected by the absence of certain components or ports of components.

The report is structured as follows. In Sect. 2 we give a summary of the model of interaction systems. In Sect. 3 we present properties of interaction systems. Section 4 states the results concerning failure of a set of ports for the properties of deadlock-freedom and liveness and presents the proofs. These results have been published without the proofs in [MCM07].

* E-mail: mmartens@informatik.uni-mannheim.de

2 Components, Connectors and Interaction Systems

In this section we present the basic definitions for interaction systems that were first introduced in [GS05]. An interaction system models the behavior of a component-based system for a set K of components. It is the superposition of a static model, called interaction model, that considers a component as a black box with interface description and specifies the "glue code", and the dynamic model, which gives the description of the local behavior of the components. For every component $i \in K$, a set A_i of actions or ports is specified and constitutes the interface. Gluing of components is achieved via so-called connectors. A connector c is a finite nonempty set of ports that contains at most one port for every component in K and describes a cooperation of those components which have a port in c. When each component is ready to perform its port in c then all ports in c can be performed conjointly. A subset of a connector is called an interaction. We may declare certain interactions to be complete. If an interaction is declared complete it can be performed independently of the environment. It is a design decision which interactions are chosen to be complete. Connectors may be of different size and one port may be contained in two or more connectors of different size. Thus the model allows for a very flexible way of gluing and consequently of cooperation among components.

Definition 1 (Interaction Model). *Let K be the set of* components *and A_i be a* port set *for component $i \in K$ where any two port sets are disjoint. Ports are also referred to as* actions*. A finite nonempty subset c of $A = \bigcup_{i \in K} A_i$ is called a* connector*, if it contains at most one port of each component $i \in K$ that is $|c \cap A_i| \leq 1$ for all $i \in K$. A* connector set *is a set C of connectors that covers all ports and contains only maximal elements:*

$$\text{1. } \bigcup_{c \in C} c = A \qquad \text{2. } c \subseteq c' \Rightarrow c = c' \text{ for all } c, c' \in C.$$

$I(c)$ denotes the set of all nonempty subsets of connector c and is called the set of interactions of c *and $I(C) = \bigcup_{c \in C} I(c)$ is the set of interactions of the connector set C. For component i and interaction $\alpha \in I(C)$, we put $i(\alpha) = A_i \cap \alpha$. We say that component i* participates *in α, if $i(\alpha) \neq \emptyset$. Let $Comp \subseteq I(C)$. We call*

$$IM := (C, Comp)$$

an interaction model*. The elements of C are also called* maximal interactions *and those of $Comp$ are called* complete interactions*.*

If not otherwise stated we always assume that $K = \{1, \ldots, n\}$ for some $n \in \mathbb{N}$ or that K is countably infinite. We refer the reader to [MCM07] for an example illustrating the concepts presented here.

So far we have only described components as black boxes with ports and have specified the possible structure of cooperation in between them. A further level of description of a component characterizes its local behavior. Basically this can be understood as a control of the way in which a component offers its ports. We assume here that this local behavior of every component $i \in K$ is given by a labeled transition system T_i. From the local transition systems and the interaction model we obtain the global behavior of the component-based system.

Definition 2 (Interaction System). *Let K be a set of components with associated port sets $\{A_i\}_{i \in K}$ and $IM = (C, Comp)$ an d interaction model for it. Let for each component $i \in K$ a transition system $T_i = \left(Q_i, A_i, \rightarrow_i, Q_i^0\right)$ be given where $\rightarrow_i \subseteq Q_i \times A_i \times Q_i$ and $Q_i^0 \subseteq Q_i$ is a non-empty set of* initial states. *We write $q_i \overset{a_i}{\rightarrow}_i q_i'$ instead of $(q_i, a_i, q_i') \in \rightarrow_i$.*

The induced interaction system *is given by $Sys := \left(IM, \{T_i\}_{i \in K}\right)$ where the* global behavior *$T = \left(Q, C \cup Comp, \rightarrow, Q^0\right)$ is obtained from the local transition systems of the individual components in a straightforward manner:*

