Channel Properties of Asynchronously Composed Systems*

Serge Haddad[1], Rolf Hennicker[2], and Mikael H. Møller[3]

[1] LSV, ENS Cachan & CNRS & INRIA, France
[2] Ludwig-Maximilians-Universität München, Germany
[3] Aalborg University, Denmark

Abstract. We consider asynchronously composed I/O-transition systems (AIOTS) with built-in communication channels and potentially infinite state space. For those systems we study various channel properties that deal with the production and consumption of messages exchanged via the communication channels. We establish useful relationships between the different properties and show that all channel properties are preserved by asynchronous composition, i.e. they are compositional. We focus on the subclass of those AIOTS which are generated by asynchronous I/O-Petri nets and we show that this class of AIOTS is closed under asynchronous composition. As a crucial result we prove that for the AIOTS generated by a Petri net all channel properties are decidable.

1 Introduction

(A)synchronous composition. The design of hardware and software systems is often component-based which well-known advantages: management of complexity, reusability, separation of concerns, collaborative design, etc. One critical feature of such systems is the protocol supporting the communication between components and in particular the way they synchronise. Synchronous composition ensures that both parts are aware that communication has taken place and then simplifies the validation of the system. However in a large scale distributed environment synchronous composition may lead to redhibitory inefficiency during execution and thus asynchronous composition should be adopted. The FIFO requirement of communication channels is often not appropriate in this context. This is illustrated by the concept of a software bus where applications push and pop messages in mailboxes. Also on the modeling level FIFO ordering is often not assumed, like for the composition of UML state machines which relies on event pools withot specific requirements.

Compositions of Petri nets. In the context of Petri nets, composition has been studied both from theoretical and practical points of view. The process algebra approach has been investigated by several works leading to the Petri net algebra [4]. Such a work is closely related to synchronous composition. In [17, 16], asynchronous composition of nets is performed via a set of places or, more

* This work has been partially sponsored by the EU project ASCENS, 257414.

generally, via a subnet modelling some medium. Then structural restrictions on the subnets are proposed in order to preserve global properties like liveness or deadlock-freeness. In [15], a general composition operator is proposed and its associativity is established. A closely related concept to composition is the one of open Petri nets which has been used in different contexts like the analysis of web services [18]. Numerous compositional approaches have been proposed for the modelling of complex applications but most of them are based on high-level Petri nets; see [11] for a detailled survey.

Channel properties. With the development of component-based applications, one is interested in verifying behavioural properties of the communication and, in the asynchronous case, in verifying the properties related to communication channels. In the seminal work of [5], the authors present several properties like *channel boundedness* and *specified receptions* and propose methods to analyse them. In [7], a two-component based system is studied using a particular (decidable) channel property, the *half-duplex property*: at any time at most one channel is not empty. More recently in [2] *synchronizability*, a property of asynchronous systems, is introduced such that when it holds the system can be safely abstracted by a synchronous one.

Our contributions. In this work we are interested in general channel properties and not in specific system properties related to particular applications. In order to analyse channel properties, we first introduce asynchronously composed I/O-transition systems (AIOTS) which are open transition systems enriched with channels. Our main hypothesis consists in omitting the FIFO requirement that potentially can decrease the performance of large scale distributed systems. Thus the state of a channel is determined by the number of messages that it contains. We define an asynchronous composition operator which introduces new channels for the communication between the composed AIOTSs.

In our study two kinds of channel properties are considered which are related to consumption requirements and to the termination of communication. Consumption properties deal with the requirements that messages sent to a communication channel should also be consumed. They can be classified w.r.t. two criteria. The first criterium is the nature of the requirement: consuming messages, decreasing the number of messages, and emptying channels. The second criterium expresses the way the requirement is achieved: possibly immediately, possibly after some delay, or necessarily in each weakly fair run. Communication termination deals with immediate or delayed closing of communication channels if the receiver is not ready to consume anymore. We establish useful relations between the channel properties and prove that all channel properties are compositional, i.e. preserved by asynchronous composition. This is an important prerequisite for modular verification.

A natural high-level formalism for specifying AIOTS is the Petri net formalism. We propose asynchronously composed Petri nets (AIOPN) with an AIOTS semantics and we show that the class of asynchronous I/O-transition systems generated by asynchronous I/O-Petri nets is closed under composition.

From a verification point of view, we study the decidability of properties in the framework of AIOPN. Thanks to several complementary works on decidability for Petri net problems, we show that all channel properties are decidable, though with a high computational complexity.

Organisation. In Section 2, we introduce AIOTSs and their asynchronous composition. Then, we introduce AIOPNs in Section 3 lifting asynchronous composition to the net level. In Section 4, we define the channel properties and study their relationships and their preservation under asynchronous composition. In Section 5, we establish that all channel properties are decidable for AIOPNs. Finally, in Section 6, we conclude and give some perspectives for future work.

2 Asynchronous I/O-Transition Systems

We first recall some basic definitions for labelled transition systems. A *labeled transition system* (LTS) is a tuple $\mathcal{S} = (\Sigma, Q, q^0, \longrightarrow)$, such that

- Σ is a finite set of labels,
- Q is a (possibly infinite) set of states,
- $q^0 \in Q$ is the initial state, and
- $\longrightarrow \subseteq Q \times \Sigma \times Q$ is a labeled transition relation.

We will write $q \xrightarrow{a} q'$ for $(q, a, q') \in \longrightarrow$, and we write $q \xrightarrow{a}$ if there exists $q' \in Q$ such that $q \xrightarrow{a} q'$. Let $q_1 \in Q$. A *trace* of $\mathcal{S}$ starting in q_1 is a finite or infinite sequence $\rho = q_1 \xrightarrow{a_1} q_2 \xrightarrow{a_2} q_3 \xrightarrow{a_3} \cdots$, such that $a_i \in \Sigma$ and $q_i \in Q$ for all i. For $a \in \Sigma$ we write $a \in \rho$, if there exists a_i in the sequence ρ such that $a_i = a$, and $\sharp_\rho(a)$ denotes the (possibly infinite) number of occurrences of a in ρ. For $q \in Q$ we write $q \in \rho$, if there exists q_i in the sequence ρ such that $q_i = q$. For $\sigma = a_1 a_2 \cdots a_n \in \Sigma^*$ and $q, q' \in Q$ we write $q \xrightarrow{\sigma} q'$ if there exists a (finite) sequence $q \xrightarrow{a_1} q_2 \xrightarrow{a_2} q_3 \cdots q_n \xrightarrow{a_n} q'$. Sometimes we need to reason about the successor states reachable from a given state $q \in Q$ with a subset $\bar{\Sigma} \subseteq \Sigma$. We define $\mathrm{Post}(q, \bar{\Sigma}) = \{q' \in Q \mid \exists a \in \bar{\Sigma} \,.\, q \xrightarrow{a} q'\}$ and we write $\mathrm{Post}(q)$ for $\mathrm{Post}(q, \Sigma)$. Further we define $\mathrm{Post}^*(q, \bar{\Sigma}) = \{q' \in Q \mid \exists \sigma \in \bar{\Sigma}^* \,.\, q \xrightarrow{\sigma} q'\}$ and we write $\mathrm{Post}^*(q)$ for $\mathrm{Post}^*(q, \Sigma)$.

In this paper we consider asynchronous systems which may be open for communication with other systems. The open actions are modeled by distinguished input and output labels while communication within an asynchronous system is modeled by communication labels. We assume that communication takes place via unbounded channels and that for each message type to be exchanged in a system there is exactly one communication channel. Given a finite set C of channels, an *I/O-alphabet over* C is the disjoint union $\Sigma = \mathsf{in} \uplus \mathsf{out} \uplus \mathsf{com}$ of pairwise disjoint sets in of input labels, out of output labels and com of communication labels, such that $\Sigma \cap C = \emptyset$, $\mathsf{com} = \{ {}^{\triangleright}a, a^{\triangleright} \mid a \in C\}$ and in and out do not contain labels of the form ${}^{\triangleright}x$ or $x^{\triangleright}$. For each channel $a \in C$, the communication label ${}^{\triangleright}a$ represents consumption of a message from the channel a and $a^{\triangleright}$ represents putting a message on a . To indicate the actual number of messages on a channel in a certain state we use a *channel valuation* function val. Under

these assumptions we model asynchronous systems by the following notion of asynchronous I/O-transition system.

Definition 1 (Asynchronous I/O-transition system). *An* asynchronous I/O-transition system *(AIOTS) is a tuple* $\mathcal{S} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$*, such that*

- $(\Sigma, Q, q^0, \longrightarrow)$ *is a labeled transition system,*
- C *is a finite set of channels,*
- $\Sigma = \mathsf{in} \uplus \mathsf{out} \uplus \mathsf{com}$ *is an I/O-alphabet over* C*,*
- $\mathrm{val} : Q \times C \longrightarrow \mathbb{N}$ *is a channel valuation, such that for all* $a \in C, q, q' \in Q$*:*
  - $\mathrm{val}(q^0, a) = 0$*,*
  - $q \xrightarrow{a^{\triangleright}} q' \implies \mathrm{val}(q', a) = \mathrm{val}(q, a) + 1$*,*
  - $q \xrightarrow{{}^{\triangleright}a} q' \implies \mathrm{val}(q, a) > 0$ *and* $\mathrm{val}(q', a) = \mathrm{val}(q, a) - 1$*, and*
  - *for all* $x \in \Sigma \setminus \{ {}^{\triangleright}a, a^{\triangleright} \}, q \xrightarrow{x} q' \implies \mathrm{val}(q', a) = \mathrm{val}(q, a)$*.* ♢

The first condition for val assumes that initially all communication channels are empty, the second condition states that at most one element can be put (removed resp.) at a time, and the last condition requires that the input and output actions of an open system do not change the valuation of any channel, since channels are used for the communication *inside* the system. Sometimes we need to reason about the number of messages on a subset $B \subseteq C$ of the channels in a state $q \in Q$. We define $\mathrm{val}(q, B) = \sum_{a \in B} \mathrm{val}(q, a)$.

Two I/O-alphabets are composable if there are no name conflicts between labels and channels and, following [1], if shared labels are either input labels of one alphabet and output labels of the other or conversely. For the composition each shared label a gives rise to a new communication channel, also called a, and hence to new communication labels $a^{\triangleright}$ for putting and ${}^{\triangleright}a$ for removing messages. The input and output labels of the alphabet composition are the non-shared input and output labels of the underlying alphabets; they are left open.

