Unifying Input Output Conformance

Martin Weiglhofer\textsuperscript{1,2} and Bernhard K. Aichernig\textsuperscript{1,*}

\textsuperscript{1} Institute for Software Technology, Graz University of Technology, Austria
\textsuperscript{2} Competence Network Softnet Austria

Abstract. Model-based conformance testing aims to assess the correctness of an implementation with respect to a specification. This raises the question of a proper conformance relation that should be established between implementations and specifications. One commonly used conformance relation is the so-called input output conformance (\textit{ioco}) relation, which is defined over labeled transition systems. In this paper we investigate a denotational semantics of the input output conformance relation over reactive processes. We formalize the underlying assumptions of the \textit{ioco} relation in terms of formal healthiness conditions and by adopted choice operators. Finally, we show that our denotational version of \textit{ioco} can be generalized in the same way as the original relation. Our work aims to provide a unification of input output conformance by lifting the definition from labeled transition systems to reactive processes.

Keywords: Input output conformance, ioco, unifying theories of programming, reactive processes, quiescence, fairness, model-based testing.

1 Introduction

Software development is a complex and error-prone task. Failures in safety-critical applications may be life-threatening. At least software failures cause high costs during and after the software development process. Therefore, software engineers need the support of tools, techniques, and theories in order to reduce the number of software failures.

Model-based black-box testing techniques aim to assess the correctness of a reactive system, i.e., the implementation under test (IUT), with respect to a given specification. The IUT is viewed as a black-box with an interface that accepts inputs and produces outputs. The goal of model-based black-box testing is to check if the observable behavior of the IUT conforms to a specification with respect to a particular conformance relation.

Industrial specifications are mostly incomplete and due to abstraction nondeterministic. Hence, a conformance relation being useful in industry needs to cope with incompleteness and non-determinism. One of the most popular of such conformance relations is the input output conformance (\textit{ioco}) relation \cite{1}.

Mature research prototypes (e.g. \cite{23}) and successful industrial case studies (e.g. \cite{15}) have shown the usability of this conformance relation in practice.

* Authors are listed in reverse alphabetical order.
However, the used theory is given in an operational semantics and some of the underlying assumptions have been stated informally only. It is the contribution of this paper to redefine $\text{ioco}$ in the denotational predicative semantics of UTP. The benefits of this new theory can be summarized as follows: (1) Instead of describing the assumptions of $\text{ioco}$ informally, the UTP formalization presents the underlying assumptions as unambiguous healthiness conditions and by adopted choice operators over reactive processes; (2) A UTP formalization naturally relates $\text{ioco}$ and refinement in one theory; (3) The denotational version of $\text{ioco}$ enables formal, machine checkable, proofs. (4) Due to the predicative semantics of UTP, test case generation based on the presented theory can be seen as a satisfiability problem. This facilitates the use of modern sat modulo theory techniques (e.g. [6]) for test case generation. (5) Finally, the UTP version of $\text{ioco}$ broadens the scope of $\text{ioco}$ to specification languages with similar UTP semantics, e.g. to generate test cases from Circus [7] specifications. Hence our work enriches UTP’s reactive processes with a practical testing theory.

The rest of this paper is structured as follows. Section 2 reviews the input output conformance relation. Section 3 comprises the formalization of $\text{ioco}$ in the UTP-framework. Finally, we discuss our results and further research in Section 4.

2 Conformance of Labeled Transition Systems

This section reviews the $\text{ioco}$ relation [1] which is defined over labeled transition system (LTS). When testing reactive systems one distinguishes between inputs and outputs. Thus, the alphabet of an LTS is partitioned into inputs and outputs.

Definition 1 (Labeled transition system with inputs and outputs). A labeled transition system is a tuple $M = (Q, A \cup \{\tau\}, \rightarrow, q_0)$, where $Q$ is a finite set of states, $A = A_I \cup A_O$ a finite alphabet partitioned into an input alphabet $A_I$ and an output alphabet $A_O$ where $A_I \cap A_O = \emptyset$. $\tau \not\in A$ an unobservable action, $\rightarrow \subseteq Q \times (A \cup \{\tau\}) \times Q$ is the transition relation, and $q_0 \in Q$ is the initial state.

The class of labeled transition systems with inputs $A_I$ and outputs in $A_O$ is denoted by $\mathcal{LTS}(A_I, A_O)$ [1]. We use the following common notations for LTSs:

Definition 2. Given a labeled transition system $M = (Q, A_I \cup A_O \cup \{\tau\}, \rightarrow, q_0)$ and let $q, q', q_i \in Q$, $a_{(i)} \in A_I \cup A_O$ and $\sigma \in (A_I \cup A_O)^*$. 

$$q \xrightarrow{a} q' =_{df} (q, a, q') \in \rightarrow$$
$$q \xrightarrow{a} =_{df} \exists q' \cdot (q, a, q') \in \rightarrow$$
$$q \xleftarrow{a} =_{df} \exists q' \cdot (q, a, q') \in \rightarrow$$
$$q \xrightarrow{\sigma} q' =_{df} (q = q') \lor \exists q_0, \ldots, q_n \cdot (q = q_0 \xrightarrow{\tau} q_1 \wedge \cdots \wedge q_{n-1} \xrightarrow{\tau} q_n = q')$$
$$q \xleftarrow{\sigma} q' =_{df} \exists q_1, q_2 \cdot q \xrightarrow{\sigma} q_1 \xrightarrow{a} q_2 \xleftarrow{\sigma} q'$$
$$q \xrightarrow{a_1 \ldots a_n} q' =_{df} \exists q_0, \ldots, q_n \cdot q = q_0 \xrightarrow{a_1} q_1 \cdots q_{n-1} \xrightarrow{a_n} q_n = q'$$
$$q \xleftarrow{\sigma} =_{df} \exists q' \cdot q \xleftarrow{\sigma} q'$$