1. *The global state space $Q := \prod_{i \in K} Q_i$ is the Cartesian product of the Q_i which we consider to be order independent. We denote states by tuples $q := (q_1, \ldots, q_j, \ldots)$ and call them* (global) states*. Elements of Q_i are called* local states *of component i.*
2. *$Q^0 := \prod_{i \in K} Q_i^0$, the Cartesian product of the local initial states. We call the elements of Q^0 (global)* initial states*.*
3. *$\rightarrow \subseteq Q \times (C \cup Comp) \times Q$, the labeled transition relation for Sys defined by*

$$\forall \alpha \in C \cup Comp \; \forall q, q' \in Q : q = (q_1, \ldots, q_j, \ldots) \overset{\alpha}{\rightarrow} q' = \left(q_1', \ldots, q_j', \ldots\right) \Leftrightarrow$$

$$\forall i \in K : q_i \overset{i(\alpha)}{\rightarrow}_i q_i' \text{ if } i \text{ participates in } \alpha \text{ and } q_i' = q_i \text{ otherwise.}$$

A state $q_i \in Q_i$ is called complete *if there is some interaction $\alpha \in C \cup Comp$ and some q_i' such that $q_i \overset{\alpha}{\rightarrow}_i q_i'$. Otherwise it is called* incomplete.

Note that a system may proceed in a global state q if q_i is complete for some $i \in K$. The converse does not hold.

Definition 3 (Enabled). *Let Sys be an interaction system and let $i \in K$ be a component. For $a_i \in A_i$ we set $en\,(a_i) := \left\{q_i \in Q_i | \exists q_i' : q_i \overset{a_i}{\rightarrow}_i q_i'\right\}$. For $\alpha \in C \cup Comp$ we set $en\,(\alpha) := \left\{q \in Q | \exists q' : q \overset{\alpha}{\rightarrow} q'\right\}$.*

If $q_i \in en(a_i)$ we say that a_i is enabled in q_i or that q_i offers a_i and analogously for q and α. Given a set of components, an interaction model $IM = (C, Comp)$ and a transition system T_i for each component i the induced interaction system describes the behavior of the composed system. In particular, in a given global state $q = (q_1, \ldots, q_j, \ldots)$ an interaction $\alpha \in C \cup Comp$ may take place provided that each component j participating in α offers $j(\alpha)$ in q_j.

Remark 1. In what follows, we often mention $Sys = \left(IM, \{T_i\}_{i \in K}\right)$. It is understood that $IM = (C, Comp)$ is an interaction model for the set K of components with port sets A_i and $T_i = \left(Q_i, A_i, \rightarrow_i, Q_i^0\right)$ for $i \in K$ and T are given as above.

3 Properties of Interaction Systems

Properties of systems have been classified into safety- and liveness-properties in [Lam77] and have been investigated in various settings, see for example [B$^+$99,CEP95]. In Sect. 3.1 we define the properties that we consider here w.r.t. absence/failure of ports. The properties are global deadlock-freedom and liveness of a set of components. These properties of interaction systems have been studied in detail in [GGMC$^+$07b,MCMM07a,GGMC$^+$07a,MCMM07b,MMMC06]. In Sect. 3.2 we define what we mean by robustness.

Remark 2. From now on we will assume that the local transition systems have the property that every local state offers at least one action. We also identify singleton sets with their element if it is convenient to do so.

3.1 Properties

Definition 4 (Reachable). *Let Sys be an interaction system, $q \in Q$. q is* reachable in *Sys if there is a sequence $q^0 \overset{\alpha_0}{\to} q^1 \overset{\alpha_1}{\to} \dots \overset{\alpha_{n-1}}{\to} q$ such that $q^0 \in Q^0$.*

First we take up the notion of global deadlock-freedom for interaction systems from [GGMC$^+$07b].

Definition 5 (Global Deadlock-Freedom). *Let Sys be an interaction system. Sys is called* globally deadlock-free *if for every reachable state $q \in Q$ there exists $\alpha \in C \cup Comp$ such that $q \in en(\alpha)$.*

A system is in a global deadlock in state q if every component needs for each of its actions enabled in q_i the cooperation of at least one other component j which in turn does not offer the desired action in q_j. In such a state the system is not able to proceed. As violations of safety properties can be expressed as deadlocks, the investigation of deadlock-freedom deserves particular attention.