Definition 2 (Alphabet composition). *Let* $\Sigma_{\mathcal{S}} = \mathsf{in}_{\mathcal{S}} \uplus \mathsf{out}_{\mathcal{S}} \uplus \mathsf{com}_{\mathcal{S}}$ *and* $\Sigma_{\mathcal{T}} = \mathsf{in}_{\mathcal{T}} \uplus \mathsf{out}_{\mathcal{T}} \uplus \mathsf{com}_{\mathcal{T}}$ *be two I/O-alphabets over channels* $C_{\mathcal{S}}$ *and* $C_{\mathcal{T}}$ *resp.* $\Sigma_{\mathcal{S}}$ *and* $\Sigma_{\mathcal{T}}$ *are* composable *if* $(\Sigma_{\mathcal{S}} \cup \Sigma_{\mathcal{T}}) \cap (C_{\mathcal{S}} \cup C_{\mathcal{T}}) = \emptyset$ *and* $\Sigma_{\mathcal{S}} \cap \Sigma_{\mathcal{T}} = (\mathsf{in}_{\mathcal{S}} \cap \mathsf{out}_{\mathcal{T}}) \cup (\mathsf{in}_{\mathcal{T}} \cap \mathsf{out}_{\mathcal{S}})$*. The composition of* $\Sigma_{\mathcal{S}}$ *and* $\Sigma_{\mathcal{T}}$ *is the I/O-alphabet* $\Sigma = \mathsf{in} \uplus \mathsf{out} \uplus \mathsf{com}$ *over the composed set of channels* $C = C_{\mathcal{S}} \uplus C_{\mathcal{T}} \uplus C_{\mathcal{ST}}$*, with new channels* $C_{\mathcal{ST}} = \Sigma_{\mathcal{S}} \cap \Sigma_{\mathcal{T}}$*, such that*

- $\mathsf{in} = (\mathsf{in}_{\mathcal{S}} \setminus \mathsf{out}_{\mathcal{T}}) \uplus (\mathsf{in}_{\mathcal{T}} \setminus \mathsf{out}_{\mathcal{S}})$*,*
- $\mathsf{out} = (\mathsf{out}_{\mathcal{S}} \setminus \mathsf{in}_{\mathcal{T}}) \uplus (\mathsf{out}_{\mathcal{T}} \setminus \mathsf{in}_{\mathcal{S}})$*, and*
- $\mathsf{com} = \{a^{\triangleright}, {}^{\triangleright}a \mid a \in C\}$ ♢

Two AIOTSs can be asynchronously composed, if their underlying I/O-alphabets are composable. The composition is constructed by introducing a new communication channel for each shared input/output action and by appropriate transitions for the corresponding communication actions that modify the valuation of the new channels (see items 3 and 4 in Def. 3). It relies on a binary

communication style. Since the states of the composition must record the number of messages on the new channels $C_{\mathcal{ST}}$, the state space of the composition adds to the cartesian product of the underlying state spaces the set $\mathbb{N}^{C_{\mathcal{ST}}}$ of valuations of the new channels. For a valuation $\boldsymbol{v} : C_{\mathcal{ST}} \mapsto \mathbb{N}$, we use the notation $\boldsymbol{v}[a \mapsto n]$ to denote the updated map $\boldsymbol{v}[a \mapsto n](x) = \begin{cases} n & \text{if } x = a, \\ \boldsymbol{v}(a) & \text{otherwise.} \end{cases}$

Definition 3 (Asynchronous composition).
Let $\mathcal{S} = (C_{\mathcal{S}}, \Sigma_{\mathcal{S}}, Q_{\mathcal{S}}, q^0_{\mathcal{S}}, \longrightarrow_{\mathcal{S}}, \mathrm{val}_{\mathcal{S}})$ *and* $\mathcal{T} = (C_{\mathcal{T}}, \Sigma_{\mathcal{T}}, Q_{\mathcal{T}}, q^0_{\mathcal{T}}, \longrightarrow_{\mathcal{T}}, \mathrm{val}_{\mathcal{T}})$ *be two AIOTSs.* $\mathcal{S}$ *and* $\mathcal{T}$ *are composable if* $\Sigma_{\mathcal{S}}$ *and* $\Sigma_{\mathcal{T}}$ *are composable. In this case their asynchronous composition is the AIOTS* $\mathcal{S} \otimes \mathcal{T} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$ *defined as follows:*

- $C = C_{\mathcal{S}} \uplus C_{\mathcal{T}} \uplus C_{\mathcal{ST}}$, *with* $C_{\mathcal{ST}} = \Sigma_{\mathcal{S}} \cap \Sigma_{\mathcal{T}}$,
- Σ *is the alphabet composition of* $\Sigma_{\mathcal{S}}$ *and* $\Sigma_{\mathcal{T}}$,
- $Q = Q_{\mathcal{S}} \times Q_{\mathcal{T}} \times \mathbb{N}^{C_{\mathcal{ST}}}$,
- $q^0 = (q^0_{\mathcal{S}}, q^0_{\mathcal{T}}, \mathbf{0})$, *with* $\mathbf{0}$ *being the zero-map,*
- $\longrightarrow$ *is inductively defined as follows for all* $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \in Q$*:*
  - *1: For all* $a \in (\Sigma_{\mathcal{S}} \setminus C_{\mathcal{ST}})$, *if* $q_{\mathcal{S}} \xrightarrow{a}_{\mathcal{S}} q'_{\mathcal{S}}$ *then* $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \xrightarrow{a} (q'_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v})$.
  - *2: For all* $a \in (\Sigma_{\mathcal{T}} \setminus C_{\mathcal{ST}})$, *if* $q_{\mathcal{T}} \xrightarrow{a}_{\mathcal{T}} q'_{\mathcal{T}}$ *then* $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \xrightarrow{a} (q_{\mathcal{S}}, q'_{\mathcal{T}}, \boldsymbol{v})$.
  - *3: For all* $a \in \mathsf{in}_{\mathcal{S}} \cap \mathsf{out}_{\mathcal{T}}$,
    - *3.1: if* $q_{\mathcal{S}} \xrightarrow{a}_{\mathcal{S}} q'_{\mathcal{S}}$ *and* $\boldsymbol{v}(a) > 0$ *then* $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \xrightarrow{\triangleright a} (q'_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}[a \mapsto (\boldsymbol{v}(a) - 1)])$,
    - *3.2: if* $q_{\mathcal{T}} \xrightarrow{a}_{\mathcal{T}} q'_{\mathcal{T}}$ *then* $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \xrightarrow{a^{\triangleright}} (q_{\mathcal{S}}, q'_{\mathcal{T}}, \boldsymbol{v}[a \mapsto (\boldsymbol{v}(a) + 1)])$.
  - *4: For all* $a \in \mathsf{in}_{\mathcal{T}} \cap \mathsf{out}_{\mathcal{S}}$,
    - *4.1: if* $q_{\mathcal{S}} \xrightarrow{a}_{\mathcal{S}} q'_{\mathcal{S}}$ *then* $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \xrightarrow{a^{\triangleright}} (q'_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}[a \mapsto (\boldsymbol{v}(a) + 1)])$,
    - *4.2: if* $q_{\mathcal{T}} \xrightarrow{a}_{\mathcal{T}} q'_{\mathcal{T}}$ *and* $\boldsymbol{v}(a) > 0$ *then* $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \xrightarrow{\triangleright a} (q_{\mathcal{S}}, q'_{\mathcal{T}}, \boldsymbol{v}[a \mapsto (\boldsymbol{v}(a) - 1)])$.
- *For all* $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \in Q$ *and* $a \in C$

$$\mathrm{val}((q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}), a) = \begin{cases} \mathrm{val}_{\mathcal{S}}(q_{\mathcal{S}}, a) & \text{if } a \in C_{\mathcal{S}} \\ \mathrm{val}_{\mathcal{T}}(q_{\mathcal{T}}, a) & \text{if } a \in C_{\mathcal{T}} \\ \boldsymbol{v}(a) & \text{if } a \in C_{\mathcal{ST}} \end{cases}$$

For the rules (1),(3.1) and (4.1), we say that the resulting transition in the composition is triggered *by* $\mathcal{S}$*, in the other cases it is triggered by* $\mathcal{T}$*. Let* ρ *be a trace of* $\mathcal{S} \otimes \mathcal{T}$ *starting from a state* $q = (q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \in Q$*. The* projection *of* ρ *to* $\mathcal{S}$*, denoted by* $\rho|_{\mathcal{S}}$*, is the sequence of transitions of* $\mathcal{S}$*, starting from* $q_{\mathcal{S}}$*, which have triggered corresponding transitions in* ρ*.* ♢

3 Asynchronous I/O-Petri Nets

Asynchronous I/O-Petri nets allow a finite representation of asynchronous I/O-transition systems. First we recall some basic notions of Petri nets. A *labeled Petri net* is a tuple $\mathcal{N} = (P, T, \Sigma, W^-, W^+, \lambda, m^0)$, such that

– P is a finite set of places,
– T is a finite set of transitions with $P \cap T = \emptyset$,
– Σ is a finite alphabet,
– W^- (resp. W^+) is a matrix indexed by $P \times T$ with values in $\mathbb{N}$; it is called the *backward* (resp. *forward*) *incidence matrix*,
– $\lambda : T \to \Sigma$ is a transition labeling function, and
– m^0 is a vector indexed by P and called the initial marking.

The labeling function λ is extended as usual to sequences of transitions. The input (output resp.) vector $W^-(t)$ ($W^+(t)$ resp.) of a transition t is the column vector of matrix W^- (W^+ resp.) indexed by t. Given two vectors $\boldsymbol{v}$ and $\boldsymbol{v'}$, one writes $\boldsymbol{v} \geq \boldsymbol{v'}$ if $\boldsymbol{v}$ is componentwise greater or equal than $\boldsymbol{v'}$. *A marking* is a vector indexed by P. A transition $t \in T$ is *firable* from a marking m, denoted by $m \xrightarrow{t}$, if $m \geq W^-(t)$. The firing of t from m leads to the marking m', denoted by $m \xrightarrow{t} m'$, and defined by $m' = m - W^-(t) + W^+(t)$. If $\lambda(t) = a$ we also write $m \xrightarrow{a} m'$. The firing of a transition is extended as usual to firing sequences $m \xrightarrow{\sigma} m'$ with $\sigma \in T^*$. A marking m is reachable if there exists a firing sequence $\sigma \in T^*$ such that $m^0 \xrightarrow{\sigma} m$.

To any labeled Petri net $\mathcal{N}$ a labeled transition system can be associated as usual. For technical simplicity, however, we consider all markings instead of the reachable markings in the state space of the transition system. The labeled transition system *associated with* $\mathcal{N} = (P, T, \Sigma, W^-, W^+, \lambda, m^0)$ is given by $\mathsf{lts}(\mathcal{N}) = (\Sigma, Q, q^0, \longrightarrow)$, such that

– Q is the set of all markings of $\mathcal{N}$,
– $\longrightarrow = \{(m, a, m') \mid a \in \Sigma \text{ and } m \xrightarrow{a} m'\}$, and
– $q^0 = m^0$.

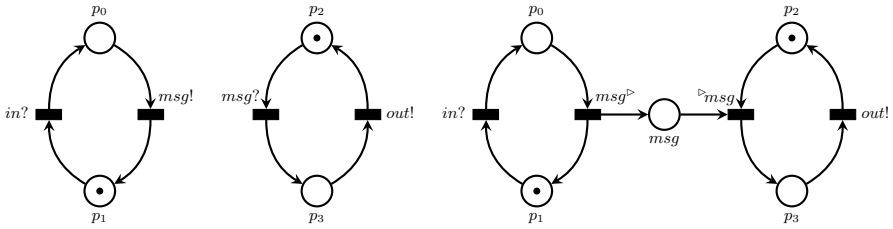
Similarly to asynchronous I/O-transition systems also asynchronous I/O-Petri nets (AIOPNs) are based on a finite set of communication channels and on an I/O-alphabet. Each channel is modeled as a place and the transitions for communication actions are modeled as expected by putting or removing tokens from the channel places. The difference between AIOPNs and modal I/O-Petri nets introduced in [8] is that AIOPNs comprise distinguished channel places but they do not support modalities for refinement (yet).

