Science of Computer Programming ••• (••••) •••–•••

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

Deciding conformance for bounded responsiveness

Richard Müller [a,b,*], Christian Stahl [b], Walter Vogler [c]

[a] Institut für Informatik, Humboldt-Universität zu Berlin, Germany
[b] Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, The Netherlands
[c] Institut für Informatik, Universität Augsburg, Germany

ARTICLE INFO

Article history:
Received 18 February 2014
Received in revised form 27 October 2015
Accepted 28 November 2016
Available online xxxx

Keywords:
Petri nets
Open nets
Conformance
Theory of computation

ABSTRACT

We study open systems modeled as Petri nets with an interface for asynchronous communication with other open systems. As a minimal requirement for successful communication, we investigate *bounded responsiveness*, which guarantees that an open system and its environment always have the possibility to mutually terminate or to communicate, while the number of pending messages never exceeds a previously known bound. Bounded responsiveness *conformance* describes when one open system can be safely replaced by another open system. We present a trace-based characterization for conformance and show *decidability*. We further develop a finite characterization of the infinite set of all conforming open systems to a given open system. We implement the decision algorithm for conformance and evaluate it using industrial-sized open systems.

1. Introduction

Today's software systems are complex distributed systems that are composed of less complex *open systems*. In this paper, we focus on open systems that have a well-defined interface and communicate with each other via *asynchronous message passing*. Examples for such systems are service-oriented systems like Web-service applications [39], systems based on wireless network technologies like wireless sensor networks [4], online games [23], distributed transportation systems [20], medical systems [18], or a software system based on electronic control units in a car or plane [8]. During system evolution, often one open system is replaced by another one—for example, when new features have been implemented or bugs have been fixed. This requires a *refinement* notion that preserves a certain *correctness criterion*.

In this paper, we model an open system as a Petri net with finitely many states. As a *minimal* correctness criterion for successful communication, *bounded responsiveness* demands that an open system and its environment always have the possibility to terminate or to communicate, while their composition is finite-state and, in particular, the number of pending messages never exceeds a previously known bound; the environment is called a *partner* then. An open system is in bounded responsiveness *conformance* with another one, if it can replace the latter without affecting this property. Responsiveness has gained interest because, in addition to deadlock freedom, it also ensures the possibility to communicate, which is crucial in the setting of interacting open systems. An example for the importance of responsiveness is Microsoft's asynchronous event driven programming language P [11]. P was used to implement and verify the core of the USB device driver stack that ships with Microsoft Windows 8. Thereby, P uses responsiveness for bounded message channels as a combination of termination

* Corresponding author at: Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, The Netherlands.
E-mail addresses: richard.mueller@informatik.hu-berlin.de (R. Müller), c.stahl@tue.nl (C. Stahl), vogler@informatik.uni-augsburg.de (W. Vogler).

http://dx.doi.org/10.1016/j.scico.2016.11.003
0167-6423/

Please cite this article in press as: R. Müller et al., Deciding conformance for bounded responsiveness, Sci. Comput. Program. (2017), http://dx.doi.org/10.1016/j.scico.2016.11.003

and interaction while additionally requiring that no message in any channel is ignored forever. We aim at a more general notion of responsiveness by focusing solely on the combination of termination and interaction.

In [47], we considered *unbounded* responsiveness, where an open system and its environment should always have the possibility to mutually terminate or to communicate. In this paper, we study bounded responsiveness for two reasons: First, in [37], we showed conformance for unbounded responsiveness to be undecidable. Second, in practice, distributed systems operate on a middleware with buffers that are of bounded size. The actual buffer size can be the result of a static analysis of the underlying middleware or of the communication behavior of an open system, or simply be chosen sufficiently large. In recent work [48], we gave a *trace-based characterization for bounded responsiveness conformance*, thereby adapting and combining results from the unbounded variant in [47] and work on traces that cannot be used reliably by any controller [30]. Due to the latter traces, conforming systems may violate language inclusion.

Our contribution in this paper is threefold. First, based on the novel characterization in [48], we prove bounded responsiveness and conformance to be *decidable*. We provide a decision algorithm for each problem and analyze its computational complexity. In [48], we mainly considered bounded responsiveness without final markings. The practically attractive but more involved approach, where also reachability of a final marking counts as successful communication, was only sketched in [48]. In this paper, all results are elaborated in detail, taking final markings into account. Second, we present a finite characterization of the infinite set of conforming nets with the help of a *maximal* partner [31]. A maximal partner may serve as an alternative decision procedure for conformance, as well as a starting point for conformance checking [35] or model discovery [36] in case no formal model of the implementation is given. In contrast to the maximal partner for deadlock freedom or less general variants of responsiveness [33,31,40], our construction of a maximal partner is up to exponentially smaller. Third, we present an implementation of the decision procedure for conformance and evaluate it using industrial-sized open systems.