Definition 6 (Run). *Let Sys be a globally deadlock-free interaction system, $q \in Q$ a reachable state. A* run *of Sys is an infinite sequence $\sigma = q \overset{\alpha_0}{\to} q^1 \overset{\alpha_1}{\to} q^2 \dots$ with $q^l \in Q$ for all $l \in \mathbb{N}$.*

Let $i \in K$ be a component and let σ be a run of Sys. If there exists l such that i participates in α_l we say that i participates *in σ.*

The notion liveness of a component has been adapted to interaction systems in [GGMC$^+$07a] and is restated in the following.

Definition 7 (Liveness). *Let Sys be a globally deadlock-free interaction system and let $K' \subseteq K$ be a nonempty set of components. K' is* live *in Sys if for every run σ of Sys there is some $i \in K'$ that participates in σ.*

3.2 Robustness of Properties

Let us now assume a situation where a set $A' \subsetneq A$ of ports may become unavailable in a running system. This might be because the ports in A' suffer some kind of failure or malfunction at a certain point of time but it is also possible to model a situation where certain actions or components are switched off for performance reasons for example. We want to formulate what it means that a property is present when A' becomes unavailable. For this we partition $C \cup Comp$ to separate those interactions that involve A' from those that don't.

Definition 8 (EXCL and WITH). *Let Sys be an interaction system as above and let $A' \subsetneq A$. We define $EXCL\,(A') := \{\alpha \in C \cup Comp | \alpha \cap A' = \emptyset\}$ and $WITH\,(A') := \{\alpha \in C \cup Comp | \alpha \cap A' \neq \emptyset\}$*

$EXCL\,(A')$ denotes the set of all maximal and complete interactions that do not involve any action from A'. Analogously $WITH\,(A')$ is the set of all maximal and complete interactions that involve some action from A'.

We consider each of the above properties separately w.r.t. absence of A'. Note that it is not possible to just delete the ports of A' from the interaction-system and then check if the definition of a certain property is satisfied by the resulting "system" for two reasons. Firstly, this construct may fail to be an interaction system according to the definition (also see [MCM07]), and secondly, the failure of A' may occur at a point of a run where actions from A' may have been previously executed in this run. We discuss deadlock-freedom in terms of robustness which means that we consider a system that is deadlock-free and remains so under failure of A'.

Definition 9 (Robustness of Deadlock-Freedom). *Let Sys be a globally deadlock-free interaction system and let $A' \subsetneq A$ be a non-empty subset of ports. In Sys global deadlock-freedom is* robust w.r.t. absence of A' *if for every reachable state $q \in Q$ there exists $\alpha \in EXCL\,(A')$ with $q \in en(\alpha)$.*

Remark 3. In a globally deadlock-free system Sys where $K' \subseteq K$ is live it is not possible that global deadlock-freedom is robust w.r.t. absence of $A' := \bigcup_{i \in K'} A_i$. If this was the case it would be possible to construct a run not letting any component from K' participate which is not possible. The converse does not hold.

We now consider liveness of a set of components in a system where global deadlock-freedom is robust w.r.t. absence of A'. First we need to adapt the notion of a run.

Definition 10 (Run without A'). *Let Sys be a globally deadlock-free interaction system and $A' \subsetneq A$. Let global deadlock-freedom in Sys be robust with respect to absence of A'.*

A run without A' *is an infinite sequence $\sigma = q \overset{\alpha_0}{\to} q^1 \overset{\alpha_1}{\to} \ldots$ starting in a reachable state q with $q^l \in Q$ and $\alpha_l \in EXCL\,(A')$ for all $l \in \mathbb{N}$.*

In a system where global deadlock-freedom is robust w.r.t. absence of $A' \subsetneq A$ such runs always exist by a simple induction argument.