Definition 4 (Asynchronous I/O-Petri net). *An* asynchronous I/O-Petri net *(AIOPN) is a tuple* $\mathcal{N} = (C, P, T, \Sigma, W^-, W^+, \lambda, m^0)$*, such that*

– $(P, T, \Sigma, W^-, W^+, \lambda, m^0)$ *is a labeled Petri net,*
– C *is a finite set of channels,*
– $C \subseteq P$*, i.e. each channel is a place,*
– $\Sigma = \mathsf{in} \uplus \mathsf{out} \uplus \mathsf{com}$ *is an I/O-alphabet over* C*,*
– *for all* $a \in C$ *and* $t \in T$*,*

$$W^-(a,t) = \begin{cases} 1 & \text{if } \lambda(t) = {}^{\triangleright}a, \\ 0 & \text{otherwise} \end{cases} \qquad W^+(a,t) = \begin{cases} 1 & \text{if } \lambda(t) = a^{\triangleright}, \\ 0 & \text{otherwise} \end{cases}$$

– *for all* $a \in C$*,* $m^0(a) = 0$*.* ♢



(a) $\mathcal{N}_1$. (b) $\mathcal{N}_2$. (c) $\mathcal{N}_3$.

Fig. 1: Three asynchronous I/O-Petri nets.

Example 5. Three examples of AIOPNs are shown in Fig. 1. For both $\mathcal{N}_1$ and $\mathcal{N}_2$, the set of channels is empty. Fig. 1c models a simple producer/consumer system with an unbounded communication channel msg. Here and in the following drawings input labels are indicated by "?" and output labels by "!".

To each AIOPN an asynchronous I/O-transition system can be associated. Markings become states and the valuation of a channel in a current state m is just the number of tokens on the channel under the marking m.

Definition 6 (Associated asynchronous I/O-transition system). *Let* $\mathcal{N} = (C, P, T, \Sigma, W^-, W^+, \lambda, m^0)$ *be an AIOPN. The AIOTS* associated with $\mathcal{N}$ *is given by* $\mathsf{aiots}(\mathcal{N}) = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$*, such that*

- $(\Sigma, Q, q^0, \longrightarrow) = \mathsf{lts}(P, T, \Sigma, W^-, W^+, \lambda, m^0)$,
- *for all* $a \in C$ *and* $m \in Q, \mathrm{val}(m, a) = m(a)$. ♢

The asynchronous composition of two AIOPNs is constructed by taking the disjoint union of the underlying nets and adding a channel place for each shared label. Every transition with shared output label a becomes a transition with the communication label $a^{\triangleright}$ that produces a token on the channel place a and, similarly, any transition with shared input label a becomes a transition with the communication label $^{\triangleright}a$ that consumes a token from the channel place a.

Definition 7 (Asynchronous composition). *Let* $\mathcal{N} = (C_\mathcal{N}, P_\mathcal{N}, T_\mathcal{N}, \Sigma_\mathcal{N}, W^-_\mathcal{N}, W^+_\mathcal{N}, \lambda_\mathcal{N}, m^0_\mathcal{N})$ *and* $\mathcal{M} = (C_\mathcal{M}, P_\mathcal{M}, T_\mathcal{M}, \Sigma_\mathcal{M}, W^-_\mathcal{M}, W^+_\mathcal{M}, \lambda_\mathcal{M}, m^0_\mathcal{M})$ *be two AIOPN.* $\mathcal{N}$ *and* $\mathcal{M}$ *are* composable *if* $\Sigma_\mathcal{N}$ *and* $\Sigma_\mathcal{M}$ *are composable and if* $P_\mathcal{N} \cap P_\mathcal{M} = \emptyset$, $(P_\mathcal{N} \cup P_\mathcal{M}) \cap (\Sigma_\mathcal{N} \cap \Sigma_\mathcal{M}) = \emptyset$, $T_\mathcal{N} \cap T_\mathcal{M} = \emptyset$. *In this case, their* asynchronous composition *is the AIOPN* $\mathcal{N} \otimes_{pn} \mathcal{M} = (C, P, T, \Sigma, W^-, W^+, \lambda, m^0)$*, defined as follows:*

- $C = C_\mathcal{N} \uplus C_\mathcal{M} \uplus C_{\mathcal{NM}}$*, with* $C_{\mathcal{NM}} = \Sigma_\mathcal{N} \cap \Sigma_\mathcal{M}$,
- $P = P_\mathcal{N} \uplus P_\mathcal{M} \uplus C_{\mathcal{NM}}$,
- $T = T_\mathcal{N} \uplus T_\mathcal{M}$,
- Σ *is the alphabet composition of* $\Sigma_\mathcal{S}$ *and* $\Sigma_\mathcal{T}$,

– W^- *(resp.* W^+*) is the backward (forward) incidence matrix defined by:*

$$\text{for all } p \in P_{\mathcal{N}} \cup P_{\mathcal{M}} \text{ and } t \in T \qquad \text{for all } a \in C_{\mathcal{NM}} \text{ and } t \in T$$

$$W^-(p,t) = \begin{cases} W^-_{\mathcal{N}}(p,t) & \text{if } p \in P_{\mathcal{N}}, t \in T_{\mathcal{N}} \\ W^-_{\mathcal{M}}(p,t) & \text{if } p \in P_{\mathcal{M}}, t \in T_{\mathcal{M}} \\ 0 & \text{otherwise} \end{cases} \qquad W^-(a,t) = \begin{cases} 1 \text{ if } \lambda(t) = {}^{\triangleright}a \\ 0 \text{ otherwise} \end{cases}$$

$$W^+(p,t) = \begin{cases} W^+_{\mathcal{N}}(p,t) & \text{if } p \in P_{\mathcal{N}}, t \in T_{\mathcal{N}} \\ W^+_{\mathcal{M}}(p,t) & \text{if } p \in P_{\mathcal{M}}, t \in T_{\mathcal{M}} \\ 0 & \text{otherwise} \end{cases} \qquad W^+(a,t) = \begin{cases} 1 \text{ if } \lambda(t) = a^{\triangleright} \\ 0 \text{ otherwise} \end{cases}$$

– $\lambda : T \to \Sigma$ *is defined, for all* $t \in T$*, by*

$$\lambda(t) = \begin{cases} \lambda_{\mathcal{N}}(t) & \text{if } t \in T_{\mathcal{N}},\ \lambda_{\mathcal{N}}(t) \notin \Sigma_{\mathcal{N}} \cap \Sigma_{\mathcal{M}} \\ \lambda_{\mathcal{M}}(t) & \text{if } t \in T_{\mathcal{M}},\ \lambda_{\mathcal{M}}(t) \notin \Sigma_{\mathcal{N}} \cap \Sigma_{\mathcal{M}} \\ {}^{\triangleright}\lambda_{\mathcal{N}}(t) & \text{if } t \in T_{\mathcal{N}},\ \lambda_{\mathcal{N}}(t) \in in_{\mathcal{N}} \cap out_{\mathcal{M}} \\ {}^{\triangleright}\lambda_{\mathcal{M}}(t) & \text{if } t \in T_{\mathcal{M}},\ \lambda_{\mathcal{M}}(t) \in in_{\mathcal{M}} \cap out_{\mathcal{N}} \\ \lambda_{\mathcal{N}}(t)^{\triangleright} & \text{if } t \in T_{\mathcal{N}},\ \lambda_{\mathcal{N}}(t) \in in_{\mathcal{M}} \cap out_{\mathcal{N}} \\ \lambda_{\mathcal{M}}(t)^{\triangleright} & \text{if } t \in T_{\mathcal{M}},\ \lambda_{\mathcal{M}}(t) \in in_{\mathcal{N}} \cap out_{\mathcal{M}} \end{cases}$$

– m^0 *is defined, for all* $p \in P$*, such that* $m^0(p) = m^0_{\mathcal{N}}(p)$ *if* $p \in P_{\mathcal{N}}$*,* $m^0(p) = m^0_{\mathcal{M}}(p)$ *if* $p \in P_{\mathcal{M}}$*, and* $m^0(p) = 0$ *otherwise.* ♢

Example 8. The composition of the two AIOPNs in Fig. 1a and Fig. 1b yields the AIOPN shown in Fig. 1c.

We can now consider the class of all asynchronous I/O-transition systems that are generated by asynchronous I/O-Petri nets and prove that this class is closed under asynchronous composition. This is a consequence of the fact that the generation of AIOTSs from AIOPNs commutes with asynchronous composition. The proof of this theorem is technical, but straightforward.

Theorem 9. *Let* $\mathcal{N}$ *and* $\mathcal{M}$ *be two composable AIOPN. Then it holds that* $\mathsf{aiots}(\mathcal{N} \otimes_{pn} \mathcal{M}) = \mathsf{aiots}(\mathcal{N}) \otimes \mathsf{aiots}(\mathcal{M})$ *(upt to bijection between state spaces).*

4 Channel Properties and Their Compositionality

In this section we consider various properties concerning the communication via the channels of asynchronous I/O-transition systems. We give a classification of the properties, show their relationships and prove compositionality of all channel properties w.r.t. asynchronous composition. Examples will be discussed by Petri-net representations.

4.1 Channel Properties

We consider two classes of channel properties and, additionally, channel boundedness. The first class deals with the requirements that messages sent to a communication channel should also be consumed; the second class concerns the termination of communication in the sense that if consumption from a channel has been stopped then also production on this channel must be stopped.

Some of the properties rely on the consideration of system runs. In principle a system run is a maximal execution trace; it can be infinite but also finite if no further actions are enabled. It is however important to note, that we deal with open systems whose possible behaviors are also determined by the environment. Hence, the definition of a system run must take into account the possibility that the system may stop in a state where the environment does not serve any offered input of the system while at the same time the system has no enabled autonomous action, i.e. an action which is not an input from the environment. Such states are called pure input states. Note that all possible communication actions inside the system can be autonomously executed. The same holds for output actions to the environment, since we are working with asynchronous communication such that messages can always be sent, even if they are never accepted by the environment. Formally, system runs are defined as follows.

Let $\mathcal{S} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$ be an AIOTS with $\Sigma = \mathsf{in} \uplus \mathsf{out} \uplus \mathsf{com}$. A state $q \in Q$ is called a *pure input state* if $\mathrm{Post}(q, \Sigma \setminus \mathsf{in}) = \emptyset$, i.e. only inputs are enabled. A pure input state is a potential deadlock, as the environment of $\mathcal{S}$ might not serve any inputs for $\mathcal{S}$. Let $q_1 \in Q$. A *run* of $\mathcal{S}$ starting in q_1 is a trace of $\mathcal{S}$ starting in q_1, that is either infinite or finite such that its last state is a pure input state. We denote the set of all runs of $\mathcal{S}$ starting from q_1 as $\mathrm{run}_{\mathcal{S}}(q_1)$.