Like in our previous works [45,47,48], we contribute to a general theory for open systems and consider an asynchronous communication scheme with unordered, unbounded, and loss-free buffers. Although we present only the theory, open systems specified in industrial languages such as WS-BPEL [21] or BPMN [9] can be translated into our formal model and then be analyzed [24,27].

We recall some background in Sect. 2, including bounded responsiveness, conformance, and a trace-based characterization thereof in the presence of final states. Sect. 3 proves the decidability of bounded responsiveness and conformance for bounded responsiveness. In Sect. 4, we present alternative decision procedures that are based on the notion of a maximal partner. We present an implementation of the decision procedure and evaluate it, using industrial-sized open systems in Sect. 5. We close with a discussion of related work in Sect. 6 and a conclusion in Sect. 7.

2. Preliminaries

This section provides the basic notions, such as Petri nets, open nets for modeling open systems, environments for describing the semantics of open nets, and a trace-based semantics for bounded responsiveness.

For two sets A and B, let $A \uplus B$ denote the disjoint union; writing $A \uplus B$ implies that A and B are implicitly assumed to be disjoint. We employ labeled transition systems (LTSs) $S = (Q, \delta, q_S, \Sigma^{in}, \Sigma^{out}, \lambda)$ extended by an initial state $q_S \in Q$ and a state labeling function $\lambda : Q \to \mathbb{N}$. The transition labels are any one of input actions $\in \Sigma^{in}$, output actions $\in \Sigma^{out}$, or the *internal* action $\tau \notin \Sigma = \Sigma^{in} \uplus \Sigma^{out}$. Thus, the transition relation δ is a subset of $Q \times \Sigma \uplus \{\tau\} \times Q$. Introducing an LTS S also implicitly introduces its components $Q, \delta, q_S, \Sigma^{in}, \Sigma^{out}, \lambda$ or Ω; the same applies to other structures later on. We employ the standard definitions of *finite*, *τ-free*, and *deterministic*; two LTSs are *action-equivalent* if they have the same sets of input and output actions. We write $q \xrightarrow{x} q'$ for $(q, x, q') \in \delta$ and $q \xrightarrow{x}$ if there exists a state q' such that $q \xrightarrow{x} q'$, and extend this to transition sequences. If $q \xrightarrow{v} q'$ ($q \xrightarrow{v}$) and $w \in \Sigma^*$ is obtained from v by removing all τ labels, then we write $q \xRightarrow{w} q'$ ($q \xRightarrow{w}$). For two action-equivalent LTSs S_1 and S_2, a binary relation $\varrho \subseteq Q_1 \times Q_2$ is a *simulation* (*weak simulation*) relation if for all $(q_1, q_2) \in \varrho$, for all $x \in \Sigma_1 \uplus \{\tau\}$ and for all states $q_1' \in Q_1$ such that $q_1 \xrightarrow{x} q_1'$, there exists a state $q_2' \in Q_2$ such that $q_2 \xrightarrow{x} q_2'$ ($q_2 \xRightarrow{x} q_2'$) and $(q_1', q_2') \in \varrho$. S_1 is simulated (weakly simulated) by S_2 if there exists a simulation (weak simulation) relation relating their initial states q_{S_1} and q_{S_2}. If ϱ and ϱ^{-1} are simulations (weak simulations), then ϱ is a *bisimulation (weak bisimulation)* relation. S_1 and S_2 are *bisimilar (weakly bisimilar)* if there exists a bisimulation (weak bisimulation) relation relating their initial states q_{S_1} and q_{S_2}.

A *trace* of an LTS S is a word $w \in \Sigma^*$ such that $q_S \xRightarrow{w}$; the *language* $L(S)$ of S is the set of all traces of S. We define $L_i(S) = \{w \in \Sigma^* \mid q_S \xRightarrow{w} q \wedge \lambda(q) = i\}$ as the language of S restricted to traces leading to states labeled with $i \in \mathbb{N}$. For words v and w, we denote with $v \sqsubseteq w$ that v is a *prefix* of w, and ε denotes the empty word.

2.1. Petri nets

We use Place/Transition Petri nets extended by either transition labels or—later—specific interface places.

Definition 1 *((Labeled) net).* A *net* $N = (P, T, F, m_N, \Omega)$ consists of finite disjoint sets P of *places* and T of *transitions*, a *flow relation* $F \subseteq (P \times T) \uplus (T \times P)$, an *initial marking* m_N, where a marking $m : P \to \mathbb{N}$ is a *multiset* over the set P, and a set Ω of final markings.

Please cite this article in press as: R. Müller et al., Deciding conformance for bounded responsiveness, Sci. Comput. Program. (2017), http://dx.doi.org/10.1016/j.scico.2016.11.003