Definition 11 (Liveness without A'). *Let Sys be a globally deadlock-free interaction system and let $A' \subsetneq A$. Let global deadlock-freedom in Sys be robust w.r.t. absence of A' and let $K' \subseteq K$ be a nonempty set of components. K'* is live without participation of A' *if for every run without A' $\sigma = q^0 \overset{\alpha_0}{\to} q^1 \overset{\alpha_1}{\to} \ldots$ there is some $i \in K'$ that participates in σ.*

Note that it is not possible, in analogy to deadlock-freedom, to consider robustness of liveness. If a set K' of components is live in a system, then for every run σ there is a component $i \in K'$ that participates in σ. This is true in particular for all runs without A'. Therefore liveness of K' without A' follows from liveness of K' and robustness of deadlock-freedom w.r.t. A'. Nonetheless it is interesting to investigate liveness of K' without participation of $A' \subsetneq A$ because it is possible that certain runs in which K' does not participate infinitely many often are no longer present when the ports from A' are not available any more.

4 Conditions for Robustness

In this section we first give the definitions needed to state the results from [MCM07]. Then we give those results together with their respective proofs.

4.1 Robustness of Deadlock-Freedom

Definition 12 (Incomplete States). *Let Sys be an interaction system and let $i \in K$ be a component. We denote by $inc\,(i) := \{q_i \in Q_i | q_i \text{ is incomplete}\}$ the set of incomplete states of component i.*

We obtain a criterion for robustness of global deadlock-freedom by adapting the condition of [GGMC$^+$07b] for global deadlock-freedom of an interaction system. This condition involves a graph G_{Sys}. The nonexistence of certain cycles in G_{Sys} guarantees deadlock-freedom. G_{Sys} can be built in time polynomial in $|C \cup Comp|$ and the sum of the sizes of the local transition systems for finite interaction systems.

Definition 13 (Dependency Graph). *Let Sys be an interaction system. The* dependency graph for *Sys is a labeled directed graph $G_{Sys} := (K, E)$ where the set of nodes is given by the components of Sys, the set of labels is given by $L := L_1 \cup L_2$ with*

$$L_1 := \{c \in C | \nexists \alpha \in Comp : \alpha \subseteq c\}$$

$$L_2 := \{(c, \alpha)\, | c \in C, \alpha \in Comp \text{ such that } \alpha \subseteq c \wedge \nexists \beta \in Comp : \beta \subsetneq \alpha\},$$

and the set of edges $E \subseteq V \times L \times V$ is defined as follows:

1. *For $c \in L_1$: $(i, c, j) \in E \Leftrightarrow j\,(c) \neq \emptyset \wedge \exists q_i \in en\,(i\,(c)) \cap inc\,(i)$.*

2. *For* $(c, \alpha) \in L_2: \quad (i, (c, \alpha), j) \in E \Leftrightarrow j(\alpha) \neq \emptyset \wedge \exists q_i \in en(i(c)) \cap inc(i)$.

Further we define the snapshot of G_{Sys} w.r.t. state $q = (q_1, q_2, \ldots)$ *as* $G_{Sys}(q) := (K, E(q))$ *where* $E(q) \subseteq E$ *such that*

1. *For* $c \in L_1: \quad (i, c, j) \in E(q) \Leftrightarrow j(c) \neq \emptyset \wedge q_i \in en(i(c)) \cap inc(i)$.
2. *For* $(c, \alpha) \in L_2: \quad (i, (c, \alpha), j) \in E(q) \Leftrightarrow j(\alpha) \neq \emptyset \wedge q_i \in en(i(c)) \cap inc(i)$.

Let $G_f = (K_f, E_f)$ *be a subgraph of* G_{Sys}. G_f *is* successor-closed *if* $K_f \neq \emptyset$ *and for all* $i \in K_f$ *and all edges* $e = (i, l, j) \in E$ *where* $l \in L$ *and* $j \in K$ *we have* $e \in E_f$ *and* $j \in K_f$.

The intuitive meaning of the graph is as follows. An edge (i, c, j) means that i and j participate in c and that there is an incomplete local state $q_i \in Q_i$ such $i(c)$ is enabled in q_i. This means that there could be a global state where i is waiting for j due to the connector c.