In the following we also assume that system runs are only executed in a runtime infrastructure which follows a weakly fair scheduling policy. In our context this means that any autonomous action a, that is always enabled from a certain state on, will infinitley often be executed. Formally, a run $\rho \in \mathrm{run}_{\mathcal{S}}(q_1)$ with $q_1 \in Q, \rho = q_1 \xrightarrow{a_1} q_2 \xrightarrow{a_2} \cdots$, is called *weakly fair* if it is finite or if it is infinite and for all $a \in (\Sigma \setminus \mathsf{in})$ the following holds:

$$(\exists k \geq 1 \,.\, \forall i \geq k \,.\, q_i \xrightarrow{a}) \implies (\forall k \geq 1 \,.\, \exists i \geq k \,.\, a_i = a).$$

We denote the set of all weakly fair runs of $\mathcal{S}$ starting from q_1 as $\mathrm{wfrun}_{\mathcal{S}}(q)$. It should be noted that for our results (like compositionality later on) it is sufficient to use weak fairness instead of strong fairness. This has the advantage that weak fairness is decidable while strong fairness is not.

Example 10. Let $\mathcal{S} = \mathsf{aiots}(\mathcal{N}_3)$ be the associated AIOTS of $\mathcal{N}_3$ in Fig. 1c. Recall that the states of $\mathcal{S}$ are markings of $\mathcal{N}_0$; we use the following notation for a state m of $\mathcal{S}$: $\langle m(p_0), m(p_1), m(msg), m(p_2), m(p_3)\rangle$. The following are traces of $\mathcal{S}$ from the initial marking $\langle 0,1,0,1,0\rangle$:

$$\rho_0 = \langle 0,1,0,1,0\rangle$$

$$\rho_1 = \langle 0,1,0,1,0\rangle \xrightarrow{in?} \langle 1,0,0,1,0\rangle \xrightarrow{msg^{\triangleright}} \langle 0,1,1,1,0\rangle \xrightarrow{{}^{\triangleright}msg} \langle 0,1,0,0,1\rangle$$

$$\rho_2 = \langle 0,1,0,1,0\rangle \xrightarrow{in?} \langle 1,0,0,1,0\rangle \xrightarrow{msg^{\triangleright}} \langle 0,1,1,1,0\rangle \xrightarrow{{}^{\triangleright}msg} \langle 0,1,0,0,1\rangle \xrightarrow{out!} \langle 0,1,0,1,0\rangle$$

Note that ρ_0 and ρ_2 are runs of $\mathcal{S}$ starting in the initial marking, while ρ_1 is not a run, as $\langle 0,1,0,0,1\rangle \xrightarrow{out!}$. Now consider the run that is an infinite alternation of $in?$ and $msg^{\triangleright}$. This run is not weakly fair, since ${}^{\triangleright}msg$ is always enabled but never taken.

Our first class of channel properties deals with the consumption of previously produced messages. We consider four groups of such properties (P1) - (P4) with different strength. In each case we consider three variants which all are parameterized w.r.t. a subset B of the communication channels. For instance, (P1.a) requires for each channel $a \in B$, that if in a reachable state q there is a message available on a then the message can be consumed possibly after the execution of some autonomous actions. To allow autonomous actions before consumption is inspired by the property of weak compatibility studied for synchronously composed transition systems in [3]. For the compositionality results later on, it will be important that we only allow autonomous actions and no (open) inputs before the consumption. Property (P1.b) requires that the message can be immediately consumed which is a stronger requirement similar to the property of specified reception in [5]. Property (P1.c) requires that the message will definitely be consumed on each weakly fair run starting from q and, due to the definition of a system run, that this will happen in any environment. The other groups of properties (P2) - (P4) express successively stronger (or equivalent) requirements on the kind of consumption. For instance, (P3) requires that the consumption will lead to a state in which the channel is empty. Again we distinguish if this can be achieved after some autonomous actions (P3.a), can be achieved immediately (P3.b), or must be achieved in any weakly fair run (P3.c).

Definition 11 (Consumption requirements). *Let* $\mathcal{S} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$ *be an AIOTS with I/O-alphabet* $\Sigma = \mathsf{in} \uplus \mathsf{out} \uplus \mathsf{com}$ *and let* $B \subseteq C$ *be a subset of its channels.*

P1: (Consuming)

a) $\mathcal{S}$ *is* B-consuming*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$$\mathrm{val}(q,a) > 0 \implies \exists q' \in \mathrm{Post}^*(q, \Sigma \setminus \mathsf{in}) \,.\, q' \xrightarrow{\triangleright a} .$$

b) $\mathcal{S}$ *is* strongly B-consuming*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$$\mathrm{val}(q,a) > 0 \implies q \xrightarrow{\triangleright a} .$$

c) $\mathcal{S}$ *is* necessarily B-consuming*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$$\mathrm{val}(q,a) > 0 \implies \forall \rho \in \mathrm{wfrun}_{\mathcal{S}}(q) \,.\, {\triangleright}a \in \rho \,.$$

P2: (Decreasing)

a) $\mathcal{S}$ *is* B-decreasing*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$$\mathrm{val}(q,a) > 0 \implies \exists q' \in \mathrm{Post}^*(q, \Sigma \setminus \mathsf{in}) \,.\, \mathrm{val}(q',a) < val(q,a) \,.$$

b) $\mathcal{S}$ *is* strongly B-decreasing*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$$\mathrm{val}(q,a) > 0 \implies \exists q' \in \mathrm{Post}(q, \Sigma \setminus \mathsf{in}) \,.\, \mathrm{val}(q',a) < val(q,a) \,.$$

c) $\mathcal{S}$ *is* necessarily B-decreasing*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$$\mathrm{val}(q,a) > 0 \implies \forall \rho \in \mathrm{wfrun}_{\mathcal{S}}(q),\ \exists q' \in \rho \,.\, \mathrm{val}(q',a) < \mathrm{val}(q,a) \,.$$

P3: (Emptying)

a) $\mathcal{S}$ *is* B-emptying*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$$\mathrm{val}(q,a) > 0 \implies \exists q' \in \mathrm{Post}^*(q, \Sigma \setminus \mathsf{in}) \,.\, \mathrm{val}(q',a) = 0 \,.$$

b) $\mathcal{S}$ *is* strongly B-emptying*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$$\mathrm{val}(q,a) > 0 \implies \exists q' \in \mathrm{Post}(q, \Sigma \setminus \mathsf{in}) \,.\, \mathrm{val}(q',a) = 0 \,.$$

c) $\mathcal{S}$ *is* B-necessarily emptying*, if for all* $q \in \mathrm{Post}^*(q^0)$ *and* $a \in B$*,*
$\mathrm{val}(q,a) > 0 \implies \forall \rho \in \mathrm{wfrun}_{\mathcal{S}}(q),\ \exists q' \in \rho\,.\,\mathrm{val}(q',a) = 0\,.$

P4: (Wholly emptying)

a) $\mathcal{S}$ *is* B-wholly emptying*, if for all* $q \in \mathrm{Post}^*(q^0)$*,*
$\mathrm{val}(q,B) > 0 \implies \exists q' \in \mathrm{Post}^*(q, \Sigma \setminus \mathsf{in})\,.\,\mathrm{val}(q',B) = 0.$

b) $\mathcal{S}$ *is* strongly B-wholly emptying*, if for all* $q \in \mathrm{Post}^*(q^0)$*,*
$\mathrm{val}(q,B) > 0 \implies \exists q' \in \mathrm{Post}(q, \Sigma \setminus \mathsf{in})\,.\,\mathrm{val}(q',B) = 0.$

c) $\mathcal{S}$ *is* B-necessarily wholly emptying*, if for all* $q \in \mathrm{Post}^*(q^0)$*,*
$\mathrm{val}(q,B) > 0 \implies \forall \rho \in \mathrm{wfrun}_{\mathcal{S}}(q),\ \exists q' \in \rho\,.\,\mathrm{val}(q',B) = 0\,.$ ♢

Note if the initial state of $\mathcal{S}$ is reachable from all other reachable states, i.e. the initial state is a *home state*, then $\mathcal{S}$ is B-wholly emptying.

The next class of channel properties concerns the termination of communication. We consider two variants: (P5.a) requires that in any weakly fair run, in which consumption from a channel a has stopped, only finitely many subsequent productions are possible, i.e. the channel is closed after a while. Property (P5.b) expresses that the channel is immediately closed.

Definition 12 (Communication stopping). *Let* $\mathcal{S}$ *be an AIOTS and* $B \subseteq C$ *be a subset of its channels.*

P5: (Communication stopping)

a) $\mathcal{S}$ *is* B-communication stopping*, if for all* $q \in \mathrm{Post}^*(q^0),\ \rho \in \mathrm{wfrun}_{\mathcal{S}}(q)$ *and* $a \in B$*,* $\sharp_\rho({}^{\triangleright}a) = 0 \implies \sharp_\rho(a^{\triangleright}) < \infty\,.$

b) $\mathcal{S}$ *is* strongly B-communication stopping*, if for all* $q \in \mathrm{Post}^*(q^0),\ \rho \in \mathrm{wfrun}_{\mathcal{S}}(q)$ *and* $a \in B$*,* $\sharp_\rho({}^{\triangleright}a) = 0 \implies \sharp_\rho(a^{\triangleright}) = 0\,.$ ♢

A standard property concerns boundedness of a channel which we do not explicitely discuss here; all results presented in the following would also hold for boundedness. It may be observed that channel boundedness implies communication stopping. Moreover, if $\mathcal{S}$ is strongly B-emptying then any channel $a \in B$ is bounded by 1, and if $\mathcal{S}$ is strongly B-wholly emptying then then the whole channel set B is bounded by 1.

Let P be an arbitrary channel property as defined above. We say that an AIOTS $\mathcal{S}$ has property P, if $\mathcal{S}$ has property P with respect to the set C of all channels of $\mathcal{S}$; we say that an AIOPN $\mathcal{N}$ has property P if its generated AIOTS has property P.

4.2 Relationships Between Channel Properties

Tab. 1 shows relationships between the channel properties. All the downward implications inside the boxes are direct consequences of the definitions. It is trivial to see that downward implication 3 is an equivalence, since *immediate* consumption leads to a decreasing valuation. Downward implications 9 and 16 are both equivalences, since repeated decreasing of messages on a channel will eventually lead to an empty channel. The implications 4, 5 and 7 will be proved

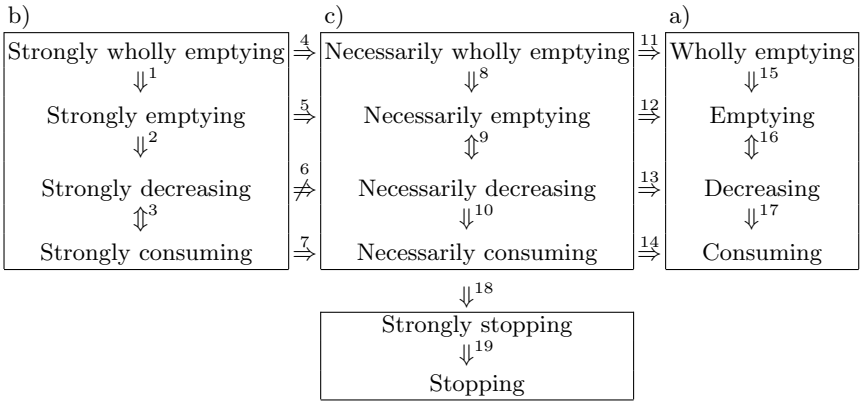


Table 1: Relationships between communication properties.

in Prop. 13, the implications 11-14 in Prop. 14, and implication 18 in Prop. 15. In the propositions we assume given an AIOTS $\mathcal{S} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$ and a subset $B \subseteq C$.

Proposition 13. *If $\mathcal{S}$ is strongly B-wholly emptying (strongly B-emptying, strongly B-consuming resp.), then $\mathcal{S}$ is necessarily B-wholly emptying (necessarily B-emptying, necessarily B-consuming resp.).*

Proof. We only prove that strongly consuming implies necessarily consuming. The other implications are simple extensions of this proof. Let $q \in \mathrm{Post}^*(q^0)$, $a \in B$ such that $\mathrm{val}(q, a) > 0$, and let $\rho \in \mathrm{run}_{\mathcal{S}}(q)$ be a weakly fair run. Assume for the contrary that ${}^{\triangleright}a \notin \rho$. By definition of AIOTS we get that for all $q' \in \rho$, $\mathrm{val}(q', a), \geq \mathrm{val}(q, a)$. By assumption $\mathcal{S}$ is strongly B-consuming, which implies that $q' \xrightarrow{{}^{\triangleright}a}$ for all $q' \in \rho$. This is a contradiction to ρ being a weakly fair run. □

Proposition 14. *If $\mathcal{S}$ is necessarily B-wholly emptying (necessarily B-emptying, necessarily decreasing, necessarily B-consuming resp.), then $\mathcal{S}$ is B-wholly emptying (B-emptying, B-decreasing, B-consuming resp.).*

Proof. The proof relies on the fact that for each $q \in \mathrm{Post}^*(q^0)$ there exists a weakly fair run $\rho \in \mathrm{wfrun}_{\mathcal{S}}(q)$, such that for all $a \in \mathsf{in}, a \notin \rho$. This run can be constructed by choosing, in a weakly fair manner in each reached state, some enabled non-input action. If no such action is enabled in the last visited state, the last state is a pure input state and we are done. Otherwise the resulting infinite run has the required property.

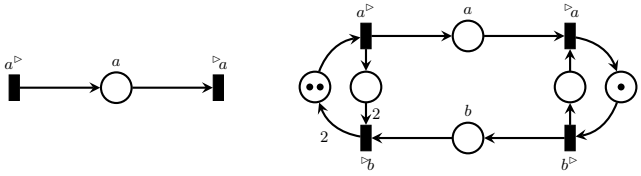
With this fact, we can prove the implication 14 in Tab. 1 as follows: Let $q \in \mathrm{Post}^*(q^0)$, $a \in B$ such that $\mathrm{val}(q, a) > 0$. By necessarily consuming, for all $\rho \in \mathrm{wfrun}_{\mathcal{S}}(q)$ we have ${}^{\triangleright}a \in \rho$. Since we know there exists a weakly fair run ρ without input actions, we get that there exists $q' \in \mathrm{Post}^*(q, \Sigma \setminus \mathsf{in})$ such that $q' \xrightarrow{{}^{\triangleright}a}$. The other implications are proven in the same way. □

Proposition 15. *If $\mathcal{S}$ is necessarily B-consuming then $\mathcal{S}$ is strongly B-stopping.*

Proof. Assume the contrary, that $\mathcal{S}$ is not strongly B-stopping. This means that there exists $q \in \mathrm{Post}^*(q^0)$, $a \in B$ and a weakly fair run $\rho \in \mathrm{wfrun}_{\mathcal{S}}(q)$ such that $\sharp_\rho({}^\triangleright a) = 0$ and $\sharp_\rho(a^\triangleright) > 0$. Then there exists $q' \in \rho$ reached after q, such that $\mathrm{val}(q', a) > 0$. Let ρ' be the suffix of ρ starting from q' which is weakly fair as well. Since $\sharp_{\rho'}({}^\triangleright a) = 0$, $\mathcal{S}$ is not necessarily consuming. □

Additionally we have that all properties in box b) of Tab. 1 imply the strongest property in box a). In particular, if $\mathcal{S}$ is strongly B-consuming then $\mathcal{S}$ is B-wholly emptying. This implication is true, since if $\mathcal{S}$ is strongly B-consuming we can by repeated consumption empty all channels in B.

Let us now discuss some counterexamples. An obvious counterexample for implication 6 and also for the converse of implication 2 is shown in Fig. 2a. Fig. 2b shows a counterexample for implication 15. The net can empty each single channel a and b but it can never have both channels empty at the same time (after the first message has been produced on a channel). The reason is that whenever a token is consumed from a then a new token will be produced in b. Counterexamples for the converse directions of implications 10 and 17 rely on the idea to produce twice while consuming once. A counterexample for the converse of implication 18 is provided by a net that first produces a finite number n of messages on a channel, then it consumes less than n of these messages and then it stops. Counterexamples for the remaining converse implications are straightforward to construct.



(a) Counterexample 1. (b) Counterexample 2.

Fig. 2: Counterexamples for non-implications in Tab 1

4.3 Compositionality of Channel Properties

Modular verification of systems is an important goal in any development method. In our context this concerns the question whether channel properties are preserved in arbitrary environments or, more precisely, whether they are preserved under asynchronous composition. In this section we show that indeed all channel properties defined above are compositional.

In order to relate channel properties of asynchronous compositions to channel properties of their constituent parts we need the next two lemmas. The first

one shows that autonomous executions of constituent parts (not involving inputs) can be lifted to executions of compositions. This is the crucial essence to prove compositionality of the properties of type (a) in Def. 11 since they rely on autonomously reachable states.[4]

Lemma 16. *Let* $\mathcal{S} = (C_\mathcal{S}, \Sigma_\mathcal{S}, Q_\mathcal{S}, q^0_\mathcal{S}, \longrightarrow_\mathcal{S}, \mathrm{val}_\mathcal{S}), \mathcal{T} = (C_\mathcal{T}, \Sigma_\mathcal{T}, Q_\mathcal{T}, q^0_\mathcal{T}, \longrightarrow_\mathcal{T}, \mathrm{val}_\mathcal{T})$ *be two composable AIOTSs, and let* $\mathcal{S} \otimes \mathcal{T} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$. *For all* $(q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$ *and* $\sigma \in ((\Sigma_\mathcal{S})_\tau \setminus \mathsf{in}_\mathcal{S})^*$ *it holds that*

$$q_\mathcal{S} \xrightarrow{\sigma}_\mathcal{S} q'_\mathcal{S} \implies \exists \boldsymbol{v'} \,.\, (q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \xrightarrow{\bar{\sigma}} (q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}),$$

with $\bar{\sigma} \in (\Sigma \setminus \mathsf{in})^*$ *obtained from* σ *by replacing any occurrence of a shared label* $a \in \mathsf{out}_\mathcal{S} \cap \mathsf{in}_\mathcal{T}$ *by the communication label* $a^\triangleright$.

Proof. Obviously it is sufficient to show the claim for an arbitrary $a \in (\Sigma_\mathcal{S} \setminus \mathsf{in}_S)$. The general result then follows by induction on the length of σ.

1. $a \in \mathsf{out}_\mathcal{S} \cap \mathsf{in}_\mathcal{T}$: By rule (3.1) in Def. 3 it follows that there exists $\boldsymbol{v'}$ such that $q_\mathcal{S} \xrightarrow{a}_\mathcal{S} q'_\mathcal{S} \implies (q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \xrightarrow{a^\triangleright} (q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'})$.
2. $a \notin \mathsf{out}_\mathcal{S} \cap \mathsf{in}_\mathcal{T}$: There are two subcases, either $a \in \mathsf{com}_\mathcal{S}$, or $a \in \mathsf{out}_\mathcal{S} \setminus \mathsf{in}_\mathcal{T}$. In both cases we get from rule (1) in Def. 3, $q_\mathcal{S} \xrightarrow{a}_\mathcal{S} q'_\mathcal{S} \implies (q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \xrightarrow{a} (q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v})$. □

The second lemma shows that the projection of a weakly fair run of a composition to a constituent part yields a weakly fair run of the constituent. This is crucial to prove compositionality of the properties of type (c) in Def. 11 and the stopping properties in Def. 12 since they rely on weakly fair runs.

Lemma 17. *Let* $\mathcal{S}$, $\mathcal{T}$ *be two composable AIOTSs, and* $\mathcal{S} \otimes \mathcal{T} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$. *Let* $q = (q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \in Q$ *and* $\rho \in \mathrm{wfrun}_{\mathcal{S}\otimes\mathcal{T}}(q)$ *be a weakly fair run. Then* $\rho|_\mathcal{S} \in \mathrm{wfrun}_\mathcal{S}(q_\mathcal{S})$, *is a weakly fair run.*

Proof. Since ρ is weakly fair, it is straightforward to show that $\rho|_\mathcal{S}$ is weakly fair as well. It remains to prove that $\rho|_\mathcal{S} \in \mathrm{run}_\mathcal{S}(q_\mathcal{S})$. There are two main cases. Either ρ is finite or infinite.

Assume ρ is finite with its last state being $q' = (q'_\mathcal{S}, q'_\mathcal{T}, \boldsymbol{v'})$. Clearly $q'_\mathcal{S}$ must be the last state of $\rho|_\mathcal{S}$. By definition of a run, q' is a pure input state. Then $q'_\mathcal{S}$ must be a pure input state of $\mathcal{S}$, hence $\rho|_\mathcal{S} \in \mathrm{run}_\mathcal{S}(q_\mathcal{S})$.

Now assume that ρ is infinite and weakly fair. In this case there are two subcases. Either $\rho|_\mathcal{S}$ is finite or infinite. If $\rho|_\mathcal{S}$ is infinite, then $\rho|_\mathcal{S} \in \mathrm{run}_\mathcal{S}(q_\mathcal{S})$.

Assume $\rho|_\mathcal{S}$ is finite such that its last state is $q'_\mathcal{S}$, with $(q'_\mathcal{S}, q'_\mathcal{T}, \boldsymbol{v'}) \in \rho$. Since ρ is weakly fair we can prove that $q'_\mathcal{S}$ is a pure input state as follows: Assume the contrary, that $q'_\mathcal{S}$ is not a pure input state, i.e. there exists $a \in (\Sigma \setminus \mathsf{in})$ such that $q'_\mathcal{S} \xrightarrow{a}$. As ρ is infinite we get that a is enabled always from $(q'_\mathcal{S}, q'_\mathcal{T}, \boldsymbol{v'}) \in \rho$,

[4] This also justifies why we did not allow inputs in the properties of type (a) in Def. 11. In fact for any input action a of a single AIOTS there is always an environment which will not serve the input and therefore a will not induce a transition with communication label ${}^\triangleright a$ in *any* composition.

which is a contradiction, since ρ is fair and a is not occurring infinitely often after $(q'_{\mathcal{S}}, q'_{\mathcal{T}}, \boldsymbol{v'}) \in \rho$ as $\rho|_{\mathcal{S}}$ is finite. Now, knowing that $q'_{\mathcal{S}}$ is a pure input state, we get that $\rho|_{\mathcal{S}} \in \mathrm{run}_{\mathcal{S}}(q_{\mathcal{S}})$. □

Theorem 18 (Compositionality). *Let $\mathcal{S}$ and $\mathcal{T}$ be two composable AIOTSs with $C_{\mathcal{S}}$ being the set of channels of $\mathcal{S}$. Let $B \subseteq C_{\mathcal{S}}$ and let P be an arbitrary channel property as defined in Sec. 4.1. If $\mathcal{S}$ has property P with respect to the channels B, then $\mathcal{S} \otimes \mathcal{T}$ has property P with respect to the channels B.*

Proof. We split the proof into two parts: consumption requirement properties and communication stopping properties.