Next we define predicates that are evaluated on Q.

Definition 14. *Let Sys be an interaction system.*

1. *For* $e = (i, c, j)$ *we set* $cond(e) := en(i(c)) \wedge \exists x \in c : \neg en(x)$.
2. *For* $e = (i, (c, \alpha), j)$ *we set* $cond(e) := en(i(c)) \wedge \exists x \in \alpha : \neg en(x)$.
3. *For a path* $p = e_1, \ldots, e_r$ *in* G_{Sys} *we set* $cond(p) := \bigwedge_{l=1}^{r} cond(e_l)$.

For an edge $e = (i, c, j)$, *cond*(e) is satisfied in state $q = (q_1, \ldots, q_i, \ldots) \in Q$ if $i(c)$ is enabled in q_i but c is not enabled in q because at least one component does not provide the necessary action.

Definition 15. *Let Sys be an interaction system.*

1. *A path* p *in* G_{Sys} *is called* critical *if* $\big(cond(p) \wedge \bigwedge_{i \in p} inc(i)\big) \not\equiv false$. *A path* p *in* $G_{Sys}(q)$ *is called* critical *if* $\big(cond(p) \wedge \bigwedge_{i \in p} inc(i)\big)(q) = true$. *A path that is not critical is called* non-critical.
2. *Let* p *be a critical cycle in a successor-closed subgraph* $G_f = (K_f, E_f)$ *of* G_{Sys}. p *is refutable, if, whenever* p *lies in* $G_f(q)$ *where* $q_i \in inc(i)$ *for all* i*, there is a non-critical path* $\hat{p}$ *in* $G_f(q)$.

A path is critical if there is some $q = (q_1, \ldots, q_i, \ldots) \in Q$ such that q_i is incomplete for all components i on the path and *cond*(e) is satisfied in q for every edge e on the path. If a cycle in G_{Sys} is critical it describes a potential circular waiting relation among components.

Theorem 1. *Let Sys be a globally deadlock-free interaction system as above and let* $A' \subsetneq A$ *be a set of ports. Global deadlock-freedom is robust in Sys w.r.t. absence of* A' *if the following conditions hold.*

1. *There is no* $a \in A'$ *such that* $\{a\} \in C \cup Comp$.
2. G_{Sys} *contains a finite successor-closed subgraph* $G_f = (K_f, E_f)$ *such that*

   (a) For all $e = (i, c, j) \in E_f$ we have $c \in EXCL(A')$.
   (b) For all $e = (i, (c, \alpha), j) \in E_f$ we have $\alpha \in EXCL(A')$.
   (c) Every critical cycle in G_f is refutable.

Proof. Let $q = (q_1, \ldots, q_i, \ldots) \in Q$ be a reachable state of Sys. We distinguish two different cases.

1. There is some $i \in K$ such that $q_i \notin inc(i)$. Then there exists $a_i \in A_i$ such that $\{a_i\} \in C \cup Comp$ and $q \in en(\{a_i\})$. Because of the first assumption above we know that $a_i \notin A'$. Therefore there exists an interaction from $EXCL(A')$ that can be executed in q.
2. Otherwise for all $i \in K_f$ we know that $q_i \in inc(i)$. Because of our assumptions that every local state of every component offers at least one action and that every action of every component is contained in at least one connector and because all q_i are incomplete we conclude that every $i \in K_f$ has at least one outgoing edge. Because $|K_f|$ is finite this implies that $G_f(q)$ contains a cycle p. Again we consider two cases:
   (a) p is noncritical. All local states are incomplete and therefore we know $\bigwedge_{i \in p} inc(i)(q) = true$. Therefore there must be some edge e on p such that $cond(e)(q) = false$. If $e = (i, c, j)$ this means that c is enabled in q. Using 2a we conclude $c \in EXCL(A')$. Otherwise $e = (i, (c, \alpha), j)$ and α is enabled in q. Assumption 2b implies $\alpha \in EXCL(A')$.
   (b) p is critical. Then it is refutable and therefore there exists a noncritical path p' in $G_f(q)$. As above we conclude that there exists $e \in p'$ such that $cond(e)(q) = false$ and that there must be some $\alpha \in EXCL(A')$ that is enabled in q.