Consumption requirement properties: We only provide a proof for the properties (P1.a),(P1.b) and (P1.c) here. The full proof can be found in appendix A.

Let $\mathcal{S} = (C_{\mathcal{S}}, \Sigma_{\mathcal{S}}, Q_{\mathcal{S}}, q^0_{\mathcal{S}}, \longrightarrow_{\mathcal{S}}, \mathrm{val}_{\mathcal{S}})$, $\mathcal{T} = (C_{\mathcal{T}}, \Sigma_{\mathcal{T}}, Q_{\mathcal{T}}, q^0_{\mathcal{T}}, \longrightarrow_{\mathcal{T}}, \mathrm{val}_{\mathcal{T}})$, $\mathcal{S} \otimes \mathcal{T} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$ with $\Sigma_{\mathcal{S}} = \mathsf{in}_{\mathcal{S}} \uplus \mathsf{out}_{\mathcal{S}} \uplus \mathsf{com}_{\mathcal{S}}$ and $\Sigma = \mathsf{in} \uplus \mathsf{out} \uplus \mathsf{com}$. Let $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$ and $a \in B$, such that $\mathrm{val}((q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}), a) > 0$.

P1.a: Assume that $\mathcal{S}$ is B-consuming. Obviously $q_{\mathcal{S}} \in \mathrm{Post}^*(q^0_{\mathcal{S}})$. By assumption there exists $q'_{\mathcal{S}} \in \mathrm{Post}^*(q_{\mathcal{S}}, (\Sigma_{\mathcal{S}})_\tau \setminus \mathsf{in}_{\mathcal{S}})$ such that $q'_{\mathcal{S}} \xrightarrow{{}^{\triangleright}a}_{\mathcal{S}}$. As a direct consequence of Lem. 16, we get there exists $\boldsymbol{v'}$ such that $(q'_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v'}) \in \mathrm{Post}^*((q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}), \Sigma \setminus \mathsf{in})$, and by definition of $\otimes$ we get $(q'_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v'}) \xrightarrow{{}^{\triangleright}a}$.

P1.b: Assume that $\mathcal{S}$ is strongly B-consuming. We get by assumption that $q_{\mathcal{S}} \xrightarrow{{}^{\triangleright}a}$. By definition of $\otimes$ this means that $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \xrightarrow{{}^{\triangleright}a}$.

P1.c: Assume that $\mathcal{S}$ is necessarily B-comsuming. Let $\rho \in \mathrm{wfrun}_{\mathcal{S}\otimes\mathcal{T}}(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v})$ be a weakly fair run. By Lem. 17 we get that $\rho|_{\mathcal{S}}$ is a weakly fair run of $\mathcal{S}$. By assumption ${}^{\triangleright}a \in \rho|_{\mathcal{S}}$, hence it follows that ${}^{\triangleright}a \in \rho$.

Communication stopping properties: We will only prove the claim for property (P5.a), it can be proven analogously for (P5.b). Let $\mathcal{S} \otimes \mathcal{T} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$, $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$, $a \in B$ and $\rho \in \mathrm{wfrun}_{\mathcal{S}\otimes\mathcal{T}}(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v})$, such that $\sharp_\rho({}^{\triangleright}a) = 0$. By Lem. 17 we get that $\rho|_{\mathcal{S}} \in \mathrm{wfrun}_{\mathcal{S}}(q_{\mathcal{S}})$. By assumption $\mathcal{S}$ is B-stopping, thus $\sharp_{\rho|_{\mathcal{S}}}(a^{\triangleright}) < \infty$. Finally as $a^{\triangleright}$ is triggered by $\mathcal{S}$ in $\mathcal{S} \otimes \mathcal{T}$, we get that $\sharp_\rho(a^{\triangleright}) < \infty$.

As a consequence of Thm. 18 we get the desired modular verification result: In order to prove that a composition $\mathcal{S} \otimes \mathcal{T}$ has a channel property P, i.e. P holds for all channels of the composition, it is sufficient to prove that S and T have property P for all their channels and to prove that $\mathcal{S} \otimes \mathcal{T}$ has property P with respect to the new channels corresponding to the shared labels $\Sigma_{\mathcal{S}} \cap \Sigma_{\mathcal{T}}$.

5 Decidability Issues

We begin this section by recalling some information related to semi-linear sets and decision procedures in Petri nets that we use in our proofs.

Let $E \subseteq \mathbb{N}^k$, E is a *linear set* if there exists a finite set of vectors of $\mathbb{N}^k$ $\{v_0, \ldots, v_n\}$ such that $E = \{v_0 + \sum_{1 \leq i \leq n} \lambda_i v_i \mid \forall i \ \lambda_i \in \mathbb{N}\}$. A *semi-linear set* [10] is a finite union of linear sets; a representation of it is given by the family of finite sets of vectors defining the corresponding linear sets. Semi-linear sets are *effectively* closed w.r.t. union, intersection and complementation. This means that one can compute a representation of the union, intersection and complementation starting from a representation of the original semi-linear sets. E is an *upward closed set* if $\forall v \in E.\ v' \geq v \Rightarrow v' \in E$. An upward closed set has a finite set of minimal vectors denoted $\min(E)$. An upward closed set is a semi-linear set which has a representation that can be derived from the equation $E = \min(E) + \mathbb{N}^k$ if $\min(E)$ is computable.

Given a Petri net $\mathcal{N}$ and a marking m, the *reachability* problem consists in deciding whether m is reachable from m_0 in $\mathcal{N}$. This problem is decidable [13] but none of the associated algorithms are primitive recursive. Furthermore this procedure can be adapted to semi-linear sets when markings are identified to vectors of $\mathbb{N}^{|P|}$. Based on reachability analysis, the authors of [9] design an algorithm that decides whether a marking m is a *home state*, i.e. m is reachable from any reachable marking. A more general problem is in fact decidable: given a subset of places P' and a (sub)marking m on this subset, is it possible from any reachable marking to reach a marking that coincides on P' with m?

In [14], the *coverability* and the *boundedness* problems are shown to be EXPSPACE-complete. The coverability problem consists in determining, given a net and a target marking, whether one can reach a marking greater or equal than the target. The boundedness problem consists in determining whether there exists a bound for every reachable marking of every place. This procedure can be adapted to check boundedness for a subset of places. In [19] given a Petri net, several procedures have been designed to compute the minimal set of markings of several interesting upward closed sets. In particular, given an upward closed set $Target$, by a backward analysis one can compute the (representation of) upward closed set from which $Target$ is reachable. Using the results of [14], this algorithm performs in EXPSPACE.

While in Petri nets, strong fairness is undecidable [6], weak fairness is decidable and more generally, the existence of an infinite sequence fulfilling a formula of the following fragment of LTL is decidable [12]. The literals are (1) comparisons between places markings and values, (2) transition firings and, (3) their negations. Formulas are inductively defined as literals, conjunction or disjunction of formulas and $GF\varphi$ where GF is the infinitely often operator and φ is a formula.

The next theorem establishes the decidability of the strong properties of type (b) of Def. 11. Observe that their proofs given in Appendix B are closely related and that they rely on the decidability of reachability and coverability problems.

Theorem 19. *The following problems are decidable for AIOPNs: Is an AIOPN $\mathcal{N}$ strongly B-consuming, strongly B-decreasing, strongly B-emptying, strongly B-wholly emptying?*

The next theorem establishes the decidability of the properties of type (a) of Def. 11. Observe that their proofs rely on (1) the effectiveness of backward analysis for upward closed marking sets (2) the decidability of reachability and home space problems and, (3) appropriate transformations of the net.

Theorem 20. *The following problems are decidable for AIOPNs: Is an AIOPN $\mathcal{N}$ B-consuming, B-decreasing, B-emptying, B-wholly emptying?*

Proof.
B-consuming. Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is B-consuming as follows.

Let $a \in B$ and E_a be the upward closed set of markings defined by:

$$E_a = \{m \mid \exists t \in T \text{ with } \lambda(t) = {}^{\triangleright}a \text{ and } m \geq W^-(t)\}$$

E_a is the set of markings from which one can immediately consume some message a. Let F_a be the upward closed set of markings defined by:

$$F_a = \{m \mid \exists m' \in E_a \ \exists \sigma \in T^*.\ \lambda(\sigma) \in (\Sigma \setminus \mathsf{in})^* \wedge m \xrightarrow{\sigma} m'\}$$

F_a is the set of markings from which one can later (without the help of the environment) consume some message a. One computes F_a by backward analysis. Let G be defined by: $G = \{m \mid \exists a \in B.\ m(a) > 0 \wedge m \notin F_a\}$
G is a semi-linear set corresponding to the markings from which some message $a \in B$ will never be consumed. Then $\mathcal{N}$ is not B-consuming iff G is reachable.

B-emptying (and B-decreasing). Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is B-emptying as follows. First one builds a net $\mathcal{N}'$:

- $P' = P \uplus \{run\}$
- $T' = T \uplus \{stop\}$
- $\forall p \in P\ \forall t \in T\ W'^-(p,t) = W^-(p,t), W'^+(p,t) = W^+(p,t),\ m'^0(p) = m^0(p)$
- $W'^-(run, stop) = 1,,\ W'^+(run, stop) = 0,\ m'^0(run) = 1$
- $\forall p \in P\ W'^-(p, stop) = W'^+(p, stop) = 0$
- $\forall t \in T$ such that $\lambda(t) \in \mathsf{in}\ W'^-(run, t) = W'^+(run, t) = 1$
- $\forall t \in T$ such that $\lambda(t) \notin \mathsf{in}\ W'^-(run, t) = W'^+(run, t) = 0$

$\mathcal{N}'$ behaves as $\mathcal{N}$ as long as *stop* is not fired. When *stop* is fired only transitions not labelled by inputs are fireable. Thus $\mathcal{N}$ is B-emptying iff for all $a \in B$ the set of markings $Z_a = \{m \mid m(a) = 0\}$ is a home space for $\mathcal{N}'$.

B-wholly emptying. Using the same construction $\mathcal{N}$ is B-weakly wholly emptying if $Z_B = \{m \mid m(B) = 0\}$ is a home space for $\mathcal{N}'$.