4.2 Liveness without A'

Here we transform the criterion of [GGMC$^+$07a] that ensures liveness of a set of components K' to handle the case of failure of A'.

We define $excl(A', K')$ the set of maximal and complete interactions that neither involve any action from A' nor any component from K'.

Definition 16. *Let $K' \subseteq K$ be a subset of components. Let $excl(A', K') := \{\alpha \in EXCL(A') \,|\, \forall i \in K' : i(\alpha) = \emptyset\}$.*

Definition 17. *Let Sys be an interaction system as above and let $j \in K$ be a component.*

1. *We set $need_j(A') := \{a_j \in A_j | a_j \in \alpha \Rightarrow \alpha \in WITH(A')\}$ the set of ports of j that only occur in maximal or complete interactions also involving A'.*
2. *Let $B_j \subseteq A_j$ be a subset of actions of j. B_j is* weakly inevitable w.r.t. *A' in T_j if the following two conditions hold:*
   (a) There is an infinite path in the transition system obtained by canceling all transitions in T_j that are labeled with an action from $need_j(A')$.

   - *(b) On every infinite path in the transition system obtained this way only finitely many transitions labeled with $a_j \in A_j \backslash B_j$ can be performed before some action from B_j must be performed.*

3. *Let $\Lambda \subseteq I(C)$ be a nonempty set of interactions and let $j \in K$ be a component. We define $\Lambda[j] := A_j \cap \bigcup\limits_{\alpha \in \Lambda} \alpha$ the set of ports of j that participate in one of the interactions of Λ.*

The set $need_j(A')$ contains exactly those actions of j that can only be performed in the global system if an action from A' is also performed at the same time. Note that it is clear that $(A' \cap A_j) \subseteq need_j(A')$. Further a subset of actions of component j is weakly inevitable w.r.t. A' in T_j if it is possible in T_j to choose an infinite path that does not contain a transition labeled with an action from $need_j(A')$ and if for all such paths there are infinitely many transitions that are labeled with some action from the set in question. The last part of the definition introduces a sort of a projection-operator that yields those actions of component j that participate in one of the interactions in Λ.

In the following we define a graph $G := (K, E)$ for an interaction system with a finite set of components and finite port sets which is a modification of the graph introduced [GGMC$^+$07a] to establish liveness. Informally, an edge $e = (i, j) \in E$ has the meaning that component j can only participate in finitely many global steps before i has to participate as well.

Definition 18. *Let $G := (K, E)$ with $E := \bigcup_{m=0}^{\infty} E_m$, where:*

$$E_0 := \{(i,j)\,|A_j \backslash excl\,(A', i)\,[j] \text{ is weakly inevitable w.r.t. } A' \text{ in } T_j\}$$

$$E_{l+1} := \left\{(i,j)\,|A_j \backslash excl\left(A', R^l(i)\right)[j] \text{ is weakly inevitable w. r. t. } A' \text{ in } T_j\right\}$$

$$R^l(i) := \{j | j \text{ is reachable from } i \text{ in } (K, \cup_{m=0}^{n} E_m)\}$$

Theorem 2. *Let Sys be a globally deadlock-free finite interaction system such that global deadlock-freedom is robust w.r.t. absence of $A' \subsetneq A$. Let $K' \subseteq K$ be a set of components.*

K' is live without participation of A' in Sys if all components i in $K \backslash K'$ such that T_i contains an infinite path that is only labeled with actions that are not in $need_i(A')$ are reachable from K' in G.

The construction of the graph and the reachability analysis can be performed in time polynomial in $|C \cup Comp|$ and the sum of the sizes of the local transition systems.

Proof. It is clear that the construction of the graph can be performed in time polynomial in $|C \cup Comp|$ and the sum of the sizes of the local transition systems because for the decision whether $(i, j) \in E_l$ only the local transition systems of i and j and $C \cup Comp$ have to be investigated. Further, the iterative construction of the set of edges can be stopped after at most $|K|^2$ steps.