□

The next theorem establishes the decidability of the necessarily properties of type (c) of Def. 11. Observe that their proofs rely on (1) the proofs of ordinary properties (2) on the decidability of the logic expressing weak fairness and, (3) on appropriate transformations of the net.

Theorem 21. *The following problems are decidable for AIOPNs: Is an AIOPN $\mathcal{N}$ necessarily B-consuming, necessarily B-decreasing, necessarily B-emptying, necessarily B-wholly emptying?*

Proof.

Necessarily B-consuming. Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is necessarily B-consuming as follows.

First one checks whether $\mathcal{N}$ is B-consuming, a necessary condition for being necessarily B-consuming. If $\mathcal{N}$ is B-consuming, then one checks whether for some $a \in B$, there exists a reachable marking m fulfilling $m(a) > 0$ from which an infinite sequence is fireable without occurrence of transitions labelled by ${}^{\triangleright}a$. To perform this test, one builds a net $\mathcal{N}'$ as follows.

- $P' = P \uplus \{run\}$
- $T' = T \uplus \{stop\}$
- $\forall p \in P\ \forall t \in T\ W'^{-}(p,t) = W^{-}(p,t), W'^{+}(p,t) = W^{+}(p,t),\ m'^{0}(p) = m^{0}(p)$
- $W'^{-}(run, stop) = 1,,\ W'^{+}(run, stop) = 0,\ m'^{0}(run) = 1$
- $W'^{-}(a, stop) = W'^{+}(a, stop) = 1$
- $\forall p \in P \setminus \{a\}\ W'^{-}(p, stop) = W'^{+}(p, stop) = 0$
- $\forall t \in T$ such that $\lambda(t) = {}^{\triangleright}a\ W'^{-}(run, t) = W'^{+}(run, t) = 1$
- $\forall t \in T$ such that $\lambda(t) \neq {}^{\triangleright}a\ W'^{-}(run, t) = W'^{+}(run, t) = 0$

$\mathcal{N}'$ behaves as $\mathcal{N}$ as long as *stop* is not fired. Transition *stop* can be fired only if $m(a) > 0$. When *stop* is fired only transitions not labelled by ${}^{\triangleright}a$ are fireable. Then one checks whether there exists an infinite weakly fair sequence that fulfills formula $GFrun = 0$ (witnessing the firing of *stop*) in $\mathcal{N}'$. Then $\mathcal{N}$ is necessarily B-consuming iff there is no such sequence.

Necessarily B-emptying (and B-decreasing). Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is necessarily B-emptying as follows.

First one checks whether $\mathcal{N}$ is B-emptying, a necessary condition for being necessarily B-emptying. If $\mathcal{N}$ is B-emptying, then one checks whether for some $a \in B$, there exists a reachable marking m from which an infinite sequence is fireable such that for every marking m' visited, $m'(a) > 0$. To perform this test, one builds a net $\mathcal{N}'$ as follows.

- $P' = P \uplus \{run\}$
- $T' = T \uplus \{stop\}$ with $\lambda(stop) = stop$
- $\forall p \in P\ \forall t \in T\ W'^{-}(p,t) = W^{-}(p,t), W'^{+}(p,t) = W^{+}(p,t),\ m'^{0}(p) = m^{0}(p)$
- $W'^{-}(run, stop) = 1,\ W'^{+}(run, stop) = 0,\ m'^{0}(run) = 1,$
- $W'^{-}(a, stop) = 1,\ W'^{+}(a, stop) = 0$
- $\forall p \in P \setminus \{a\}\ W'^{-}(p, stop) = W'^{+}(p, stop) = 0$
- $\forall t \in T\ W'^{-}(run, t) = W'^{+}(run, t) = 0$

$\mathcal{N}'$ behaves as $\mathcal{N}$ as long as *stop* is not fired. Transition *stop* can be fired only if $m(a) > 0$ and it consumes one token of a. Transition *stop* can be fired only once due to place *run*. Then one checks whether there exists an infinite weakly fair sequence that fulfills formula $GFrun = 0$ (witnessing the firing of *stop*) in $\mathcal{N}'$. Then $\mathcal{N}$ is necessarily B-emptying iff there is no such sequence. Indeed there is an infinite infinite weakly fair sequence in $\mathcal{N}'$ after the firing of *stop* iff from some marking m in $\mathcal{N}$, there is an infinite weakly fair sequence where the marking of a is never null from some state.

Necessarily B-wholly emptying. Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is necessarily B-wholly emptying as follows.

First one checks whether $\mathcal{N}$ is B-wholly emptying, a necessary condition for being necessarily B-wholly emptying. If $\mathcal{N}$ is B-wholly emptying, then one checks whether there exists a reachable marking m from which an infinite sequence is fireable such that for every marking m' visited, $m'(B) > 0$. To perform this test, one builds a net $\mathcal{N}'$ as follows.

- $P' = P \uplus \{run, B\}$
- $T' = T \uplus \{stop\}$ with $\lambda(stop) = stop$
- $\forall p \in P\ \forall t \in T\ W'^{-}(p,t) = W^{-}(p,t), W'^{+}(p,t) = W^{+}(p,t),\ m'^{0}(p) = m^{0}(p)$
- $\forall t \in T\ W'^{-}(B,t) = \sum_{a \in B} W^{-}(a,t)$,
  $W'^{+}(B,t) = \sum_{a \in B} W^{+}(a,t),\ m'^{0}(B) = 0$
- $W'^{-}(run, stop) = 1,\ W'^{+}(run, stop) = 0,\ m'^{0}(run) = 1,$
- $W'^{-}(B, stop) = 1,\ W'^{+}(B, stop) = 0$
- $\forall p \in P\ W'^{-}(p, stop) = W'^{+}(p, stop) = 0$
- $\forall t \in T\ W'^{-}(run, t) = W'^{+}(run, t) = 0$

In $\mathcal{N}'$ there is an additional place B containing the sum of tokens of places $a \in B$ whose management is straightforward. As in the previous constructions, there is a control transition *stop* that modifies the behaviour of $\mathcal{N}$. As long as *stop* is not fired, $\mathcal{N}'$ behaves as $\mathcal{N}$. In order to fire *stop* (which can be done only once), B is decreased. Then one checks whether there exists an infinite weakly fair sequence that fulfills formula $GFrun = 0$ (witnessing the firing of *stop*) in $\mathcal{N}'$. $\mathcal{N}$ is necessarily B-wholly emptying iff there is no such sequence. □

The next theorem, whose proof is given in Appendix B, establishes the decidability of the communication stopping properties.

Theorem 22. *The following problems are decidable for AIOPNs: Is an AIOPN $\mathcal{N}$ B-stopping, B-strongly stopping?*

6 Conclusion and Future Work

We have introduced asynchronously composed I/O-transition systems and studied various properties of communication channels. Useful links between the channel properties are established and we have shown that all channel properties are compositional. When AIOPNs are generated by asynchronous I/O-Petri nets we have proved that all channel properties are decidable.

This work can be extended in at least three directions. The first direction would introduce new operations on AIOTS, like hiding, which would allow to design component systems in a hierarchical way by encapsulating subsystems. The second direction concerns more general communication schemes like broadcasting. Finally, we want to establish conditions for the preservation of channel properties along the "vertical axis" namely by refinement, in particular within the framework of modal Petri nets as considered in [8].

References

1. L. de Alfaro, T. A. Henzinger. Interface-based Design *Engineering Theories of Software-intensive Systems*, NATO Science Series: Mathematics, Physics, and Chemistry, Vol. 195, Springer, pp. 83-104, 2005.
2. S. Basu, T. Bultan, M. Ouederni. Synchronizability for verification of asynchronously communicating systems. *Proc. of the 13th Int. Conf. on Verification, Model Checking, and Abstract Interpretation (VMCAI 2012)*, LNCS 7148, 56-71, 2012.
3. S. Bauer and P. Mayer and A. Schroeder and R. Hennicker. On weak modal compatibility, refinement, and the MIO workbench. *In Proc. 16^{th} Int. Conf. Tools and Algor. for the Constr. and Analysis of Systems (TACAS'10)*, vol. 6015 of LNCS, pages 175–189, Springer, 2010.
4. E. Best, R. Devillers, M. Koutny. Petri Net Algebra. *Springer Monographs in Theoretical Computer Science*, 2001.
5. D. Brand and P. Zafiropulo. On communicating finite-state machines. *JACM*, volume 30(2), pages 323–342,1983.
6. H. Carstensen. Decidability questions for fairness in Petri nets. *4th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, LNCS 247, 396-407, 1987.
7. G. Cécé and A. Finkel. Verification of programs with half-duplex communication. *Information and Computation*, 202(2): 166-190, 2005.
8. D. Elhog-Benzina, S. Haddad and R. Hennicker. Refinement and asynchronous composition of modal Petri nets. *In Transactions on Petri Nets and Other Models of Concurrency*, V, LNCS 6900, 96-120, 2012.
9. D. Frutos and C. Johnen. Decidability of home space property. *LRI*, report 503, 1989.
10. S. Ginsburg and E. H. Spanier. Semigroups, Presburger formulas and languages. *Pacific Journal of Mathematics*, 16(2) pages 285–296, 1966.
11. L. Gomes, J.P. Barros. Structuring and composability issues in Petri Nets modeling. *IEEE Transactions on Industrial Informatics* 1(2), 112123, 2005.
12. P. Jancar. Decidability of a temporal logic problem for Petri nets. *Theor. Comput. Sci.*, 74(1): 71-93, 1990.
13. E. Mayr. An algorithm for the general Petri net reachability problem. In *Proc. of the 13th Annual ACM Symposium on Theory of Computing (STOC'81)* pages 238–246, 1981.
14. C. Rackoff. The covering and boundedness problems for vector addition systems. *TCS*, 6: 223-231, 1978.
15. W. Reisig. Simple composition of nets. *30th Int. Conf. on Applications and Theory of Petri Nets*, LNCS 5606, 23-42, 2009.
16. Y. Souissi. On liveness preservation by composition of nets via a set of places. *11th Int. Conf. on Applications and Theory of Petri Nets*, LNCS 524, 277-295, 1990.
17. Y. Souissi, G. Memmi. Composition of nets via a communication medium. *10th Int. Conf. on Applications and Theory of Petri Nets*, LNCS 483, 457-470, 1989.
18. C. Stahl, K. Wolf. Deciding service composition and substitutability using extended operating guidelines. *Data Knowl. Eng.*, 68(9): 819-833, 2009.
19. R. Valk, M. Jantzen. The residue of vector sets with applications to decidability problems in Petri nets *Advances in Petri Nets 1984*, LNCS volume 188 pages 234–258, 1984.

A Additional Compositionality Proofs

Proof. (of Theorem 18)
Let $\mathcal{S} = (C_\mathcal{S}, \Sigma_\mathcal{S}, Q_\mathcal{S}, q^0_\mathcal{S}, \longrightarrow_\mathcal{S}, \mathrm{val}_\mathcal{S})$, $\mathcal{T} = (C_\mathcal{T}, \Sigma_\mathcal{T}, Q_\mathcal{T}, q^0_\mathcal{T}, \longrightarrow_\mathcal{T}, \mathrm{val}_\mathcal{T})$, $\mathcal{S} \otimes \mathcal{T} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$ with $\Sigma_\mathcal{S} = \mathsf{in}_\mathcal{S} \uplus \mathsf{out}_\mathcal{S} \uplus \mathsf{com}_\mathcal{S}$ and $\Sigma = \mathsf{in} \uplus \mathsf{out} \uplus \mathsf{com}$. We split this proof into the following three parts, non-necessarily channel properties, necessarily channel properties, and communication stopping properties.

Non-necessarily channel properties: Before we prove each case we state two simple consequences of Lem. 16: For all $(q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$ and $q'_\mathcal{S} \in Q_\mathcal{S}$,

(1) $q'_\mathcal{S} \in \mathrm{Post}^*(q_\mathcal{S}, (\Sigma_\mathcal{S})_\tau \setminus \mathsf{in}_\mathcal{S}) \Rightarrow \exists \boldsymbol{v'}.(q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}) \in \mathrm{Post}^*((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), \Sigma \setminus \mathsf{in})$
(2) $q'_\mathcal{S} \in \mathrm{Post}(q_\mathcal{S}, (\Sigma_\mathcal{S})_\tau \setminus \mathsf{in}_\mathcal{S}) \Rightarrow \exists \boldsymbol{v'}.(q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}) \in \mathrm{Post}((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), \Sigma \setminus \mathsf{in})$

P1: Assume that $\mathcal{S}$ is B-consuming, and let $(q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$ and $a \in B$ such that $\mathrm{val}((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), a) > 0$. Obviously $q_\mathcal{S} \in \mathrm{Post}^*(q^0_\mathcal{S})$. By assumption there exists $q'_\mathcal{S} \in \mathrm{Post}^*(q_\mathcal{S}, (\Sigma_\mathcal{S})_\tau \setminus \mathsf{in}_\mathcal{S})$ such that $q'_\mathcal{S} \xrightarrow{\triangleright a}_\mathcal{S}$. By (1) above there exists $\boldsymbol{v'}$ such that $(q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}) \in \mathrm{Post}^*((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), \Sigma \setminus \mathsf{in})$, and by definition of $\otimes$ we get $(q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}) \xrightarrow{\triangleright a}$.
If $\mathcal{S}$ is strongly B-consuming, we get by assumption that $q_\mathcal{S} \xrightarrow{\triangleright a}$. By definition of $\otimes$ this means that $(q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \xrightarrow{\triangleright a}$.

P2: Assume that $\mathcal{S}$ is B-decreasing, and let $(q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$ and $a \in B$ such that $\mathrm{val}((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), a) > 0$. Then $q_\mathcal{S} \in \mathrm{Post}^*(q^0_\mathcal{S})$. By assumption there exists $q'_\mathcal{S} \in \mathrm{Post}^*(q_\mathcal{S}, (\Sigma_\mathcal{S})_\tau \setminus \mathsf{in}_\mathcal{S})$ such that $\mathrm{val}_\mathcal{S}(q'_\mathcal{S}, a) < \mathrm{val}_\mathcal{S}(q_\mathcal{S}, a)$. By (1) there exists $\boldsymbol{v'}$ such that $(q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}) \in \mathrm{Post}^*((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), \Sigma \setminus \mathsf{in})$. Finally as $a \in C_\mathcal{S}$ and $\mathrm{val}_\mathcal{S}(q'_\mathcal{S}, a) < \mathrm{val}_\mathcal{S}(q_\mathcal{S}, a)$ we get that $\mathrm{val}((q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}), a) < \mathrm{val}((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), a)$.
If $\mathcal{S}$ is strongly B-decreasing the claim follows by the same reasoning using (2) from above.

P3: The proof is totally analogous to the case P2.

P4: Assume that $\mathcal{S}$ is B-wholly emptying, and let $(q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$ such that $\mathrm{val}((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), B) > 0$. Then $q_\mathcal{S} \in \mathrm{Post}^*(q^0_\mathcal{S})$. By assumption there exists $q'_\mathcal{S} \in \mathrm{Post}^*(q_\mathcal{S}, (\Sigma_\mathcal{S})_\tau \setminus \mathsf{in}_\mathcal{S})$ such that $\mathrm{val}_\mathcal{S}(q'_\mathcal{S}, B) = 0$. By (1) there exists $\boldsymbol{v'}$ such that $(q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}) \in \mathrm{Post}^*((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), \Sigma \setminus \mathsf{in})$. Finally as $B \subseteq C_\mathcal{S}$ we get that $\mathrm{val}((q'_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v'}), B) = \mathrm{val}_\mathcal{S}(q'_\mathcal{S}, B) = 0$.
If $\mathcal{S}$ is strongly B-wholly emptying the claim follows by the same reasoning using (2) from above.

Necessarily channel properties: We will only prove the claim for property (P1.c), as it can be proven analogously for the other necessarily properties.

Let $\mathcal{S} \otimes \mathcal{T} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$, $(q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$ and $a \in B$, such that $\mathrm{val}((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}), a) > 0$. Let $\rho \in \mathrm{wfrun}_{\mathcal{S}\otimes\mathcal{T}}((q_\mathcal{S}, q_\mathcal{T}, \boldsymbol{v}))$ be weakly fair.

By Lem. 17 we get that $\rho|_\mathcal{S}$ is a weak fair run of $\mathcal{S}$. By assumption $\triangleright a \in \rho|_\mathcal{S}$, hence it follows that $\triangleright a \in \rho$. □

Stopping properties: We will only prove the claim for property (P5.a), it can be proven analogously for (P5.b).

Let $\mathcal{S} \otimes \mathcal{T} = (C, \Sigma, Q, q^0, \longrightarrow, \mathrm{val})$, $(q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}) \in \mathrm{Post}^*(q^0)$, $a \in B$ and $\rho \in \mathrm{wfrun}_{\mathcal{S}\otimes\mathcal{T}}((q_{\mathcal{S}}, q_{\mathcal{T}}, \boldsymbol{v}))$, such that $\sharp_\rho({}^\triangleright a) = 0$.

By Lem. 17 we get that $\rho|_{\mathcal{S}} \in \mathrm{wfrun}_{\mathcal{S}}(q_{\mathcal{S}})$. By assumption $\mathcal{S}$ is B-stopping, thus $\sharp_{\rho|_{\mathcal{S}}}(a^\triangleright) < \infty$. Finally as $a^\triangleright$ is triggered by $\mathcal{S}$ in $\mathcal{S} \otimes \mathcal{T}$, we get that $\sharp_\rho(a^\triangleright) < \infty$.

B Additional Decidability Proofs

Proof. (of Theorem 19)
Strongly B-consuming (and strongly B-decreasing). Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is B-strongly consuming as follows. Let E be the set of markings defined by:

$$E = \{m \mid \exists a \in B\ m(a) > 0 \text{ and } \forall t \in T \text{ with } \lambda(t) = {}^\triangleright a\ m \not\geq W^-(t)\}$$

$\mathcal{N}$ is B-strongly consuming iff E is not reachable. Since E is a semi-linear set, its reachability is decidable.

Strongly B-emptying. Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is B-strongly emptying as follows.

First by coverability analysis, one decides whether the following upward closed subset is reachable.

$$E = \{m \mid \exists a \in B\ m(a) > 1\}$$

If E is reachable then $\mathcal{N}$ is not B-strongly emptying. Otherwise one checks whether $\mathcal{N}$ is B-strongly consuming in order to decide.

Strongly B-wholly emptying. Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is B-strongly wholly emptying as follows.

First by coverability analysis, one decides whether the following upward closed subset is reachable.

$$E = \{m \mid m(B) > 1\}$$

If E is reachable then $\mathcal{N}$ is not B-strongly wholly emptying. Otherwise one checks whether $\mathcal{N}$ is B-strongly consuming in order to decide. □

Proof. (of Theorem 22)
B-stopping. Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is B-stopping as follows. Observe that this property is expressed by the event-based LTL formula $\varphi = \bigwedge_{a\in B} GFa^\triangleright \Rightarrow GF\,{}^\triangleright a$. By definition, this property is satisfied for finite runs. However *$\neg\varphi$ is not a formula of the fragment of [12].* In order to check whether there exists a weakly fair infinite sequence falsifying this formula one builds net $\mathcal{N}_a$ as follows.

- $P' = P \uplus \{run\}$
- $T' = T \uplus \{stop\}$
- $\forall p \in P\ \forall t \in T\ W'^-(p,t) = W^-(p,t), W'^+(p,t) = W^+(p,t),\ m'^0(p) = m^0(p)$
- $W'^-(run, stop) = 1,,\ W'^+(run, stop) = 0,\ m'^0(run) = 1$
- $\forall p \in P\ W'^-(p, stop) = W'^+(p, stop) = 0$
- $\forall t \in T$ such that $\lambda(t) = {}^\triangleright a\ W'^-(run, t) = W'^+(run, t) = 1$
- $\forall t \in T$ such that $\lambda(t) \neq {}^\triangleright a\ W'^-(run, t) = W'^+(run, t) = 0$

$\mathcal{N}_a$ behaves as $\mathcal{N}$ as long as *stop* is not fired. Transition *stop* can be fired only once. When *stop* is fired only transitions not labelled by ${}^{\triangleright}a$ are fireable. Then one checks whether there exists an infinite weakly fair sequence that fulfills formula $GFrun = 0 \wedge GFa^{\triangleright}$ in $\mathcal{N}'$. Then $\mathcal{N}$ is B-stopping iff there is no such sequence in any $\mathcal{N}_a$.

B-strongly stopping. Given an AIOPN $\mathcal{N}$ and B a subset of its channels, one decides whether $\mathcal{N}$ is necessarily B-strongly stopping as follows.

For all $a \in B$, one builds a net $\mathcal{N}_a$ starting from $\mathcal{N}$. Since the formal specification of $\mathcal{N}_a$ is cumbersome, one describes it in words.

- $\mathcal{N}_a$ has two additional places run and wit, with $m'^0(run) = 1$, $m'^0(wit) = 0$.
- Place run loops around all transitions labelled by ${}^{\triangleright}a$.
- Every transition t labelled by $a^{\triangleright}$ has a copy t' with the same inputs and outputs, plus an additional input run and an additional output wit.

$\mathcal{N}_a$ behaves as $\mathcal{N}$ until a transition t' is fired. This firing is possible only once. Once a transition t' is fired place wit is marked and transitions labelled by ${}^{\triangleright}a$ are no more fireable. Define the semi-linear set E_a by:

$$E_a = \{m \mid m(wit) = 1 \wedge \forall t \in T\ \lambda(t) \notin \mathsf{in}\ m \not\geq W^-(t)\}$$

Observe that a marking of E_a is a pure input marking of the original net (i.e. when restricted to P) that has been reached by a finite sequence when an occurrence of $a^{\triangleright}$ has not been followed later by an occurrence of ${}^{\triangleright}a$.

So $\mathcal{N}$ is strongly B-stopping iff for all $a \in B$, in $\mathcal{N}_a$ there does not exist an infinite weakly fair sequence fulfilling $GFrun = 0$ (witnessing a *bad* weakly fair infinite sequence in $\mathcal{N}$) and E_a is not reachable (witnessing a *bad* maximal sequence in $\mathcal{N}$). □