First we will prove the following two claims by induction over l:

1. $(i,j) \in E_l$ implies that j can only participate finitely many times in any run σ without A' of Sys before i has to participate.
2. $j \in R^l(i)$ implies that j can only participate finitely many times in any run σ without A' of Sys before i has to participate.

Consider an arbitrary run σ without A'.

Let $(i,j) \in E_0$. Consider the set $excl(A', i)[j]$. It contains those actions of j that occur in some connector neither involving A' nor i. Therefore $A_j \backslash excl(i)[j]$ is the set of actions of j that only occur in maximal or complete interactions involving A' or i. Now assume j participates infinitely many often in σ. Because σ only contains interactions from $EXCL(A')$ we get an infinite path in T_j that is not labeled with any action from $need_j(A')$. This path must contain infinitely many transitions labeled with some $a_j \in A_j \backslash excl(A', i)[j]$ because this set is weakly inevitable w.r.t. A' in T_j according to the definition of E_0. This means that σ contains some α_r involving an action from this set. Because $\alpha_r \in EXCL(A')$ the above implies that i participates in α_r.

Now let $j \in R^0(i)$ and assume that j participates infinitely many often in σ. By induction on the length of a path from i to j we show that eventually i also has to participate in σ. If $(i,j) \in E_0$ the claim follows from the argument above. Now let $p = i \rightarrow \ldots \rightarrow k \rightarrow j$ be a path of length $s+1$ that only visits edges in E_0. k participates infinitely many often in σ because $(k,j) \in E_0$ and j participates infinitely many often in σ. k is reachable from i over a path of length s. By induction we conclude that i has to participate in σ as well.

Let both statements be true for l and consider an edge $(i,j) \in E_{l+1}$. As above we consider $excl\left(A', R^l(i)\right)[j]$ and conclude that it contains those actions of j that occur in some connector neither involving A' nor any component from $R^l(i)$. Therefore $A_j \backslash excl\left(R^l(i)\right)[j]$ is the set of actions of j that only occur in maximal or complete interactions involving A' or some component from $R^l(i)$. Now assume that j participates infinitely many often in σ. As above σ yields an infinite path in T_j that is not labeled with any action from $need_j(A')$. It contains infinitely many transitions labeled with some $a_j \in A_j \backslash excl\left(A', R^l(i)\right)[j]$ because this set is weakly inevitable w.r.t. A' in T_j according to the definition of E_{l+1}. Because K is finite and because σ contains only $\alpha_r \in EXCL(A')$ this means that there is some component $k \in R^l(i)$ that participates infinitely many often in σ. From the induction hypothesis and $k \in R^l(i)$ we conclude that i participates in σ.

Finally we consider $j \in R^{l+1}(i)$ and assume that j participates infinitely many often in σ. We show that the second statement is true by induction on the length of a path from i to j. If $(i,j) \in \bigcup_{m=0}^{l+1} E_m$ the claim follows from the previous parts of the proof. Let $p = i \rightarrow \ldots \rightarrow k \rightarrow j$ be a path of length $s+1$ that only visits edges from $\bigcup_{m=0}^{l+1} E_m$. We conclude that k participates infinitely many often in σ because $(k,j) \in \bigcup_{m=0}^{l+1} E_m$. k is reachable from i over a path of length s. By induction we conclude that i has to participate in σ.

The proof of the theorem is straightforward now. Let j be reachable from i in G over a path p. This path visits only finitely many edges which means that there exists $n_0 \in \mathbb{N}$ such that all edges along p lie in $\bigcup_{m=0}^{n_0} E_m$. The second fact above implies that for any run σ without A' the component j can only participate finitely many times before i also has to participate.

Then it is clear that K' is live without A' in Sys if all components j in $K \backslash K'$ such that T_j contains an infinite path that is only labeled with actions that are not in $need_j(A')$ are reachable from K' in G. Indeed, if $K' = K$ liveness without A' follows from robustness of deadlock-freedom w.r.t. A'. Otherwise for any run without A' there must be some component j that participates infinitely many often because K is finite. This means that T_j contains an infinite path that is only labeled with actions that are not in $need_j(A')$ and therefore j is reachable from some component in K' and the argument above yields that K' participates.

References

[AG97] Robert Allen and David Garlan. A Formal Basis for Architectural Connection. *ACM Trans. Softw. Eng. Methodol.*, 6(3):213–249, 1997.

[Arb02] Farhad Arbab. Abstract Behavior Types: A Foundation Model for Components and Their Composition. In *Proceedings of FMCO'02*, volume 2852 of *LNCS*, pages 33–70. Springer, 2002.

[B+99] Beatrice Berard et al. *Systems and Software Verification.* Springer, 1999.

[BB06] Remi Bastide and Eric Barboni. Software Components: A Formal Semantics Based on Coloured Petri Nets. In *Proceedings of FACS'05*, volume 160, pages 57–73. ENTCS, 2006.

[BBS06] Ananda Basu, Marius Bozga, and Joseph Sifakis. Modeling Heterogeneous Real-Time Components in BIP. In *Proceedings of SEFM'06*, pages 3–12. IEEE Computer Society, 2006.

[Bro99] M. Broy. Towards a Logical Basis of Software Engineering. In M. Broy and R Steinbrüggen, editors, *Calculational System Design, IOS 1999*, volume 158 of *NATO ASI Series, Series F: Computer and System Sciences*, pages 101 – 131. Springer, 1999.

[CEP95] Allen Cheng, Javier Esparza, and Jens Palsberg. Complexity Results for 1-Safe Nets. *Theoretical Computer Science*, 147(1-2):117–136, 1995.

[GGMC+07a] G. Gössler, S. Graf, M. Majster-Cederbaum, M. Martens, and J. Sifakis. An Approach to Modelling and Verification of Component Based Systems. In *Proceedings of SOFSEM07*, volume 4362 of *LNCS*, pages 295–308. Springer, 2007.

[GGMC+07b] G. Gössler, Susanne Graf, Mila Majster-Cederbaum, Moritz Martens, and J. Sifakis. Ensuring Properties of Interaction Systems. In *Program Analysis and Compilation*, volume 4444 of *LNCS*. Springer, 2007.

[Gös01] Gregor Gössler. PROMETHEUS — A Compositional Modeling Tool for Real-Time Systems. In *Proceedings of RT-TOOLS 2001.* Technical report 2001-014, Uppsala University, Department of Information Technology, 2001.

[GS02] Gregor Gössler and Joseph Sifakis. Composition for Component-Based Modeling. In *Proceedings of FMCO'02*, volume 2852 of *LNCS*, pages 443–466. Springer, 2002.

[GS03] Gregor Gössler and Joseph Sifakis. Component-Based Construction of Deadlock-Free Systems. In *Proceedings of FSTTCS 2003*, volume 2914 of *LNCS*, pages 420–433. Springer, 2003.

[GS05] Gregor Gössler and Joseph Sifakis. Composition for Component-Based Modeling. *Sci. Comput. Program.*, 55(1-3):161–183, 2005.

[Lam77] Leslie Lamport. Proving the Correctness of Multiprocess Programs. *IEEE Trans. Software Eng.*, 3(2):125–143, 1977.

[MCM07] Mila Majster-Cederbaum and Moritz Martens. Robustness in Interaction Systems, 2007. accepted for publication at FORTE'07.

[MCMM07a] M. Majster-Cederbaum, M. Martens, and C. Minnameier. A Polynomial-Time-Checkable Sufficient Condition for Deadlock-freeness of Component Based Systems. In *Proceedings of SOFSEM07*, volume 4362 of *LNCS*, pages 888–899. Springer, 2007.

[MCMM07b] M. Majster-Cederbaum, M. Martens, and C. Minnameier. Liveness in Interaction Systems, 2007. Submitted for publication.

[MMMC06] M. Martens, C. Minnameier, and M. Majster-Cederbaum. Deciding Liveness in Component-Based Systems is NP-hard. Technical report TR-2006-017, Universität Mannheim, 2006.

[Sif05] Joseph Sifakis. A Framework for Component-based Construction, 2005. SEFM 2005: pp. 293 - 300.